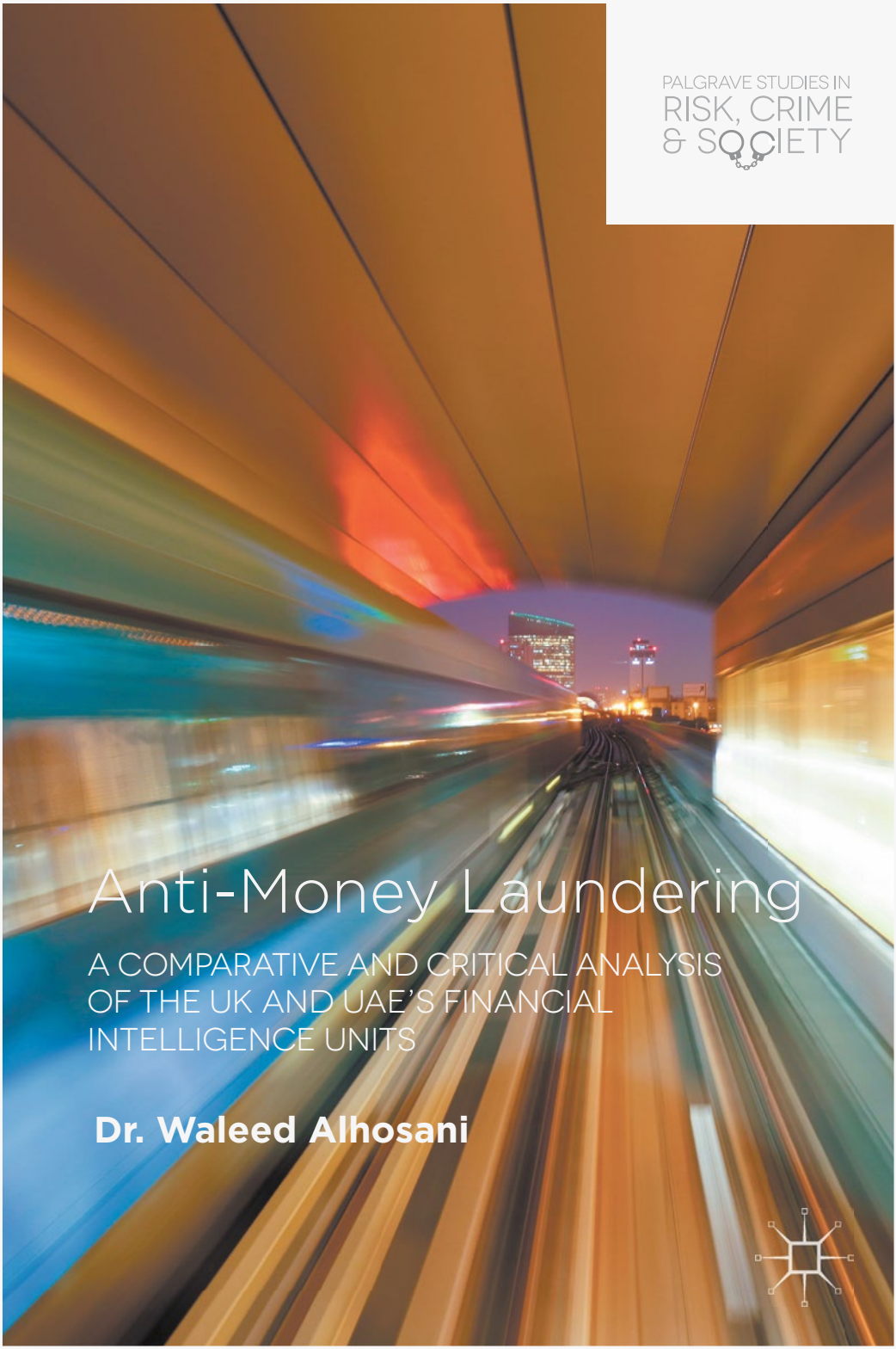

PALGRAVE STUDIES IN
RISK, CRIME
& SOCIETY

Anti-Money Laundering

A COMPARATIVE AND CRITICAL ANALYSIS OF THE UK AND UAE'S FINANCIAL INTELLIGENCE UNITS

Dr. Waleed Alhosani

Palgrave Studies in Risk, Crime and Society

Series Editors

Kieran McCartan
Department of Health and Social Sciences
University of the West of England
Bristol, United Kingdom

Philip N. S. Rumney
Department of Law
University of the West of England
Bristol, United Kingdom

Nicholas Ryder
Department of Law
University of the West of England
Bristol, United Kingdom

Risk is a major contemporary issue which has widespread implications for theory, policy, governance, public protection, professional practice and societal understandings of crime and criminal justice. The potential harm associated with risk can lead to uncertainty, fear and conflict as well as disproportionate, ineffective and ill-judged state responses to perceived risk and risky groups. Risk, Crime and Society is a series featuring monographs and edited collections which examine the notion of risk, the risky behaviour of individuals and groups, as well as state responses to risk and its consequences in contemporary society. The series will include critical examinations of the notion of risk and the problematic nature of state responses to perceived risk. While Risk, Crime and Society will consider the problems associated with 'mainstream' risky groups including sex offenders, terrorists and white collar criminals, it welcomes scholarly analysis which broadens our understanding of how risk is defined, interpreted and managed. Risk, Crime and Society examines risk in contemporary society through the multi-disciplinary perspectives of law, criminology and socio-legal studies and will feature work that is theoretical as well as empirical in nature.

More information about this series at
http://www.springer.com/series/14593

Dr. Waleed Alhosani

Anti-Money Laundering

A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units

palgrave
macmillan

Dr. Waleed Alhosani
Dubai Public Prosecution
Assistant Chief Prosecutor
SHARJAH, United Arab Emirates

Palgrave Studies in Risk, Crime and Society
ISBN 978-1-137-59454-9 ISBN 978-1-137-59455-6 (eBook)
DOI 10.1057/978-1-137-59455-6

Library of Congress Control Number: 2016944839

Cover illustration: © Gavin Hellier/Alamy Stock Photo.

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Macmillan Publishers Ltd. London

I wish to dedicate this work to my wonderful parents. Without them, this work would not have been possible. They have encouraged me relentlessly to strive for knowledge since the day I was born. I am eternally indebted to their constant support, both emotionally and financially.
I am also indebted to my brothers and sisters, my wife and my sons, Saqer and Saeed, who were always there for moral support.

Table of Cases

UAE

Attorney general v Mashreq bank 2548/2011
Attorney general v Others 370/2008
HSBC Bank v Others 2901/2005

UK

Ahmad (Mohammad) v HM Advocate [2009] HCJAC 60
Attorney-General v Guardian Newspapers Ltd [1990] 1 AC 109
Bankers Trust Co v Shapira [1980]1 WLR 1274
Barker v Wilson [1980]1 WLR 884
Bowman v Fels [2005] EWCA Civ 226
Brandeaux Advisers (UK) Ltd v Chadwick [2010] EWHC 3241 (QB)
Bucknell v Bucknell [1969] 1 WLR 1204
Christofi v Barclays Bank Plc [1998] 1 W.L.R. 1245
Christofi v Barclays Bank Plc [2000] 1 WLR 937
DB Deniz Nakliyati TAS v Yugopetrol [1992]1 WLR 437
Durant v Financial Services Authority [2003] EWCA Civ 1746
Eckman v Midland Bank Ltd [1973] QB 519

Table of Conventions, Statutes and Regulations

International Conventions

European Convention on Human Rights 1950
United Nations Convention against Corruption 2005
United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) 1988
United Nations Convention against Transnational Organised Crime 2000 (Palermo Convention)

Switzerland

Swiss Federal Act on Banks and Savings Banks 2009

UAE

Central Bank Regulation 24/2000 and its Addendum 2922/2008
Constitution of the United Arab Emirates 1971
Dubai International Financial Centre Non-Financial AML/ATF Regulations
Dubai Multi Commodities Centre AML/ATF Policy

Emirates Securities and Commodities Authority Regulation 17/2010 concerning AML and CFT and its amendment 40/2011
Federal Law No. 1 of 2004 on Combating Terrorism Offences
Federal Law No. 18 of 1993 on Commercial Transactions
Federal Law on Money Laundering Criminalisation 2002
Federal Law 8/2004 regarding the Financial Free Zones
Federal Penal Procedures Code 35/1992
Insurance Authority Regulation 1/2009 regarding AML and CFT in insurance activities
Penal Code 1987
Union Law No. 10 of 1980 Concerning the Central Bank, the Monetary System and Organisation of Banking

UK

Bankers' Books Evidence Act 1879
Banking Act 1979
Banking and Financial Dealings Act 1971
Commissioners of Revenue and Customs Act 2002
Coroners and Justice Act 2009
Crime and Courts Act 2013
Criminal Justice Act 1988
Data Protection Act 1998
Drug Trafficking Act 1994
Drug Trafficking Offences Act 1986
Financial Services Act 2012
Financial Services and Markets Act 2000
Human Rights Act 1998
Money Laundering Regulations 2007
Money Laundering (Amended) Regulations 2012
Payment Services Regulations 2009
Proceeds of Crime Act 2002
Serious Crime Act 2007
Serious Organised Crime and Police Act 2005
Terrorism Act 2002

Contents

Abbreviations

ABCUL	Association of British Credit Unions Ltd
ABI	Association of British Insurers
AED	Arab Emirates Dirham
AFM	Association of Financial Mutuals
AML	Anti-money laundering
AMLSCU	Anti-Money Laundering and Suspicious Cases Unit
APG	Asia/Pacific Group on Money Laundering
ARA	Assets Recovery Agency
ATF	Anti-Terrorist Financing
ATM	Automated teller machines
BCOBS	Banking Conduct of Business Sourcebook
BNIs	Bearer-Negotiable Instruments
BPC	Border Policing Command
BSED	Banking Supervision and Examination Department
CBR 24/2000	Central Bank Regulations 24/2000
CCA 2013	Crime and Courts Act 2013
CDD	Customer due diligence
CEOP	Child Exploitation and Online Protection Centre
CFATF	Caribbean Financial Action Task Force
CFT	Combating the financing of terrorism
CPS	Crown Prosecution Service
CTRs	Cash transaction reports
DFSA	Dubai Financial Services Authority

DIFC	Dubai International Financial Centre
DMCC	Dubai Multi Commodities Centre
DNFBPs	Designated non-financial business and professions
DPA 1998	Data Protection Act 1998
DPRK	Democratic People's Republic of Korea
DVLA	Driver Vehicle Licensing Authority
EAG	Eurasian Group
EC	European Commission
ECC	Economic Crime Command
ECDD	Enhanced customer due diligence
ECHR	European Convention on Human Rights
EEA	European Economic Area
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
ESCA	Emirates Securities and Commodities Authority
ESW	Egmont Secure Web
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIU	Financial Information Unit (UAE)
FIU	Financial Intelligence Unit
FLMLC 2002	Federal Law on Money Laundering Criminalisation 2002
FPEPs	Foreign politically exposed persons
FSA	Financial Services Authority
FSMA 2000	Financial Services and Markets Act 2000
FSRBs	FATF-Style Regional Bodies
FT	Financing of terrorism
GAFISUD	Financial Action Task Force on Money Laundering in South America
GCC	Gulf Cooperation Council
GDCI	General Department of Criminal Investigations
GDP	Gross domestic product
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
GIFCS	Group of International Finance Centre Supervisors
GTBUK	Guaranty Trust Bank UK Limited
HMCE	Her Majesty's Customs and Excise
HMIC	Her Majesty's Inspectors of Constabulary

HMRC	Her Majesty's Revenue and Customs
ICO	Information Commissioner's Office
IMF	International Monetary Fund
IT	Information technology
ITMS	Intelligent Transactional Monitoring Systems
ITWG	Information Technology Working Group
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
LEAs	Law enforcement agencies
LIV	Limited Intelligence Value
LWG	Legal Working Group
ME	Mutual Evaluation
MENAFATF	Middle East and North Africa Financial Action Task Force
MER	Mutual Evaluation Report
ML	Money laundering
MLRO	Money Laundering Reporting Officer
MLRs 2007	Money Laundering Regulations 2007
MONEYVAL	Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOU	Memorandum of Understanding
MSBs	Money Services Businesses
MVTS	Money or value transfer services
NAMLC	National Anti-Money Laundering Committee
NAMLL	National anti-money laundering laws
NCA	National Crime Agency
NCCT	National Committee to Combat Terrorism
NCIS	National Crime Intelligence Service
NCS	National Crime Squad
NPIA	National Policing Improvement Agency
NTFIU	National Terrorist Financial Investigation Unit
OCC	Organised Crime Command
OECD	Organisation for Economic Corporation and Development
OFCs	Offshore Financial Centres
OGBS	Offshore Group of Banking Supervisors
OMLP	Office for Money Laundering Prevention
OpWG	Operational Working Group
OWG	Outreach Working Group

PEPs	Politically exposed persons
POCA 2002	Proceeds of Crime Act 2002
PRA	Prudential Regulation Authority
RBA	Risk-based approach
SAFIU	Saudi Arabia Financial Intelligence Unit
SARs	Suspicious activities reports
SCA 2007	Serious Crime Act 2007
SOCA	Serious Organised Crime Agency
SOCPA 2005	Serious Organised Crime and Police Act 2005
STRs	Suspicious Transactions Reports
SYSC	Senior Management Arrangements Systems and Controls
TBUK	Turkish Bank (UK)
TF	Terrorist Financing
TWG	Training Working Group
TYFQ	Twice Yearly Feedback Questionnaire
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
US	United States

List of Figures

List of Tables

1

Introduction

Background to the Main Issue

The Purpose of Money Laundering

Criminals commit crimes for many reasons. One of these is to profit and obtain value or money in a variety of forms, for instance cash or all types of property, whether real or personal, heritable or moveable. They also try to obscure the illegal origin of these proceeds. They perform a number of money laundering (ML) activities/transactions to ensure that their illegal activities/transactions are not discovered. The term ML denotes the process(es) which criminals use to obscure the real origin of the proceeds which have been derived from criminal activity and to make illegal proceeds appear as if they were legitimate property.[1] ML is an effective way for criminals to avoid prosecution, conviction and confiscation of illegal proceeds[2] since their origin is disguised or turned into legitimate

[1] Commonwealth Secretariat, *Combating Money Laundering and Terrorist Financing*: *A Model of Best Practice for the Financial Sector*, *the Professions and other Designated Businesses* (Second Edition, Commonwealth Secretariat 2006), 6.

[2] Ibid.

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_1

proceeds.[3] This depends on the criminal activity which generates the illegal proceeds[4] which can take various forms, such as drug trafficking, human trafficking, embezzling, fraud, tax evasion, bribe and piracy. These crimes are "predicate offences" for ML and cover any crime which generates illegal proceeds. The criminalisation of ML has therefore two important objectives. Firstly, to prevent criminals from committing crimes which generate illegal proceeds, namely predicate offences for ML. Secondly, to prevent money launderers from enjoying their illegal proceeds.[5]

Indeed, the predicate offences for ML depend on the national legislation which a particular country has adopted and/or the international treaties which the country is a party to. A country can basically adopt one of the following four approaches:

1. The "all offences basis" means that all crimes are considered predicate offences for ML under domestic law, for instance as the United Kingdom (UK) system recognises.[6]
2. Using the "threshold" approach which means a threshold is connected either to the punishment of imprisonment applicable to the predicate offence or to a group of serious offences.[7]
3. There is a list of predicate offences, as in the United Arab Emirates (UAE).[8]
4. Undertaking a combination of these approaches.[9]

[3] Doug Hopton, *Money Laundering*, *a Concise Guide for All Business* (Second Edition, Gower Publishing Limited 2009), 1.

[4] Kenneth Murray, 'A suitable case for treatment: money laundering and knowledge' (2012) 15 (2) Journal of Money Laundering Control 188, 192.

[5] Leonardo Borlini, 'Issues of the International Criminal Regulation of Money Laundering in the Context of Economic Globalization' [November 1, 2008] Paper No. 2008–34 Paolo Baffi Centre Research 1, 12. Available online at SSRN: http://ssrn.com/abstract=1296636 (accessed on 19th May 2015).

[6] As will be analysed in Chap. 7.

[7] FATF Recommendation 3 and its Interpretative Note.

[8] As will be analysed in Chap. 5.

[9] FATF Recommendation 3 and its Interpretative Note.

ML is a global phenomenon since its activities are not confined to the borders of one country. This is done either through physical transfers to another country or via online transfers. ML is the third largest industry in the world after the oil trade and foreign exchange.[10] The Managing Director of the International Monetary Fund (IMF) estimated that 2 to 5 % of the world's gross domestic product (GDP) constitutes ML.[11]

At the national level, ML causes social and economic harm. Social harm is caused through increased crime levels, as predicate offences are committed to obtain profits. Accordingly, without the commission of crimes there is no ML.[12] Countries with high crime levels have more corrupt officials and professionals, who assist in disguising the sources of the illegal proceeds.[13] Economic harm is also caused since the stability of the country's financial and economic system is undermined and less trust exists in the financial institutions of the country.[14]

Stages of ML

The process of ML normally involves the following three stages: (1) placement, (2) layering and (3) integration.

Placement is the first stage which money launderers use to introduce the illegal proceeds from the commission of the predicate offences into the financial system. Bank deposits or cheque cashing businesses are often used to convert the cash into negotiable instruments, such as money orders

[10] Angela Leong , *The Disruption of International Organised Crime* : *An Analysis of Legal and Non-Legal Strategies* (Ashgate Publishing Limited 2007), 41.

[11] Nicholas Ryder, *Money Laundering– An Endless Cycle*? (First Published, Routledge Cavendish 2012), 2. See also, Michel Camdessus, 'Money Laundering: The Importance of International Countermeasures' as presented at the Plenary Meeting of the FATF on ML in Paris February 10, 1998. Available online at: http://www.imf.org/external/np/speeches/1998/021098.htm (accessed on 20th May 2015).

[12] Leonardo Borlini (n 5) 13.

[13] Barbara Crutchfield George and Kathleen A. Lacey, 'Crackdown on Money Laundering: A Comparative Analysis of the Feasibility and Effectiveness of Domestic and Multilateral Policy Reforms' (January 1, 2003) 23 (2) Northwestern Journal of International Law & Business 1, 5.

Available online at SSRN: http://ssrn.com/abstract=1431264 (accessed on 20th May 2015).

[14] Ibid.

or traveller's cheques.[15] It is difficult to introduce large amounts of money generated from the commission of predicate offences, so that a technique known as "smurfing" is used, which separates the large amounts into small amounts below the reporting thresholds, for instance through bank deposits.[16] The main purpose of the smurfing technique is to avoid suspicious transactions reports (STRs) and suspicious activities reports (SARs).

The second stage is layering, which involves various complex transactions to hide and distance the relationship between the money and the predicate offence. These complex transactions take a number of forms, for example the transfer of money to another bank account within/outside the jurisdiction, the purchase of real estate or precious metals and other high-value goods for the purpose of resale.[17] In addition, money can be transferred to bank accounts located in Offshore Financial Centres (OFCs), which enjoy a high degree of banking confidentiality.

The last stage of the ML process is integration, which aims at reintegrating the laundered money into the financial and economic system[18] after distancing it from the illegal source in order to look like a normal and legitimate business activity or a personal/commercial transaction.

Online banking services can also be used to transfer funds much more easily and rapidly between banks accounts located within and outside a particular jurisdiction. More importantly, there is no longer a need to use computers to transfer money electronically, but instead "Smartphones"[19] can be used for mobile banking services, including for the electronic transfer of money, the purchase of goods or services and the payment of bills.[20] The relevant persons in banks and other financial institutions

[15] Bonnie Buchanan, 'Money Laundering – a global obstacle' (2004) 18 (1) Research in International Business and Finance 115, 117.

[16] Nicholas Ryder, *Financial Crime in the 1st Century*: *Law and Policy* (Edward Elgar Publishing Limited 2011), 12.

[17] Jonathan E. Turner, *Money Laundering Prevention*: *Deterring*, *Detecting and Resolving Financial Fraud* (John Wiley & Sons, Inc. Hoboken, Ney Jersey 2011), 9.

[18] Nicholas Ryder (n 16) 13.

[19] Such as an iPhone.

[20] Celina B. Realuyo, 'It's All about the Money: Advancing Anti-Money Laundering Efforts in the U.S. and Mexico to Combat Transnational Organized Crime' [May 2012] Woodrow Wilson International Centre for Scholars, Mexico Institute, 12. Available online at: http://www.wilsoncenter.org/sites/default/files/Realuyo_U.S.-Mexico_Money_Laundering_0.pdf (accessed on 19th February 2015).

have therefore to possess a high degree of integrity, experience and to pay attention in order to detect suspicious transactions/activities.[21] Of course, not all ML activity comprises the three stages since each ML process depends on various factors, such as knowledge and experience of the money launderer, the nature of the predicate offence and the robustness and effectiveness of the anti-money laundering (AML) laws and regulations in the relevant jurisdiction(s).[22]

The Need to Establish a Financial Intelligence Unit (FIU)

ML transactions and activities cannot be easily specified since they develop according to the experience of the perpetrators and the development of information technology (IT), which result in techniques for conducting ML activities. As a result, there has been an urgent need to create an agency at the national level, which is able to identify and analyse complex patterns suggestive of ML activities and transactions. In the early 1990s, the need arose to create a central and specialised entity at the national level, which could collect, analyse and disseminate information associated with ML. This is due to the fact that the law enforcement agencies (LEAs) had only limited access to the relevant financial information.[23] Throughout this period, a number of FIUs were established. The number increased in the following years, especially with the establishment of the Egmont Group in 1995.[24] When a group of FIUs met at the Egmont Arenberg Palace in Brussels, it was decided to set up the "Egmont Group of Financial Intelligence Units" in order to foster international cooperation amongst FIUs to detect and prevent ML.

The establishment of national FIUs has received a lot of attention at both the national and international level after the Egmont Group adopted

[21] Barbara Crutchfield George and Kathleen A. Lacey (n 13) 4.

[22] Doug Hopton (n 3) 3.

[23] International Monetary Fund Handbook, *Financial Intelligence Units*: *An Overview* (International Monetary Fund 2004), 1.

[24] See www.egmontgroup.org (accessed on 20th December 2015).

Article 7 (1)(b) of the 2000 UN Convention against Transnational Organised Crime (Palermo Convention 2000)[25] and Article 14 (1)(b) of the UN Convention against Corruption.[26]

International AML standards have also been published by the Financial Action Task Force (FATF)[27] which has established nine regional groups known as the FATF-style regional bodies (FSRBs), which facilitate the global implementation of the FATF Recommendations. The task force drew up various principles in 1990 in order to counteract ML, which have come to be known as the "Forty FATF Recommendations." The initial 1990 Recommendations and their very first revision in 1996 did not explicitly mention the term "FIU," which first appeared in Recommendation 26 of the 2003 revision of the FATF Recommendations, though, apart from noting that it is a national agency, it did not provide any in-depth details about its core functions. Recommendation 29 of the 2012 FATF Recommendation, which replaced Recommendation 26 of the 2003 FATF Recommendations, sets out more accurately the core functions and powers of the FIU. Most countries have now established an FIU, including the UK and the UAE.

---

[25] Article 7 (1)(b) is as follows:

> (b) Shall, without prejudice to articles 18 and 27 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money laundering.

Palermo Convention 2000 entered into force on 29 September 2003.

[26] Article 14 (1)(b)) is as follows:

> (b) Without prejudice to article 46 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering.

The UN Convention against Corruption entered into force on 14 December 2005.

[27] See www.fatf-gafi.org (accessed on 20th November 2015).

The Reason for Choosing the Subject of the Research

There are two reasons for choosing this subject for research. Firstly, the UAE Mutual Evaluation Report (MER)[28] has noted that the UAE FIU is not properly fulfilling its function of counteracting ML, is not discharging its duties and powers and is not sufficiently independent when dealing with STRs on ML.[29] The UAE MER assesses the laws and regulations and the UAE FIU as only "partly compliant" with Recommendation 26 of the 2003 FATF Recommendations.[30] Secondly, there are practical reasons for choosing this topic. Article 8 (1) of the Federal Law on Money Laundering Criminalisation 2002 (FLMLC 2002) requires the UAE FIU to transmit STRs on ML to the prosecution for investigation. However, during my work as a prosecutor in Dubai for over four years,[31] it became apparent that there is a lack of legislation in relation to both the powers of the UAE FIU to deal with STRs on ML and its relationship with the reporting entities, such as banks, though this ambiguity has not been investigated. Hence, it is crucial to analyse critically whether the UAE FIU adheres to the FATF Recommendations, including the recent 2012 FATF Recommendations, and to assess whether the UAE FIU has sufficient legal powers to deal with STRs on ML.

Structure of the Book

Chapter 2 presents an overview of the relevant literature for this research. I explore the previous research about the role of the FIU in the SARs/STRs[32] regime pursuant to three aspects, namely (1) international standards, (2) the UAE's legal framework and (3) the UK's legal framework.

---

[28] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the Financial Action Task Force (FATF) on 20 June 2008.

[29] Ibid.

[30] Ibid 45.

[31] From 2005 to the beginning of 2009.

[32] The UAE's AML system uses the term "STRs" and the UK's AML system uses the term "SARs."

In Chap. 3 I examine how the requirements of the STRs/SARs regime for the banking sector do not conflict with the well-established doctrine of banking confidentiality. As these requirements fall under the obligation by law and the public interest disclosures.

In Chap. 4 I assess the beginnings of the establishment of the FIU and the features of the four FIU models. I further scrutinise the nature of the FIU from the perspective of international standards with which countries have to comply. Hence I evaluate the importance of the FATF Recommendations for countries and critically analyse the core and non-core functions of an FIU pursuant to the latest relevant FATF Recommendations.

In Chap. 5 I provide a detailed description of the UAE's AML laws and regulations, then critically evaluate the UAE FIU's functions and powers when dealing with the STRs and its relationship with the reporting entities and LEAs. The legal basis for the STRs regime and the requirements imposed by the regime on reporting entities, especially the banking sector, are also critically analysed.

In Chap. 6 I analyse interviews with individuals working in the UAE about the function of the UAE FIU and the requirements of the STRs regime. I conclude with a critique of the findings of the interviews.

In Chap. 7 I examine the UK AML laws and regulations and relevant requirements before investigating the UK's SARs regime and the UK FIU model.

In Chap. 8 I critically analyse the relevant UK laws, which form the backbone of the SARs regime and the types of disclosures, which reporting entities have to make.

In Chap. 9 I assess the UK FIU model, its role in the SARs regime and its relationship with the reporting entities and LEAs. The consent procedures contained in the SARs regime and practical problems associated with them are also critically evaluated.

Chapter 10 contains the conclusion and recommendations. I also provide suggestions for further study.

Scope of the Study

The FIU is not only responsible for combating ML, but also the financing of terrorism (FT), though the latter is outside the scope of this book for two main reasons (however, it is acknowledged that there is often a link between ML and FT since the former can be utilised for the latter). Firstly, FT has its own characteristics and elements, and separate laws deal with the issue in the UAE[33] and the UK,[34] including the requirements of STRs/SARs on FT. Secondly, inclusion of this topic in this research would unduly widen the scope of it.

As regards the UK component of this research, the statutory functions and responsibilities of the Serious Organised Crime Agency (SOCA)—which is now the National Crime Agency (NCA) due to the Crime and Courts Act 2013 (CCA 2013)—are outside the scope of this study, despite the UK FIU having been situated within SOCA, which now forms part of its successor, namely the NCA. This is because the main functions of the NCA relate to detecting and curbing serious and organised crime, which threatens the UK's national security and financial system, but which does not form part of this research.

The research focuses on the role of the FIU at the domestic level in counteracting ML in the UAE and the UK and the relevant FATF requirements. Hence, in this book I do not discuss how the FIU exchanges and requests information from its foreign counterparts at the international level. This research covers the FIU's core functions in counteracting ML, namely receiving, analysing and disseminating STRs/SARs on ML to the LEAs or Office of Prosecution, so that they can conduct further investigations and can commence prosecution. In addition, the FIU also has to fulfil a number of non-core functions; for instance it has to provide feedback to the reporting entities, and some of the non-core functions are no less important than its core functions. Therefore I analyse all the non-core functions of the FIU in counteracting ML. I further cover the domestic STRs/SARs regime since the effectiveness of the FIU's work, particularly its analytical function, depends on receiving high quality STRs/SARs from the reporting entities.

[33] Federal Law No. 1 of 2004 on Combating Terrorism Offences.

[34] Terrorism Act 2002.

In this regard, it should be borne in mind that the LEAs of a country are another success factor behind the STRs/SARs regime since they receive such reports from the FIU, which, after analysing, the proper decision/action can be taken. As a result, reporting entities, the FIU and the LEAs stand in a triangular relationship, and only if they all fulfil their functions properly can ML be successfully combated at the national level.

Thus, an evaluation of the role of the FIU in counteracting ML necessarily entails an analysis of the requirements of the STRs/SARs system on ML, contained in UAE and UK AML laws, since it sets out the requirements which reporting entities have to fulfil when informing the FIU about suspicious transactions. Yet since STRs/SARs, which are submitted by banks, contain confidential customer information which conflicts with the banking confidentiality doctrine, this research also advocates that banks can submit STRs/SARs without this breaching the doctrine.

This book also deals with the regulations, which are imposed on reporting entities, for example customer due diligence (CDD) measures and record keeping. Banks and other financial institutions have to adhere to these obligations since they assist in determining whether or not to make an STR/SAR to the FIU. In other words, without the adoption of these obligations, reporting entities could not fulfil the requirements of the STRs/SARs regime set out in AML laws. The regulations imposed on the banks will be analysed in depth. In other words, the narrow focus of this research is on banks, out of all the reporting entities, for two reasons. Firstly, as will be illustrated later, banks submit the majority of the STRs/SARs to the FIU, and this issue is a common feature all over the world, including in the UAE and the UK. Secondly, it is difficult to analyse all regulations and obligations imposed on all reporting entities since this will widen the scope of the research which could result in our losing the main theme and objectives. For these reasons, entities such as insurance companies, securities and real estate agencies are excluded. Nevertheless, the general obligations imposed on banks are almost the same as those imposed on other financial institutions.

The scope of the study is therefore confined to the role and powers of the FIU in dealing with STRs/SARs on ML in the UAE and UK, the legal basis and requirements of the STRs/SARs regime in both countries and the relevant regulations imposed on banks and other financial institutions

with a view to fulfilling STRs/SARs requirements as spelled out in UAE and UK AML laws. In addition, the relevant FATF Recommendations will be analysed in order to assess to what extent both systems comply with the international standards. This requires an examination of: (1) the doctrine of banking confidentiality and how the submission of STRs/SARs by banks does not undermine it, (2) the ML characteristics and the requisite *actus reus* and *mens rea* required under UAE and UK laws and (3) the advantages and disadvantages of the four FIU models with particular emphasis on the administrative model adopted by the UAE FIU and the law enforcement model chosen by the UK FIU.

Methodology of the Research

This research is based on three grounds, namely the functions of the FIU, including in relation to the STRs/SARs requirements, in counteracting ML 1) in the UAE, 2) in the UK and 3) according to the FATF Recommendations. Thus, choosing the proper methodology is crucial in order to achieve the research objectives, especially when taking into account the aforementioned considerations. At the same time, the adoption of one method of study could not be the right decision to achieve the pursued aim, but rather the adoption of more than one method is essential in order to set up a clear and comprehensive picture for the research framework and aims. Accordingly, a mixed methods approach has been adopted to accommodate the research objectives. Three methods are employed, namely doctrinal legal analysis, empirical investigation and comparative method; each method is explained and justified below.

Doctrinal Legal Analysis

All available primary sources and secondary sources are used in this research. The interpretative method[35] is involved. Relevant AML legal

[35] The interpretative method means drawing inferences and assumptions from the critical analysis of the collected data/information. It completes the analytical function and aims to clarify extensively the results of the analysis. As such, the analytical function should take place before the inter-

provisions in the UAE and the UK constitute the primary sources and are subjected to critical analysis. UAE and UK case law is also critically analysed. Secondary sources, such as books, journals and reports, which fall within the research scope, are also examined.[36] This requires that evidence and arguments discussed by scholars are presented.[37] In addition, I will put forward my own interpretations and arguments.[38]

The relevant FATF Recommendations, the UAE MER[39] and the UK MER[40] are also critically evaluated in order to assess whether the UAE FIU and the UK FIU fulfil the international standards, including STRs/SARs requirements.

Empirical Investigation

Whilst secondary sources about the UK FIU and the SARs requirements exist, there are insufficient data and information available about the UAE FIU and the STRs requirements. Unfortunately, no UAE case law exists to clarify or interpret the statutory responsibilities of the UAE FIU or the role which compliance officers at reporting entities play within the

pretative function. The interpretative method must not be applied subjectively, but objectively, since a wrong interpretation can result in misleading results. Therefore, it should be grounded on the basis of understanding.

See Antonio Diaz Andrade, 'Interpretive Research Aiming at Theory Building: Adopting and Adapting the Case Study Design' (March 2009) 14 (1) The Qualitative Report 42, 45. Available online at: http://www.nova.edu/ssss/QR/QR14-1/diaz-andrade.pdf (accessed on 22nd February 2015).

See also Khushal Vibhute and Filipos Aynale m, 'Legal Research Methods' [2009] Prepared under the Sponsorship of the Justice and Legal System Research Institute, 58 & 59.

Available online at: http://chilot.files.wordpress.com/2011/06/legal-research-methods.pdf (accessed on 22nd February 2015).

See also Hubert knoblaunch and Rene Tuma, 'Videography: An Interpretive Approach to Video-Recorded Macro-Social Interaction' in Eric Margolis and Luc Pauwels (eds), *The Sage Handbook of Visual Research Methods* (SAGE Publications Ltd. 2011), 414 at 419 & 420.

[36] For the aims and advantages of doctrinal legal research, see Khushal Vibhute and Filipos Aynale m (n 35) 73–83.

[37] For a high-quality analysis, see Robert K. Yin, *Case Study Research*: *Design and Methods* (Fourth Edition, SAGE Publications 2009), 160–161.

[38] Ibid.

[39] (N 28).

[40] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF 29 June 2007.

STRs regime. It is said that the objective of empirical investigation, especially qualitative research, is to "understand, explain, explore, discover, and clarify situations, feelings, perceptions, attitudes, values, beliefs, and experiences of group of people."[41] In addition, it is crucial to gather data/information at the site "where participants experience the issue or problem under study."[42] The empirical investigation approach has therefore been selected as a second method in order to gather reliable data about the UAE FIU and the STRs requirements. A number of employees at various sectors in the UAE have been interviewed to provide more in-depth information related both directly and indirectly to the theme of this research.[43]

The main reason for selecting this approach is that it is difficult, if not impossible, to employ the quantitative method, for example to formulate a survey or a questionnaire. This is because each relevant sector has a relationship with the UAE FIU that comes from a different perspective, so that one questionnaire could not ascertain the views of employees working at these various sectors. Therefore, the qualitative method, especially interviews, appears most suitable since it is an accepted approach to obtain data/information in any professional and academic field.[44] For the purpose of this approach, a number of specific questions have been designed for each interviewee with a view to probing his or her experience and observations in this regard.[45]

The interviews are semi-structured and this means that the interviewer/researcher asks the interviewee specific questions, though there is room for flexibility, so that he or she can also pose follow-up questions in order to understand further the interviewee's answers.[46]

---

[41] Ranjit Kumar, *Research Methodology* (Third Edition, SAGE Publications Ltd. 2011), 104.

[42] John W. Creswell, *Research Design* (Fourth Edition, SAGE Publications Ltd. 2014), 185.

[43] For the aims of individual and group interviews, see Lisa Webley, 'Qualitative Approaches to Empirical Legal Research' in Peter Cane and Herbert M. Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010), 926 at 936.

[44] Ranjit Kumar (41) 128.

See also Lisa Webley (n 43) 937.

[45] The interviewer/researcher has asked relevant questions to confirm a number of important facts. See Robert K. Yin (n 37) 107.

[46] For the major types of interview, see Alan Bryman, *Social Research Methods* (Fourth Edition, Oxford University Press 2012), 212–230.

Four sectors have been chosen for the empirical investigation, namely (1) the UAE FIU, (2) the banking sector, (3) the public prosecution office and (4) the police. The relevant period is between March and May 2012. The reason for selecting these sectors is that the UAE FIU is best placed for providing data and information about its responsibilities and annual statistics about STRs. The banking sector, especially compliance officers, have been selected for the purpose of empirical investigation, as the majority of STRs are submitted by these officers to the UAE FIU. In addition, the LEAs, such as the police and the public prosecution office, have been selected for this method, as they are the end users of the STRs. In other words, these sectors have been selected since they have experience in AML investigations and prosecutions after receiving information from the UAE FIU.

All information and data gathered through interviews are presented in a narrative manner[47] and are analysed with a view to identifying current functions and responsibilities of the UAE FIU and critically evaluating the STRs regime. The interview questions were sent in advance to the interviewees, so that they could have some opportunity to reflect on the questions prior to the interviews.[48] The information and data were recorded during the interviews through note taking, as the interviewees refused to allow any electronic means of recording.[49]

Comparative Method

This method basically depends on a comparison between more than one legal system[50] in order to understand their similarities and differences. In general, there are various purposes to which this method can be put, for instance to understand the law, law unification or harmonisation, or

[47] For the approaches of data processing in qualitative studies, see Ranjit Kumar (n 41) 277 & 278.

[48] For qualitative data collection types, see John W. Creswell (n 42) 189–193.

[49] For cases where no recording devices are allowed during the interview, see Robert K. Yin (n 37) 109.

[50] Konrad Zweigert and Hein Kötz, *An Introduction to Comparative Law* (Third Edition, Oxford University Press 1998), 4.

to solve specific problems.[51] It is also an effective approach to provide practical solutions at the national level or to find a solution to a common problem at the international level.[52] Therefore, such a method can be done by comparing institutions/agencies, which fulfil the same role, but are based in different legal systems.[53] In addition, there are two levels of comparison, also referred to as units of comparison, namely (1) macro-comparison which focuses on general questions or issues, and (2) micro-comparison which focuses on specific elements or legal problems.[54]

By applying the above features of the comparative method to this research, I strive to focus on the micro-comparison level. This means comparing the two national institutions—the UAE FIU and the UK FIU— since they have the same core functions in counteracting ML, though the UAE FIU employs the administrative model, whilst the UK FIU employs the law enforcement model. Nevertheless, adopting the micro-comparison level entails examining the two units in both countries within their legal framework and context.[55] The comparative method is an ideal approach to assess how the adoption of legal regulations, which have been successfully enacted in other jurisdictions, can solve similar problems.[56] The elements of the comparison comprise the role of the FIU in counteracting ML in the UAE and the UK and their powers in handling STRs/SARs. This requires an evaluation of the relevant AML laws in the two countries in order to assess in which situations STRs/SARs have to be submitted by the reporting entities. The comparison also extends to the relationship between the FIU and the LEAs in both countries since these agencies are the third limb within the triangular

[51] For the purposes of comparative law research, see Gerhard Dannemann, 'Comparative Law: Study of Similarities and Differences?' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford University Press 2008), 383 at 401–408.

[52] Geoffrey Wilson, 'Comparative Legal Scholarship' in Mike McConville and Wing Hong Chui (eds), *Research Methods for Law* (Edinburgh University Press 2007), 87 at 88.

[53] Konrad Zweigert and Hein Kötz (n 50) 34–36.

[54] For macro-comparison and micro-comparison in detail, see Esin Örücü, 'Developing comparative law' in Esin Örücü and David Nelken (eds), *Comparative law : a handbook* (Hart 2007), 43 at 56–62.

[55] J. Paul Lomio, Henrik S. Spang Hanssen and George D. Wilson, *Legal Research Methods in a Modern World: A Coursebook* (Third Edition, DJØF Publishing 2011), 65.

[56] Michael Salter and Julie Mason, *Writing Law Dissertations* (First Published, Pearson Education Limited 2007), 183.

relationship of entities within the STRs/SARs regime, in addition to the FIU and the reporting entities.

There are three main reasons for selecting the UK FIU as a comparator. Firstly, it represents the FIU law enforcement model, which is different to the UAE FIU administrative model. Secondly, the UK MER has made a number of positive remarks about the UK FIU.[57] The UK FIU has improved the quality of SARs, which have been submitted by the reporting entities, and has effectively assisted LEAs with the investigation/prosecution.[58] Thirdly, the UK's SARs regime on ML, especially the consent procedures, is an innovative system,[59] which encompasses three types of disclosures, namely required, authorised and protected disclosure which the reporting entities have to follow. All of these aspects are crucial for proposing the optimal model for the UAE FIU. The comparative method critically compares the results and draws conclusions.[60] Therefore, I critically assess whether the UAE FIU could adopt the UK FIU model or, in case this is not possible, whether the UAE FIU model can be amended in such a way that the benefits of the UK FIU model become integrated within the UAE FIU model.

In addition to a comparison of the functions of the UAE FIU and the UK FIU, the relevant international standards (the FATF Recommendations) are used as a threshold against which we can assess whether the UAE and UK FIU fulfil their functions. By spelling out the applicable legal framework, we can identify which problems exist at the national level and propose legal and practical solutions to ensure that national laws and regulations are in line with the applicable international standards.[61]

[57] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 40) 78–89.

[58] Ibid.

[59] Jayesh D'Souza, *Terrorist financing, money laundering, and tax evasion – Examining the performance of Financial Intelligence Unit* (Taylor & Francis Group, LLC 2012), 123.

[60] J. Paul Lomio, Henrik S. Spang Hanssen and George D. Wilson (n 55) 66.

[61] Michael Salter and Julie Mason (n 56) 189.

2

Financial Intelligence Units in the UK and UAE to Date

This chapter deals with the existing literature about the features of the FIU and its functions in AML. This necessarily entails focusing on the SARs/STRs on ML which are received by the FIU. Indeed, the SARs/STRs regime forms the backbone of the tasks of the FIU. We will therefore explore the relevant literature about the role of the FIU in relation to the SARs/STRs regime. The chapter is divided into three sections, each dealing with a specific theme: (1) FIUs and international standards, (2) the UAE's FIU legal framework and (3) the UK's FIU legal framework.

FIUs and International Standards

Since their adoption in 1990, the FATF Recommendations have been revised and updated on three occasions, in 1996, 2003 and more recently in 2012. Furthermore, in 2001, FATF also expanded its mandate in order to combat Terrorist Financing (TF) and launched Nine Special Recommendations, which deal with this crime. By 2004, the overall FATF Recommendations had thus increased to what is also known as

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_2

the "40 + 9 Recommendations." Ping[1] explains how the revisions of the Recommendations have been undertaken in order "to take into account changes in money laundering methods, techniques and trends."[2] Gilmore[3] explains how the FATF is considered the leading global standard setter for counteracting ML and how the initial 1990 FATF Recommendations focus on the following three areas: (1) improving the legal system at the national level, (2) enhancing the role of the financial systems in counteracting ML and (3) strengthening international cooperation.[4] He further cogently explains the reasons behind the revisions of the Recommendations in 1996 and 2003.[5]

Jensen and Ann Png[6] show that:

> Implementation of the FATF Recommendations have been enhanced through their endorsement as AML/Combating the Financing of Terrorism (CFT) international standards by the Executive Boards of the IMF and the World Bank, and the undertaking of mutual evaluations by the FATF and its associated bodies.[7]

The initial 1990 FATF Recommendations and their very first revision in 1996 did not explicitly mention the term "FIU." Instead, it was only mentioned that financial institutions had to report any suspicious transaction to the "competent authorities." The term "FIU" was explicitly mentioned for the very first time in the 2003 revision of the FATF Recommendations. Recommendation 26 of that revision mentioned the term "FIU" and its authority in relation to STRs on ML or TF and stated:

---

[1] H.E. Ping, 'The measures on combating money laundering and terrorist financing in the PRC: from the perspective of financial action task force' (2008) 11 (4) Journal of Money Laundering Control 320.

[2] Ibid 321.

[3] William C. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (Fourth Edition, Council of Europe 2011).

[4] Ibid 96–100.

[5] Ibid 101–114.

[6] Neil Jensen and Png-Cheong Ann, 'Implementation of the FATF 40 + 9 Recommendations: a perspective from developing countries' (2011) 14 (2) Journal of Money Laundering Control 110.

[7] Ibid 111.

> Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

This Recommendation briefly referred to the core functions of an FIU, which consist of receiving, analysing and disseminating the STR, but without explaining each function. The Interpretative Note to Recommendation 26 also did not add any useful elements about this particular aspect, but instead only emphasised the importance of international cooperation.

Pursuant to the recent revision of the FATF Recommendations in 2012, Recommendation 26 has been revised and replaced by the 2012 FATF Recommendation 29, presumably since it lacked clarity. The Recommendation now provides that:

> Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

More importantly, the Interpretative Note to Recommendation 29 comprehensively explained and clarified the role of the FIU from different perspectives.

An examination of the functions of the FIU requires scrutiny of the pivotal STRs system. The 2012 FATF Recommendation 20 has therefore adopted the STRs/SARs regime in cases where there is "suspicion" or "reasonable grounds for suspicion" that the transaction/activity relates to ML and provides that:

> If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the FIU.

Shehu[8] discusses the nature of the binding force of the FATF Recommendations and notes that:

> Although … the FATF has no legal basis to enforce them on any jurisdiction other than its members, in practice, they are compulsory on all jurisdictions, whether they are members or not. Persistent failure to comply with them will result, initially, in a report that the jurisdiction in question does not have an adequate regime of AML measures: this will imply that the jurisdiction's financial sector would be regarded as posing significant ML/TF risks to the international system … then the FATF, after a review of the situation may issue a statement alerting the international financial community to the perceived deficiencies.[9]

On 18 October 2013, the FATF published a public statement identifying jurisdictions with high-risk and non-cooperative jurisdictions that pose a risk to the international financial system.[10]

In addition, one of the most effective mechanisms to assess whether a country is complying with the FATF Recommendations is the MER, which is published by the FATF. This Report identifies to what degree a country's legal system complies with the FATF standards. The laws, regulations and AML measures of a country are scrutinised in the MER, and how well a country is implementing the FATF standards in practice is also examined. Shehu notes of the FATF MER: "the Mutual Evaluation (ME) exercise conduct[ed] by the FATF and other relevant organisations

[8] Abdullahi Y. Shehu, 'Promoting financial sector stability through an effective AML/CFT regime' (2010) 13 (2) Journal of Money Laundering Control 139.

[9] Ibid 142 and 143.

[10] The statement is available on the FATF's website at: www.fatf-gafi.org (accessed on 2nd November 2014).

has proved to be a useful tool in ensuring consistent compliance with the standards"[11] and explains that:

> The ME process is not complete until the final report is published. In accordance with this and in line with FATF procedures, particularly the need to instill transparency into the ME process, MERs are to be shared with all members, international partners, and any member of the public that is interested in the report. These reports are discussed in open session during the … plenary meetings … The ME process is a demonstration of the commitment of member states to implement the FATF standards.[12]

Jensen and Ann make clear that:

> For each mutual evaluation, the country's level of compliance with the FATF Recommendations is discussed and adopted at plenary sessions of the FATF and FATF-styled regional bodies, or by the Executive Boards of the IMF and the World Bank, and ultimately disclosed as public information. This rigorous scrutiny through mutual evaluation, public disclosure and its associated peer pressure has contributed significantly to the development of AML/CFT regimes around the world.[13]

Clark and Russell[14] note that a common definition of an FIU, which has also been adopted by the Egmont Group in1997, is that it is:

> A central, national agency responsible for receiving (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:
> (a) concerning suspected proceeds of crime, or
> (b) required by national legislation or regulation,
> in order to combat money laundering.[15]

---

[11] Abdullahi Y. Shehu (n 69) 147.

[12] Ibid.

[13] Jensen Neil and Ann Png-Cheong (n 67) 111.

[14] Andrew Clark and Matthew Russell, 'Reporting Regimes' in Andrew Clark and Peter Burrell (eds), *A Practitioner's Guide to International Money Laundering Law and Regulation* (City & Financial Publishing 2003), 115.

[15] Ibid.

Four Models of FIU

The above definition has been extended in order to combat potential FT as well. Clark and Russell[16] also highlight that there are four models for an FIU, namely the administrative, law enforcement, judicial/prosecutorial and hybrid model, and explain the advantages and disadvantages of each particular one. They attribute the differences in the different models to four reasons attributable to a country's circumstances, namely (1) the national legal system, (2) the nature of the national AML legislation, (3) political issues and (4) customs and cultural aspects.[17] However, they also suggest that the core functions of an FIU will not be affected by a specific model.

The IMF's Handbook, *Financial Intelligence Units*: *An Overview*,[18] deals with the FIU in the same way as Clark and Russell and gives details about the advantages and disadvantages of the four FIU models and stresses that all national FIUs have to fulfil the three principal tasks in relation to combating ML, irrespective of the particular model. Firstly, the FIU receives STRs/SARs from the reporting entities. Secondly, an FIU analyses these reports through its human resources. Thirdly, based on its analysis, an FIU disseminates the results to the national competent authority for further investigation and/or prosecution. The IMF Handbook also lists additional functions of an FIU, for example to conduct research, to provide general and specific feedback to the reporting entities, and to increase public awareness about combating ML. Indeed, these additional functions of the FIU are also crucial in combating ML at the national level and are no less important than its key functions.

Schott[19] suggests that national authority should take into account a number of considerations in establishing their FIU model. The author states that:

---

[16] Ibid.

[17] Ibid.

[18] International Monetary Fund Handbook, *Financial Intelligence Units*: *An Overview* (International Monetary Fund 2004).

[19] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Second Edition and Supplement on Special Recommendation IX, 2006 The World Bank).

> Although no single model will work for all countries, some criteria are essential; the discussion below is given in the form of questions:
>
> • Will or does the FIU possess relevant capacity and expertise in financial operations? If not, what is needed?
>
> • What is the relationship between the proposed or existing FIU and the financial industry in the domestic context? What would enhance that relationship?
>
> • Will or does the institution possess a culture conducive to protecting the confidentiality of financial information and to mitigating potential harm to individual privacy?
>
> • Will or does the proposed FIU possess the actual legal authority, technical capacity, and experience to provide appropriate and timely international cooperation?
>
> • Would the legal framework applicable to the proposed or existing FIU allow it to take part in the international administrative type of cooperation and would the legal framework allow for rapid, efficient, spontaneous and/or "upon request" international information exchanges relating to suspicious transactions?[20]

D'Souza[21] provides a good account of an optimal FIU. The author briefly describes the four FIUs' models and states in relation to the administrative type that:

> they lack the authority enjoyed by these entities in obtaining evidence and taking immediate action such as freezing assets or arresting suspects.[22]

The author notes in relation to the law enforcement type that:

> [they] are attached to police units … have certain law enforcement powers and work with other law enforcement agencies, reaping the benefits of their expertise and sources of information in solving financial crime. However, reporting entities may hold back when making financial

[20] Ibid VII-18.

[21] Jayesh D'Souza, *Terrorist financing, money laundering, and tax evasion- Examining the performance of Financial Intelligence Units* (Taylor and Francis Group, LLC 2012).

[22] Ibid Xi.

> disclosures if they feel their clients may be investigated for other crimes besides terrorist financing and money laundering.[23]

More importantly, D'Souza discusses the key factors of successful FIUs and challenges facing them and argues that:

> FIUs increase their probability of success by constantly updating technology, hiring those with relevant work experience and training them to keep up with the latest trends in financial crime, and plugging gaps in financial investment.[24]

Simonova[25] describes an FIU from different angles as ideal for providing the reporting entities with training and guidance to improve their participation in counteracting ML. The author states that the FIUs are:

> in an ideal position of collecting valuable data on money laundering techniques from all over the world. At the national level, they are a link between financial institutions and law enforcement agencies having useful contacts to each side … There is no other institution which is better suited for educating financial institutions in preventing and detecting money laundering … It would be more appropriate if national FIUs took a more active role in educating financial institutions in AML techniques through regular publication of updated typologies and other guidance.[26]

The Legal Framework of the FIU in the UAE

The FLMLC 2002 criminalises ML in the UAE. In addition, a number of regulations and circulars have been issued by the regulatory and supervisory authorities, for example the Central Bank of the UAE and the Emirates Securities and Commodities Authority (ESCA).

---

[23] Ibid.

[24] Ibid 143.

[25] Anna Simonova, 'The risk-based approach to anti-money laundering: problems and solutions' (2011) 14 (4) Journal of Money Laundering Control 346.

[26] Ibid 355.

The FLMLC 2002 defines "ML" as:

> Every act involving conveyance, transfer or depositing of property or concealment or disguise of the true nature of said property attained from any of the offences provided for in Clause 2 of Article 2 of this Law.[27]

Article 2 (2) of the FLMLC 2002 makes clear that, for "property" to be included in the scope of this definition, "property" has to constitute "proceeds" emanating from one of the following offences:

> a: Narcotics and psychotropic substances
> b: Kidnapping, piracy, and terrorism
> c: Offences committed in violation of the provisions of Environmental Law
> d: Illicit dealing in fire-arms and ammunition
> e: Bribery, embezzlement, and damage to public property
> f: Deceit, breach of trust, and related offences
> g: Any other related offences provided for in international treaties to which the State is a party.[28]

Articles 7 and 8 of the FLMLC 2002 govern the establishment and tasks of the UAE FIU and which represent the administrative FIU model. Article 7 provides that:

> A Financial Information Unit shall be established with the Central Bank and deal with money laundering and suspected cases to which reports on suspected transactions shall be sent by all financial institutions and other related financial, commercial and economic establishments. However, the committee shall determine the format for reporting suspicious transactions and the method of sending said form to it. The said Unit shall make the information obtained by it available to the Law Enforcement Agencies for their investigations. This Unit may also exchange with the similar units in other countries, especially in cases of the information provided to it in respect of suspicious cases, in pursuance of the international treaties to which the state is a party or on reciprocity basis.[29]

[27] Article 1 of the FLMLC 2002.
[28] Article 2 (2) of the FLMLC 2002.
[29] Article 7 of the FLMLC 2002.

Whilst Article 8 provides that:

> 1: The Unit provided for in Article 7 hereof shall, after studying the cases reported to it, notify the public prosecution to take the necessary actions.
>
> 2: However, if money laundering cases are directly reported to the public prosecution it must take the necessary action after seeking the opinion of said Unit on the contents of the report.[30]

The functions of the UAE FIU are not further detailed in any articles or books, but a number of textbooks provide a general explanation of the provisions of the AML laws and regulations. Lovett and Barwick[31] provide a good account of the provisions in terms of the definition of ML and the primary offences contained in the Act. The authors also state that:

> The UAE Central Bank had already pre-empted the legislation by setting up a FIU in July 1999 in the form of the Anti-Money Laundering and Suspicious Cases Unit (AMLSCU) … staffed with over 100 specialists.[32]

Lovett and Barwick further explain that the UAE Central Bank has the power to issue freezing orders over suspected funds for up to seven days.

Ghattas[33] discusses the statutory provisions contained in the FLMLC 2002 and the relevant regulations/circulars issued by the Central Bank and other authorities, such as ESCA. Ghattas also states how the UAE FIU has been established as a reporting entity for the financial institutions in relation to submitting STRs, and also shares information about STRs with UAE LEAs and foreign FIUs.

Whilst these sources briefly refer to the STRs requirements of reporting entities in the UAE, none mentions that the FLMLC 2002 and the

---

[30] Article 8 of the FLMLC 2002.

[31] Graham Lovett and Charles Barwick, 'United Arab Emirates' in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth (eds), *Anti-Money Laundering: International Law and Practice* (John Wiley & Sons Ltd., Chichester 2007), 643.

[32] Ibid 650.

[33] Hani Ghattas, 'United Arab Emirates' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 1049.

Central Bank Regulations 24/2000 (CBR 24/2000) are ambiguous in relation to the STRs basis since the Act requires "actual knowledge" about ML activity, whilst the CBR 24/2000 only requires "reasonable grounds to suspect" ML activity. The sources also do not analyse the core and non-core functions of the UAE FIU.

The most recent and most important and reliable source, which deals with the UAE AML system and with the UAE FIU tasks in particular, is the UAE MER on AML and CFT adopted by the FATF in 2008.[34] The report criticises the UAE AML controls in a number of respects, for example, in relation to CDD and enhanced customer due diligence (ECDD), the meaning of beneficial ownership and the basis and requirements of STRs. Accordingly, the UAE Central Bank issued an Addendum to Regulation 24/2000 (Addendum 2922/2008) on 17 June 2008 in order to close certain loopholes identified in the UAE MER.

In addition to the above criticisms, the UAE MER also criticised the UAE FIU in relation to a number of other issues, such as its core and non-core functions, its independence and its authority.

The UAE MER states that:

> In practice, the FIU serves as the national centre for analysing STRs. Article 7 of the AML law provides that the FIU shall "deal" with money laundering and suspicious cases. There is no direct explicit grant of power in the AML law to permit the FIU to undertake analysis.[35]

The report also notes that there is "lack of operational independence of the (UAE) FIU,"[36] and that "assessors were not able to conclude that the FIU was effective in its core functions of receiving, analysing and disseminating STRs,"[37] especially in light of inadequate statistics about received and disseminated STRs. More importantly, the assessors rated the UAE laws, regulations and the FIU as only "partly compliant"[38] with

[34] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF on 20 June 2008.

[35] Ibid 38.

[36] Ibid 45.

[37] Ibid.

[38] Ibid.

the 2003 FATF's Recommendation 26 in relation to the requirements, which an FIU has to fulfil.

Despite the UAE MER having been published in 2008, only two sources have discussed these issues, but without addressing or scrutinising the tasks of the UAE FIU. Firstly, Hamdan[39] observes that during the period between June 2002 and May 2009 the UAE FIU received 80,592 STRs about ML from the reporting entities, but only 285 STRs were transmitted to the public prosecution office. Secondly, Alkaabi and others[40] state that the public prosecution office sent only 20 STRs out of the 285 received to the courts. In addition, only 7 % of these 20resulted in an actual conviction.

Hence, the question arises as to why there is such a huge discrepancy between the numbers of STRs received by the UAE FIU and the number which are then transmitted to the public prosecutions office. Furthermore, no sources are available which evaluate whether the current functions and authority of the UAE FIU are compatible with the 2012 FATF Recommendation 29, which replaces the 2003 FATF Recommendation 26, and which governs all aspects of the FIU.

On the other hand, it is assumed that the UAE FIU annual reports provide valuable statistics about the STRs on ML; however, they are not accurate since current statistics, contained in the AMLSCU annual reports, only show the annual number of STRs on ML, TF and other financial crimes, such as fraud. Hence, despite crucial information and statistics being contained in the AMLSCU's annual reports, statistics about STRs on ML that are submitted are still vague, though according to the statistics on STRs in 2010, most involved suspected cases of ML and other types of financial crimes.[41] Moreover, the 2009 and 2010 AMLSCU annual reports show that banks, established in the UAE, sub-

[39] Sara Hamdan, 'Suspect funds on the rise' *The National*, Jun 23 2009, available online at: http://www.thenational.ae/business/banking/suspect-funds-on-the-rise (accessed on 19th February 2015).

[40] Alkaabi, Ali and others, 'A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA' [January 20, 2010] Finance and Corporate Governance Conference 2010 Paper 1. Available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539843 (accessed on 13th November 2015).

[41] 'AMLSCU Annual Report—2010' as produced by the AMLSCU.

mitted the majority of STRs. For instance, in 2010, 2465 STRs out of 2871 were submitted by banks, equal to 88.7 %.[42]

The Legal Framework of the FIU in the UK

The UK AML system is firstly based on the Proceeds of Crime Act 2002 (POCA 2002), which was amended by the Serious Organised Crime and Police Act 2005 (SOCPA 2005), the Serious Crime Act 2007 (SCA 2007) and recently the CCA 2013. The Money Laundering Regulations 2007 (MLRs 2007),[43] as amended by the Money Laundering (Amended) Regulations 2012, also play an important role since they require reporting entities, such as banks and other financial institutions, to adopt a number of internal procedures to detect SARs to combat ML. Part 7 of POCA 2002 deals with ML offences and s.340 (11) defines ML as an act which:

> (a) constitutes an offence under section 327, 328 or 329,
> (b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),
> (c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or
> (d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.[44]

The UK FIU used to be situated within SOCA, but is now part of the NCA. SOCA replaced the National Crime Intelligence Service (NCIS) and the National Crime Squad (NCS) and assumed its tasks from April 2006 onwards. After seven years, SOCA was abolished and replaced by the NCA which started its function on 7 October 2013. However, the shift from SOCA to the NCA does not affect the responsibilities and functions of the UK FIU, namely to deal with the SAR system. The

[42] 'AMLSCU Annual Reports—2009' as produced by the AMLSCU and 'AMLSCU Annual Report—2010' (n 102).

[43] Which replaced the MLRs 2003.

[44] S.340 (11) of POCA 2002.

UK FIU represents the FIU law enforcement model. As a result of this change, reporting entities have now to submit STRs to the NCA and no longer to SOCA. SOCA is the largest body to have been moved into the NCA, and its budget and staff form the core of the latter in order to deliver a stronger, more integrated and efficiently coordinated national response to serious and organised criminality.

S.1 (3)(b) of the CCA 2013 provides that the NCA is to have "the functions conferred by the Proceeds of Crime Act 2002." In addition, s.1 (5) of the Act provides that:

> The NCA is to have the function (the "criminal intelligence function") of gathering, storing, processing, analysing, and disseminating information that is relevant to any of the following
> (a) activities to combat organised crime or serious crime;
> (b) activities to combat any other kind of crime;
> (c) exploitation proceeds investigations (within the meaning of section 341(5) of the Proceeds of Crime Act 2002), exploitation proceeds orders (within the meaning of Part 7 of the Coroners and Justice Act 2009), and applications for such orders.[45]

In 2006, Sir Stephen Lander[46] reviewed the UK's SARs regime in light of the creation of SOCA and its functions as the UK FIU in order to assess the effectiveness of the regime. Sir Stephen defines the FIU as "the unit that receives and distributes SARs."[47] The review made 24 recommendations, which can be grouped into the following four categories: (1) nine recommendations dealing with SOCA being the UK FIU, (2) three recommendations in relation to the reporting entities, (3) 11 recommendations about LEAs exploiting the SARs and (4) one recommendation about the implementation of the recommendations.

[45] S.1 (5) of the POCA 2002.

[46] The review was commissioned in July 2005. Sir Stephen Lander, 'Review of the suspicious activity reports regime' as produced by the SOCA in March 2006, available on the SOCA's website at: www.soca.gov.uk (last accessed on 13th September 2014).

[47] Ibid 3.

Harfield[48] explores the K FIU model, as well as the underlying reasons, and its powers, responsibility and accountability. The author argues that:

> The vision the Government has set for [SOCA] is far closer to problem solving "policing" in the sense of sustaining safer communities than the "law enforcement" paradigm of criminal investigation inherent in the modern police service with its performance emphasis on detections and prosecutions.[49]

Keith Bristow, the first Director General, explains that the reason for the establishment of the NCA is to fight serious and organised crime more effectively. He also notes that:

> It will have the capabilities to tackle serious and organised crime in areas that have previously had a fragmented response – such as the border, cyber and economic crime – and those where we need to increase our impact, such as child protection and human trafficking.[50]

Radmore[51] further explains that the NCA acts as the UK FIU and that:

> The NCA will, among other things, take over the activities of the Serious Organised Crime Agency. As a result, it will become the entity to which firms must report knowledge or suspicion of money laundering or terrorist finance, and seek approval to continue with transactions where appropriate.[52]

---

[48] Clive Harfield, 'SOCA: a paradigm shift in British policing' (2006) 46 (4) British Journal of Criminology 743.

[49] Ibid 747.

[50] 'NCA Annual Plan 2013–14', as produced by the NCA in October 2013, 4.

[51] Emma Radmore, 'Deferred Prosecution Agreements – for more enforcement action?' May 2013 Financial Regulation International 1. Available online at: http://www.dentons.com/insights/articles/2013/june/18/deferred-prosecution-agreements-for-more-enforcement-action (accessed on 24th December 2014).

[52] Ibid.

Harrisons and Ryder[53] argue that the CCA 2013 transfers the role of SOCA to the NCA; however, they also note that the Act does not expressly mention that this means that the NCA now fulfils the role of the UK FIU. The authors state that the CCA 2013:

> transfers SOCA's role under the Proceeds of Crime Act 2002 to the NCA … No mention, however, has been made regarding SOCA's role as the UK's FIU … with the introduction of the NCA … there is no mention with regards to the inclusion or delegation of SOCA's role as the UK's FIU. The future situation is therefore presently unclear.[54]

In fact, even Part 1 of SOCPA 2005, which is now defunct under the CCA 2013, which created SOCA and spelled out its powers and functions in relation to serious organised crime, did not explicitly mention that SOCA acts as the UK's FIU. Instead, Part 1 of SOCPA 2005 clarified that SOCA has the function of criminal intelligence gathering, storing, processing, analysing and disseminating information relevant to combating serious organised crime. This necessarily meant that SOCA acted as the UK's FIU. Similarly, the CCA 2013 explicitly mentions that the NCA has the function of criminal intelligence gathering, storing, processing, analysing and disseminating information, which is relevant to combating organised and serious crime, Which necessarily means that the NCA now acts as the UK FIU.

Johnston[55] emphasises that the vast majority of NCA work is the same as that of SOCA; however, the NCA has different powers. He notes that:

> Its first director-general Keith Bristow, a former chief constable of Warwickshire, will be able to insist that top officers do his bidding, which will make him the most powerful police officer in the land. So while this might look like a simple rebranding exercise, in fact it marks a fundamental change to the way policing has been carried out in this country for more than 170 years, essentially as a locally controlled function.[56]

---

[53] Karen Harrison and Nicholas Ryder, *The Law Relating to Financial Crime in the United Kingdom* (Ashgate Publishing Limited 2013).

[54] Ibid 26, 27 and 163.

[55] Philip Johnston, 'The National Crime Agency: Does Britain need an FBI?' *The Telegraph*, 7 October 2013.

[56] Ibid.

Preller[57] summarises the core and non-core functions of the UK FIU in relation to the SARs regime and states that:

> The role of SOCA [UK FIU] is essential to the next stage, i.e. collation stage … the FIU in the UK is a policing agency and not an administrative agency as opposed to other AML regimes … Furthermore, it is also SOCA's duty to store all SARs-related intelligence in a nation-wide database (i.e. ELMER), which has been accessible by all UK LEAs.[58]

Whilst Booth and others[59] elucidate the three types of disclosure under POCA 2002 and discuss in detail their legal consequences, they also clarify that the term "SAR" is wider than "disclosure":

> In the UK practice, "SAR" is the generic term for disclosures used by the FIU at SOCA, and by law enforcement, regulators, and the regulated sector. SOCA also uses the term "consent requests" for disclosures about criminal property combined with a request for consent … The term "SAR" is generally used for the reports made to SOCA and it applies to all types of money laundering disclosure under POCA, including consent reports.[60]

D'Souza also analyses the UK FIU model and studies its organisational framework, functions and powers in relation to the SARs regime and expounds that the UK FIU:

> Facilitates regular dialogue between law enforcement end users and other stakeholders of the SARs regime to ensure that there is constructive communication and input into policy development and into developing and publicising best practices and guidance.[61]

---

[57] Sabrina Fiona Preller, 'Comparing AML legislation of the UK, Switzerland and Germany' (2008) 11 (3) Journal of Money Laundering Control 234.

[58] Ibid 236.

[59] Robin Booth and others, *Money Laundering Law and Regulation*: *A Practical Guide* (First Published, Oxford University Press 2011).

[60] Ibid 93 and 104.

[61] Jayesh D'Souza (n 82) 154.

In addition to POCA 2002, the MLRs 2007 is important for counteracting ML. Blair and Brent[62] discuss the requirements which the MLR 2007 imposes upon the relevant persons. The authors highlight that relevant persons are not confined to the financial sector, as the purpose of the MLR 2007:

> is to extend the scope of the regime to persons outside the financial sector. This reflects the fact that money launderers and terrorist financers utilise methods outside these sectors to conceal the proceeds of crime as controls in the traditional financial sectors have been imposed.[63]

The MLRs 2007 impose key requirements, for example in relation to CDD, record keeping and supervision, which are further explained by Stott and Ullah[64] who point out that:

> There is a marked shift under MLR 2007 towards ongoing obligations on organisations to subject their customers to adopt a "risk-based approach" to their AML compliance.[65]

When considering the UK FIU, it is crucial to refer briefly to the UK MER on AML, which was adopted by the FATF in June 2007.[66] The report states that:

> Overall, the UK FIU substantially meets the criteria of [the 2003 FATF's] Recommendation 26 [in relation to the requirements of the FIU] and appears to be a generally effective FIU.[67]

---

[62] William Blair and Richard Brent, 'Regulatory Responsibilities' in William Blair and Richard Brent (eds), *Banks and Financial crime*: *the International Law of Tainted Money* (Oxford University Press 2008), 241.

[63] Ibid 244.

[64] Christ Stott and Zai Ullah, 'Money Laundering Regulations 2007: Part 1' (2008) 23 (3) Journal of International Banking Law and Regulation 175.

[65] Ibid 175.

[66] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF on 29 June 2007.

[67] Ibid 6.

However, SOCA was rated as "lacking compliance" with the 2003 FATF Recommendation 26[68] for three reasons. Firstly, the UK FIU did not publish annual reports about its functions, although it did start after the UK MER had been published.[69] Secondly, the proactive analysis function had not been sufficiently carried out by SOCA. Thirdly and most importantly, there were concerns about the consent system, especially after a SAR was submitted to SOCA, now the NCA, since:

> The reporting entity has the duty to monitor all the transactions carried on by the same customer, being ready to seek the consent again in all cases that could seem very similar to those for which consent has already been granted.[70]

Simpson and Smith[71] therefore note that:

> [There] may be additional instructions for a transaction from a particular customer, after a consent request to SOCA has been made. In such circumstances, further SARs or consent requests should be made to SOCA.[72]

SARs annual reports started to be published in 2007 by the SARs Regime Committee. The committee evaluates the SARs regime and produces annual reports to the Home Office and Treasury Ministers. The SARs annual report generally explains how the effectiveness of the regime can be increased by explaining how the UK FIU can use feedback methods in respect of the reporting entities, carrying out case studies about submitted SARs and recently also giving examples about how to exploit ARENA practically.[73] ARENA is a system which has been established by the NCE. LEAs can use this system in relation to SARs search and studies. SARs annual reports highlight practical negative aspects, for example, the report for 2010 indicated that a high number of unnecessary SARs had been submitted by some sectors, especially

---

[68] Ibid 88.

[69] Ibid.

[70] Ibid 79.

[71] Mark Simpson and Nicole Smith, 'UK Part III: Practical implementation of Regulations and Rules' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 95.

[72] Ibid 134.

[73] 'Suspicious Activity Reports Regime, Annual Report 2011', as produced by the SOCA, 37.

those containing consent requests, although these SARs did not in fact fall under the POCA 2002 provisions. The report noted that this practice may have been because the relevant reporting entities submitted SARs without applying appropriate CDD procedures or submitted consent requests as standard SARs.[74]

In addition, Annexes C and D of the SARs annual reports[75] contain detailed statistics about submitted SARs on ML. Nevertheless, the report does not include statistics about the number of SARs, out of all those received, which the UK FIU has disseminated to LEAs and other government bodies. The report also does not indicate the number of SARs out of all those received, which the UK FIU, having analysed them, decided to delete due to there being no suspected/known ML. In addition, the report does not state how many SARs have resulted in a conviction.

Conclusion

The IMF's *Handbook*[76] provides a good account of the four models of an FIU and the advantages and disadvantages of each. It further elaborates both the core and non-core functions of an FIU at both national and international levels. Schott[77] suggests a number of considerations that have to be taken into account by national authorities when determining which model to choose when considering an FIU. In addition, D'Souza[78] provides a brief comparison between the administrative model and the law enforcement model and discusses the key factors of successful FIUs and the challenges facing them.

In relation to the UAE FIU, Hamdan[79] observes a huge discrepancy between the numbers of STRs received by the UAE FIU and the number then transmitted to the Public Prosecutions Office. Nevertheless,

[74] 'Suspicious Activity Reports Regime, Annual Report 2010', as produced by the SOCA, 14.

[75] Annexes C and D of the Suspicious Activity Reports Regime, Annual Reports 2010, 2011, 2012 and 2013.

[76] International Monetary Fund Handbook (n 79).

[77] Paul Allan Schott (n 80).

[78] Jayesh D'Souza (n 82).

[79] Sara Hamdan (n 100).

the functions of the UAE FIU are not further detailed in any articles or books, but a number of text books provide a general explanation about the provisions of the AML laws and regulations. None of these sources mentions that the FLMLC 2002 and the CBR 24/2000 are ambiguous in relation to the basis of STRs. The sources also do not analyse the core and non-core functions of the UAE FIU. In addition, the UAE FIU annual reports do not provide accurate statistics about STRs on ML since current statistics only show the annual number of STRs on ML, TF and other financial crimes, such as fraud. Hence, despite crucial information and statistics being contained in these annual reports, statistics about STRs on ML are still vague.

In relation to the UK FIU, D'Souza[80] analyses the UK FIU model within SOCA, now the NCA, and provides a study of its organisational framework, functions and powers in relation to the SARs regime. Furthermore, Booth and others[81] elaborate the three types of disclosure under the SARs regime contained in POCA 2002. In addition, Harrisons and Ryder[82] argue that the CCA 2013 does not expressly mention that the NCA now fulfils the role of the UK FIU. However, the 2013 Act explicitly mentions that the NCA has the function of criminal intelligence in gathering, storing, processing, analysing and disseminating information, which is relevant to combating organised and serious crime, and this necessarily means that the NCA acts as the UK's FIU. More importantly, though the UK SARs annual reports contain detailed statistics about submitted SARs on ML, they do not include statistics about the number of SARs, out of all SARS received, which the UK FIU has disseminated to LEAs and other government bodies. The annual reports also do not indicate the number of SARs out of all SARS received, which the UK FIU having analysed them, decided to delete due to there being no suspected/known ML. Moreover, the reports do not state how many SARs have resulted in a conviction.

No sufficient sources available in relation to the STRs system and UAE FIU. This means that no sources available regarding: 1) statistics on sub-

[80] Jayesh D'Souza (n 82).

[81] Robin Booth and others (n 120).

[82] (N 114).

mitted STRs by the reporting entities annually, 2) the core and non-core functions of the UAE FIU in the STRs system and more importantly 3) the basis of submitting STRs to the UAE FIU. This is in contrast to the UK's SAR's regime, where a great number of sources are available, including annual reports and case law.

There is no one particular model that is optimal for every time and place. Success of a particular FIU model in a country does not necessarily mean that such a model will achieve the same success in another country. This is due to the fact that the choice of an FIU model depends on several factors, notably the particular conditions of individual countries, such as the political, legal and judicial system. Furthermore, a particular model could be suitable for a country for a specific period of time, but may no longer be suitable when circumstances change.

In addition to the core functions, the FIU also has to fulfil a number of non-core functions—for instance it has to provide feedback to the reporting entities; some of these functions are no less important than the core functions.

3

Banking Confidentiality Versus Disclosure

Introduction

This chapter deals with the well-established doctrine of banking confidentiality, which applies to all banking transactions across the world. The banking sector is the most attractive area for ML activities/transactions and will therefore be analysed in the following chapters. The sector, out of all reporting entities, also submits the majority of SARs/STRs on ML to the national FIU annually, as analysed in Chaps. 6 and 9. The submitting of SARs/STRs can conflict with the principle of banking confidentiality since such reports contain information about a customer's bank account and financial affairs, which might lead to criminal or civil liability being imposed. The main objective of this chapter is to justify on which legal grounds SARs/STRs can be submitted in a way which does not prejudice the principle of banking confidentiality, ensuring that the principle is respected and safeguarded without it being exploited for ML activities.

The first section deals with the principle of banking confidentiality and its basis and scope. I evaluate the principle and discuss why it is a prerequisite for personal, commercial and financial transactions. I also analyse the scope of information, which the principle covers, as well as

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_3

its time scale. In the second section I assess critically the UK exceptions and how these have been interpreted by the judiciary and discusses possible overlaps. I further establish under which exception(s) the duty to submit SARs falls. In the last section I scrutinise how the UAE deals with the principle, namely by evaluating it and its exceptions under the applicable UAE statutory provisions; however, there are insufficient cases which shed light on how these statutory provisions should be interpreted. The section also sets out when a submitted STR falls within the scope of the exceptions.

The Confidential Nature of the Contract Between a Banker and a Customer

The General Concept of the Banker–Customer Relationship

Banking confidentiality represents the soul of the banker–customer relationship.[1] It contains aspects of agency, which impact on the contractual relationship. For example, the obligation of secrecy and loyalty is imposed upon an agent towards his or her principal. This is the case even if the agent is an estate agent, a solicitor, a company director or even a doctor. The scope of the obligation differs from one type of agent to another. For instance, a director might be required (by a court) to testify or divulge information about his or her company despite this being contrary to the company's interests. In contrast, the obligation of secrecy is more practical, notably in relation to the client and solicitor relationship, where the latter is prevented (in a court) from testifying about his dealings with his client.[2]

[1] Zubair Khan Muhammad, 'An Analysis of Duty of Confidentiality Owed by Banker to its Customers' [20th April, 2011] 1, available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1815825 (accessed on 27th February 2015).

[2] E. P. Ellinger, Eva Lomnicka and C.V.M Hare, *Ellinger's Modern Banking Law* (Fifth Edition, Oxford University Press 2011), 171.

Justifying Confidentiality

It has been said[3] that the customer's credit usually relies on the strong observance of confidence, and this is the justification for imposing the duty of secrecy on the banker–customer relationship, hence public policy constituted the reason for imposing the duty of confidentiality. However, such rationalisation can be easily refuted since credit does not rely on hiding the situation of a person's bank account. This is further supported by the fact that, already in ancient times, traders would be provided with bank references without needing the express consent of the customer, enabling traders to obtain information about a person's credit. Hiding fundamental information about the financial affairs of creditors may even be equated with a seller defrauding customers through concealing defects in products, and thus may not constitute a real justification for imposing the duty of secrecy on the banker–customer contract.[4]

Indeed, there are two reasons which led to the imposition of the agent's commitment of secrecy. The first reason is historical: the duty arose to protect the principal guardian from groundless attempts by intruders to enquire about his affairs.[5] He had to safeguard his principal's confidence and protect his interests. The second argument is economic in nature and can be illustrated by the relationship of solicitor and client. The client would not feel comfortable discussing his financial affairs if his solicitor could be forced to disclose his client's information.[6]

So in fact and at law, a person who undertakes work assumes a confidential duty to those engaging him or her, which includes being able to rely on their judgment. The commitment of confidentiality does not arise only between solicitor and client. It extends to other forms of agency relationships,[7] such as accountant and customer, banker and customer, and the doctor and patient relationship.

---

[3] R Ponser, mentioned in Ross Cranston, *Principles of Banking Law* (Second Edition, Oxford University Press 2002), 169.

[4] Ibid.

[5] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 172.

[6] Ibid.

[7] Ibid 171 & 172.

Justifying Banking Confidentiality

Similarly, in the context of the banker–customer relationship, there are two arguments which support enforcing a duty of secrecy on banks. The first argument may be considered the main one for the obligation of banks' confidentiality; it also perhaps overlaps with the second argument. The idea behind the first argument is rooted in the belief of protecting an individual's "personal autonomy."[8] In reality, the main reason is to ensure that both private and commercial customer's finances are kept secret. A bank which did not ensure that information pertaining to its customer's finances was kept secret would very soon acquire a bad reputation and would thus lose the public's trust. The second argument relates to the sensitive nature of business information. It is easy to imagine circumstances where a bank engaging in divulging confidential information would place the customer at risk from competitors. This is particularly so as information about a business has an intrinsic market value, which of course increases where confidential information is concerned.[9]

The duty of confidentiality is justified and essential from the perspective of developing countries and developed countries alike. In developing countries, the duty safeguards customers and their wealth from criminals. If a bank divulged a customer's financial affairs, the customer could become a victim of crimes, such as kidnapping for compensation or robbery.[10] Similarly in developed countries, the duty of banking confidentiality is essential for two reasons. Firstly, it ensures that customers can get banking services from any bank without any difficulties. For instance, if a bank divulged that a customer had difficulties paying debts in the past, the customer could be rejected when applying to open a bank account at another bank. Secondly, the duty safeguards a customer's account, particularly "online banking"[11] facilities provided by

[8] Ross Cranston (n 146) 169.

[9] Ibid.

[10] Zubair Khan Muhammad (n 144) 3.

[11] Online banking means electronic means, provided by a bank, such as internet, mobile phones and Automated Teller Machines (ATM). A customer can utilise such means to transfer money between bank accounts, to access his bank account(s) and/or to pay his bills. See, Peyman Akbari,

his or her bank,[12] such as his login details and online purchases or transfers. If the bank divulged the customer's financial affairs or his account details, the account could be "hacked electronically" and the "hacker" could exploit the online banking service by withdrawing funds from his account. Hence, online banking is particularly associated with security and confidentiality,[13] so that the customer is the only person who is able to log in to his or her bank account by providing, for example, a secure username and password. Therefore, in the internet age, the issue of secrecy has been further heightened, especially since bankers hold a considerable amount of personal information about a customer on their databases.[14]

Data Protection

In this context, it is important to consider the Data Protection Act 1998 (DPA 1998).[15] The Act protects the processing of information about individuals, including manual and computer records if held in "relevant filing systems."[16] For the DPA 1998 to apply, it has to be shown that the data is personal data.[17] This means that to come within the remit of the DPA 1998 individuals have to be identifiable and have also to be alive.

Reza Rostami and Akbar Veismoradi, 'Study of Factors Influencing Customer's use of Electronic Banking Services by Using Pikkarainens Model (Case Study: Refah Bank of Kermanshah, Iran)' (September 2012) Vol., 3 (5) International Research Journal of Applied and Basic Sciences 950. Available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145494 (accessed on 3rd March 2015).

[12] Zubair Khan Muhammad (n 144) 3.

[13] Hemant Kassean, Mridula Gungaphul and Dhiren Murughesan, 'Consumer Buyer Behaviour: The Role of Internet Banking in Mauritius' [2012] European Business Research Conference Proceedings 1. Available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2131206 (accessed on 3rd May 2015).

[14] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 173 & 174.

[15] The DPA 1998 repealed and replaced the DPA 1984.

[16] The term "relevant filing systems" is defined in section 1 of the Act as "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible."

[17] The term "personal data" means "data which relate to a living individual who can be identified (a) from those data, or

In *R v Rooney*[18] Bean J opined that "the information itself does not have to include the identity of the individual."[19] In the *Durant v Financial Services Authority* (*FSA*) case,[20] the Court of Appeal deliberated on two issues, namely (1) what makes "data" "personal" within the meaning of "personal data"? And (2) what is meant by a "relevant filing system"?[21] It was explained that data will relate to an individual if it "is information that affects [a person's] privacy, whether in his personal or family life, business or professional capacity."[22] The Court of Appeal explained in relation to the second issue that:

> Parliament intended to apply the Act to manual records only if they are of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system. That requires a filing system so referenced or indexed that it enables the data controller's employee responsible to identify at the outset of his search with reasonable certainty and speed the file or files in which the specific data relating to the person requesting the information is located … without having to make a manual search of them.[23]

Hence, the DPA 1998 only applies to personal information, which is stored in a relevant filing system. This means that a bank has to comply with the Act since it holds personal information/data about customers in structured files[24] and this information/data affects a customer's privacy, namely his or her business or professional capacity.[25]

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual" s.1 (1) of the DPA 1998.

[18] [2006] EWCA Crim 1841.

[19] Ibid para 13. See also Francis Aldhouse, 'DPA section 55: securing convictions' (February 2007) 4 (2) The Newsletter for Data Protection Professionals 10, available online at: http://www.e-comlaw.com/data-protection-law-and-policy/article_template.asp?ID=351&Search=Yes&txtsearch=going (last accessed on 20th August 2015).

[20] [2003] EWCA Civ 1746.

[21] 'The Durant Case and its impact on the interpretation of the Data Protection Act 1998', Information Commissioner's Office 27/02/06; available online at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf (accessed on 25th August 2015).

[22] [2003] EWCA Civ 1746 (n 163) para 28.

[23] Ibid para 48.

[24] (N 159).

[25] (N 165).

Durant[26] was unsuccessful since the FSA did not have his files in a structured or referenced system and the information was not easily accessible. A bank which fails to comply with the DPA 1998 may be ordered to pay financial compensation to the individual who has been damaged or distressed by virtue of s.13 of the DPA 1998, though the bank can argue as defence that it has taken all such care in the circumstances as was reasonably required to comply with the requirement concerned. A bank's customer can also evoke his or her right to have the Information Commissioner's Office (ICO) carry out a so-called "compliance assessment"[27] on the legality of the bank's processing and order the bank to comply by issuing an enforcement notice. The ICO can also serve an information notice[28] on the bank. If the bank fails to comply with either of these notices, it will have committed a criminal offence. However, only a serious breach and one which is likely to cause substantial damage or distress will lead to the ICO imposing a fine. Moreover, the ICO has the power to carry out an audit and may even apply for "a warrant to enter and search premises and to seize evidence."[29]

The Basis of the Duty of Confidentiality

The Duty of Secrecy Is Rooted in both the Criminal Law and Common Law

The Criminal Law

There are some jurisdictions which have placed the banking duty of secrecy on a constitutional or statutory basis. UAE is an example of such a case and will be discussed in the third section below. Switzerland is

[26] (N 163).

[27] S.42 of the DPA 1998, for further information, see http://66.102.9.132/search?q=cache:QmVMbxrTq-kJ:www.ico.gov.uk/for_organisations/data_protection_guide/the_role_of_the_information_commissioners_office.aspx+right+to+request+an+assessment+by+the+ICo&cd=1&hl=en&ct=clnk&gl=uk (last accessed on 19th August 2010).

[28] S.43 of the DPA 1998.

[29] 'The role of the Information Commissioner's Office', available online at: http://66.102.9.132/search?q=cache:QmVMbxrTq-kJ:www.ico.gov.uk/for_organisations/data_protection_guide/the_role_of_the_information_commissioners_office.aspx+right+to+request+an+assessment+by+the+ICo&cd=1&hl=en&ct=clnk&gl=uk (last accessed on 22nd August 2010).

another example of a country which has based the duty of confidentiality on the criminal law. The breach of Article 47 of the Swiss Federal Act on Banks and Savings Banks 2009[30] could thus lead to imprisonment or a fine. Jurisdictions which have adopted this type of legislation argue that they distinguish between activities where individuals/businesses seek to escape from capital gains tax, exchange-control or financial laws—which are considered legitimate in those jurisdictions—and illegal activities. Such jurisdictions deny that countries with strong bank confidentiality rules also attract drug traffickers, money launderers and other criminals, who exploit banking confidentiality to avoid the creation of an "audit trail" which investigators can track.[31]

The Common Law

In contrast, a number of jurisdictions established the duty of confidentiality on common law, and English law is an example of such an approach. This means that the bank's duty of secrecy is implied in the contract between the bank and the customer.[32] However, the contract is not always the issue. For example, a contract does not confer protection in a situation where a third party has obtained confidential information and has divulged this, whether advertently or inadvertently or with consent. Instead, equity protects the duty of confidentiality independently of the contract. It also offers aid since the courts are entitled to grant an

[30] Article 47 (1–3) of the Swiss Federal Act on Banks and Savings Banks 2009 (known as the Banking Law of 1934) provides that:

1: Imprisonment of up to three years or fine will be awarded to persons who deliberately:

B: Disclose a secret that is entrusted to him in his capacity as body, employee, appointee, or liquidator of a bank, as body or employee of an audit company or that he has observed in this capacity;

B: Attempts to induce such an infraction of the professional secrecy.

2: Persons acting with negligence will be penalized with a fine of up to 250,000 francs.

3: In case of a repeat within five years of the prior conviction, the fine will amount to 45 day rates at a minimum.

[31] Ross Cranston (n 146) 170 & 171.

[32] Fayyad Alqudah, 'Banks' duty of confidentiality in the wake of computerised banking' (1995) 10 (2) Journal of International Banking Law 50, 51.

injunction, thus indirectly buttressing any duty of contract. In addition to contract law and the use of equity, tort law offers another remedy. For instance, a third party might tortiously induce a confidant bank to disclose information to it in breach of contract.[33]

Scope and Duration of the Duty of Secrecy

The Scope of Secrecy

When examining a bank's duty of secrecy, it is important to make recourse to the seminal case of *Tournier v National Provincial and Union Bank of England*.[34] This case firmly established the principle of banking confidentiality.[35] The Court clarified that the principle constitutes the general rule, which governs the banker–customer relationship. However, a departure can be made from this principle in four situations, which are analysed in the next section. Indeed, the decision of the Court is rooted in self-evident logic. If a banker divulged to any person financial information about a customer, this will harm the customer's business or his or her reputation. This logic is a valid reason to uphold the principle in any country.

In *Tournier*, the claimant had his account with the defendant bank which made payment demands. It was agreed that the claimant would make payments in order to reduce his overdraft, but he failed to keep up the payments after the third instalment. A third party wrote a cheque to the claimant and he indorsed it to another person. Upon making enquiries, the bank became aware that the endorsee of the cheque was a bookmaker. The branch manager then telephoned the claimant's employers apparently to determine the private address of the claimant, but the branch manager divulged during the course of the conversation that the

[33] Ross Cranston (n 146) 171.

[34] [1924] 1 KB 461.

[35] Prior to 1924, there were only three reported cases which dealt with banking confidentiality, namely (1) *Tassell v Cooper* [1850] 9 CB 509, (2) *Foster v Bank of London* [1862] 3 F. & F. 214 and (3) *Hardy v Veasey* (1867–68) L.R. 3 Ex. 107. For further details about the development of the principle of banking confidentiality, see Robert Stokes, 'The Genesis of Banking Confidentiality' (2011) 32 (3) The Journal of Legal History 279, 279–294.

claimant's account was overdrawn and that he had dealings with bookmakers. As a direct result of the conversation, the claimant's employers decided not to renew his contract of employment.

The Court of Appeal found that the bank breached its duty of confidentiality. Atkin LJ noted that:

> The obligation extends to information obtained from other sources than the customer's actual account, if the occasion upon which the information was obtained arose out of the banking relations of the bank and its customers.[36]

Thus, a bank's duty is to treat information as secret,[37] and this obligation is not only limited to information that the bank knew from the condition of the account of the customer, but covers all information derived from the banking relationship.[38] Indeed, the duty includes any information gathered by the bank, directly and indirectly, including assessments and/or general impression.[39] It covers both financial and personal details about a customer, for example his name, his address, who is paying or receiving payments, personal information about his employer, information about the customer's bank balance or his transactions at various times.[40] The duty is imposed regardless of whether customers are depositors or borrowers; hence, the duty is independent of the customer's credit status.[41]

The Duration of Secrecy

Banking confidentiality remains in existence even upon the closure of the customer's account or it ceasing to be active.[42] The obligation of

[36] (N 177) 485 para 23.

[37] Alastair Hudson, *The Law of Finance* (Second Edition, Sweet & Maxwell 2013), 899.

[38] Charles Proctor, *The Law and Practice of International Banking* (Oxford University Press 2010), 678.

[39] Ross Cranston (n 146) 172.

[40] Fayyad Alqudah (n 175) 50.

[41] Ross Cranston (n 146) 172.

[42] Charles Proctor (n 181) 679.

confidentiality also remains in existence after the customer's death.[43] On the other hand, the duty of confidentiality does not extend to information gained prior to the beginning or gained after the termination of the banker–customer relationship.[44]

Nonetheless, a bank still has to be extremely careful in these situations for the following three reasons:

1. A bank may have given an express undertaking to the customer to keep information confidential.[45]
2. Information obtained prior to the commencing of the banker–customer relationship could still be classified as falling within the scope of the duty of confidentiality, if the same information is conveyed/gathered at the start of the relationship.[46]
3. A bank may receive information under conditions which fall within the scope of the general law of confidence.[47]

It is useful to note that, in the *Tournier* case,[48] the duty of confidentiality was held to exist impliedly[49] since, at that time, the duty of confidentiality was an unclear notion.[50]

The above circumstances raise the following questions. Firstly, is it true that if there is no bank account and no express undertaking relating to secrecy, is there then no banker–customer relationship? Secondly, nowadays, there are "'multifunctional banks" which offer a considerable number of banking and financial services, and these services have exceeded the routine operations of deposit, withdrawal and lending. Thus, could a duty of confidentiality be imposed on banks in these circumstances? To answer these questions, recourse has to be made to the general principles

[43] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 178.
[44] Ibid 177.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] (N 177).
[49] Ibid 473 para 11 and 480 para 18.
[50] Zubair Khan Muhammad (n 144) 3.

governing breach of confidence. Lord Goff illustrated these in the case of *Attorney-General v Guardian Newspapers Ltd*.[51] He stated that:

> A duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.[52]

Limiting Principles

The duty covers all information obtained by a banker due to his position;[53] nevertheless there are three limiting principles to this wide general principle. The first is that the principle of confidentiality only applies to information to the degree that it is secret. The second is that the duty of confidence does not apply to trivial and useless information. The third is that, despite it normally being in the public interest that law protects and preserves confidential information and that this forms the basis for the law protecting secrets, there may be nonetheless circumstances where other public interest considerations outweigh secrecy and it becomes essential to divulge information.[54]

These limiting principles can also be applied outside the banking field with regard to safeguarding confidential information and can relate to circumstances where information is disclosed to a bank by a customer, or a non-customer when showing a business plan when requested to secure bank funding. It is crucial that these principles are taken account of.[55]

It is important to note that the duty of confidentiality is a legal and possibly also a moral duty which is qualified.[56] In the *Tournier* case,[57]

---

[51] [1990] 1 AC 109.

[52] Ibid 281.

[53] Zubair Khan Muhammad (n 144) 2.

[54] (N 194) 282.

[55] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 179.

[56] Wadsley Joan, 'Bank's confidentiality: a much reduced duty' (1990) 106 (Apr) Law Quarterly Review 204, 205.

[57] (N 177).

the Court of Appeal held that there are four exceptions with regard to a bank's duty of secrecy. The four exceptions were set out by Bankes LJ as:[58]

> On principle … the qualifications can be classified under four heads:
> (a) where disclosure is under compulsion by law;
> (b) where there is a duty to the public to disclose;
> (c) where the interests of the bank require disclosure;
> (d) where the disclosure is made by the express or implied consent of the customer.[59]

Exceptions to the Bank's Duty of Confidentiality

The *Tournier* case[60] clearly illustrates that there are four exceptions to the bank's duty of confidence. Indeed, qualifications to the duty of secrecy are almost accepted in all jurisdictions around the world.[61] Accordingly, the duty of confidentiality does not arise if any of these qualifications apply.[62] Hence, it becomes important to scrutinise each of the exceptions in detail.

Obligation by Law

Disclosure by Virtue of a Court Order

A bank must disclose confidential information about the relevant customer when required by a court order or statutory provision.[63] For exam-

[58] Ibid 473 para 1.

[59] These exceptions were confirmed in *Christofi v Barclays Bank Plc* [2000] 1 WLR 937. In addition, *Tournier* was applied in *Christofi v Barclays Bank Plc* [1998] 1 W.L.R. 1245, but distinguished in *Brandeaux Advisers (UK) Ltd v Chadwick* [2010] EWHC 3241 (QB).

[60] (N 177).

[61] Ross Cranston (n 146) 174.

[62] Ibid 174 & 175.

[63] Arun Srivastava, 'UK Part II: UK law and practice' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition,

ple, during legal proceedings, the court can require a bank to divulge information about its customer's account[64] (*Bucknell v Bucknell*[65] and *Eckman v Midland Bank Ltd*).[66] In such a case, the public interest and the administration of justice require that a bank discloses information about its customer's account. Judges sometimes require full disclosure for the sake of establishing the truth and in order to reach a decision. The Bankers' Books Evidence Act 1879 contains the procedure, which has to be followed, to obtain evidence about a customer's bank account and which has been broadened by Schedule 6, Part 1 of the Banking Act 1979.[67]

If the court summons a bank, then it must respond and provide the requested information about its customer's account. Indeed, a bank cannot refuse a court's order and claim privilege. This is simply because if a bank ignores or refuses a court order and does not respond, the bank will be held to be in contempt of court.[68]

In the Chancery Division case *Harding v Williams*[69] it was held that once evidence has been produced, it can be used against any party. S.7 of the Bankers' Books Evidence Act 1879 entitles a judge to make an order for inspection of the banker's book, which can also be made *ex parte*, for example, without the other party being present, though the bank has to be informed prior to the application being made, so that it has a chance to oppose the order. The courts are very thorough when it comes to granting an order (*South Staffordshire Tramways Co v Ebbsmith*)[70] and exercise this right prudently and carefully.[71] Hence, having a mere suspicion is

---

Bloomsbury Professional 2010), 27 at 50.

[64] Alastair Hudson (n 180) 901.

[65] [1969] 1 WLR 1204.

[66] [1973] QB 519.

[67] Pursuant to s.3 of the Bankers' Books Evidence Act 1879, a bank has to provide a copy of the relevant entry and under s.4 it has to be shown that the entry is a normal bank entry and this can be done by way of an affidavit from a bank officer. The affidavit will confirm that the original and the copy match since this is required under s.5 of the Act. S.6 of the Act provides that a bank does not have to produce evidence or its book, except where a judge has ordered this for a special cause.

[68] Ross Cranston (n 146) 176.

[69] [1880] 14D 197.

[70] [1895] 2 QB 669.

[71] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 181.

insufficient to be granted an order, though in *Williams v Summerfield*[72] an order for inspection was permitted.

In addition, there is no requirement that a bank obtains a customer's consent when being required to do so by court, as made clear in *Bankers Trust Co v Shapira*.[73] Hence, mandatory disclosure substitutes the customer's consent, though Lord Denning also explicated that it was "a strong thing to order a bank to disclose the state of its customer's account and the documents and correspondence relating to it."[74] Hence, an order to inspect without serving the customer does not happen frequently. However such an order is made, it could only endure for a short period of time.[75] Moreover, banks do not have to inform their customer that a disclosure has been made since notification could possibly impede the investigation. However, in *R v Marlborough St Metropolitan Stipedendiary Magistrate*, *ex parte Simpson*,[76] where a man had been charged for using the earnings of a prostitute and an *ex parte* order was obtained without notice, the Court of Appeal explicated that notice ought to have been given and also that an inspection order should not last indefinitely. However, if the bank informs the customer about the disclosure, it may commit the so-called tipping off offence.[77] This is particularly necessary since banking secrecy cannot be exploited by individuals/entities engaged in ML, terrorism, insider dealing, company fraud, drug trafficking, human trafficking, tax evasion and banking supervision abuse. An order can also be made against a person close to the person against whom proceedings are being brought, as in *South Staffordshire Tramways Co v Ebbsmith*[78] and *DB Deniz Nakliyati TAS v Yugopetrol*.[79]

---

[72] [1972] 2 QB 512; cf. *Sommers v Sturdy* [1957] 10 DLR (2d) 269.

[73] [1980]1 WLR 1274.

[74] Ibid 1282 para 30.

[75] *Owen v Sambrook* [1981] Crim LR 329; *R v Nottingham Justices*, *ex parte Lynn* [1984] 79 Crim App Rep 234.

[76] [1980] Crim LR 305.

[77] This particular offence will be analysed in Chap. 8.

[78] (N 213).

[79] [1992]1 WLR 437.

S.9 (2) of the Bankers' Books Evidence Act 1879 defines what documents are covered when an order is granted. In the Divisional Court case *Barker v Wilson*,[80] it was held that the term "documents" also included any records generated through modern technologies.[81]

Disclosure by Virtue of a Statutory Provision

In addition, a bank may also be required legally to disclose information about the relevant customer to the competent authorities. Such a disclosure also does not breach the principle of banking confidentiality, so long as the conditions of the relevant act[82] are met. The clearest and most relevant instance for a bank to disclose confidential information is contained in POCA 2002, which obliges banks to report SARs to the NCA if it knows/suspects or has reasonable grounds for knowledge/suspicion that the transaction is involved in ML. Otherwise, a bank may commit a criminal offence.[83]

Indeed, the submission of SARs/STRs on ML by banks constitutes the clearest example of the exception required by law to banking confidentiality; and this legal duty is not just imposed by the UK, but by almost all countries in the world.[84] This is simply because the SAR/STR represents the most effective weapon in counteracting the global phenomenon of ML.[85]

---

[80] [1980]1 WLR 884.

[81] In the case of *Barker v Wilson*, the Court considered the meaning of the phrases "bankers' books" and "an entry in a banker's book." Bridge LJ stated that "it seems to me that clearly both phrases are apt to include any form of permanent record kept by the bank of transactions relating to the bank's business, made by any of the methods which modern technology makes available, including, in particular, microfilm." Ibid 887 para 21.

[82] Such as s.337 (1) and s.338 (4) of POCA 2002, which will be critically analysed in Chap. 8.

[83] S.330, s.331 and s.332 of POCA 2002, see Chap. 8.

[84] Such as in the UAE, as will be critically assessed in Chap. 5.

[85] Joy Tan, 'Can we still bank on secrecy?' (2011) 26 (9) Journal of International Banking and Finance Law 564, 564, See pp 136-138 in Chap. 5.

There are other tools which can prevent/detect ML or at least mitigate the consequences of it. For instance, the proceeds of crime can be confiscated and assets can be recovered, information can be exchanged between countries and a cash declaration system can be used. For detailed information about the confiscation of crime proceeds and assets recovery, see Nicholas Ryder, *Financial Crime in the 21st Century*: *Law and Policy* (Edward Elgar Publishing Limited 2011), 178–213. See also Jonathan Fisher, 'UK Part IV: Confiscating the Proceeds of Crime' in Mark Simpson, Nicole Smith

Public Interest Disclosure

Public interest disclosure, established in *Weld Blundell v Stephens*[86] and confirmed in the *Tournier* case,[87] constitutes another exception to the banker's duty of confidentiality. What may be deemed to be in the public interest is markedly different from what the public might be interested in. Previously, it was possible to divulge information about any inequity, the exception being based upon the unfairness rule; whereas nowadays, the exception extends to misdeeds, such as crime and fraud. This is irrespective of the act having actually been committed or only being contemplated.[88] Presently, the public interest exception depends on various statutory provisions, which require banks to divulge confidential information to the competent authorities.[89] Accordingly, certain situations may constitute a potential risk to the country or are contrary to the public interest and may thus override the banker's duty of secrecy.[90] Indeed the public interest is more important than the interest of an individual.[91] For example, during the war years,[92] a bank owed a duty to the public to divulge confidential information about a customer who was dealing with the enemy.[93] Furthermore, a bank has a duty to divulge information to the authorities in case a customer is a terrorist or money launderer, as

---

and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 145 at 186.

The cash declaration system will be illustrated from the perspective of the FATF in (n. 498) of Chap. 4. For the UAE system, see (n. 629) of Chap. 5; and for the UK system, see (n. 1001) of Chap. 8.

[86] [1920] AC 956, 965.

[87] (N 177).

[88] Paul Latimer, 'Bank secrecy in Australia: terrorism legislation as the new exception to the Tournier rule' (2004) 8 (1) Journal of Money Laundering Control 56, 58.

[89] Ross Cranston (n 146) 178.

[90] Charles Proctor (n 181) 696.

[91] Zubair Khan Muhammad (n 144) 6.

[92] Paul Latimer (n 231) 58.

[93] Mourant, 'The duty of confidentiality: The rule and four exceptions', June 2007, available online at: www.mourant.com (last accessed on 16th August 2010).

this is considered to be in the public interest[94] and necessary to protect national security and the financial system and is required by law.[95] The disclosure may be made as a result of an official inquiry by the police or other regulatory authority, for example an inquiry into banking regulations by the banking supervisor or in relation to another jurisdiction in case of a multinational bank.

The Overlap with the First Exception

The public interest exception may overlap with the previously mentioned exception, namely the obligation by law. Legislation may require banks to disclose confidential information in certain circumstances[96] and this certainly could mean that the public interest exception is impractical. In common law, as in the UK, the divulging of confidential information is often allowed if this is considered to be in the public interest. At the same time, banks are obliged to adhere to the duty of secrecy and to keep information confidential, but have to divulge information if this is necessary in the public interest or required by law. Otherwise, banking integrity and financial markets would be at risk. Money launderers, drug traffickers, human traffickers and other serious offenders would be able to launder their criminal proceeds easily and secretly. This latter is only one of the aspects impacting on the public interest and which has to be balanced against the duty of secrecy.[97]

Nevertheless, nowadays the exception of public interest disclosure is mitigated since there are a number of statutes which require bankers to divulge customer information. The statutory provisions have thus been enacted with a view to protecting the public interest of a country.

---

[94] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 189.

[95] S.21 A of the Terrorism Act 2000 is applied where there is a terrorism suspicion and s.330, s.331 and s.332 of POCA 2002 apply where there is a suspicion of ML.

[96] See Staughton J in *Libyan Arab Foreign Bank v Bankers Trust Co*, [1988] 1 Lloyd's Rep 259.

[97] Ross Cranston (n 146) 170 & 179.

Divulging Information Which Is in the Interest of the Bank

A bank may issue proceedings against a customer to, for example, repay his or her overdraft.[98] In such a case, the bank must evidence the amount of the overdraft on a summons which is a public document. As the bank, plaintiff, must divulge the amount of the overdraft with a view to reaching the right judgment by the judge.[99]

In *Sunderland v Barclays Bank Ltd*[100] the bank refused cheques drawn on it by a woman. The refusal was on the ground that her credit balance was insufficient and the bank knew that these cheques were in favour of bookmakers. The branch manager of the defendant bank told the plaintiff's husband when he interceded at her request that the majority of the cheques were drawn for gambling debts. The plaintiff initiated an action for damages for the bank's breach of its duty of confidentiality. Du Parcq LJ rejected the plaintiff's action and considered that the disclosure was in the interest of the bank since the plaintiff permitted her husband to speak with the bank; hence, she intentionally agreed to the disclosure. For that reason, the manager was entitled to "give the information which explained what the bank, rightly or wrongly, had done … the interests of the bank required disclosure."[101]

It might be contended that the bank took this action to maintain its reputation, but it is hard to understand why the bank was allowed to inform the plaintiff's husband that the cheques were drawn in favour of bookmakers.[102] A reasonable justification could have been that there was insufficient money in the account.

In conclusion, it appears that this exception is so wide and, in practice, can cause a number of unjustified disclosures. In addition, it seems that this exception should be given a narrow interpretation, which is already implied in the previous one, the duty to the public to disclose. Therefore,

---

[98] Charles Proctor (n 181) 693.

[99] Ross Cranston (n 146) 175.

[100] [1938] 5 LDAB 163.

[101] Ibid.

[102] E. P. Ellinger, Eva Lomnicka and C.V.M Hare (n 145) 192.

this third exception may be redundant. The duty to the public to disclose for justice to be administrated effectively may provide the best justification for divulging information in such a case.

Disclosure with a Customer's Permission

This constitutes the last exception to the bank's duty of secrecy. There are two ways to obtain the customer's consent: expressly or impliedly.[103] As regards express consent, when a customer gives his express consent, for marketing purposes,[104] to divulge confidential information by his bank, this will absolve the bank from responsibility for breach of duty of secrecy. Indeed, a bank ought to gain express consent from its customer in writing as a matter of prudence. A bank could for example include a clause in the customer's loan documentation, granting express consent to the bank with regard to passing on confidential information to credit reference agencies, upon default.

It is worth noting that express consent can be general or qualified. If the express consent is qualified, this means that it is given solely for a specific aim. Generally, there is no limited period for an express consent to be valid, but it may become invalid where circumstances change, and it is advisable to renew it periodically. For instance, before divulging information to the customer's auditors about any security or contingent responsibilities, and the situation of the customer's bank accounts, then the bank ought to require the customer's written consent.[105]

The second is implied consent, which had often been used to provide trade credit references, although the scope of this had been limited by the Business Banking Code,[106] which provided that a reference could only be obtained if express consent had been sought from the customer. As a result, the customer had to be given 28 days notice before a bank could make a disclosure, though if the customer disputed some of the amounts

[103] Zubair Khan Muhammad (n 144) 7.

[104] Ibid.

[105] Ross Cranston (n 146) 179 & 181.

[106] The Banking Code (March 2008), available online at: http://www.bankingcode.org.uk/pdfdocs/PERSONAL_CODE_2008.PD (accessed on 9th June 2014).

with the bank, then the bank was not allowed to make the disclosure.[107] The Business Banking Code was withdrawn on 1 November 2009 and has been replaced by the Banking Conduct of Business Sourcebook (BCOBS) and the Payment Services Regulations 2009, which were enforced by the FSA and now by the Financial Conduct Authority (FCA), as well as the Lending Code, the latter being enforced by the Lending Standards Board.[108] Under s.3, paras 36–37 of the updated Lending Code 2012 customers have to be informed in case credit checks are carried out with credit reference agencies. A record of such an action must be retained.[109] S.3 para 40 further explains that a disclosure to a credit reference agency is normally made when debt repayments have not been made on time, amounts are disputed or an unsatisfactory proposal has been made. However, s.3 para 48 also requires that a customer is given 28 days notice prior to the disclosure and is informed as to how this may affect their credit rating.

Assessing the Four Exceptions

There is no doubt that the four exceptions established in the *Tournier* case[110] are crucial, together with the clearly defined scope of the principle of banking confidentiality. Nevertheless, after nearly a century since the *Tournier* case,[111] three significant conclusions can be reached in relation to these four exceptions.

Firstly, the obligation by law represents the strongest exception to banking confidentiality. This is because the public interest disclosure falls within this exception. When a law obliges a banker to divulge informa-

---

[107] Cartwright Peter, *Consumer Protection in Financial Services* (International Banking, Finance & Economic Law 1999), Kluwer Law International, 93 & 94.

[108] Financial Conduct Authority, 'The Banking Conduct Regime', available online at: http://www.fca.org.uk/firms/being-regulated/banking/Conduct-regime (accessed on 30th October 2014); Lending Standards Board, The Lending Code, Setting standards for banks, building societies and credit card providers (March 2012, revised 1st May 2012), available online at: http://www.lendingstandardsboard.org.uk/docs/lendingcode.pdf (accessed 7th March 2014).

[109] Furthermore, banks have also to comply with the DPA 1998.

[110] (N 177).

[111] Ibid.

tion about a customer, this obligation aims to protect the public interest, for instance when national security or the integrity of the financial system of a country mandates this.

Secondly, the exception for a bank to make a disclosure is wide and redundant and should be implied in the duty of public disclosure. When a bank discloses a customer's information during litigation to advance its interest, this impliedly means that such a disclosure is made in order to ascertain the truth. This is also in the public interest. In other words, the administration of justice permits a bank to disclose information about a customer and there is no need for a separate exception in such a case.

Thirdly, a disclosure with the permission of a customer, especially with express consent, is the second strongest exception to banking confidentiality. This is because the customer contractually permits the banker to divulge confidential information without this triggering criminal or civil liability.

As a result, nowadays there appear to be two main exceptions to banking confidentiality, namely the obligation by law and with the permission of the customer. Whilst the public interest disclosure and the bank interest disclosure are exceptions, they are not separate exceptions since in reality they fall under the obligation of the law. In addition, a competent court can evaluate whether a disclosure is legal or in excess of what the exceptions permit.

The above situation of banking confidentiality and its four exceptions has been analysed in terms of the UK system, but what about the banking confidentiality in respect of the UAE system?

The Situation in the UAE

Banking confidentiality was previously governed by Circular No. 257, which was issued on 9 March 1976 by the UAE Council Cash. The Circular allows banks to disclose information about their customer in two instances: (1) where there is a court order or (2) by sending such confidential information to the Managing Director of the Board of the

Council cash.[112] After the establishment of the Central Bank in 1980 by virtue of Union Law No. 10 of 1980 Concerning the Central Bank, the Monetary System and Organisation of Banking,[113] the principle of banking confidentiality became governed by the Penal Code, namely Article 379 of Federal Law No. 3 of 1987.[114]

The Article explicitly mentions two exceptions to the principle of secrecy out of the four exceptions illustrated in the *Tournier* case,[115] namely (1) where an obligation arises by law and (2) where the customer has permitted this; however, there are no cases in the UAE which define the scope of banking confidentiality or explain its exceptions, as for example the *Tournier* case[116] does in the UK. Recently, based on Article 379 of the UAE Penal Code 1987, the Criminal Division of the Dubai Court, in the case of *Attorney General v Mashreq Bank*,[117] convicted three defendants to one year's imprisonment. They were employees of the Mashreq Bank in Dubai and disclosed bank account information about a customer (victim) to other defendants, who managed to transfer

---

[112] Circular No. 257/1976 stipulates that:

> So far as divulging information about customers' affairs is concerned, banks are free to rely on one of the two exceptions. They may rightly demand a court order before they release information or they may at their discretion pass the required details under private and confidential cover to the Managing Director of the Board who will act as an intermediary. In the latter case the Board will protect the bank from any possible legal action which might arise at a later date.

[113] Nevertheless, the law does not contain any provision which deals with the banker's duty of confidentiality.

[114] Article 379 of the UAE Penal Code 1987 provides that:

> 1: Punishment by detention for a period of not less than one year and by a fine of not less than Arab Emirates Dirham (AED) 20,000 or by either of these two penalties, shall apply to any one who is entrusted with a secret by virtue of his profession, trade, position, or art and who discloses it in cases other than those lawfully permitted, or if he uses such a secret for his own private benefit or for the benefit of another person, unless the person concerned permits the disclosure or use of such a secret.
>
> 2: A penalty of imprisonment for a period not exceeding five years shall apply to a culprit who is a public official or in charge of a public service, and has been entrusted with the secret during, because of or one the occasion of the performance of his duty or service. AED20,000 is about £3300.

[115] (N 177).

[116] Ibid.

[117] Dubai Court Judgment, Criminal Division, case No. 2548/2011.

AED128,000[118] from his account. The judgment defines a secret as "any matter, which by its nature and circumstances, the defendant has known by virtue of his profession or position."[119] The Court also corroborated that it did not matter whether the defendant disclosed the secret for his own private benefit or for the benefit of another person.[120]

As in the UK, banking confidentiality is not absolute, but qualified. Hence, banks may be required to disclose confidential information if there is a court order or this is required by law. For instance, the FLMLC 2002 obliges banks and other financial institutions to report STRs to the UAE FIU if they know that the transaction is involved in ML. Failing to do so can result in the bank committing a criminal offence,[121] an issue that will be critically analysed in Chap. 5.

As a result, the statutory provision forms an exception to the duty of banking confidentiality and requires a bank to provide information about a customer to the authorities, as this protects national security and the financial system. Moreover, the principle of banking confidentiality will not be breached if the banker reports that the customer's bank account is involved in an ML transaction since the statutory provision grants immunity for banks in such a case.[122]

Assessing Article 379 of the UAE Penal Code 1987

The scope of this Article is not confined to banking confidentiality, but covers other contractual relationships, such as that of a doctor and his or her patient. It provides clearly that the obligation by law is the strongest exception to the duty of confidentiality. Although the Article illustrates that the customer's permission is the second exception to the principle of confidentiality, it does not clarify the form of such permission, that is whether express permission is required or whether implied permission is also acceptable. The Article has also not been judicially

[118] Which is about £21,300.

[119] (N 260) and the Appeal Court in Dubai affirmed the conviction on 5 October 2012.

[120] Ibid.

[121] Article 15 of the FLMLC 2002.

[122] Article 20 of the FLMLC 2002 which will be illustrated in (n 623) of Chap. 5.

interpreted and it appears that it requires the express permission from the customer for the second exception to be evoked. Nevertheless, the text of the Article does not specifically state that the customer's consent has to be expressly provided. The court has therefore discretion to permit implied permission in circumstances when this is appropriate.

Conclusion

The duty of the bank to keep a customer's information secret is crucial for financial transactions; however, the duty is not an absolute, but qualified. In common law jurisdictions, such as the UK, a banker can disclose or may be required to disclose customer information where one of the four exceptions, as illustrated in the *Tournier* case,[123] apply, and which will not be in breach of the duty of banking confidentiality. However, the exceptions are mitigated nowadays and do not exist exactly[124] as stated in the *Tournier* case.[125] Instead, there are a number of statutes which require a banker to divulge customer information. The statutory provisions have been enacted with a view to protecting the public interest. An example is the submission of a SAR/STR on ML to a national FIU. This is an exception to the principle of banking confidentiality and falls under the umbrella of the first exception, namely the obligation by law. Hence, national laws require that the banking sector and other financial institutions submit SARs/STRs to the FIU in cases where it is known/suspected that the customer account is used for ML. At the same time, such a case also falls within the second exception and can be considered a public interest disclosure since SARs/STRs on ML are being submitted to protect national security and the integrity of the financial and banking system.

Nowadays the second exception, namely to divulge information when this is in the public interest, is mitigated, since there are a number of statutes which require bankers to divulge customer information. The statutory provisions have thus been enacted with a view to protecting

[123] (N 177).

[124] Zubair Khan Muhammad (n 144) 9.

[125] (N 177).

the public interest of the country and its financial system. In addition, it appears that the third exception, namely divulging information, which is in the interest of the bank, is so wide that, in practice, it can cause a number of unjustified disclosures. It should therefore be narrowly interpreted, particularly since this exception is already subsumed in the duty to disclose to protect the public interest. The third exception appears redundant, as the duty to disclose, for justice to be administrated effectively, may provide the best justification for banks to divulge information.

In the UAE, banking confidentiality is protected by virtue of Article 379 of the UAE Penal Code 1987 and only the following two exceptions exist: (1) disclosure required by law and (2) disclosure with the permission of the customer. Yet, disclosure required by law can also include situations where a disclosure is required to protect the public interest since statutory provisions require that STRs on ML are submitted to the UAE FIU to protect national security and the financial system of the country. Public interest disclosure is thus implied whenever disclosure is required by law. Nevertheless, the scope of banking confidentiality has not been defined in UAE cases and the exceptions have also not been explained, unlike in the UK where the seminal *Tournier* case[126] provides important clarifications.

This chapter has spelled out the legal justifications for banks to submit STRs to the national competent authority, namely the FIU, and has explained why this does not conflict with the principle of banking confidentiality. In the subsequent chapter I will analyse the international requirements with respect to STRs for banks and other reporting entities, as well as the international requirements in relation to the functions which the FIU should discharge when dealing with STRs.

[126] Ibid.

4

The Nature of the FIU from the Perspective of International Standards

Introduction

In this chapter I discuss the FIU from the perspective of international standards. The FATF is considered to be a global standard setter for counteracting ML.[1] In section "The General Features of the FATF", I examine the Forty FATF Recommendations, which set out the international standards for combating ML, and I assess whether these Recommendations are obligatory and therefore have to be implemented and adopted by national anti-money laundering laws (NAMLL) in member states. I scrutinise the international requirements which reporting entities, such as banks and other financial institutions, have to discharge in relation to AML. This includes CDD measures, record keeping and STRs requirements. These requirements are essential for reporting entities to identify an STR and to determine whether or not to send the STR to the national FIU. In addition, it will be discussed how the FATF mechanism assists in assessing whether provisions of NAMLL are compatible with the Recommendations.

[1] And now also for counteracting TF and the proliferation of weapons of mass destruction.

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_4

In section "The Function of the FIU in Counteracting the ML Process", I critically evaluate the role, which the FIU plays, in combating ML and the features of the four common models for the FIU found all over the world. This requires an analysis of the core functions and constitutive elements of the FIU, so that each function can be fully understood irrespective of the particular FIU model. I also critically analyse the recent revision of the FATF Recommendation, which deals with the functions of an FIU in counteracting ML, the unit's authorities and other relevant updated Recommendations, such as STRs requirements. The main objective of this chapter is to evaluate the international requirements which an FIU has to fulfil and to assess whether such requirements clearly illustrate the related duties and powers which an FIU thus requires. This is essential since the international standards set out a good model, which all countries should adopt.

The General Features of the FATF

General Background

Creation of the FATF

In July 1989, at the Paris summit of the heads of the economic powers (Group of Seven, G7),[2] chaired by the President of the European Commission (EC),[3] the AML system was born, both at the national and international level. The G7 set up the FATF to combat existing ML threats, particularly those associated with illicit drug trafficking. It was intended that action would be taken and best practice and standards would be promulgated.[4] In 1990, the FATF presented its first report. This report contained minimal AML principles which have become known as the "Forty FATF

[2] The seven leading industrial countries in the world are the USA, the UK, France, Germany, Canada, Italy and Japan.

[3] Eight other countries were invited to the summit as well, namely Australia, Austria, Belgium, Luxembourg, the Netherlands, Spain, Sweden and Switzerland. See William C. Gilmore, *Dirty Money – The Evaluation of International Measures to Counter Money Laundering and the Financing of Terrorism* (Fourth Edition, Council of Europe 2011), 91.

[4] Jackie Johnson, 'Little enthusiasm for enhanced CDD of the politically connected' (2008) 11 (4) Journal of Money Laundering Control 291, 297.

Recommendations." The Recommendations outlined three core ideas, namely (1) enhancing domestic legal systems through AML laws and regulations, (2) improving the tasks of the banking sector and other financial institutions when it comes to combating ML and (3) increasing international cooperation mechanisms for the purpose of AML.[5]

Revisions of the Forty Recommendations

The Forty Recommendations were amended three times. The first time was in 1996.[6] This was done in order to ensure that they kept pace with possible threats. They covered three areas: (1) the scope of the predicate offence for the purpose of ML was extended, so that not only drug crimes, but all serious crimes, were covered; (2) the importance of the SARs/STRs obligations for financial institutions was emphasised; and (3) non-financial business had to implement the requirements of SARs/STRs.[7]

In 2001, as a consequence of the terrorist attacks in the United States (US), the FATF launched its Eight Special Recommendations for combating the financing of terrorism (CFT). Since then, the FATF expanded its mission to include, besides combating ML, counteracting TF. For this purpose, it issued the Ninth Special Recommendation in 2004. Therefore, the overall FATF Recommendations came to be known as 40 + 9 Recommendations or FATF Standards, and they form a strong framework in counteracting ML and TF. After that, in 2003, the Forty Recommendations were updated again, for a second time, in order to deal with a number of aspects, such as CDD and the role of FIU.[8] The update was also done for the following reasons:

---

[5] H.E. Ping, 'The measures on combating money laundering and terrorist financing in the PRC: from the perspective of financial action task force' (2008) 11 (4) Journal of Money Laundering Control 320, 321.

[6] For the revised FATF Recommendations 1996 in detail, see William C. Gilmore (n 272) 101–105.

[7] Ali Shazeeda A., *Money Laundering Control in the Caribbean* (Kluwer Law International 2003), 62.

[8] Mark Simpson, 'International initiatives' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 193 at 222.

1. To increase the transparency of legal persons and arrangements.[9]
2. To strengthen the identification procedures in respect of clients/activities who/which represent a higher risk to ML.[10]
3. To adopt the principal measures, imposed upon regulatory and supervisory entities, in the AML structure.[11]
4. To incorporate designated non-financial business and professions (DNFBPs) in the AML composition.[12]
5. To undertake a robust criteria for predicate offences.[13]

In 2008, the FATF expanded its mandate to combat the proliferation and financing of weapons of mass destruction.[14] More recently, on 16 February 2012, the FATF revised, for the third time, all its standards (40 + 9 Recommendations) to cover weapons of mass destruction[15] and other issues, which are discussed below.

Characteristics of the FATF

Presently, 34 states[16] are members of the FATF along with two regional organisations.[17] The number of members[18] illustrates the importance

[9] Commonwealth Secretariat, *Combating Money Laundering and Terrorist Financing: A Model of Best Practice for the Financial Sector, the Professions and other Designated Businesses* (Second Edition, Commonwealth Secretariat 2006), 21.

[10] Mark Simpson (n 277) 222.

[11] Commonwealth Secretariat (n 278) 21.

[12] William C. Gilmore (n 272) 109.

[13] Commonwealth Secretariat (n 278) 21 and William C. Gilmore (n 272) 109.

[14] The FATF Forty Recommendations, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', February 2012. Available online at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed on 15th May 2015).

[15] Ibid.

[16] Which are Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Italy, Japan, the Netherlands, Luxembourg, Mexico, New Zealand, Norway, Portugal, Republic of Korea, the Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, the UK and the US.

[17] Which are the EU and the Gulf Cooperation Council (GCC).

The GCC encompasses six member countries: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE.

[18] These are the following minimum entry conditions for any country wanting to become a member of the FATF:

of the FATF organisation across jurisdictions, particularly since its members are from the key financial centres around the world.[19] The FATF has established nine regional groups, known as the FATF-Style Regional Bodies (FSRBs),[20] in order to facilitate the global implementation of the Forty FATF Recommendations.

1. It should, strategically speaking, be an important state.
2. It has to apply the FATF Recommendations for at least three years.
3. The country has to carry out annual self-evaluation exercises in addition to two mutual assessments rounds.
4. It has to pledge politically that it will prohibit ML.
5. The country concerned must make it a criminal offence to launder the proceeds of serious crimes.
6. The relevant country has to oblige the banking sector and other financial institutions, in its jurisdiction, to identify their customers and to adopt STRs.
7. It must be a vital member of the relevant FATF-Style Regional Bodies (FSRBs), where such exist, or be ready to build cooperation with the FATF or to initiate the setting up of such a regional entity.

Doug Hopton, *Money Laundering*, *A Concise Guide for All Business* (Second Edition, Gower Publishing Limited 2009), 19.

See also 'FATF membership policy', 29 February 2008, available on the FATF website at: www.fatf-gafi.org (accessed on 15th November 2014).

[19] 'FATF members and observers', available online at: http://www.fatf-gafi.org/pages/aboutus/membersandobservers (accessed on 18th May 2015).

[20] The FSRBs are:

1. Asia/Pacific Group on ML (APG), see http://www.apgml.org (accessed on 24th October 2014).
2. Caribbean Financial Action Task Force (CFATF), see http://www.cfatf-gafic.org (accessed on 24th October 2014).
3. Eurasian Group (EAG), see http://www.eurasiangroup.org (accessed on 24th October 2014).
4. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), see http://www.esaamlg.org (accessed on 24th October 2014).
5. The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), see www.coe.int/moneyval (accessed on 27th October 2014).
6. The Financial Action Task Force on ML in South America (GAFISUD), see http://www.gafisud.info (accessed on 27th October 2014).
7. Inter-Governmental Action Group against ML in West Africa (GIABA), see www.giaba.org (accessed on 27th October 2014).
8. Middle East and North Africa Financial Action Task Force (MENAFATF), see www.menafatf.org (accessed on 27th October 2014).
9. The Group of International Finance Centre Supervisors (GIFCS), formally the Offshore Group of Banking Supervisors (OGBS), see www.ogbs.net (accessed on 27th October 2014).

Moreover, the OGBS is one of the FATF observers and the rest of the FSRBs are FATF Associate Members. See 'FATF members and observers' (n 288).

These groups carry out the same function and follow the same procedures as the FATF. However, the main task of each regional group is to check whether its member states have implemented the FATF Recommendations both at the regional and domestic level. As all member states are obliged to adopt and implement the FATF standards, each regional group evaluates whether this has been done. Hence, FSRBs represent the actual mechanism for the FATF standards to be obeyed and globally implemented.[21] As a result, more than 180 states and jurisdictions are members of the FATF or FSRBs, which have endorsed, recognised or adopted and assumed political responsibility towards implementing the FATF standards on counteracting ML and TF.[22]

Defining the FATF

Having clarified the nature of the FATF,[23] it is noteworthy that there is no precise definition of it. However, one could say that it is a policy-making entity whose purpose is to make legislative and regulatory suggestions at the national and international level, all with a view to developing a strengthened legal structure for fighting ML and TF. It is thus an intergovernmental entity, not a treaty organisation, and indeed a voluntary

[21] Alain Damais, 'The Financial Action Task Force' in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth (eds), *Anti-Money Laundering*: *International Law and Practice* (John Wiley & Sons Ltd., Chichester 2007), 69 at 77.

[22] Abdullahi Y. Shehu, 'Promoting financial sector stability through an effective AML/CFT regime' (2010) 13 (2) Journal of Money Laundering Control 139, 142.

In addition to FSRBs, the FATF has built strong relations with international organisations, such as the IMF and the World Bank. The FATF Recommendations have also gained acceptance at the international level. The World Bank and the IMF have also offered training and support to facilitate enhanced implementation of the FATF standards. Moreover, in 2002, the Executive Board of these two institutions accepted the FATF principles for counteracting ML. Following this, in 2005, the United Nations (UN) Security Council adopted the Resolution S/RES/1617 (2005) on 29 July in order encourage all its member countries to adopt and apply the FATF Recommendations.

The Resolution: "strongly urges all Member States to implement the comprehensive, international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing."

[23] The FATF is an independent entity; however, it is situated within the Organisation for Economic Co-operation and Development (OECD).

Norman Mugarura, 'The institutional framework against money laundering and its underlying predicate crimes' (2011) 19 (2) Journal of Financial Regulation and Compliance 174, 182.

task force,[24] which aims at developing rules which deal with ML crimes through the introduction of principles and standards which offer useful guidance for all states.[25] The organisation has four major tasks: (1) to introduce or revise international benchmarks to counteract ML and TF; (2) to scrutinise how such benchmarks are implemented and fulfilled by countries through a number of mechanisms, including assessments; (3) to carry out studies in relation to techniques, methods and trends of ML and TF; and (4) to identify and counteract existing and new threats, including new technologies and aspects of them which can be exploited by criminals.[26]

FATF's Mandate

The FATF reviews its mission approximately every five years. Its mandate is not for an unlimited time period, and authority for its mission derives from its member governments. Its members previously agreed that the mandate would last until the end of 2012;[27,28] more recently, they agreed to renew it for the period from 20 April 2012 to 31 December 2020.[29] Moreover, in light of new threats to the global financial system, the FATF decided, pursuant to its mandate, to continue making changes to its standards if and when necessary in the future.[30]

---

[24] Norman Mugarura (n 292) 182.

[25] Nicholas Ryder, *Financial Crime in the 21st Century*: *Law and Policy* (Edward Elgar Publishing Limited 2011), 16.

See also 'FATF revised mandate 2008–2012', available on the FATF website at: www.fatf-gafi.org (accessed on 30th October 2014).

[26] 'An introduction to the FATF and its work' 2010, available on the FATF website at: www.fatf-gafi.org (accessed on 30th October 2013).

[27] Robin Booth and others, *Money Laundering Law and Regulation*: *A Practical Guide* (First Published, Oxford University Press 2011), 7.

[28] Alain Damais (n 290) 72.

See also 'Mandate for the Future of the FATF, September 2004–December 2012' and 'FATF Revised Mandate 2008–2012', also available on the FATF website.

[29] For further information about the FATF mandate, see 'Financial Action Task Force Mandate (2012–2020)' 20 April 2012, 4, available on the FATF website.

[30] The FATF Recommendations, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' 2012 (n 283) 9.

The FATF's Forty Recommendations[31]

The 2012 revision was predominantly done to incorporate four aims: (1) to deal with new and existing threats in relation to ML and TF; (2) to illustrate and improve a number of existing Recommendations, such as functions of an FIU, as will be analysed below; (3) to enhance the requirements and conditions of institutions which pose a higher ML and TF risk; and (4) to offer all countries an opportunity to adopt more specific systems in areas and fields suffering from higher risks of ML and TF.

The 2012 revision is characterised by two main features. Firstly, Recommendations dealing with TF have been integrated within the Recommendations dealing with ML, so that only Forty Recommendations deal with these two crimes. In other words, the Nine Special Recommendations have been revised and integrated within the Forty Recommendations in order to avert the need for Special Recommendations.[32] Secondly, for the first time, the FATF introduced a new Recommendation (Recommendation 7), which deals with targeted financial sanctions in order to combat the proliferation of weapons of mass destruction and its financing.[33] The FATF invites all countries to amend their national systems—in the areas of counteracting ML, TF and proliferation of weapons of mass destruction and its financing—in order to be compatible with the Recommendations.[34]

The Forty Recommendations constitute the applicable global standards for all countries. The FATF has also issued Interpretative Notes

---

[31] The FATF Recommendations, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' 2012 (n 283).

[32] Ibid.

[33] These sanctions should also be compatible with the United Nations Security Council Resolutions in this regard. The FATF Recommendation 7 states that:

> Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

[34] The FATF Recommendations, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (n 283) 9.

about a number of its Recommendations, which provide some examples and guidance in order to increase understanding and to facilitate the implementation of its Recommendations; however, the examples are not obligatory and inclusive.[35] These Interpretative Notes must be read and understood together with their relevant Recommendations.[36]

The FATF revised Recommendations comprise seven categories.[37] However, for the purpose of discussing and dealing with the general aim of this chapter, only the principles relating to combating ML will be analysed. Hence, the FATF Recommendations can generally be divided into three parts: (1) legal systems, (2) measures imposed on financial institutions[38] and DNFBPs[39] and (3) measures implemented by regulatory and LEAs.[40]

---

[35] Ibid 8.

[36] In addition to the General Glossary to all Recommendations, some Interpretative Notes contain a Glossary of specific terms, which are used in particular Recommendations.

The General Glossary to the Forty Recommendations and the Interpretative Notes to the Forty Recommendations are available online at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed on 30th November 2015).

[37] These categories are:

A. Policies and coordination in relation to counteracting ML and FT.
B. ML and confiscation.
C. TF and financing of proliferation.
D. Preventive measures.
E. Transparency and beneficial ownership of legal persons and arrangements.
F. Powers and responsibilities of competent authorities and other institutional measures.
G. International cooperation.

The FATF Recommendations, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (n 283) 4 & 5.

[38] Financial institutions are any natural or legal person who conducts a business in relation to one or more of the activities or operations listed in the General Glossary for or on behalf of a customer. The General Glossary (n 308).

[39] DNFBPs comprise dealers in precious metals and stones, casinos, real estate agents and professionals, such as lawyers and accountants. For more details about DNFBPs, see the General Glossary (n 308).

[40] In addition, there are Recommendations which deal with methods to increase international cooperation. This category of the FATF Recommendations solely deals with international cooperation amongst countries for the purpose of combating ML. The Recommendations introduce three types of international cooperation: (1) FATF Recommendation 37 deals with mutual legal assistance; (2) FATF Recommendation 39 addresses extradition requests, for example ML is an extraditable offence which has to be respected by countries; and (3) FATF Recommendation 40 deals with information sharing between competent authorities and their foreign counterparts.

Legal Systems[41]

Firstly, according to the first Recommendation, a country should take actions or implement procedures which can reduce the risks emanating from ML and TF. Therefore, prior to taking those actions or implementing procedures, it is necessary to identify, understand and evaluate the risks of ML which threaten the country.[42] A country should apply a risk-based approach (RBA). In other words, after having undertaken a risk evaluation, a country is required to adopt an RBA in order to ensure that actions, measures and procedures to prevent or detect ML are compatible with the risks which have been identified in the risk evaluation. An RBA generally means that the country requires its financial institutions and DNFBPs to implement enhanced measures and procedures in cases where there are higher risks of ML. Enhanced measures and procedures can prevent or detect risks. In contrast, entities may adopt simplified measures and procedures where there are lower risks.[43]

A country, upon having established prevalent risks, should adopt a national AML policy, which has to be regularly reviewed by a designated authority or through a different mechanism.[44] In addition, policy-makers and all competent authorities, such as the FIU, LEAs and supervisors, are required to coordinate and cooperate with each other, so as to develop a policy, at both the domestic and operational level.[45]

The TAFT Recommendations aim to criminalise the largest group of predicate offences for ML. TAFT Recommendation 3 requires countries to ensure that all serious crimes fall within the scope of the predicate offence in order to fulfil the Recommendation. Adherence to this requirement can be achieved through the numerous permissible approaches

[41] FATF Recommendations 1 to 4.

[42] FATF Recommendation 1.

[43] The Interpretative Note to Recommendation 1 provides further detail in relation to RBAs.

[44] FATF Recommendation 2.

[45] Ibid.

Moreover, criminal law and criminal procedures have also to be brought in line. The FATF Recommendation 3 emphasises that countries have to criminalise ML, particularly following the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (The Vienna Convention) and the 2000 United Nations Convention against Transnational Organised Crime (The Palermo Convention).

under national law.[46] Furthermore, independent of the chosen approach, each country must, at least, implement the scope of predicate offences in the range of offences, which are contained in the General Glossary to the Recommendations.[47]

Measures Imposed on Financial Institutions and DNFBPs[48]

This category forms the largest part of the Forty Recommendations. This demonstrates how important it is for financial institutions to adopt preventative measures in order to prevent/reduce being used/exploited as a conduit for ML processes. The Forty Recommendations also emphasise that country implementation of the Recommendations should not be obstructed through financial institutions using confidentiality laws as a pretext.[49] This category of the Recommendations encompasses three aspects: CDD measures, record keeping procedures and STRs.

---

[46] These approaches include:

1. Using an all-offences basis, or
2. Using the "threshold" approach which means a threshold is connected either to the punishment of imprisonment applicable to the predicate offence or to a group of serious offences, or
3. Adopting a list of predicate offences, or
4. Undertaking a combination of such systems.

For additional information, see the Interpretative Note to Recommendation 3.

[47] According to the General Glossary, the term "designated categories of offences" comprises 21 offences, such as participation in an organised criminal group and racketeering, fraud and illicit trafficking in narcotic drugs and psychotropic substances. There were 20 offences in the 2003 Forty Recommendations, and the revised Recommendations 2012 add the new offence of tax crimes (relating to direct or indirect taxes). For additional information, see the General Glossary (n 308).

Moreover, FATF Recommendation 4 requires countries to adopt the same procedures as set out in the 1988 and the 2000 UN Conventions in order to ensure that countries' administrative and LEAs are able to identify the instrumentalities of crime and its proceeds, prevent illegal proceeds from escaping and ultimately to confiscate the proceeds.

Ann-Cheong Pang, 'International Legal Sources III-FATF Recommendations' in William Blair and Richard Brent (eds), *Banks and Financial crime*: *the International Law of Tainted Money* (Oxford University Press 2008), 87 at 92.

[48] FATF Recommendations 9 to 23, whilst Recommendations 5 to 8 deal with TF and the financing of proliferation.

[49] FATF Recommendation 9.

CDD Measures[50]

This mechanism consists of a number of elements. Firstly, financial institutions must not keep anonymous accounts or accounts which are held in fictitious names. Secondly, financial institutions have to identify and verify their client's identity,[51] as well as adopt CDD measures,[52] in four situations: (1) where establishing business relations; (2) where carrying out occasional transactions;[53] (3) where potential ML or TF is suspected; and (4) where the veracity or adequacy about a client's "identification data,"[54] which has been previously obtained, is in doubt. Thirdly, there are simplified CDD and ECDD measures depending on a "risk sensitive basis" in terms of type of transactions, business relationship or client.[55]

[50] Or Know Your Customer (KYC) procedure, which means that the complete profile of the customer is collected. KYC is narrower than the CDD procedure.

See Louis De Koker, 'Money laundering control and suppression of financing of terrorism: some thoughts on the impact of customer due diligence measures on financial exclusion' (2006) 13 (1) Journal of Financial Crime 26, 28.

[51] Or "beneficial owners" which have been defined in the General Glossary as the "natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."

[52] These measures are detailed in Recommendation 10 and will be analysed in Chap. 7.

Most important is that financial institutions have to terminate the business relationship with a customer, refuse to open accounts or perform transactions in cases where they are unable to conduct CDD measures, as set forth in Recommendation 10.

[53] If the occasional transaction exceeds the designated threshold (USD/EUR15,000) or in cases of wire transfers set forth in the Interpretative Note to Recommendation 16.

[54] FATF Recommendation 10.

Pursuant to the General Glossary, the term "identification data" means documents, data or information which is reliable and constitutes an independent source.

[55] See FATF Recommendation 10 and its Interpretative Note.

ECCD measures have to be applied in particular cases, for example to politically exposed persons (PEPs)[56] and correspondent banking.[57] Moreover, financial institutions cannot have or continue a correspondent banking relationship with any "shell banks,"[58] whilst simplified CDD procedures can be applied in cases where there are lower risks.[59]

Fourthly, financial institutions have to pay great attention to risks in relation to the following particular cases: (1) money or value transfer services (MVTS),[60] whether by natural or legal persons, which must be licensed or registered and comply with the relevant FATF Recommendations;[61] (2) all new products, business practices and usage of new technologies, which must be assessed and identify ML risk before they are launched;[62] (3) domestic and cross-border wire transfers;[63] and (4) all transactions and business relationships with persons, companies

[56] FATF Recommendation 12.

Foreign PEPs refer to "individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials," whilst domestic PEPs refer to "individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials" and International organisation PEPs refer to "persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions." See the General Glossary (n 308).

[57] FATF Recommendation 13.

[58] The term "shell bank" means "a bank that has no physical presence in the country in which it is incorporated and licensed and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The mere existence of a local agent or low level staff does not constitute physical presence," see the General Glossary (n 308).

[59] Interpretative Note to FATF Recommendation 10.

For further details about the levels of CDD, see the first section of Chap. 7.

[60] MVTS are "financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*," see the General Glossary (n 308).

[61] FATF Recommendation 14 and its Interpretative Note.

[62] FATF Recommendation 15.

[63] FATF Recommendation 16 and its Interpretative Note.

and other financial institutions which come from countries which apply the FATF Recommendations in an inadequate manner or do not apply them at all.[64] If this is the case, countries have to apply further adequate countermeasures.[65]

Record Keeping Procedures

Financial institutions have to maintain the necessary transactions records, whether pertaining to domestic or international matters, for at least five years in order to respond as quickly as possible to an information request from the competent authorities. Moreover, financial institutions must keep all records,[66] which they have obtained through CDD procedures, business correspondence, account files and any analysis of the results also for at least five years after the date of the occasional transaction or after the termination of the respective business relationship.[67]

STRs

The FATF Recommendations adopt the STRs regime in cases where there is "suspicion" or "reasonable grounds for suspicion"[68] that the transaction/activity relates to ML.[69] Hence, banks and other financial institutions are under an obligation to inform the FIU promptly when they suspect or have reasonable grounds to suspect that the transaction/activity relates to ML.[70] In fact, the STRs regime is the most important mechanism in the AML system, as it allows the FIU (which is the only authorised entity to receive STRs)[71] to identify whether the transaction/

[64] FATF Recommendation 19.

[65] Examples of such countermeasures have been provided in the Interpretative Note to FATF Recommendation 19.

[66] Such as copies of driving licences, identity cards and passports.

[67] FATF Recommendation 11.

[68] For the meaning of "suspicion" and "reasonable grounds for suspicion," see Chaps. 7 and 8.

[69] Or TF, FATF Recommendation 20.

[70] FATF Recommendation 20.

[71] This will be analysed in section "The Function of the FIU in Counteracting the ML Process" below.

activity actually relates to ML and which after arriving at a decision can take the next appropriate step.[72]

Banks and other financial institutions are required to develop their internal systems for the purpose of AML,[73] particularly with a view to increasing and improving the quality of STRs. This requires adopting a number of procedures, including training of relevant officers from time to time. Branches and majority owned subsidiaries of financial groups have to apply the same AML measures as are applied in the home country, which ensures that the FATF Recommendations[74] are implemented.

Directors of financial institutions, their officers and employees are precluded from divulging to any person that an SRT has been/is going to be reported to the FIU and a failure to comply with this means that the respective director, officer or employee will commit the "tipping off"[75] offence.

Measures Should Be Implemented by the Regulatory and LEAs[76]

Under this category of Recommendations, the FIU must be established in countries which deal with ML cases.[77] "Supervisors"[78] must

[72] FATF Recommendation 21(a) provides that financial institutions, which divulge information about the STR to the FIU, so long as done in good faith, should be immune from any criminal/civil liability, including breach of contract, legislation, regulation or any other administrative provision.

[73] FATF Recommendation 18.

[74] FATF Recommendation 18 and its Interpretative Note.

[75] FATF Recommendation 21(b).

Tipping off offences will be analysed in Chaps. 5 and 8.

Under FATF Recommendations 22 and 23, DNFBPs have also to adopt CDD measures, comply with record keeping procedures and STRs requirements. Additionally, regulatory and supervisory entities should ensure that financial institutions implement the FATF Recommendations dealing with CDD measures, record keeping procedures and STRs. The regulatory and supervisory measures have also to be imposed on DNFBPs. See FATF Recommendations 26 and 28 along with their Interpretative Notes.

[76] FATF Recommendations 24 to 35.

[77] FATF Recommendation 29; the FIU will be critically analysed in detail in section "The Function of the FIU in Counteracting the ML Process" below.

[78] The term "supervisors" is defined in the General Glossary as "the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions (financial supervisors) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the

be legally permitted to inspect, supervise and monitor institutions in order to ensure that the financial institutions comply with AML measures and procedures. These officers should also possess powers to punish financial institutions in case they fail to adopt and follow AML measures and procedures.[79] Authorities should also employ adequately skilled employees, ensure confidentiality standards and have technical and financial recourses at their disposal in order to discharge their duties properly.[80]

The country's LEAs should possess sufficient powers to request relevant records, documents or information from the particular financial institution, DNFBPs and other natural or legal persons. The country's competent authorities must also be able, legally, to identify property as soon as possible, monitor it and to start procedures to freeze or seize the concerned property[81] which is/may be suspected to constitute "criminal property."[82]

The competent authorities have also to keep comprehensive statistics about their work, such as on the STRs, prosecutions and convictions,[83] since they form the basis for any assessment about a country's AML system.[84]

---

power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions."

[79] FATF Recommendation 27.

[80] Interpretative Note to Recommendation 26.

[81] FATF Recommendations 30 & 31.

[82] In relation to investigations, competent authorities must be aware of investigative techniques so that they can access computer systems, conduct undercover operations and intercept communications. Most importantly, competent authorities have to able to identify particular assets without the owner being informed. FATF Recommendation 31.

[83] FATF Recommendation 33.

Moreover, pursuant to Recommendations 24 and 25, countries are required to adopt preventive measures to preclude money launderers from exploiting "legal persons" and/or "legal arrangements."

For the meaning of "legal persons" and "legal arrangements," see the General Glossary (n 308).

[84] In addition, a variety of effective and dissuasive criminal, civil or administrative sanctions can be employed by all countries and imposed upon legal and natural persons who fail to fulfil AML requirements. These sanctions do not have to be limited to financial institutions and DNFBPs, but can also be extended to their directors and senior management. FATF Recommendations 35.

The Binding Force and Mutual Assessment

As mentioned above, the FATF Recommendations have been accepted and supported by international organisations, such as the UN Security Council, the IMF and the World Bank, and by governments of major countries, such as the USA.[85] Nevertheless, the recommendations are not legally binding. The FATF Recommendations spell out a legal structure, which can be adopted dependent on the particular conditions prevailing in a particular country.[86] The FATF Recommendations therefore are not to be considered "hard law," but only "soft law."[87]

However, the FATF can adopt number of actions, which in reality amount to forceful sanctions against members which fail to obey its Recommendations. The actions involve three steps. Firstly, the FATF can issue a letter and send its president with a special delegation to the non-complying country. Secondly, the FATF can put all countries on alert when it comes to transactions and business relationships with persons, companies and other financial institutions from the concerned country.[88] Lastly, the FATF can remove the non-obeying country from its membership, which nearly happened in February 2000, when the FATF threatened Austria unless it adopted adequate procedures to reform its practice pertaining to anonymous passbook accounts.[89] On 18 October 2013, the FATF published a public statement identifying

[85] James Thuo Gathii, 'The Financial Action Task Force and Global Administrative Law' [2010] Paper No. 10-10 Journal of the Professional Lawyer, Forthcoming; Albany Law School Research 1. Available online at: http://ssrn.com/abstract=1621877 (accessed on 26th October 2014).

[86] Neil Jensen and Png-Cheong Ann, 'Implementation of the FATF 40 + 9 Recommendations: a perspective from developing countries' (2011) 14 (2) Journal of Money Laundering Control 110, 113.

[87] Barbara Crutchfield George and Kathleen A. Lacey, 'Crackdown on Money Laundering: A Comparative Analysis of the Feasibility and Effectiveness of Domestic and Multilateral Policy Reforms' (January 1, 2003) 23 (2) Northwestern Journal of International Law & Business 1, 54.

[88] Pursuant to FATF Recommendation 19, see (n 338).

This occurred in the case of Turkey in 1996. For more details, see Norman Mugarura (n 292) 185.

[89] For additional information about this case, see Mark Simpson (n 277) 224.

See also Norman Mugarura (n 292) 185.

jurisdictions with high-risk and non-cooperative jurisdictions that pose a risk to the international financial system.[90]

FATF MERs

One of the most effective mechanisms to assess whether a country is complying with the FATF Recommendations is the MER[91] which represents a political pressure.[92] This mechanism ensures that member states of the FATF or FSRBs[93] have their processes scrutinised to ensure that they have adopted an adequate level of compliance with the Forty FATF Recommendations. MER is thus a process which determines the level at which a country's legal system complies with the FATF standards.

In the MER, a country's laws, regulations and AML[94] measures are scrutinised and examined to see how well a country is doing at transposing the FATF standards in practice.[95] The FATF or FSRB Secretariat appoints an assessor team which comprises a number of experts in the fields of law, finance, regulations and law enforcement. Individuals

[90] Namely, Iran and the Democratic People's Republic of Korea (DPRK).

The other jurisdictions with strategic AML/CFT deficiencies are Algeria, Ecuador, Ethiopia, Indonesia, Kenya, Myanmar, Pakistan, Syria, Tanzania, Turkey and Yemen.

See FATF Public Statement, 'High-risk and non-cooperative jurisdictions, jurisdictions for which an FATF call for action applies' published by the FATF on 18 October 2013, available online at: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatf-public-statement-oct-2013.html (accessed on 2nd November 2014).

[91] Paul Hynes, Nathaniel Rudolf and Richard Furlong, *International Money Laundering and Terrorist Financing*: *A UK Perspective* (First Edition, Sweet & Maxwell/Thomson Reuters 2009), 461.

[92] Philip J. Ruce, 'The Bank Secrecy Act: Considerations for Continuing Banking Relationships After the Filing of a Suspicious Activity Report' (December 5, 2011) 30 (1) Quinnipiac Law Review 43, 65 & 66. Available at SSRN: http://ssrn.com/abstract=1968413 (accessed on 16th December 2013).

[93] Where the FATF conducts MERs for its members and each FSRB conducts MERs for its members.

[94] In addition to combating TF.

[95] Mark Simpson (n 277) 223.

from international organisations can also assume an observer status[96] with the FATF, such as the IMF.[97]

MERs illustrate a country's compliance level with each FATF Recommendation. There are generally five possible levels of compliance.[98] MERs will not be recognised as a formal report unless it has been discussed and adopted by the FATF/FSRB plenary meeting. After this has been done, the MER becomes a public report.[99] A country, which is under examination, will be required to report back to the plenary within two and a half years from the adoption of the MER.[100] The country has to demonstrate that it has tried to address any highlighted vulnerabilities.[101]

---

[96] The FATF observers are listed on the FATF website and have a specific AML mission and other functions. For more detail, see www.fatf-gafi.org (accessed on 29th October 2014).

To become an FATF observer, see 'FATF policy on observers', June 2008, available on the FATF website at: www.fatf-gafi.org (accessed on 29th October 2013).

See also Laurel S. Terry, 'An Introduction to the Financial Action Task Force and its 2008 Lawyer Guidance' [2010] Journal of the Professional Lawyer 3, 8.

Available at SSRN: http://ssrn.com/abstract=1680555 (accessed on 29th October 2014).

[97] The assessor team usually visits and meets with the officials in the examined country for two weeks and then issues its draft MER. For further details, see David Chaikin, 'How effective are suspicious transaction reporting systems?' (2009) 12 (3) Journal of Money Laundering Control 238, 242.

[98] Which are Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC) and Not applicable (NA). For further details regarding compliance ratings, see FATF Reference Document, 'Methodology for Assessing Compliance with the FATF 40 Recommendations and FATF 9 Special Recommendations' 27 February 2004 (updated as of February 2009).

See also FATF Reference Document, 'Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems' February 2013. Available on the FATF website at: www.fatf-gafi.org (accessed on 19th February 2015).

[99] As it becomes available on the FATF or the relevant FSRB website.

[100] FATF Reference Document, 'Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations' October 2013, 19, available online at: www.fatf-gafi.org/media/fatf/…/FATF-4th-Round-Procedures.pdf (accessed on 29th March 2015).

[101] A regular follow-up is the default mechanism to realise an ongoing monitoring system and all members are subjected to this mechanism. In addition, the plenary may decide to subject a country to an enhanced follow-up and in such an instance a country has to report back more frequently. The decision to subject a country to an enhanced follow-up depends on the following elements:

"(a) After the discussion of the MER: a country will be placed immediately into enhanced follow-up if any one of the following applies:
(i) it has 8 or more NC/PC ratings for technical compliance, or
(ii) it is rated NC/PC on any one or more of R.3, 5, 10, 11 and 20, or
(iii) it has a low or moderate level of effectiveness for 7 or more of the 11 effectiveness outcomes, or
(iv) it has a low level of effectiveness for 4 or more of the 11 effectiveness outcomes.

Subsequently, the FATF/FSRB will issue follow-up report[102] in which it evaluates the reforms.[103] International organisations which have observer status, such as the IMF and the World Bank, may also conduct evaluations in order to assess a country's compliance level with each FATF standard. Again the report will not be publically available unless it has been adopted by the Executive Boards of these organisations.[104]

FATF MERs and Other MERs

One can observe similarities and differences between MERs carried out by the FATF or the relevant FSRB and evaluations carried out by international organisations, such as the IMF and the World Bank. Firstly, one similarity is that the FATF Methodology for Assessing Compliance with FATF standards[105] and a Handbook for Countries and Assessors[106] are employed; accordingly both the FATF/FSRBS MERs and the evaluations by international organisations use the same technique/mechanism. Secondly, a difference lies in the level of assessor team. As mentioned above, in the case of the MERs, the FATF or FSRB, the secretariat appoints an assessor team which comprises a number of experts in the fields of law, finance, regulation and law enforcement, and international organisations may have observer status with the FATF, such as the IMF. In contrast, evaluations carried out by international organisations, such as the IMF,

(b) After the discussion of a follow-up report: the Plenary could decide to place the country into enhanced follow-up at any stage in the regular follow-up process, if a significant number of priority actions have not been adequately addressed on a timely basis."

However, a follow-up assessment about its MER takes place after five years, irrespective of whether it has been placed under a regular or enhanced follow-up.

For further details about the procedures of regular/enhanced follow-ups and follow-up assessments, see FATF Reference Document, 'Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations' (n 374) 18–21.

[102] As happened with the UK's ME. Its MER was published on 29 June 2007 and its follow-up report was published on 16 October 2009. The UK's MER and its follow-up report are available on the FATF website at: www.fatf-gafi.org (accessed on 20th September 2014).

[103] David Chaikin (n 371) 243.

[104] Jensen Neil and Ann Png-Cheong (n 360) 111.

[105] (N 372).

[106] April 2009, available on the FATF website at: www.fatf-gafi.org (accessed on 20th September 2014).

are generally conducted by its own staff, though occasionally experts are used from outside the organisation. Another difference is that the MERs will not be recognised as a formal report and be publically available unless it has been discussed and adopted in the FATF/FSRB plenary meeting, while the IMF evaluation will not be publically available unless it has been adopted by the Executive Boards,[107] nevertheless these evaluations can be considered as MERs if they have been discussed and adopted in the FATF/FSRB plenary meeting for such purpose.[108]

The Function of the FIU in Counteracting the ML Process

This section analyses the legal framework of the FIU, as well as its characteristics from the perspective of international standards.

The Legal Framework of the FIU

This subsection assesses the FIU from a number of aspects, namely the FIU's general rules in terms of its nature, aims, models and its roles in relation to combating ML.

The Beginning of the FIU

During the early 1990s, the need arose to create a central specialised unit in order to collect, analyse and disseminate information associated with ML. Throughout this period, a number of FIUs were established, with Australia and the USA establishing the first ones.[109] The number

[107] Ann-Cheong Pang (n 320) 90.

[108] As occurred with the UAE ME 2008, where the evaluation was firstly conducted by the IMF, and was then discussed and adopted as a MER in the MENAFATF and FATF plenary meeting. The UAE MER will be analysed in the following chapter.

[109] This goes back more than 20 years. For further details, see Kilian Strauss, 'The Situation of Financial Intelligence Units in Central and Eastern Europe and the Former Soviet Union' [November 2010] Working Paper Series No 09 Basel Institute on Governance, 6. Available online

increased in the following years, especially with the establishment of the Egmont Group in 1995.[110] The Egmont Group was established in the Egmont Arenberg Palace in Brussels when a group of FIUs[111] met and decided to set up the "Egmont Group of Financial Intelligence Units"[112] in order to foster international cooperation amongst FIUs for the purpose of detecting and preventing ML.

The Egmont Group is an informal body consisting of national FIU members, which meet annually to increase cooperation, information exchange and the sharing of expertise.[113] The major aim of the Group is to offer its FIU members[114] an environment so that they can develop their AML[115] systems. This is done through a number of mechanisms, for example the FIUs exchange of financial intelligence information via the Egmont Secure Web (ESW). [116] Hence, an international communication network is established amongst FIUs.[117]

---

at: http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN044510.pdf (accessed on 18th March 2015).

[110] International Monetary Fund Handbook, *Financial Intelligence Units*: *An Overview* (International Monetary Fund 2004), available online at: http://www.imf.org/external/pubs/ft/fiu/fiu.pdf (accessed on 7th November 2014).

[111] Comprising representatives from the countries of Australia, Austria, Belgium, Canada, France, Finland, Germany, Italy, Japan, Monaco, the Netherlands, New Zealand, Slovenia, Sweden, the UK and the US and the observers from a number of international organisations, such as the EC and the FATF.

See Andrew Clark and Matthew Russell, 'Reporting Regimes' in Andrew Clark and Peter Burrell (eds), *A Practitioner's Guide to International Money Laundering Law and Regulation* (City & Financial Publishing 2003), 115 at 116.

[112] See www.egmontgroup.org (accessed on 24th November 2014).

[113] Ibid.

[114] Currently, there are 156 FIU members in the Egmont Group. The UK and the UAE FIUs are members.

See Appendix A for the list of Egmont Group members in 'The Egmont Group Annual Report (2012–2013)', available online at: www.egmontgroup.org/library/download/314 (accessed on 22nd March 2015).

[115] And counteracting TF.

[116] Egmont Group, 'Information Paper on Financial Intelligence Units and the Egmont Group', (September 2004), 3, available online at the Egmont Group website mentioned above.

[117] H. Freis James, 'Global Markets and Global Vulnerabilities: Fighting Transnational Crime Through Financial Intelligence' (April 25, 2008) Financial Crimes Enforcement Networks U.S. Department of the Treasury 1, 11. Available online at: http://www.fincen.gov/news_room/speech/html/20080425.html (accessed on 8th November 2014).

The Egmont Group defines an FIU as a national entity specialised in receiving and analysing STRs regarding ML and then, upon its analysis, disseminating/disclosing the financial information to the competent authorities or foreign FIUs.[118] The definition clearly spells out the core functions of any FIU; and this is what will be analysed in detail below.[119]

[118] The Egmont Group defines an FIU as:

> A central, national agency responsible for receiving (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:
>
> (i) concerning suspected proceeds of crime and potential financing of terrorism, or
> (ii) required by national legislation or regulation,
>
> in order to combat money laundering and terrorism financing. See "Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit" (undated), 1 & 2, available online at the Egmont Group website mentioned above.

It should be noted that the Egmont Group adopted the definition of an FIU in 1996 and amended it in June 2004 to illustrate the role of the FIU in counteracting TF. Moreover, such definition has been agreed by the Palermo Convention 2000 and the 2005 UN Convention against Corruption. See (n. 25 & 26) of Chap. 1.

The UK ratified Palermo Convention 2000 in 2006 and the UAE in 2007. In addition, the UK and the UAE ratified the UN Convention against Corruption in 2006.

[119] The Egmont Group has also published various documents, for example, "Principles for Information Exchange" and "Best Practices for the Exchange of Information" in order to foster information exchange amongst FIUs and to promulgate exchange of information guidelines. All of these documents and others, such as (Statement of Purpose: Guernsey, 23rd June 2004), are available online at the Egmont Group website mentioned above. Within the Egmont Group, there are five working groups, which deal with overcoming global AML obstacles: the Legal Working Group (LWG), the Outreach Working Group (OWG), the Training Working Group (TWG), the Operational Working Group (OpWG) and the IT Working Group (ITWG).

Wouter Muller, 'The Egmont Group' in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth (eds), *Anti-Money Laundering*: *International Law and Practice* (John Wiley & Sons Ltd., Chichester 2007), 83 at 89 & 90.

See also Egmont Group, "Information Paper on Financial Intelligence Units and the Egmont Group" (n 390) 3 & 4.

In addition, such working groups meet on a periodical basis and report to the Heads of FIUs about their functions. See "The Egmont Group Annual Report (June 2009–July 2010)," 19, available online at: www.egmontgroup.org/library/download/99 (accessed on 8th November 2014).

The Key Functions of the FIU in Relation to Counteracting ML

Regardless of their particulars models and names,[120] all FIUs share common core functions in relation to counteracting ML. Generally, there are three basic roles an FIU plays: receiving the STRs, analysing the STRs and then disseminating/disclosing the financial information to the competent authorities or foreign FIU. These functions will be analysed below.

Receiving the STRs

The first core function of an FIU is to receive STRs/SARs.[121] An FIU is the only national entity which is specialised in this task. Through this function, an FIU forms a centralised repository of STRs. Indeed, STRs are a vital link between preventive measures and law enforcement for the purpose of combating ML. This is simply because all financial institutions and DNFBPs[122] are legally obliged to report to the FIU what they know[123] or their suspicion[124] about the transaction/activity involving

[120] It is worth noting that the name of FIU could be different from one country to another, for example the name in the UAE is AMLSCU within the Central Bank, in the UK it is FIU and is within the NCA, as will be analysed in Chaps. 5, 6 and 9.

[121] It should be mentioned that some jurisdictions, such as the UK, adopt the term "SARs" and other jurisdictions, such as the UAE, adopt the term "STRs." In fact, the term "transaction" is slightly narrower than the term "activity," especially because suspicious transactions do not include suspicious activities; in contrast, the latter include suspicious transactions, as well as other conditions which increase suspicion regarding illicit activities. Nevertheless, such a difference could be resolved, especially when a number of countries require that the reporting institutions have to report unexecuted transactions for suspicious reasons. See International Monetary Fund Handbook (n 384) 42.

See also Philip J. Ruce, 'The Bank Secrecy Act: The Not-so-Safe Harbor Provision and the Whitney Rule's Double Standard for SAR Supporting Documentation' (July/August 2011) 3 (7) Financial Fraud Law Report 608, 612, available online at: http://ssrn.com/abstract=1866455 (accessed on 11th December 2014).

[122] DNFBPs are identified according to the national legislation of a country.

[123] The notion of "knowledge" will be discussed in Chap. 7.

[124] The notion of "suspicion" and "reasonable grounds to suspect" will be analysed in Chaps. 7 and 8.

ML or proceeds resulting from criminal activities.[125] The FIU, in turn, analyses such information and disseminates the information/results about a case to the competent authority.

In most cases, reporting entities do not know whether a crime has been committed or even the source of the money. They are also unable to ask the client for further information since this risks tipping-off. Hence, the elements of STRs usually comprise providing information about a particular customer and his or her transaction and the reason(s) why such a transaction is related to ML. The reporting entities do not have to provide tangible evidence that the particular transaction constitutes ML.[126] They only have to report when they have knowledge or suspect that a particular transaction/activity is involved in ML.[127]

A country often exempts reporting entities, their directors, officers and employees from privacy law or banking confidentiality when it comes to STRs or cash transactions.[128] This is done to foster an ideal environment for detecting and preventing ML. Reporting entities have to appoint a sufficiently trained staff, who are well versed with STRs and know when to inform the FIU, as well as the relevant procedures.[129]

Analysing the STRs

Analysing the STRs is the second function of an FIU, which it receives from the reporting entities and, upon its analysis, decides whether the STR contains sufficient content for the purpose of disseminating it to the competent authority. An FIU may receive an enormous amount of STRs

---

[125] Which are predicate offences for the purpose of ML. These predicate offences are usually listed in the national legislation of an individual country.

[126] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Second Edition and Supplement on Special Recommendation IX, 2006 The World Bank), VI-21.

[127] Besides receiving the STRs, there is a cash transactions reporting systemfor when a transaction exceeds a fixed amount. The requirements of this system are subjected to the national legislation of a country. This will be illustrated later in the present chapter.

[128] Such as the UAE, where Article 20 of the FLMLC 2002 provides immunity, as illustrated in (n 623) of Chap. 5. The UK's AML system also grants immunity, as analysed in Chap. 8.

[129] Abdullahi Y. Shehu (n 291) 146.

which is disproportionate to its capacity. If this happens, STRs received from foreign FIUs can be given higher priority in the analytical process.[130] Technology is essential since STRs can be stored in an electronic database which saves time when it comes to retrieving data about any specific STR. Otherwise it would be far too time-consuming to retrieve and analyse a specific STR, and particularly where this has to be done as quickly as possible when it comes to ML.[131] Tactical, operational and strategic analyses are the three elements which constitute the analytical function of an FIU.

Tactical Analysis

FIUs should have sufficiently experienced staff to fulfil their function of understanding, examining and interpreting the information contained in an STR. This function is crucial for the mission of any FIU, as its partners (police officers or prosecutors) generally deal with all kinds of offences and are not experts in financial transactions.[132]

The tactical analysis involves gathering additional information about the relevant person, transaction or company other than provided in the STR. This is known as "link analysis" and means that all relevant data is accessed as much as possible.[133] An FIU has therefore also the ability and legal authority to gather additional information other than what has been provided in the STR in order to evaluate the STR properly and decide whether or not to disseminate it to the competent authority. An FIU can obtain additional information from several sources, including its own database,[134] information which is publicly available,[135] information

[130] In accordance with the internal criteria of the particular FIU. International Monetary Fund Handbook (n 384) 56.

[131] Ibid 56 & 57.

[132] H. Freis James (n 391) 15.

[133] Richard K. Gordon, 'Losing the War Against Dirty Money: Rethinking Global Standards on Preventing Money Laundering and Terrorism Financing' [May 4, 2010] Paper No. 2010–20 Case Legal Studies Research 1, 43. Available online at SSRN: http://ssrn.com/abstract=1600348 (accessed on 10th November 2014).

[134] Such as a former STR.

[135] Such as company status, accounting bodies and audit companies.

from government databases[136] or from a foreign FIU, especially where the subject of the STR involves bank account(s) which are located in another country. Where necessary, an FIU can also request further information from the reporting entity which submitted the initial STR.[137]

It is worth noting that the reporting entities are not able to conduct a "link analysis,"[138] as such legal power is only granted to an FIU for the purpose of understanding, examining and interpreting the information contained in an STR.

Operational Analysis

This type of analysis serves the investigation stage, through which an FIU comes to appreciate a number of issues, including investigative leads, activity models and the link between the subject and accomplices. The FIU uses a method called "financial profiling," which tries to recognise inconsistencies between a suspect's income and cash outflow.[139] Thus, all the tactical information, mentioned above, is used and translated into operational intelligence in order to be transmitted to the competent authority, as well as to invent a number of suppositions regarding the probable actions of the suspect.[140]

Strategic Analysis

This analysis is not associated with individual STRs, but with new trends. The scope of information used in a strategic analysis is wider than in a tactical analysis. All the collected and analysed information is employed in order to formulate a new/amended strategy for the future work of an FIU.[141] This process is called "strategic intelligence" and essentially means fostering

[136] Like police records, tax records and vehicle registries.

[137] International Monetary Fund Handbook (n 384) 58.

[138] Richard K. Gordon (n 407) 43.

[139] Jayesh D'Souza, *Terrorist financing, money laundering and tax evasion – Examining the performance of Financial Intelligence Unit* (Taylor & Francis Group, LLC 2012), Xiv.

[140] International Monetary Fund Handbook (n 384) 89.

[141] Jayesh D'Souza (n 413) Xiv.

the knowledge about ML methods and new patterns in order to introduce guidelines or typologies.[142] Strategic analysis may, for example, indicate that specific entities could be, more than others, vulnerable and therefore be more easily exploited by money launderers.[143] This method can also lead to additional requirements being imposed on new entities.[144] As an FIU is a national agency, it plays a vital role in participating in the design of an ideal national system and plan, which effectively combat ML at the national level.

Disseminating STRs

The FIU function of disseminating STRs can be principally divided into three phases. The first two phases take place at the national level, whilst the third phase deals with the international information exchange. The first phase relates to the transmission of the STR file to the competent authority. After conducting the analytical function, and considering the STR to be associated with ML, the FIU is obligated to pass the case file to the competent authority. This could be the police or the prosecution.[145] In some jurisdictions, the FIU has to transmit the STR file to the police for additional investigations, while in other jurisdictions the file of the STR must be directly transmitted to the prosecution. In such a case, the prosecuting authority initiates proceedings if the evidence is adequate; otherwise it may request an additional investigation.[146] The determination of whether an FIU has to transmit an STR file to the police or the prosecuting authority is governed by domestic FIU law. In both cases, it is pertinent to transmit the STR file to the competent authority in a timely fashion in order to avoid any delay for the process of prosecution or additional investigation.[147]

During the second phase, the FIU can share information with other domestic entities other that the police or the prosecuting authority. For instance, after transmitting the STR file to the competent authority, police

[142] Richard K. Gordon (n 407) 48.

[143] Jayesh D'Souza (n 413) Xiv.

[144] International Monetary Fund Handbook (n 384) 89.

[145] It should be noted that when the FIU transmits the STR file to the competent authority, the original/initial STR, which was provided by the reporting entity, could constitute a small part of the whole STR file. International Monetary Fund Handbook (n 384) 57.

[146] Ibid 60 & 61.

[147] Paul Allan Schott (n 400) VII-8.

or prosecution, the FIU is authorised to assist a number of domestic entities[148] through the provision of relevant financial information in order that they can carry out their function. In other cases—when the relevant conduct does not relate to ML or related crimes, but constitutes a breach of administrative rules or serves statistical purposes—the FIU may be entitled[149] to act as an assistant body by transmitting financial intelligence to the respective financial regulator or supervisor.

The last phase of the disseminating function is the information exchange at the international level. As ML often involves cross-border activities, the FIU should be able to share/exchange lawfully the financial intelligence with other foreign FIUs.[150] This phase is essential for the international fight against ML. It also provides the concerned FIU with useful information and thereby assists with the analysing process. The process of information exchange between the FIU and the foreign FIU has to be carried out through effective and secure channels[151] as very sensitive information is exchanged. The Egmont Group has highlighted the importance of information exchange amongst FIUs and issued its "Principles for Information Exchange" and "Best Practices for the Exchange of Information."[152]

The FIUs' Non-core Functions

Apart from the above core roles of an FIU in combating ML, it also fulfils a number of other non-core functions which sometimes play a vital role in combating ML and are thus of no less importance than the core functions. The following are the FIU's non-core functions:

Conducting Research

An FIU can benefit from its analytical function and specialised knowledge and undertake research in specific areas. For instance, it can utilise its strategic analysis, mentioned above, in order to provide the government

[148] Such as customs and tax authorities. Jayesh D'Souza (n 413) Xv.

[149] This is according to the national legislations of an individual country.

[150] Jayesh D'Souza (n 413) Xv.

[151] Paul Allan Schott (n 400) VII-9.

[152] See (n 393).

with ideas about how to reform its AML system.[153] It can suggest that specific entities could be vulnerable and more prone to exploitation by money launderers than others. Moreover, through its research, an FIU may assist the government in proposing a number of amendments in the national AML system, such as enhancing preventive measures because new patterns of ML have emerged in specific areas, such as the football or the sports sector in general. An FIU can also adopt this function in order to develop its own core functions,[154] even if the NAMLL does not explicitly task it with this function.

Providing Feedback to the Reporting Entities

Indeed, this function is often one of the most important of any FIU and is no less important than the above mentioned core functions. An FIU must provide feedback/comments to the reporting entities in relation to their STRs in order to improve their quality. If the FIU did not adopt such a function, the reporting entities would not receive any feedback about their STRs. The reporting entities would then be unable to improve the quality of their STRs. However, in practice, many reporting entities contend that they receive little or inadequate feedback from the FIU with regard to the effectiveness of their STRs.[155] The reason for this could be two-fold. Firstly, the FIU may not have access to all financial transactions data, and this negatively affects its ability to provide feedback to the reporting entities.[156] Secondly and most likely, the FIU may fear that the provision of the information may help actual launderers, who will utilise the information to create new laundering techniques.[157] In both cases, the NAMLL should grant an authority to the FIU to access all financial transaction data and should require the FIU to provide feedback, comments and guidelines to the reporting entities and any common inaccuracies should be highlighted. The FIU's fear that its information may

[153] Paul Allan Schott (n 400) VII-17.
[154] International Monetary Fund Handbook (n 384) 79 & 80.
[155] Paul Allan Schott (n 400) VII-23.
[156] Richard K. Gordon (n 407) 48.
[157] Ibid.

help actual launderers appears unjustified, especially as all the reporting entities, the competent authorities and the FIU are working on one common objective, which is to increase the effectiveness of counteracting ML for the purpose of detecting or preventing such crime.

An FIU also plays an important role in fostering public awareness about AML aspects, provides training for the staff of reporting entities and monitors compliance with NAMLL.[158] The proper performance of the FIU functions very much depends on having adequate and qualified human resources. An FIU ought to employ a great number of experts in the fields of banking, insurance, lawyers and securities in order to be able to analyse STRs properly. The FIU can also work with experts, who have been seconded by other departments with sufficient knowledge about financial crimes,[159] including supervisory authorities, the police and justice personnel.[160] Apart from having adequate human resources, sophisticated technology is essential for the fulfilment of FIU functions, particularly the storage of the STRs on electronic databases, which facilitates easy access to all financial transactions data without delay. Furthermore, all employees of an FIU should possess the highest level of integrity, fidelity and honesty since such an entity deals with an enormous amount of sensitive information.

Forms of FIUs

This section deals with FIU models around the world. It is difficult to propose an optimal model for the UAE FIU without the main features of well-known FIU models having been thoroughly analysed; otherwise the proposal and recommendations of this research will be just theoretical and ineffective and will lack credibility.

---

[158] This is according to the national legislations of an individual country. See International Monetary Fund Handbook (n 384) 70–81.

[159] There is no internationally clear and accepted definition for the term "financial crime"; however, the IMF has noted that the term includes any crime which results in a financial loss, such as financial fraud and non-violent illegal activities, such as ML and tax evasion. International Monetary Fund, Financial System Abuse, *Financial Crime and Money Laundering – Background Paper*, (International Monetary Fund 2001), 3. Available online at: http://www.imf.org/external/np/ml/2001/eng/021201.pdf (accessed on 16th November 2014).

[160] International Monetary Fund Handbook (n 384) 29.

The form of an FIU depends on the particular conditions and circumstances of individual countries, such as the national legal system, AML legislation and customs and cultural issues.[161] Generally, there are four FIU models: (A) the administrative model, (B) the law enforcement model, (C) the judicial model and (D) the hybrid model.

The Administrative Model

Under this model, the FIU is either an "autonomous" entity subject to the regulatory or supervisory authority, for example the ministry of finance[162] or the Central Bank,[163] or it is an "independent" agency.[164] The FIU acts as an intermediate agency "buffer" between banks and reporting entities in general and the LEAs which are responsible for financial crime investigations—the police or the prosecution.[165] The FIU receives STRs from the reporting entities, gathers and analyses the relevant information and then transmits particular STR files to the competent authority for investigations or prosecution as, under this model, it is precluded from conducting these two latter tasks.

The administrative-type FIU offers a number of benefits:

1. The reporting entities perceive the FIU as a specialised and technical body.[166] It is a national agency, which has experts who can analyse financial transactions/activities and substantiate ML suspicions better than the reporting entities.
2. The FIU decides whether to transmit STR files to the competent authority, hence it is dependent on the analysis and not on the decision

[161] For further details, see Andrew Clark and Matthew Russell (n 385) 127–129.

[162] As in the case of the FIU in Slovenia which is called the Office for Money Laundering Prevention (OMLP). For further information on OMLP, see http://www.uppd.gov.si/en/about_the_office/ (accessed on 13th May 2015).

[163] As in the case of the UAE FIU which will be critically analysed in Chap. 5.

[164] International Monetary Fund Handbook (n 384) 11.

[165] 'The Egmont Group Annual Report (June 2009–July 2010)' (n 393) 15.

[166] International Monetary Fund Handbook (n 384) 11.

of the reporting entities, which often have insufficient information about the subject and background of the STR.[167]

3. This model prevents direct relations being built between the reporting entities and the LEAs since the FIU works as a "buffer" between them.[168] The benefit here is that the LEAs will not pay attention to disclosures of STRs since it is the FIU which decides, based on its own analysis and dependent on what information it has gathered, whether this constitutes a real STR. If this is not warranted, the FIU will not transmit the STR file to the competent authority.[169] In other words, the LEA will not investigate or take any decision/action in relation to an STR, unless the FIU disseminates the STR to it. As the FIU is separate from the LEAs and the judicial body,[170] the integrity of analysing STRs is preserved, especially since reporting entities may have relations with LEAs.[171] For this reason, the administrative type of FIU is the best one for the banking sector.
4. The FIU can exchange/share relevant information with foreign FIUs in an easy manner, regardless of their particular types.[172] This is unlike the judicial type of FIU, which may find it difficult to exchange information with foreign FIUs.

There are also a number of disadvantages with this type of model:

1. If it is an "autonomous" entity,[173] the FIU is likely to be directly subject to the supervision of political authorities and thus be hampered in the proper execution of its functions.[174]

[167] Ibid.
[168] Andrew Clark and Matthew Russell (n 385) 125.
[169] International Monetary Fund Handbook (n 384) 10–11.
[170] Jayesh D'Souza (n 413) Xi.
[171] International Monetary Fund Handbook (n 384) 12.
[172] Ibid 11.
[173] As in the case of the UAE FIU, see Chap. 5.
[174] International Monetary Fund Handbook (n 384) 11.

2. As the FIU is separated from the law enforcement system, there is a potential risk of delay when it comes to arresting a suspect or freezing a suspicious transaction.[175]
3. Unlike law enforcement or judicial authorities, the FIU often has limited powers for gathering evidence.[176]

Indeed, the above disadvantages make it more difficult to analyse STRs efficiently. The USA, the UAE[177] and France are examples of countries which have adopted this particular FIU model.

The Law Enforcement Model

In this model, the FIU is closer to the LEAs than in any other model. This enables the FIU to utilise its sources, information and experience. Similarly, LEAs can easily access the information held by the FIU and thereby enhance the usefulness of the information during any investigation.[178] In this model, the FIU is usually part of the police agency, either the general body or a specialised unit. Banks and the reporting entities transmit the STRs to the FIU, which gathers and analyses the STR information and disseminates the file to the competent authority for further investigation or prosecution. Additionally, the FIU directly supports the authorities with the investigation or prosecution.[179]

This model has a number of positive and negatives aspects. The positive aspects include:

1. The law enforcement procedures in relation to STRs on ML will be initiated without undue delay when necessary. In contrast to the administrative model, actions will be taken much quicker. The FIU

[175] Jayesh D'Souza (n 413) Xi.
[176] Ibid.
[177] The UAE FIU will be critically analysed in Chap. 5.
[178] Paul Allan Schott (n 400) VII-12.
[179] Andrew Clark and Matthew Russell (n 385) 124.

has law enforcement powers and can for example freeze particular transactions.[180]
2. There is no need to create a new agency with a new administrative and legal system since the FIU forms part of the LEAs.[181] Thus, this model can be cost saving.
3. Information exchanges can be done quicker through usage of a comprehensive police national and international criminal information exchange network, such as Interpol.[182]
4. Accessing criminal information intelligence will be easier to obtain than under the previous model.[183]

The negative aspects of the law enforcement FIU model encompass the following elements:

1. The reporting entities may be fearful or reluctant to disclose information to the FIU because of the potential that the information is disclosed or used in other crimes.[184]
2. The investigation receives more attention than preventive measures[185] since the FIU adopts the law enforcement model and thereby the preventive measures may not be given as much attention in the AML policy at national level.
3. Reporting entities may fear or be reluctant to disclose information to the FIU and alert LEAs, especially if there is not much more than a "suspicion."[186] This is because the FIU has law enforcement powers, including the power to freeze a particular transaction. At the same time, the reporting entities may fear that in some cases the STRs may not really be involved in ML, so that their reputation can be negatively affected, especially if the reporting entity were a bank.

[180] In this case, the judicial supervision will be applied in the same manner as to LEAs in the concerned country. See International Monetary Fund Handbook (n 384) 14.

[181] Ibid.

[182] Paul Allan Schott (n 400) VII-12.

[183] Andrew Clark and Matthew Russell (n 385) 124.

[184] Other than ML or TF. Jayesh D'Souza (n 413) Xi.

[185] Paul Allan Schott (n 400) VII-12.

[186] International Monetary Fund Handbook (n 384) 14.

4. It may take time to establish mutual trust between reporting entities and LEAs since there is no intermediate between them[187] as in the administrative model.

Countries, such as the UK,[188] Germany and Austria have adopted this type of FIU model.

The Judicial/Prosecutorial Model

Under this FIU model, the public prosecution forms part of the judicial system of the country. The main feature of this model is that the FIU is built on the country's judicial system, or often is located in the prosecution's office. However, a specialised police force which investigates financial crimes may be set up. This model of the FIUs is suitable for countries which impose robust and strict banking confidentiality laws, since this establishes a direct channel with the judicial authorities and ensures cooperation with financial entities.[189] This model is useful for countries which do not have complex or large financial institutions with lots of data; otherwise this type of model may not be as successful as the previous two.[190] In this model, the reporting entities transmit the STRs to the FIU, which is located within the judicial or prosecutorial system.[191] The FIU, in turn, receives and analyses the relevant information. The main difference with this model is that, in practice, the FIU does not disseminate the STR file to the competent authority since it has the power to investigate or prosecute the STR files itself.[192] The positive aspects of this model are:

[187] Ibid.

[188] The UK FIU will be assessed in Chap. 9.

[189] Jayesh D'Souza (n 413) Xii.

[190] Andrew Clark and Matthew Russell (n 385) 123 & 124.

[191] Luxembourg and Cyprus adopt the prosecutorial model FIU. Paul Allan Schott (n 400) VII-14.

[192] International Monetary Fund Handbook (n 384) 60.

1. The FIU can conduct searches of properties and arrest suspects, and judicial action can be taken without delay.[193]
2. Unlike the administrative model, the FIU is independent, so there is no political interference[194] and this, in turn, implants trust amongst financial institutions and reporting entities in general.
3. The STRs will be transmitted, by the reporting entities, directly to the FIU which has the power to investigate or prosecute.[195]

The disadvantages of the judicial model are almost the same as under the administrative one, except that the third disadvantage is not applicable.[196] Moreover, in practice, the judicial model of the FIU could face difficulties when it comes to exchanging information with foreign FIUs, if they have not adopted this model.[197]

The Hybrid Model

In this category, the FIUs try to utilise the positive aspects from the above mentioned models. The advantages of at least two models are combined. The FIU serves as a link between the judicial and law enforcement authorities.[198] This is also called the "administrative-regulatory model."[199] In addition to its functions of receiving, analysing and disseminating the STRs files to the competent authority for investigation or prosecution, the FIU is often in charge of formulating regulations and adopting compliance tests for entities which are subject to STRs obligations.[200] Employees from regulatory or LEAs may work under a variety of hybrid FIU models[201] in order to speed up the FIU functions of analysing and

[193] Andrew Clark and Matthew Russell (n 385) 123.
[194] International Monetary Fund Handbook (n 384) 16.
[195] Ibid.
[196] Namely the FIU often has limited powers for gathering evidence, ibid.
[197] Ibid.
[198] 'The Egmont Group Annual Report (June 2009–July 2010)' (n 393) 17.
[199] Andrew Clark and Matthew Russell (n 385) 126.
[200] Ibid.
[201] International Monetary Fund Handbook (n 384) 17.

transmitting the STRs files, and thus accelerate the speed of investigations. These employees have the authority of their particular entity. More importantly, in this model, the FIU can play a vital role in setting up AML controls at the national level.[202] Jurisdictions such as Norway, Denmark and Jersey have adopted this type of FIU model.[203]

Evaluating the Four FIU Models

The administrative model is the most popular model in the world[204] for two main reasons. Firstly, the FIU is considered a separate agency from the LEAs in a country, which means that it acts as a link between the reporting entities and the LEAs when dealing with STRs. There is no direct communication between the reporting entities and the LEAs within this model since the FIU undertakes this communication. Secondly, there is flexibility when it comes to communication with foreign FIUs. Under the administrative FIU model, information about STRs can be exchanged with a foreign FIU without too many restrictions. Exchange of information means requesting and providing information. Nevertheless, this model suffers from problems when it comes to the effectiveness of the AML and analysing STRs in particular. The FIU does not have a wide range of powers to increase the quality of its analytical function. For example, it has limited access to the data/information to deal with an STR and cannot freeze suspected transactions which can possibly delay the proper action being taken.[205] More importantly, the FIU suffers from a lack of independence since it is often subjected to the supervision of political authorities or its analytical function is influenced by those who

[202] Andrew Clark and Matthew Russell (n 385) 126.

[203] International Monetary Fund Handbook (n 384) 17.

It is worth noting that 80 member states of the Egmont Group have adopted the administrative FIU model, whilst 28 have adopted the law enforcement FIU model. In addition, eight member states have adopted the hybrid FIU model and just four have adopted the judicial/prosecutorial FIU model. See 'The Egmont Group Annual Report (June 2009–July 2010)' (n 393) 18.

[204] 'The Egmont Group Annual Report (June 2009–July 2010)' (n 393) 18.

[205] As is the case with the UAE FIU, which does not have the power to freeze transactions, though the Central Bank has this power, as analysed in Chap. 5.

are outside the FIU.[206] This last aspect negatively affects the core functions of the FIU since analysing STRs must be confined to those who are working within the FIU and are specialised and experts in the field of AML.

In contrast, the FIU law enforcement model, which is the second most popular model in the world,[207] seems more effective in dealing with STRs than the previous model, for two main reasons. Firstly, the FIU takes decisions/actions much more quickly than the FIU under the administrative model. It can freeze suspected transactions[208] and information can be quickly exchanged with the LEAs through a comprehensive network. Secondly, the FIU plays a constructive role in increasing the quality of STRs, which are submitted by the reporting entities[209] and assists with the investigation and prosecution conducted by the LEAs and prosecution office.[210]

However, this model has two problems. Firstly, the reporting entities are often reluctant to submit all STRs to the FIU since there is no "buffer" between the reporting entities and the LEAs. The FIU has law enforcement powers, that is it can freeze particular transactions, which might make the reporting entities fear that in some cases the STRs may not really be involved in ML, resulting in their reputation being negatively affected, especially if the reporting entity was a bank. Secondly, the adoption of this model may be problematic in countries which follow a federal system. In these countries, there are two authorities, namely the federal authority and the local authority, which deal with specific areas.[211] The question therefore arises as to how the FIU can carry out its functions in areas which do not fall within the purview of the federal authority. In other words, if the FIU was established within the federal

[206] As in the case with the UAE FIU, where the vast majority of STRs are analysed by Central Bank employees, who are located outside the UAE FIU, as critically analysed in Chaps. 5 and 6.

[207] "The Egmont Group Annual Report (June 2009–July 2010)" (n 393) 18.

[208] As in the case of the UK FIU, which can freeze transactions, as analysed in Chap. 8.

[209] As in the case of the UK FIU, which provides general/specific feedback to the reporting entities, as evaluated in Chap. 9.

[210] As in the case with the UK FIU, which will be evaluated in Chap. 9.

[211] For instance, in the UAE, there are some cities which have their own judicial and police system and are not governed by the federal one; see Chap. 6.

system of a country, what will be the legal basis for it to receive STRs from reporting entities located in area (A), which is not governed by the federal authority, but by the local authority? In addition, what is the legal basis for the FIU to transmit the results of analysing STRs to the police/prosecution in area (A), which has its own police and judicial system? This means that more than one FIU would have to be established within the country and this violates FATF Recommendation 29, which requires that only one FIU is established as the national agency, as further analysed in the following section.

The judicial FIU model is the least favoured one in the world.[212] This is due to difficulties faced when exchanging information with foreign FIUs at the international level. The judicial FIU model imposes restrictions on the exchange of information with foreign FIUs and this is also why only a few countries have adopted this model. In addition, this model is difficult to implement in countries with a federal system, as shown above.

As a result, there are core functions which an FIU must fulfil when dealing with STRs, namely receiving, analysing and disseminating, regardless of its particular model. In addition, there is no one particular model that is optimal for every time and place. The choice of an FIU model depends on several factors, which in turn depend on the political, legal and judicial system of the country. Furthermore, a particular model may be suitable for some time, before a different model becomes more appropriate.

Examining the Functions of the FIU Within the FATF Recommendations

The initial 1990 FATF Recommendations and their very first revision in 1996 did not explicitly mention the term "FIU." Instead, it was only stated that financial institutions have to report any suspicious transaction to the "competent authorities." Moreover, the term "competent authorities" was not given a definition by the 1990, the 1996 or even the 2003 FATF Recommendations. This opened the door to a host of interpretations, including those made by any other government entity

[212] 'The Egmont Group Annual Report (June 2009–July 2010)' (n 393) 18.

specialised in receiving suspicious transactions about ML from financial entities.[213] However, the General Glossary of the 2012 revision provides a clear definition of the term to include the FIU, authorities that have the function of investigating and prosecuting ML, and authorities that have AML supervisory responsibilities aimed at ensuring compliance by financial institutions with AML requirements.[214]

The Situation Under the 2003 FATF Recommendations

The term "FIU" was explicitly mentioned for the very first time in the 2003 revision of FATF Recommendation 26.[215] A domestic FIU is the sole entity which is specialised in receiving, analysing and then disseminating the files of STRs to the competent authority for further investigations or prosecution. The Recommendation also adopted the Egmont Group's definition in relation to the FIU.[216] For the FIU to perform properly its core functions, especially analysing the STRs, the Recommendation required that an FIU should be legally authorised to access, directly or indirectly, financial, administrative and law enforcement information. This access should be on a "timely basis." The term "timely basis" requires

---

[213] International Monetary Fund Handbook (n 384) 17.

Furthermore, in the context of issuing the 2001 FATF Special Recommendations, the Special Recommendation IV extended the authority of the "competent authorities" from receiving suspicious transactions on ML to receiving suspicious transactions on TF.

[214] The General Glossary states that the term "competent authorities" refers to "all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities." The General Glossary to the Forty Recommendations (n 308).

[215] Recommendation 26 of the 2003 revision mentioned the term "FIU" and its authorities in relation to STRs on ML and stated that:

> Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

[216] (N 392).

that the country ensures that there is a link, directly or indirectly, between its competent authorities, including the FIU.[217]

The Recommendation briefly referred to the core functions of an FIU, which are those of receiving, analysing and disseminating the STR, but without explaining the meaning of each one. When Recommendation 26 was prepared, the four types of FIUs were not considered. Equally, the Interpretative Note to Recommendation 26 did not add any useful elements in this regard.[218]

The methodology emphasises the following constituent elements for the FIUs:

1. The creation of the FIU could be either within an existing authority[219] or as an independent national entity. In both cases, the functions of the FIU must be independent[220] in order to avoid any unjustified interference in its functions.
2. The reporting entities should be provided with guidance,[221] for example about the procedures pertaining to the transmission of STRs to the FIU and details about specific reporting forms. Guidance can be either provided by the FIU or by another competent authority of the country.

[217] An electronic link between the entities is therefore essential.

[218] The Interpretative Note to the FATF Recommendation 26 (the 2003 FATF Recommendations revision) only states that:

> Where a country has created a FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

The Interpretative Note only emphasised the international cooperation aspects, for example the "Egmont Group Statement of Purpose" information exchange between the FIUs. The Interpretative Note did not add any useful information about the core or additional FIU functions or the types of the FIUs.

[219] As is the case in the UAE where the FIU is within the Central Bank. This will be critically analysed in Chap. 5.

[220] FATF Reference Document, 'Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems' (n 372) 74.

[221] Ibid 80.

3. The FIU itself or via the competent authority in a country should posses legal powers to gather additional information about specific STRs from the concerned reporting entity in order to perform its functions properly.[222]
4. Information about its activities, such as statistics, trends and typologies, should be periodically released and made publicly available by the FIU.[223]

These elements have been set out in the FIU methodology; however, it does not provide any useful information about the types of FIUs or their core/additional functions. Non-core functions, such as conducting research and providing feedback to the reporting entities, are essential and no less important than the core functions. This is because these functions increase the quality of the STRs which are being submitted by the reporting entities and thereby assist the FIU to amend/revise its future strategy.

The Situation Under the Revision of the 2012 FATF Recommendations

The 2012 FATF Recommendation 29 replaced the 2003 FATF Recommendation 26. Prior to examining the revised Recommendation and its Interpretative Note, it is crucial to take recourse briefly to the relevant 2012 Recommendations, which are directly or indirectly related to the FIUs or the STRs.

In addition to the FATF Recommendations 9, 18, 20 and 21,[224] the competent authorities of a country are required to maintain inclusive

---

[222] The FIU should have "authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or forward or disseminate specific information." FATF Reference Document, 'Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems' (n 372) 74.

[223] 'Methodology for Assessing Compliance with the FATF 40 Recommendations and FATF 9 Special Recommendations' (n 372) 34.

[224] Which were discussed above.

FATF Recommendations 32 and its Interpretative Note require all countries to adopt a "declaration system" and/or "disclosure system" in order to address three issues, namely (1) detect physical

records and statistics about their own works[225] for the purpose of periodically gauging their own work and to measure generally the effectiveness of the national AML system.[226] The national FIU is also required to keep comprehensive statistics about received and disseminated STRs. This is crucial in order to evaluate the effectiveness of the functions of the FIU when dealing with STRs received from the reporting entities. In addition, the competent authorities of a country are required to provide entities with guidelines and feedback about STRs[227] in order to assist the reporting entities to improve the national measures, which have been adopted to counteract ML.

The provided guidelines and feedback could spell out supplementary procedures which assist the reporting entities in implementing AML measures more effectively or could describe methods or techniques which can be employed to combat ML. General or specific case feedback should also be given.[228] Obviously, the national FIU is best placed to provide

---

cross-border transportation of currency and BNIs; (2) prevent, restrain or confiscate currency and BNIs in suspicious cases which are associated with ML; and (3) stop or restrain currency or BNIs in cases of false declaration or disclosure and impose appropriate sanctions in these cases. Moreover, according to the Glossary of specific terms, false declaration means: "a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required," and false disclosure means: "a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required."

The term "declaration system" means that any person has to submit a truthful declaration to the designated competent authorities if he or she made a physical cross-border transportation of currency or BNIs of a value which is over the maximum threshold of USD/EUR15,000. The "disclosure system" means that a traveller is obliged to give the authorities a truthful answer when being request to do so. The declaration could be either through a written system or an oral system. The written system could apply to all travellers or to travellers who carry an amount of currency or BNIs, which exceed the threshold. See the Interpretative Note to FATF Recommendation 32.

[225] For example statistics about ML investigations and convictions. FATF Recommendation 33.

[226] Ann-Cheong Pang (n 320) 95.

[227] FATF Recommendation 34.

[228] General feedback may comprise:

1. Clear ML activity cases.
2. The numbers of STRs in relation to ML and the results of analysing the STRs, for example, what total percentage of STRs were received in a year and how many have been disseminated to the competent authority for investigation or prosecution.
3. Current trends, techniques and patterns in relation to ML.

Specific or case by case feedback could encompass:

this type of feedback since it has comprehensive knowledge and keeps statistics about STRs, which it has received from the reporting entities.[229] Hence, Recommendation 34 directly addresses national FIUs. Indeed, the FIU providing feedback to the reporting entities can be considered the fourth core function of the FIU since this increases the quality of the STR. This, in turn, also improves the analytical function of the FIU.

FIUs or any other competent authorities cannot properly perform their tasks unless they have adequate human, financial and technical resources. The employees should also possess a high degree of integrity. Each country is thus responsible for providing its competent authorities, including the FIU, with resources and employing the right kinds of employees. A country is also responsible for putting in place efficient procedures and mechanisms to ensure that a high level of cooperation and coordination exists amongst its own domestic authorities.[230] Hence, the FIU, LEAs and the reporting entities are working together in the same field and for one purpose, namely to prevent and detect ML. Apart from domestic cooperation, cooperation has also to exist at the international level, particularly when it comes to the exchange of information about STRs on ML with foreign FIUs.[231]

As mentioned above, the 2003 FATF Recommendation 26 and its Interpretative Note did not provide any in-depth details about the core

1. The result of analysing individual STRs and the decisions of the FIU on whether to disseminate it to the competent authority or the decision that there was no suspicious ML activity involved in the particular transaction.
2. Illustrating any deficiencies about the reported STR.

See FATF Reference Document, 'Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations' (n 372) 33.

[229] Paul Allan Schott (n 400) VII-23.

[230] FATF Recommendation 2.

[231] FATF Recommendation 40.

At the international level, the methodology adds that national FIUs should be legally entitled on behalf of foreign FIUs to undertake the following tasks:

1. Search its own databases, notably for information about STRs.
2. With direct or indirect access, search other databases, such as public databases, law enforcement databases and commercially available databases.

FATF Reference Document, 'Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations' (n 372) 46.

See also FATF Reference Document, 'Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems' (n 372) 86–89.

functions of an FIU, but instead noted its functions in broad terms.[232] There was no reference to the types of FIUs, either in Recommendation 26 or its Interpretative Note. The Recommendation has been revised and replaced by the 2012 FATF Recommendation 29 due to its lack of clarity. The Recommendation now provides that:

> Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.[233]

When comparing the aforementioned Recommendation with the 2003 FATF Recommendation 26, it can be clearly noted that Recommendation 29 has been formulated more accurately. It explains that the three core functions of an FIU are receiving STRs on ML and associated predicate offences, analysing them and then disseminating the results of the analysis. Moreover, it explicitly stresses that an FIU has to possess powers which enable it to obtain additional information legally about specific STR from the concerned reporting entity, in order to carry on its functions properly. However, neither the FATF Recommendation 29, nor its Interpretative Note, explicitly requires that the FIU stores all STRs which have ever been received from the reporting entities. In practice, the FIUs do store STRs, but the international standards should explicitly require it. This procedure is crucial and assists the FIU to discharge its analytical function, as it can extract results from previous STRs which can assist in establishing a causal relationship between an existing STR and previous STRs and thus identify a money launderer through a specific STR or highlight a common ML pattern in relation to particular STRs, which in turn can help with the promulgation of more robust requirements for the reporting entities in

[232] International Monetary Fund Handbook (n 384) 91.

[233] FATF Recommendation 29.

relation to specific transactions.[234] Therefore, the FATF Recommendation 29 and its Interpretative Notes should be amended to require a FIU to store all STRs. Moreover, the Recommendation 29 should stress the role of a FIU to participate in improving national AML controls and regulations where the FIU is the best place in doing so, as it analyses all STRs.

The Interpretative Note to FATF Recommendation 29

More importantly, the Interpretative Note to the Recommendation provides a comprehensive explanation and clarifies the role of the FIU from different perspectives.[235]

Firstly, it stresses that Recommendation 29 equally applies to all FIUs in the world, irrespective of their models, and also that, in all cases, its operation has to be independent and autonomous. An FIU has to be free from any unjustified interference/influence, whether it is political, governmental, or industrial, in order to avoid prejudicing its operational independence.[236] Secondly, the Interpretative Note illustrates the core functions of FIUs. In addition to receiving all STRs, under the national legislation, an FIU has to be the national agency for receiving other types of information, such as cash transaction reports (CTRs) and the declarations/disclosure system. After receiving STRs and other required information, an FIU must analyse the reports which consists of "operational and strategic analysis," although the Interpretative Note makes no reference to the term "tactical analysis." This is maybe due to the fact that FATF Recommendation 29 explicitly grants an authority to the FIU to require additional information in the course of analysing STRs. However, the term "tactical analysis" should be included explicitly in the Recommendation, and should be emphasised, since this is the core element of the analytical function. The analytical function fulfils a vital role since, through carrying out this function, the FIU decides whether to

[234] It is worth noting that the CCA 2013 explicitly requires the NCA to store STRs received from the reporting entities, as analysed in Chap. 9. This is unlike the UAE AML system, which does not require that the AMLSCU stores the STRs.

[235] Interpretative Note to FATF Recommendation 29.

[236] Interpretative Note to FATF Recommendation 29.

disseminate an STR file and the results of an analysis to the competent authority for "spontaneous dissemination" or not.[237] The FIU should also be able to provide, upon request, all information, which is held by it, to the requesting competent authority.[238]

Thirdly, in order to undertake its proper analysis, the Interpretative Note explains that the FIU must possess the legal authority to obtain additional information from all reporting entities and must be able to access information from other sources, for example public sources or information which is held by other authorities.[239] Besides these powers, security and confidentiality rules should be in place, which govern and control the FIU and the information which is held by it, its usage, and storage and transmission procedures.[240] An FIU's staff must be aware of their responsibilities when dealing with such sensitive information.

Fourthly, the employees of the FIU must display high professional standards, should possess adequate qualifications, integrity and the necessary skills, so that the functions and responsibilities of the FIU can be properly discharged.[241] This is particularly important since the FIU is the sole national agency specialised in receiving, analysing and disseminating STRs and other systems such as CTRs.[242]

Lastly, it is suggested that countries should assess the possibility and utility of adopting a CTRs system. Under such a system, banks and other financial institutions, which are situated in a particular country, have to report any cash transaction, whether nominated in domestic or international currency, if they are in excess of a fixed amount. Countries are not obliged to adopt this reporting system, but the Interpretative Note suggests that they should evaluate the feasibility of adopting it. Dependent on its own conditions, each country has the right to set its reporting threshold. For example if a country adopts 20,000 as a

[237] If it is concluded that there is no suspicion of ML activity involved in the particular STR.

[238] FATF Recommendation 31.

[239] This is unlike the AMLSCU in the UAE, which does not have the legal authority to request additional information, as critically analysed in Chaps. 5 and 6.

[240] Interpretative Note to FATF Recommendation 29.

[241] Ibid.

[242] In addition, the Interpretative Note emphasises the importance of international cooperation, for example the "Egmont Group Statement of Purpose" and also the information exchange between FIUs at the international level. The Interpretative Notes also call FIUs to apply for membership in the Egmont Group.

reporting threshold, this means that the concerned bank or financial institution has to report any cash transaction in excess of this amount to the national central agency in that country. However, other cash transactions could also be subjected to the reporting system, even if they are below the reporting threshold. For example, if the amount of the cash transaction is 19,900, the transaction can still be subjected to the reporting system since it may be likely that the client is trying to escape from the reporting conditions or a transaction has been divided.[243]

Conclusion

There is no one particular model which is optimal for all times and places. The choice of the FIU model depends on several factors, which depend on the situation of a country, that is the political, legal and judicial system. A particular model could be suitable for a country for a specific period of time, but may no longer be suitable when circumstances change. However, irrespective of the model, the FIU has to fulfil certain core functions when dealing with STRs, namely receiving, analysing and disseminating.

The FATF Recommendations are of paramount importance so that an FIU can counteract ML. The 2003 FATF Recommendation 26 has been replaced by the 2012 FATF Recommendation 29, which further illustrates and explains the core functions of an FIU, its responsibilities, duties and powers concerning combating ML. This was necessary since the FIU in any country plays such a vital role in counteracting this type of crime because it analyses STRs on ML and thereby filters STRs and other reporting systems, such as CTRs received from reporting entities. Since, upon the analytical function, an FIU decides whether to disseminate an STR file and the results of the analysis to the competent authority for "spontaneous dissemination" or not.

Thus, the FATF Recommendations, especially Recommendations 29 and its Interpretative Note, have given great attention to the FIU and its core functions and responsibilities in counteracting ML. They have further illustrated the analytical function and that it also comprises

[243] Paul Allan Schott (n 400) VI-24 & VI-25.

operational and strategic analysis. The Interpretative Note to Recommendation 29 does not employ the term "tactical analysis," although it stresses that the FIU must have legal authority to obtain additional information from all reporting entities and to access information from other sources, such as public sources and information held by other authorities. The term "tactical analysis" should be explicitly included in the Recommendation and it should be emphasised that this type of analysis constitutes the core element of the analytical function. In addition, neither the FATF Recommendation 29, nor its Interpretative Note, explicitly requires the FIU to store all STRs which have ever been received from the reporting entities. However, the Recommendation should explicitly require this, as it enhances the FIU's analytical function.

Recommendation 34 requires the competent authority, notably FIUs, to provide feedback and guidelines to reporting entities with a view to increasing their effective role in combating ML. The FIU should further furnish entities with practical information about how to avoid sending any deficient STRs in the future since it is ideally placed to provide such feedback. As mentioned in Recommendation 29, an FIU is a "national centre," which assists the government with combating ML. One of the FIU's contributions, in AML at the national level, is to provide reporting entities with valuable feedback in order to assist them in conducting their functions, especially ensuring that STRs are transmitted without any deficiencies. The functions of the reporting entities would not be further developed if there is no such feedback loop.

On the other hand, neither the FATF Recommendations nor their Interpretative Notes set out or explain other non-core functions of an FIU, for example conducting research, despite the fact that these non-core functions can also play an important role when it comes to counteracting ML and are therefore of no less importance than the core functions. These functions can also assist an FIU with developing its own core functions. Furthermore, despite the FATF Recommendations and their Interpretative Note emphasising that financial institutions have to provide ongoing training programmes for their employees,[244] the FATF Recommendations or their Interpretative Note contain no provisions

[244] Interpretative Note to FATF Recommendation 18.

about this. However, a regular training programme for staff of the FIU constitutes one of the most crucial elements for increasing the quality and to ensure that tasks are properly carried out.

After having examined the FIU in terms of its nature, types, aims and functions in relation to the fight against ML from the perspective of international requirements, are the UAE FIU current powers sufficient to enable it to deal with STRs efficiently? What are the negative aspects in relation to its current functions? These are the questions which will be analysed in the following two chapters.

5

The Emergence of the UAE FIU in Counteracting ML

Introduction

This chapter focuses on how the legal system of the UAE combats ML, with the particular purpose of evaluating the role which the UAE's FIU plays through dealing with STRs received from the reporting entities. The powers granted to it are also critically assessed. Section "How the Legal System of the UAE Combats ML" examines the UAE's legal system in relation to counteracting ML. In this section, the requirements, which are imposed on banks and other reporting entities, in respect of detecting and preventing ML, are evaluated. These requirements are set out in regulations and circulars, which are issued by the supervisory and regulatory authorities, for instance the Central Bank. However, some of these requirements are still vague, for instance the meaning of CDD. In this section I also critically analyse the different ML definitions in the FLMLC 2002 and the CBR 24/2000 and the practical consequences of having different definitions for ML.

Section "The UAE FIU's Role and Powers in the Fight Against ML" focuses on the role which the UAE FIU plays in the fight against ML and its powers to achieve this objective. Its core and non-core functions

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_5

are critically evaluated, along with how independent the FIU is and the relationship it has with the reporting entities and the LEAs. More importantly, I analyse the difference between the FLMLC 2002, which adopts a subjective basis, and the CBR 24/2000, which adopts an objective basis, for triggering the duty to submit an STR and the serious legal consequences this has.

The reason for starting the chapter with the regulations and circulars is that the obligations contained in them have to be taken into account by banks and other financial institutions before STRs are submitted to the UAE FIU. The implementation of these obligations by financial institutions assists them in making the right decisions in relation to the submission of STRs to the UAE FIU. In other words, compliance with the STRs regime under the FLMLC 2002 necessarily firstly entails adopting the relevant obligations under such regulations and circulars.

How the Legal System of the UAE Combats ML

This section is divided into two subsections. The first discusses which regulations and circulars are promulgated by the Central Bank and other relevant public authorities in order to spell out the important functions and duties of financial institutions and other entities in order to combat ML. In the second subsection I analyse the principal offences of ML and the duties which public authorities have to discharge in order to counteract ML and which are set out in the FLMLC 2002.[1]

[1] It is important to stress that, prior to enacting the FLMLC 2002, the UAE Penal Code 1987 contains an Article which possibly criminalises ML activities. Article 407 states that:

> Whoever acquires or conceals property derived from crime, with full awareness of that, without necessarily being involved in its commitment, shall be subject to the penalty assigned for that crime, from which he knows the property has emanated.
>
> In case the perpetrator is not aware that the property is derived from a crime, but has acquired it in circumstances, which indicate its unlawful sources, the penalty would then be imprisonment for a period not exceeding six months and a fine not exceeding AED5000 or either of the two penalties.

It can be clearly seen that the term "ML" was not explicitly mentioned in the text of the Article, nevertheless, the first paragraph could be understood as criminalising ML because it contains broad terms, such as "property derived from crime." Moreover, the Article covers two forms of ML which

Regulations and Circulars of the UAE

General Background

The banking industry in the UAE is supervised by the UAE Central Bank which plays a vital role. Quality standards for the banking sector have been developed through supervision[2] by the Central Bank, which was itself established in 1980 pursuant to Union Law No. 10 of 1980 Concerning the Central Bank, the Monetary System and Organisation of Banking.[3] The main office is based in Abu Dhabi, but there are also five further branches in five cities.[4] It is divided into three main sections: Banking Operations, Accounts and Administrative Affairs.[5]

---

are possession and concealment of criminal property and does not cover other forms, such as disguising or transferring property. More importantly, prior to enacting the FLMLC 2002, no ML case had been transferred to the court under this Article. Nevertheless, a number of cases have been referred to the court in other circumstances. For example, the first paragraph of the Article was evoked where the perpetrator concealed a mobile phone which was acquired from theft by another perpetrator; whilst the second paragraph was applied in the case of a person buying a very cheap mobile phone from another person.

See Hani Ghattas, 'United Arab Emirates' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 1049 at 1050.

[2] Ashruff Jamall, 'Gulf Cooperation Council' in Andrew Clark and Peter Burrell (eds), *A Practitioner's Guide to International Money Laundering Law and Regulation* (City & Financial Publishing 2003), 665 at 722.

[3] The Union Law No. 10 of 1980 is available on the UAE Central Bank website at: www.centralbank.ae/en/index.php (accessed on 30th January 2014).

[4] Dubai, Sharjah, Ras Al Khaimah, Fujairah and Al Ain.

[5] The UAE's Central Bank consists of seven departments, which are the Banking Supervision and Examination Department (BSED), Banking Operations, Research and Statistics, Administrative Affairs, Financial Control, the Treasury and Internal Audit. It also has seven sections: IT, Personnel, Correspondent Banking, Public Relations, General Secretariat and Legal Affairs, UAE SWITCH and the Governor's Office Division. There are also the following seven units: the AMLSCU, IT Projects Unit, the Strategy Unit, the Legislative Development Unit, the Banking and Monetary Statistics Unit, the Financial Stability Unit and the Benchmarking Unit. It also has a Risk Bureau. The BSED is responsible for the integrity of the financial institutions, such as local banks, money exchange bureaus, financial investment companies and financial consultancies, branches and representative offices of foreign banks, brokers dealing in shares and financial instruments and finance companies. The AMLSCU will be critically analysed in section "The UAE FIU's Role and Powers in the Fight Against ML".

For further information about the organisation of the UAE Central Bank, its department and units, see http://www.centralbank.ae/en/index.php?option=com_content&view=article&id=147&Itemid=109 (accessed on 30th January 2015).

The financial sector in the UAE is divided into entities operating in the domestic market and entities licensed to carry out business in the financial free zone located in the Dubai International Financial Centre (DIFC)[6] and the Dubai Multi Commodities Centre (DMCC);[7] however, the FLMLC 2002 is applicable in the domestic sector, as well as in the financial free zone.[8] The regulatory authorities are responsible for supervision and compliance and issue regulations which have to be implemented by all affected stakeholders. The Central Bank is responsible for banks, finance companies and money exchange bureaus in the domestic sector, while the ESCA is responsible for security brokers. The Insurance Authority is responsible for insurance companies, while the Dubai Financial Services Authority (DFSA)[9] is responsible for financial services providers in the DIFC.[10]

The Bank is the main body which issues policies and measures governing AML and which supervises how the financial sector implements its polices and measures. It is therefore responsible for overseeing the majority of the institutions in the financial sector. Under Article 11 of the FLMLC 2002, authorities which deal with the licensing and supervision of "financial institutions"[11] or "other financial, commercial and economic establishments"[12] have to create appropriate mechanisms in order to ensure that these institutions comply with AML rules and regulations and the requirements of STRs.

[6] See www.difc.ae (accessed on 4th February 2015).

[7] See www.dmcc.ae (accessed on 4th February 2015).

[8] Under Article 3 (2) of Federal Law 8/2004 regarding the Financial Free Zones, all federal laws are applicable in the Financial Free Zones except federal civil and commercial laws.

[9] See www.dfsa.ae (accessed on 4th February 2015).

[10] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF on 20 June 2008, 10.

[11] The term "financial institutions" has been defined in Article 1 of the FLMLC 2002 as "any bank, financing company, money exchange house, a financial and monetary broker or any other establishment licensed by the Central Bank whether publically or privately owned."

[12] The term "other financial, commercial and economic establishments" has been defined in Article 1 of the FLMLC 2002 as "establishments licensed and supervised by agencies other than the Central Bank such as insurance companies, bourses and others."

The next section deals with the regulations and circulars which are issued by the Central Bank and other relevant public authorities which have a licensing, supervisory or regulatory character.

UAE CBR 24/2000 and Its Addendum 2922/2008

As mentioned above, the Central Bank is the most important supervisory authority for financial institutions in the UAE and ensures that financial institutions adhere to AML controls.[13] The most important regulation, which the Bank has issued to combat ML, is the Regulation Concerning Procedures for AML No. 24 of 2000 (CBR 24/2000)[14] and its Addendum 2922/2008.[15] Regulation 24/2000 was initially adopted in order to implement the Forty FATF Recommendations into domestic law. The Addendum 2922/2008 was adopted in order to close certain loopholes, which had been identified in the UAE MER concerning its AML system and combating the financing of terrorism (CFT) and which criticised the AML controls in a number of respects, for example, in relation to CDD and ECDD, the meaning of beneficial ownership and the basis of STRs.[16] The Addendum 2922/2008 contains additional measures to counteract ML and also amends and adds a number of Articles to Regulation 24/2000. The regulation is addressed to "all banks, money exchange bureaus, finance companies and other financial institutions operating in the country, as well as their Board Members and employees"[17] and which the Central Bank has licensed and supervises. The regulation is also applicable to "branches and subsidiaries of UAE incorporated financial institutions operating within foreign jurisdictions which do not apply any such procedures or fewer procedures."[18]

---

[13] Graham Lovett and Charles Barwick, 'United Arab Emirates' in Wouter H. Muller, Christian H. Kalin and John G. Goldsworth (eds), *Anti-Money Laundering*: *International Law and Practice* (John Wiley & Sons Ltd., Chichester 2007), 643 at 650.

[14] CBR 24/2000 was issued on 14 November 2000 and became effective on 1 December 2000.

[15] Addendum 2922/2008 was issued on 17 June 2008 and entered into force with immediate effect.

[16] For more details about the criticism, see "The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528).

[17] Article 2 of CBR 24/2000.

[18] Ibid.

Before the regulations and their various elements are examined, it is important to understand how CBR 24/2000 defines ML since this definition will be later compared with the ML definition in the FLMLC 2002. CBR 24/2000 defines ML as:

> Any transaction aimed at concealing/or changing the identity of illegally obtained money, so that it appears to have originated from legitimate sources, where in fact it has not.
>
> This definition includes monies that are destined to finance terrorism or criminal acts.[19]

The regulation addresses four core aspects: CDD, record keeping, staff training and STRs. The last element will be critically analysed in Section "The UAE FIU's Role and Powers in the Fight Against ML", whilst the first three elements are evaluated below.

Regulation 24/2000 does not employ the term "CDD," but instead it appeared for the first time in the Addendum 2922/2008, especially in Topic 2 in relation to ongoing due diligence. More importantly, neither Regulation 24/2000 nor its Addendum 2922/2008 defines the term "CDD."[20] Nevertheless, CDD procedures can be divided into two main types under Regulation 24/2000[21] and its Addendum 2922/2008, namely standard CDD and ECDD procedures. There is also ongoing CDD.

Standard CDD procedures apply to two fields: bank accounts and wire transfers.

Bank Accounts

All banks have to obtain certain documents when opening an account for an individual, legal persons and associations. Firstly, in order to open

[19] Article 1 of CBR 24/2000.

[20] The meaning of the term "CDD" will be further analysed in Chap. 7.

[21] Circular No. 14/93 was issued by the Central Bank on 20 June 1993 and was directed to all banks in relation to returned unpaid cheques, current accounts, saving accounts and call accounts. It came into force on 1 September 1993 and required all banks to obtain certain documents for accounts, though Regulation 24/2000 reinforces Circular 14/93 and expanded the scope of obligations in terms of the entities which perform such obligations and added additional requirements.

an account for an individual, banks have to obtain documents which state the full name of the account holder, the place of his or her work and his or her current address.[22] Secondly, in order to open an account for a legal person, the bank has to obtain the name and address from all account holders and partners. The bank has also to retain permanently a copy of a valid trade licence[23] in the bank's records and has to obtain any copy of a new trade licence and also register the renewal date.[24] Lastly, for associations,[25] the bank cannot open an account without obtaining an original certificate signed by the Minister of Social Affairs, confirming the identities and permitting the association to open a bank account.[26]

CBR 24/2000 was criticised by the UAE MER[27] since the regulation did not explicitly require that banks and other financial institutions had to identify the beneficial ownership of companies or to understand the ownership and control structure of the customer. For that reason, Addendum 2922/2008 requires all banks and other financial institutions to identify carefully the ownership and control structure of all legal entities.[28]

---

[22] Banks also have to retain a copy of the individual's passport, after physically checking the original passport, and a competent account opening officer has to initial the copy as being a "true copy of original" Article 3 (1) of CBR 24/2000.

[23] A trade licence is granted to a legal person, by administrative authorities in the UAE, to permit the practice of commercial business. Federal Law No. 18 of 1993 on Commercial Transactions governs the requirements of such trade licences and all aspects in relation to commercial business.

[24] The bank has also to keep the names and addresses of shareholders whose shareholdings exceed 5 % of the concerned company's shares in cases where the legal persons are publicly sharing companies. Article 3 (1) of CBR 24/2000.

[25] The term "associations" has been clarified by CBR 24/2000 which means cooperative, charitable, social, or professional societies.

[26] Article 3 (2) of CBR 24/2000.

In addition, other financial institutions, under Article 3 (4) of CBR 24/2000, have to comply with all the above obligations when they "receive money from their customers to manage investment accounts or from pooled investment accounts." Article 3 (3) emphasises that all information about account holders must be up to date and all banks have to know the account holder's name, as stated in the passport or in the trade licence in the case of a legal person. This is because banks are precluded from opening accounts with assumed names or numbers: Article 4 of CBR 24/2000.

[27] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 61.

[28] Furthermore, every person has to show that he has appropriate legal authority in order to be able to act on behalf of another person. Pursuant to Addendum 2922/2008, all banks and other financial institutions have to recognise beneficial owners and obtain satisfactory evidence about the identity in respect of companies, as well as in relation to businesses, which are opening accounts or which are transferring money. Topic 1 of Addendum 2922/2008.

Wire Transfers

The term "wire transfer" was not explicitly included in the text of Regulation 24/2000, but was mentioned for the very first time in Addendum 2922/2008. However, Regulation 24/2000 requires that banks carefully and systematically identify any person, who is a non-account holder, and who wishes to pay by cash for transfers/drafts of AED40,000 or equivalent sums in other currencies[29] or more. In such a case, identification means obtaining the customer's name, full address of the beneficiary and the physical checking of the customer's actual identification. All information has also to be entered on a particular form. The same requirements are applicable to money exchange bureaus in case the value of the transaction reaches AED2000[30] or an equivalent sum in another currency or more.[31]

This provision was criticised by the UAE MER because of the big gap between the threshold for money exchange bureaus (AED2000)[32] and the threshold for banks (AED40,000).[33] The FATF requirement is considerably lower than the threshold for banks. Hence, there is a big gap between the threshold for banks (AED40,000, which is approximately USD11,000) and the FATF threshold requirement (which is USD1000).[34] For that reason, the threshold for banks has been reduced by Addendum

[29] Which is about £6900.

[30] Which is about £345.

[31] Article 5 (1) of CBR 24/2000.

In addition, the UAE Central Bank issued Notice No. 1815/2001 on 3 October 2001 in relation to outgoing transfers. The Notice immediately requires all money exchange bureaus in the UAE to record details of individuals and institutions who/which transfer an amount of AED2000 or more to complete a specific form provided by the Central Bank. The details have to be confirmed through physically checking the passport, the UAE ID Card for UAE Nationals, the Labour Card for non-UAE Nationals or the UAE driving licence. The phone number has also to be recorded. A copy of cheques or travellers cheques has to be retained by the money exchange bureau in case the transfer is made through one of them.

[32] Which is about £345.

[33] Which is about £6900.

'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 75.

[34] The 2012 FATF Recommendation 16 and its Interpretative Note replaced the 2001 FATF Special Recommendation VII; however, the threshold has remained the same.

2922/2008 from AED40,000 to AED3500[35] or any equivalent sum in another currency or more in order to comply with the FATF requirement and also to reduce the gap between the threshold amount for banks and the threshold amount for money exchange bureaus. Moreover, the amendment resulted in two further important developments. Firstly, the term "wire transfers" was mentioned for the very first time. Secondly, the regulation requires banks and money exchange bureaus to have in place "effective risk based procedures" in order to identify and handle the transfers in such cases[36] in relation to inward transfers, especially where the originator's information in relation to these transfers is insufficient. However, Addendum 2922/2008 does not clarify the meaning of the term "effective risk based procedures" and also does not provide any examples for cases where there is a "lack in complete originator information."[37]

Regulation 24/2000 alerted banks and other financial institutions to areas where they could be vulnerable when it comes to ML activities, for example, cash transactions, customer accounts, international banking and financial transactions,[38] though Regulation 24/2000 did not mention the term "ECDD" and did not require that these procedures had to be adopted.[39] ECDD procedures were mentioned in Addendum 2922/2008 and thus have to be applied in relation to three specific fields, namely (1)

[35] Which is about £600.

[36] Topic 3 of Addendum 2922/2008 which amended Article 5 (1) of Regulation 24/2000. It should be noted that the threshold for money exchange bureaus has remained at AED2000.

[37] A further obligation requires banks and money exchange bureaus to complete a specific form, namely form No. (CB9/9000/2), and to retain it in a special file in case of receipt of a transfer/draft which is for AED40,000 (about £6900) or more and is to be paid to a non-account holder in cash or in travellers cheques. Article 5 (2) of CBR 24/2000.

However, all banks and money exchange bureaus are required to verify the identification of the customer and have to adopt the above-mentioned procedures in case they suspect ML, even if the relevant amount is less than AED40,000. Simplified CDD can only be adopted where the threshold is less than AED3500 (about £600) for banks and less than AED2000 (about £345) for money exchange bureaus. Banks and money exchange bureaus are then not required to adopt any of the above mentioned requirements. Although Regulation 24/2000 and its Addendum 2922/2008 did not mention this for transfers via banks, it has been impliedly mentioned for transfers in relation to money exchange bureaus.

The Central Bank Notice 1815/2001 stipulates that money exchange bureaus should provide the transferor with a receipt if the amount of the transfer is less than AED2000. (n 550).

[38] Articles 8–14 of CBR 24/2000.

[39] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 62.

foreign politically exposed persons (FPEPs), (2) correspondent banks and (3) businesses and individuals.

FPEPs

In addition to standard CDD procedures, all banks and other financial institutions have to obtain written approval from senior management in cases where they open accounts for FPEPs.[40] Under Addendum 2922/2008, any senior official, who works in the executive, legislative, administrative, military, or judicial branches of a foreign government, will be considered an FPEP, as well as his or her "immediate family members" and "close associates."[41] However, Addendum 2922/2008 does not provide a definition or spell out its constituent elements, neither does it define the term "immediate family members" nor the term "close associates,"[42] and this leads to uncertainties for banks and other financial institutions.

Correspondent Banks

Apart from standard CDD, banks and other financial institutions are obliged to fulfil two main commitments when any of them enters into a cross-border correspondent banking relationship.[43] Firstly, before entering into any such relationship, they have to obtain approval from senior management of the concerned financial institution. This approval has to be in writing. Secondly, they have to conduct research, from publicly available information, about the status of the concerned correspondent bank, such

[40] This obligation necessitates that the financial institutions have controls in place in order to be able to recognise whether an existing customer, the beneficial owner, or even a potential customer is a FPEP.

[41] Topic 4 (a) of Addendum 2922/2008.

[42] While the MLRs 2007 of the UK contain a clear definition and state the components for those two terms; see (n 832) of Chap. 7.

[43] Nevertheless, no obligation was imposed on banks and other financial institutions in the UAE in this regard. Moreover, Regulation 24/2000 did not mention the term "correspondent banks." See "The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism" (n 528) 62.

as its reputation, business and quality of supervision that it is subject to and whether it has been subjected to any ML or TF investigation.[44]

Businesses and Individuals

Banks and other financial institutions are required to apply ECDD in relation to specific businesses and individuals, namely (1) private banking customers, (2) non-resident account holders, (3) dealers in luxury merchandise, (4) dealers in precious metals and stones, (5) dealers in real estate and (6) auction houses.[45] No specific/enhanced measures are contained in the regulation in relation to the aforementioned cases. Instead, the regulation stipulates that "more strict CDD procedures"[46] have to be applied, though without clarifying which procedures. The regulation should impose strict procedures and also apply them in the above cases since, without clarifying these procedures, this requirement is useless.

Ongoing CDD

Regulation 24/2000 does not state that banks have a duty to undertake ongoing CDD and must adopt appropriate procedures. The Regulation also does not require banks and other financial institutions to obtain information about the intended nature of the business relationship at the start.[47] Nevertheless, Addendum 2922/2008 reformed this area and all banks and other financial institutions are now required to obtain information in cases of doubt and they also have to adopt ongoing CDD to maintain the business relationship. Moreover, all banks have to identify

[44] Banks and other financial institutions are further required to pay great attention in cases where the correspondent bank has got its headquarters in a country which is reported to be involved in high level public corruption or criminal activities, such as drug trafficking. In addition, banks and other financial institutions in the UAE are required to have adequate internal controls in place to appreciate and identify the purpose behind opening an account, the concerned correspondent bank's ownership and its management structure and customers and third parties who are going to use the account. Institutions have also to observe transactions which are conducted via the account. Topic 4 (b) of Addendum 2922/2008.

[45] Topic 4 (c) of Addendum 2922/2008.

[46] Ibid.

[47] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 61.

the purpose and the intended nature of the business relationship from the outset when the banker–customer relationship commences.[48] In addition, Addendum 2922/2008 briefly defines ongoing CDD as "another round of CDD procedures [which] should be undertaken."[49] As mentioned above, although the term "CDD" is mentioned for the very first time in Addendum 2922/2008, there is no clear definition, and the constituent elements of the term are also not clarified.[50] Indeed, without the term and its constituent elements being defined, there is disparity amongst the reporting entities about how to adopt measures to prevent and detect ML.

Record and File Keeping

The main reason for the requirement of record and file keeping is to ensure that the basic information about the account holder can be provided by banks and other financial institutions in case these are requested by the competent authorities,[51] such as the UAE FIU. Banks and financial institutions are thus required to establish a system for file keeping, so that they can respond without delay to the request from the relevant authorities. Accordingly, all correspondence, statements and notes about transactions should be kept in special files.[52]

---

[48] Topic 2 of Addendum 2922/2008 states that banks are required also to conduct CDD procedures which were opened prior to the issuing of CBR 24/2000 on 14 November 2000.

[49] Ibid.

[50] Banks and other financial institutions are also precluded from entering directly or indirectly into relationships with "shell banks and companies." Pursuant to topic 5 of Addendum 2922/2008, the term means that such institutions have no physical presence, although Regulation 24/2000 does not mention the prohibition. See 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 88.

[51] Article 18 (1) of CBR 24/2000.

[52] Article 18 (2) of CBR 24/2000.

The regulation also requires, under Article 19 of CBR 24/2000, that other information is maintained, such as a copy of the passport of the individual, a copy of the trade licence for institutions, information about the origin of funds for money transfers, the destination of funds for transfers via accounts and information about whether funds are deposited or withdrawn by cash or cheques. All of these records have to be maintained and made available to the Central Bank investigators at least for five years and documents, which are required to open accounts, have also to be kept for five years after the account is closed. Article 22 of CBR 24/2000.

Staff Training

The "compliance officer"[53] in a bank or any other financial institution is the person who is responsible for training employees who handle cash, supervise accounts or prepare reports or are dealing with any aspects relating to ML.[54] The Central Bank is the entity which is responsible for directing banks and other financial institutions in relation to training methods concerning counteracting ML. It also runs workshops for employees of banks and other financial institutions.[55]

A bank or any other financial institution will be penalised in case it fails to comply with any or all of the obligations and requirements mentioned above.[56] Although Addendum 2922/2008 does not clarify such sanctions or penalties, it does state that such penalties are "in accordance with the prevailing laws and regulations."[57] There are no sanctions or financial penalties in cases where reporting entities, such as banks, fail to comply with the aforementioned requirements. This renders the requirements useless in practice since these entities are aware that there are no sanctions when they do not adhere to the requirements.

Other Relevant Regulations and Circulars

This section outlines regulations in relation to counteracting ML from other regulatory authorities, such as ESCA and the Insurance Authority.

---

[53] The "compliance officer" is responsible for STRs in banks and other financial institutions. This is equivalent to the "nominated officer", who is responsible for SARs in banks and other financial institutions in the UK.

[54] Article 17 of CBR 24/2000.

[55] Ibid.

[56] Topic 11 of Addendum 2922/2008.

[57] Ibid.

ESCA[58] Regulation Concerning AML and CFT and Its Amendment

ESCA Regulation 17/2010 concerning AML and CFT was issued on 16 March 2010[59] and its amendment 40/2011 was issued on 27 October 2011. This regulation consists of 34 Articles and applies to markets, companies and institutions, which are licensed by the ESCA and to members of its boards of directors and employees.[60] The regulation contains definitions, for example, for ML, beneficial ownership, suspicious transactions and unusual transactions.[61] The amendment makes clear that the term "unusual transaction" covers any transaction that a customer attempts to implement and there are reasonable grounds to consider it to be dubious due to its nature.[62] The regulation requires that certain documents have to be obtained and retained by companies or institutions for both normal and nominal persons.[63] It is proscribed to open an account or to carry out a deal or a transaction with pseudonyms for both natural and nominal persons.[64] A "compliance officer" who is responsible for STRs, must be appointed by the markets, companies and institutions.[65] The regulation also contains examples of what could be considered a suspicious transaction, on reasonable grounds, and explains that this encompasses cash deposits, but also transactions traded in securities or commodities and which have to be immediately notified to the UAE FIU.[66] More importantly, the regulation

[58] See www.sca.ae/english (accessed on 15th February 2015).

[59] ESCA Regulation 17/2010 replaces the Circular issued by the Authority's Board of Directors on 18 February 2004. It and its amended version are available online on SECA's website mentioned above.

[60] The regulation also applies to all branches of companies and institutions which are located outside the UAE if the countries where such branches are located do not apply the requirements contained in the resolutions or apply fewer of them. Article 2 of ESCA Regulation 17/2010.

[61] Article 1 of ESCA Regulation 17/2010 and its amendment.
The definition of ML contained in the ESCA Regulation is the same as in FLMLC 2002.

[62] Ibid.

[63] Articles 3 and 15 of ESCA Regulation 17/2010.

[64] Article 4 of ESCA Regulation 17/2010.

[65] Article 12 of ESCA Regulation 17/2010.

[66] Article 9 of ESCA Regulation 17/2010 and its amendment.
Companies and institutions, licensed by the ESCA, are required by Article 7 to record a cash deposit in a specific form when its value reaches AED40,000 or more, or even less than this amount in cases of suspicions about ML.

adopts "suspicion on reasonable grounds" [67] as a basis for submitting STRs to the UAE FIU.[68] However, FLMLC 2002 adopts actual knowledge as a basis for submitting STRs. This inconsistency in relation to STRs has serious legal consequences, which will also be critically evaluated.

Insurance Authority Regulation 1/2009 Regarding AML and CFT in Insurance Activities[69]

The regulation comprises 20 Articles, which apply to all insurance companies established in the UAE and foreign companies in the UAE, and which are licensed to undertake insurance activities, as well as cooperative insurance and reinsurance companies, and also applies to all professionals associated with insurance activities.[70] The regulation also applies to companies and professions associated with insurance activities and which are licensed to operate in the financial free zones.[71] More importantly, the regulation adopts "suspicion" [72] or "unusual transactions" as a basis for submitting STRs to the UAE FIU.[73] However, FLMLC 2002 adopts actual knowledge as a basis for submitting STRs. This inconsistency in relation to STRs has serious legal consequences.

Unlike CBR 24/2000 and its Addendum 2922/2008 and ESCA Regulation 17/2010, the main feature of Regulation 1/2009 is that the compliance officer of insurance companies and professions associated with insurance activities has to be a UAE national and has to carry out a fitness test in order to be permitted to carry out his or her functions.[74] Indeed, the requirement about the nationality of the

---

[67] The term "suspicious on reasonable grounds" will be analysed in Chap. 8.

[68] Article 1 of ESCA Regulation 17/2010.

[69] Insurance Authority Regulation 1/2009 issued on 4 November 2009 and replaces the Circular issued by the Ministry of Economy on 6 January 2002 on AML procedures.

The definition of ML contained in the Articles 1 and 2 of Insurance Authority Regulation 1/2009 is the same as in the FLMLC 2002.

[70] Article 3 (1)(2) of Insurance Authority Regulation 1/2009.

[71] Article 3 (3) of Insurance Authority Regulation 1/2009.

[72] The term "suspicion" will be critically analysed in Chap. 7.

[73] Article 8 of Insurance Authority Regulation 1/2009.

[74] Moreover, Article 9 of Insurance Authority Regulation 1/2009 provides that employees, who receive training from a compliance officer in insurance companies, must be subjected to the same

compliance officer is unique. The STRs contain sensitive information about a customer and the person who deals with STRs should possess a high level of integrity and honesty. The nationality requirement thus provides additional assurance about the integrity of the compliance officer. Therefore, it is arguable that CBR 24/2000 and the ESCA Regulations should contain the same requirement about the nationality of the compliance officer.

The regulation also gives examples of areas in the insurance sector which could be vulnerable to ML activities more than others, such as life insurance and marine insurance.[75] For instance, life insurance in a large amount and pay such amount in a single payment in advance. Furthermore, insurance in a large amount in a way inconsistent with the available information on the insured or his/her wealth in the UAE.[76] These two examples raise suspicion on the origin of the paid amount whether it's emanated from legal activity or from criminal activity.

---

fitness test and have to receive training about regulations and which has also to include practical aspects. In addition, the regulation also provides that a number of documents have to be obtained and retained by insurance companies and cooperative insurance companies in certain situations. Articles 11, 14 and 15 of Insurance Authority Regulation 1/2009.

[75] Article 12 of Insurance Authority Regulation 1/2009.

[76] Ibid.

In addition to the regulations mentioned above, there are a number of further regulations, such as the DIFC Non-Financial AML/Anti-Terrorist Financing (ATF) Regulations and the DMCC AML/ATF Policy. DIFC Regulations entered into force on 18 July 2007, available online at: http://www.difc.ae/sites/default/files/DIFC_Non_Financial_AML_CFT_Regulations.pdf (accessed on 8th February 2014).

The DMCC AML/ATF policy is available online at: http://www.dmcc.ae/jltauthority/wp-content/uploads/2011/07/G-02-AML-CFT-PP-20-September-2010.pdf (accessed on 8th February 2014).

Article 1 (1) of the DIFC Regulations provides that the regulations apply to DNFBFs, such as real estate agents, lawyers and notaries working within the jurisdiction of DIFC. The DMCC AML/ATF Policy applies to all DMCC staff, its members and affiliates and its subsidiary companies and divisions. For further information in relation to the DIFC AML/ATF Regulations and the DMCC AML/ATF Policy, see Hani Ghattas (n 519) 1069–1072.

Moreover, there are a number of AML Circulars, which are issued by the Ministry of Justice about AML requirements and which apply to notaries in UAE courts and lawyers, namely Ministry of Justice Circulars 1/2008 and 8/2010 and Ministry of Justice Circulars 30/2008 and 9/2010. AML Circular Reference: 3/1/st/at/319 on 16 July 2002, which is issued by the Ministry of Economics, is directed to all auditors, persons or firms, irrespective of their nationality. These Circulars, including the Ministry of Justice Circulars mentioned above, are available on the Central Bank's website at: http://www.centralbank.ae/en/index.php?option=com_content&view=article&id=75&Itemid=95 (accessed on 8th February 2015).

UAE FLMLC 2002

This section analyses the main provisions which are contained in FLMLC 2002.[77] Three elements will be analysed: firstly the definition of ML and its scope of implementation under the FLMLC 2002; secondly, the ML offences, which are contained in the FLMLC 2002; and thirdly, the powers of government entities, which are contained in the FLMLC 2002.

Definition and Scope of ML

FLMLC 2002 defines ML as:

> Every act involving conveyance, transfer or depositing of property or concealment or disguise of the true nature of said property attained from any of the offences provided for in Clause 2 of Article 2 of this Law.[78]

For the purpose of applying this definition, the term "property" means any kinds of asset whether movable or fixed, corporeal or incorporeal, including instruments or documents which provide "title to assets or any right pertaining thereto."[79] In addition, there is a condition for property to be included in the scope of the definition where "property" constitutes "proceeds"[80] emanating from one of the closed list offences in Article 2 (2) of FLMLC 2002.[81]

---

[77] FLMLC 2002 entered into force on 22 January 2002.

[78] Article 1 of FLMLC 2002.

[79] Ibid.

[80] Article 1 of FLMLC 2002 defines the term of "proceeds" as "every property directly or indirectly obtained through commission of any of the offences provided for in Clause 2 of Article 2 hereof."

[81] These offences are:

A: Narcotics and psychotropic substances.
B: Kidnapping, piracy and terrorism.
C: Offences committed in violation of the provisions of Environmental Law.
D: Illicit dealing in fire-arms and ammunition.
E: Bribery, embezzlement and damage to public property.
F: Deceit, breach of trust and related offences.
G: Any other related offences provided for in international treaties to which the State is a party. Article 2 (2) of FLMLC 2002.

These offences constitute predicate offences for ML. Two main observations can be made about the definition of ML and its predicate offences. Firstly, the definition is different from the definition provided in CBR 24/2000.[82] The variation causes ambiguity and uncertainty for reporting entities,[83] notably banks, because CBR 24/2000 adds to the second part of the definition of ML that "this definition includes monies that are destined to finance terrorism or criminal acts."[84] The FLMLC 2002 does not have such an addition and this causes confusion for financial institutions, which perform STRs requirements. The definition of ML, contained in CBR 24/2000, covers money intended for financing terrorism or criminal acts. This means that even money from legitimate business, but which is used for financing terrorism or criminal acts, is covered by the definition. However, such an interpretation could confuse reporting entities and courts since FLMLC 2002 provides that money/property must emanate from one or more of the predicate offences for ML listed in the Act. Yet, the definition of ML in FLMLC 2002 does not cover cases where money is derived from legitimate business, but is used to finance terrorism or criminal acts.

For example, when a compliance officer in a bank studies an STR with a view to considering whether to submit it to the UAE FIU, it is unclear which definition of ML he or she should consider. Is it the definition in FLMLC 2002 or the one in CBR 24/2000? The latter definition conflicts with the former definition. This is clearly evidenced when money, which is derived from legitimate business, is used to finance terrorism. This case falls within the definition of ML under CBR 24/2000. However, it is not considered ML under FLMLC 2002, which requires that money has to be derived from one of the criminal activities (predicate offences), which are listed in the Act. Accordingly, no criminal liability arises in such a case and the judge cannot convict a person. Hence, the two definitions, namely the definitions in CBR 24/2000 and FLMLC 2002 must be harmonised

[82] Article 1 of CBR 24/2000 (n 538).

[83] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism'(n 528) 11.

[84] Article 1 of CBR 24/2000.

in order to eliminate any differences. The definition of CBR 24/2000 must be amended in order to be compatible with the definition in FLMLC 2002.[85]

The second observation is that, at first glance, FLMLC 2002 makes no reference to theft as a predicate offence for ML; nevertheless the expression "and related offences"[86] could open the door to it.[87] Furthermore, the predicate offences set forth in FLMLC 2002 do not meet FATF standards[88] since FLMLC 2002 only currently covers six out of the 2003 FATF's 20 "designated categories of offences." Now, pursuant to the 2012 FATF Recommendations, the number of these offences has increased to 21 after tax crimes have been added.[89]

ML Offences

FLMLC 2002 introduced three types of offences in relation to ML, namely principal offences, failing to report an ML case and the tipping off offences.

[85] This is the same definition of ML as in ESCA Regulation 17/2010 and Insurance Authority Regulation 1/2009, which are both compatible with the definition in FLMLC 2002 (n 580 and 588).

It is worth noting that no previous research has analysed the definition and the variation was therefore not identified, nor the practical consequences.

[86] Mentioned in (f) (n 600).

[87] Graham Lovett and Charles Barwick (n 531) 650.

[88] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 9.

[89] See Chap. 4 (n 320).

Under FLMLC 2002, ML can be committed either by individuals or by legal persons. It accordingly imposes criminal liability upon financial institutions if they commit any ML activities contained in Article 2 (1), irrespective of whether the acts are in their own names or in the name of account holders. Article 3 of FLMLC 2002.

Furthermore, all information about offences listed in FLMLC 2002 and which are obtained by entities are considered confidential. The information must not be divulged except to the extent necessary for the purpose of investigations, legal action or cases relating to a violation of FLMLC 2002. Article 12 of FLMLC 2002.

The Principal Offences in Relation to ML

FLMLC 2002 establishes three principal offences for ML and which are committed by an individual/legal person who perpetrates or assists with one of the following three acts:

1. Transfer, conveyance or depositing the proceeds in order to conceal or disguise their illegal source.
2. Disguising or concealing the proceeds in terms of their source, nature, location, movement, disposition, ownership or pertinent rights.
3. Acquisition, possession or usage of the proceeds.[90]

Furthermore, the condition that the proceeds in relation to any of the three acts have to have been obtained from any of the predicate offences mentioned above.[91] Otherwise, the commission of the act would not be considered an ML offence; nevertheless, it could constitute a different offence under the UAE Penal Code 1987.

There is no definition for the terms "concealment" or "disguise" contained in FLMLC 2002, nor has any judicial interpretation been provided. However, a number of examples will be provided in Chap. 7 when the UK system is being considered.

The Offence of Failing to Report an ML Case

This offence is committed when reporting entities fail to submit STRs on ML. Article 15 of FLMLC 2002[92] spells out the basis for submitting STRs and makes clear that it applies to chairmen, members of boards of directors, managers and employees of banks and other financial institu-

[90] Article 2 (1) of the FLMLC 2002.

[91] See (n 600).

[92] Article 15 of the FLMLC 2002 states that:

> Chairman, members of Boards of Directors, managers and employees of financial institutions and other financial, commercial and economic establishments who have known but refrained from notifying the unit provided for in Article 7 of this Law of any act that occurred in their institutions and was related to the money laundering offence, shall be punished with imprisonment or with a fine not exceeding Dhs. 100,000 and not less than Dhs. 10,000 or with both punishments.

tions if they do not inform the FIU about an act at their institution, which is related to an ML offence.

The offence depends on fulfilling one requirement, namely that the person charged must have actual knowledge, "who have known,"[93] that an ML offence has occurred in his or her institution. Accordingly, the offence cannot be committed on a mere negligence basis.[94]

A number of significant observations can be made in relation to this offence. Firstly, the offence is applied to individuals who work in banks and other financial institutions, hence any persons outside these entities, who have actual knowledge about the occurrence of an ML offence in any other entity, will not be subject to this provision.[95]

Secondly, FLMLC 2002 does not require that the information or matters, on which the employee's knowledge is based or which give reasonable grounds for suspicion, must have come to him in the course of his work in the banks or other reporting entities in general.[96] Accordingly, if the information/matters came to him outside his work, the employee will commit the offence of failing to report, if indeed he failed to do so, since it is the same whether the information/matters came to him in the course of his work or outside of it. For example, if during a private social event, a banker received information from his friend that the bank account of customer A contains proceeds derived from drug trafficking, the banker has to investigate the account and determine whether or not to submit an STR to the AMLSCU. A failure to do so would result in criminal responsibility. This result widens the scope of STRs, so that it becomes difficult to determine its scope. The requirement must be confined to information or matters about which the employee has knowledge or which give him reasonable grounds for suspicion during the course of his business.

---

[93] Ibid.

[94] The penalties for the offence are imprisonment or a fine between AED10,000 (about £1725) and AED100,000 (about £17,245) or both. Article 15 of FLMLC 2002 does not mention the period of imprisonment; however, pursuant to the general rule contained in Article 69 of the UAE Penal Code 1987, the term "imprisonment" must not be less than one month and not more than three years, unless the law provides another period.

[95] They rather will be subject to Article 274 of the UAE Penal Code 1987 which provides that any person who has known that a crime occurred and did not inform the competent authorities shall be punished with a fine not exceeding AED1000 (about £150).

[96] This is unlike UK AML law, which requires this, as shown in Chap. 8.

Thirdly, the offence cannot be committed on a mere negligence basis which means that if a person, who works in a bank or other financial institution, suspects or has reasonable grounds to suspect that an ML offence occurred in his or her institution and does not inform the FIU, he or she would not commit the offence since FLMLC 2002 states that it only applies to the persons "who have known."[97] Thus, the absence of the term "suspect"[98] or "reasonable grounds to suspect"[99] may not assist banks and other reporting entities in detecting STRs effectively. However, the basis of submitting STRs under FLMLC 2002 is subjective, whilst under CBR 24/2000 it is objective. This variation for submitting STRs causes ambiguity for the reporting entities, especially the banking sector, and this is what has been confirmed in interviews with this sector in the following chapter.[100]

Lastly, there is no specific offence for the compliance officer if he or she has been informed by any employee in his institution that the ML offence has been committed through the institution and he or she did not report this to the FIU. This is despite the compliance officer (further discussed below) being responsible for informing the FIU about ML cases. It is true that his or her job, amongst other things, is to evaluate STRs, which are received from employees, and to decide, based on his or her experience, whether or not to report an STR to the FIU. The issue is that there is no specific offence if he or she has been informed by an employee of his institution that an ML offence has been committed through the institution and he or she does not respond and report this to the FIU. Such a case is different from STRs which he or she has an authority to evaluate; instead such a case is rather about actual knowledge that the institution has used for the purpose of ML.

Article 15 of FLMLC 2002 provides the legal basis for submitting STRs to the UAE FIU and which is considered a lawful and required disclosure. However, there can be unlawful and prohibited disclosures, which will be critically evaluated below.

---

[97] Article 15 of FLMLC 2002.

[98] The term "suspicion" is analysed in Chap. 7.

[99] The term "reasonable grounds to suspect" is analysed in Chap. 8.

[100] One banker confirmed that the basis of STRs is objective, whilst another banker stated that it is both objective and subjective.

The Tipping Off Offences

These offences apply to individuals who work in banks and other financial institutions. FLMLC 2002 contains two kinds of tipping off offences. Firstly, the tipping off offence in relation to ML disclosure and which occurs when a person informs another that his or her transaction is being checked for potential ML activity.[101] Secondly, the tipping off offence in relation to an ML investigation, which occurs if a person informs another that his or her transaction is being investigated by the competent authorities because of the possibility of his involvement in ML activity.[102]

The two provisions are formulated in narrow terms and only cover circumstances where the disclosure is made to the person undertaking the transaction, which is checked or under investigation. This means that there is no offence if the person informs a third party, who is related to or associated with the person undertaking the transaction, that the transaction is being checked or investigated for potential ML.[103] The absence of the term "third party" in the above provision may result in the person undertaking the transaction, knowing that through a "third party"[104] his or her transaction is being checked or investigated for potential ML. Therefore, no criminal liability will be imposed in such a case.

---

[101] Article 16 of FLMLC 2002.

[102] Ibid.

A person who is being charged for either offence may be imprisoned for not more than one year or can be fined between AED5000 (about £865) and AED50,000 (about £8,620), or both. Article 16 of FLMLC 2002.

[103] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 80.

This is unlike UK AML law, which requires this, as shown in Chap. 8.

[104] Article 17 of FLMLC 2002 imposes a further offence if a person reports in bad faith to the competent authorities that an ML offence has been committed by another person, in order to cause damage to another person. He or she will be punished with a maximum the punishment defined as "false notification offence." The latter offence is provided for in Article 276 of the UAE Penal Code 1987. In addition, Article 20 of FLMLC 2002 provides good faith immunity for "financial institutions" and "other financial, commercial and economic establishments" and members of their boards of directors, their legally authorised representatives and employees from criminal, civil and administrative responsibility "which may result from providing required information or from breaking any restriction imposed by legislative, contractual, regulatory, or administrative text for ensuring confidentiality of information."

Conflict with CBR 24/2000

Some of the provisions contained in CBR 24/2000 are possibly inconsistent with the above provision. The reporting entity, after reporting to the FIU, is required to inform the customer of the Central Bank's action and has to request the customer to provide documents and information in order to prove that the transaction is lawful.[105] Hence, on the one hand there is an obligation contained in FLMLC 2002 to avoid tipping off, whilst on the other hand the text in CBR 24/2000 requires the reporting entity to request documents from the customer in order to show that the particular transaction is lawful. This requirement results in the customer being alerted to the fact that his or her transaction is being treated as suspicious.[106] Article 15 (6) of CBR 24/2000 must be amended in order to remove the conflict with Article 16 of FLMLC 2002.

Powers of Government Entities Contained in FLMLC 2002

This part deals with a number of powers, which government entities possess as a result of the provisions in FLMLC 2002. A discussion of these powers is essential for two reasons. Firstly, the powers, contained in FLMLC 2002, provide the general legal basis for the government entities to deal with AML and STRs in particular. Secondly, and more importantly, a critical assessment of the powers of the government entities is important in order to provide recommendations in Chap. 10, particularly in order to strengthen the relationship between the LEAs and the UAE FIU. This, in turn, improves the functions of the UAE FIU to deal with STRs, especially regarding its analytical function.

Firstly, authorities, which license and supervise[107] banks and other financial institutions, can create appropriate mechanisms in order to ensure that these institutions comply with AML rules and regulations and the requirements of STRs.[108]

---

[105] Article 15 (6) of CBR 24/2000.

[106] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 80.

[107] Such as the Central Bank, ESCA, as mentioned above.

[108] Article 11 of FLMLC 2002.

Secondly, FLMLC 2002 allows the UAE Central Bank to pass Regulations.[109] For example, one regulation requires travellers, who carry cash amounts in excess of a fixed amount, which is set by the Central Bank, to notify them of this. Accordingly, CBR 24/2000 requires travellers to make declarations when they enter or leave the UAE if they carry cash and monetary/financial bearer instruments.[110]

Thirdly, the Central Bank has the right to "freeze"[111] the suspected property with financial institutions up to seven days. Public prosecutors have got the same right in relation to suspected property, proceeds or "instruments."[112] The competent court has the same right but can freeze assets for an unlimited period.[113] Whilst FLMLC 2002 stipulates the period for freezing assets for the Central Bank and an unlimited period for competent courts, it does not spell out the period for public prosecutors. It also does not set out what procedures apply at the end of the seven days in relation to the assets, which have been frozen by the Central Bank. However, CBR 24/2000 states that if the supervisory authority in the transfer country did not respond within the seven days, the Central Bank should take the decision to lift the

[109] Article 6 of FLMLC 2002.

[110] This regulation was issued on 9 January 2011 and entered into force on 1 September2011. It requires a traveller upon entering or leaving the UAE to make a declaration on the appropriate form, stating whether he or she carries cash and/or bearer instruments of a value exceeding AED100,000 (about £17,245) or the equivalent sum thereof in another currency and/or monetary/financial bearer instruments. In addition, the regulation imposes a number of obligations on customs officials at airports, seaports and border crossings. See Regulations regarding the declaration by travellers entering or leaving the UAE carrying cash or monitory/financial bearer instruments.

It should be noted that the previous threshold of the declaration system was AED40,000 and was applied only to travellers entering the UAE.

The threshold contained in the regulation exceeds that contained in the Interpretative Note to FATF Recommendation 32 which provides that the maximum threshold is USD/EUR15,000 (which is equivalent to AED52,500). See Chap. 4 (n 498).

[111] The term "freezing or seizure" has been defined in Article 1 of FLMLC 2002 as "temporary prohibition on conveyance, transfer, disposition, or movement of property according to an order issued by the competent authority."

[112] Article 1 of FLMLC 2002 defines the term "Instruments" as "anything used or intended to be used in any manner in the commission of any of the offences provided for in Clause 2 of Article 2 of this Law."

[113] Article 4 of FLMLC 2002. In addition, Article 5 (2) of the same Act provides that the Central Bank is the sole entity which executes decisions pertaining to seizure of and provisional attachment on property with financial institutions.

freeze.[114] Uncertainty exists in relation to transfers between accounts within the UAE. Chapter 10 provides recommendations to deal with the issue surrounding the periods of freezing suspected transaction(s), the proper authority specialised in issuing the freezing decision and the consequent procedures.

Fourthly, FLMLC 2002 requires the Minister of Finance and Industry to establish the National Anti-Money Laundering Committee (NAMLC) with the governor of the Central Bank being the chairman governor and representatives of seven entities.[115] The NAMLC has the responsibility for proposing AML regulations and controls in the UAE, facilitating information exchange between parties represented therein, representing the state on international forums in relation to AML and any other issues referred to it by the competent authorities.[116] It can be seen that FLMLC 2002 does not require representative(s) from the FIU; nevertheless, it requires a representative(s) from the Central Bank, which does not necessarily mean being a representative(s) of the FIU; however, the FIU is part of the Central Bank, as will be seen in the next section. Moreover, when considering the duties of the NAMLC, the term "any other matters referred to it by the competent authorities of the State"[117] causes confusion since FLMLC 2002 does not define the terms "matters" and "competent authorities." Since its inception, the NAMLC has only issued one Circular about financial remittances and which is directed at both nationals and residents in the UAE.[118]

---

[114] Article 15 (6) of CBR 24/2000.

[115] These entities are (1) the Central Bank, (2) the Ministry of Interior, (3) the Ministry of Justice, (4) the Ministry of Finance and Industry, (5) the Ministry of Economics, (6) Authorities responsible for issuing trade and industrial licences and (7) the State Custom Board. Article 9 of FLMLC 2002.

[116] Article 10 of FLMLC 2002.

[117] Ibid.

[118] Cautionary Notice Regarding Financial Remittances issued on 10 December 2001. Available on the Central Bank's website at: http://www.centralbank.ae/en/pdf/amlscu/CautionaryNotice-2001.pdf (accessed on 8th February 2015).

Chater 10 of this book provides recommendations to deal with improving the effectiveness of the NAMLC in AML at the national level and its role to assist constructively the UAE FIU in its functions.

Lastly, FLMLC 2002 requires the creation of an FIU, which is responsible for STRs, and which will be critically analysed in the following section.[119]

The UAE FIU's Role and Powers in the Fight Against ML

This section critically analyses the role of the UAE's FIU to deal with STRs. The relevant requirements in CBR 24/2000 and the provisions contained in FLMLC 2002 will be evaluated. The section is therefore divided into two parts. The first part evaluates CBR 24/2000 in relation to STR requirements and procedures, as they are directly associated with the functions of the UAE FIU, whilst the second section critically analyses the provisions, which are contained in FLMLC 2002, in relation to the role and functions of the UAE FIU to deal with the AML process and particularly STRs.

CBR 24/2000 in Relation to STR Requirements and Procedures

Investigators of the Central Bank firstly observe, when they conduct examinations of banks, whether the movements in some accounts are proportionate to the income of a number of individual or financial entities. This practice started as a result of Circular 163/98,[120] which was issued by the Central Bank and applies to all customer accounts held by all banks, irrespective of whether they are local or foreign and which are established in the UAE. The Circular requires banks to inform the Central Bank immediately in two cases. Firstly, where substantial funds are transferred into the customer's account without any justification. Secondly, if the account holder continuously deposits medium/large cash

[119] Articles 21 and 22 of FLMLC 2002 deal with international cooperation in relation to AML.

[120] This Circular was issued on 28 February 1998, available online on the UAE Central Bank website mentioned above.

amounts or cheques, which could suggest that he or she is conducting the management of funds.[121] However, the Circular does not clarify the term "medium/large cash amounts" and also does not spell out which procedures should be used in order to inform the Central Bank; it is also silent on the penalty for failing to comply with these obligations.[122]

At a later stage, detailed provisions about STR requirements and procedures were adopted under CBR 24/2000, as well as its Addendum 2922/2008. The regulation specifies four elements, namely appointment of a compliance officer, requirements for reporting STRs about ML, tipping off and penalties in cases of a failure to comply with the requirements.

Appointment of a Compliance Officer

All banks and other financial institutions are required to appoint a compliance officer. This officer, amongst other issues, is responsible for submitting STRs to the UAE FIU, training staff in his or her institution, as well as periodically ensuring that internal controls in his or her institution operate sufficiently and comply with AML regulations.[123]

Moreover, Addendum 2922/2008 clarifies and adds a number of additional requirements for financial institutions in order to improve the function of compliance officers. Firstly, the compliance officer must undergo a "fit and proper" test, along with all employees who work in areas relevant to AML.[124] However, the Addendum does not provide any explanation about the quality or the elements of such a test. Secondly, a periodic and independent audit function must be adopted in relation to the compliance officer's duties.[125] Thirdly, the training courses about practical aspects must be provided for the employees, who work in areas relevant to AML/STRs.[126] The duties for financial institutions are thus

[121] Ibid.
[122] Graham Lovett and Charles Barwick (n 531) 651.
[123] Article 16 (3) of CBR 24/2000.
[124] Topic 10 of Addendum 2922/2008.
[125] Ibid.
[126] Ibid.

spelt out by Addendum 2922/2008 after the UAE MER pointed out that the compliance officers' duties were unclear.[127] Nevertheless, the Addendum does not state which qualifications a compliance officer has to have or even indicate what level of experience is necessary. Instead, it states that all banks and other financial institutions are responsible for providing periodic training courses for their compliance officers and relevant employees. It does not clarify whether these training courses must be provided on an annual or semi-annual basis. More importantly, there are no sanctions/financial penalties contained in the Addendum for not providing these training courses. Hence, banks and other reporting entities do not take this requirement seriously[128] since there are no financial penalties.

More importantly, under CBR 24/2000, a compliance officer and the relevant employees in the financial institution have to attend training courses about STRs/AML, which are run by the Central Bank.[129] However, it is not clarified whether these training courses must be held on an annual or semi-annual basis.[130] In addition, there are no sanctions for banks or other financial institutions when their compliance officer and relevant employees do not attend these training courses. Indeed, a compliance officer and relevant employees can benefit from these training courses if the AMLSCU's (UAE FIU's) staff were to provide these courses, as they have more knowledge about STRs requirements. This would improve the quality of future STRs.

In addition, unlike the Insurance Authority Regulation 1/2009, the Addendum 2922/2008 does not require the compliance officer to be a UAE national, despite such a requirement being essential since the compliance officer deals with highly sensitive information, transactions and controls.

---

[127] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 87.

[128] This is what has been confirmed in the interviews with the banking sector in the UAE. See Chap. 6.

[129] Article 17 of CBR 24/2000.

[130] This is what has been confirmed in the interviews with the banking sector in the UAE where the bankers stated that these training courses are held irregularly. See Chap. 6.

STR Reporting Requirements and Procedures

All banks and other financial institutions, including their Board Members, managers and employees have to report cases if there are reasonable grounds for suspicion that the funds are derived from criminal activity or are going to be used for TF to the Head of AMLSCU.[131] The report can be made manually or via an "On-Line Reporting System.".[132]

The regulation does mention the expression "ML;" however, it mentions "a criminal activity," which is a predicate offence for ML and is listed in the above mentioned FLMLC 2002.[133] The expression "reasonable grounds to suspect" does not mean actual knowledge, so that a "reasonable grounds to suspect" is sufficient. However, there is no judicial interpretation for the terms "reasonable grounds" and "suspicious" in relation to ML cases. As a result, Addendum 2922/2008 adopts an "objective test" for the basis of suspicion in ML cases.[134] In contrast, FLMLC 2002 adopts a "subjective" basis. The serious legal consequence of this conflict will be critically analysed later. The regulation also does not mention the case when persons in financial institutions know that funds stem from criminal activity. The expression "actual knowledge" could be adopted for the purpose of the regulation; however, it would be better if the term "actual knowledge" were explicitly included in the regulation, especially since FLMLC 2002 makes express reference to it.[135]

---

[131] Topic 6 of Addendum 2922/2008 amended Article 16 (1) of CBR 24/2000. Form (CB9/200/6) for the submission of STRs is attached to the CBR 24/2000. The FIU in the UAE Central Bank is called AMLSCU.

[132] Except in cases of suspicious transactions relating to terrorism, terrorist organisations or terrorist purposes. In these cases the reporting of STRs must be immediately in writing to the AMLSCU and the concerned financial institution must freeze the transaction/account: Article 16 (5) of CBR 24/2000.

[133] See (n 600).

[134] In fact, the amendment was made because of the lack of clarity. On one hand, there was the term "unusual transaction" contained in Article 16 (1) of CBR 24/2000, on the other hand, the term "suspected transactions" was used in Article 16 (2) of the same regulation. This difference led to a lack of clarity in relation to how to judge a suspicion, i.e. whether it is a "subjective" or "objective test" or both. For more details, see 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 87–89.

[135] Article 15 of FLMLC 2002 (n 611).

The regulations do not require that the information or matters on which the employee's knowledge is based, or which give reasonable grounds for suspicion, must have come to him in the course of his work in the banks or other financial institutions.[136] Nor do they require the reporting entities to make a decision whether or not to submit an STR to the AMLSCU within a specific time from when reasonable grounds for suspicion arose.[137] The absence of this requirement leads to decisions about submitting or not submitting an STR to the AMLSCU being different between the reporting entities, notably banks.[138]

Banks and other financial institutions have also to examine the background of any "unusual transaction" and its purpose, and document their findings.[139] This requirement has even to be adhered to when an examination has led to the decision not to report a case as suspicious to the AMLSCU.[140] These findings must be kept by the financial institution for at least five years.[141] Indeed, the regulations do not contain any guidance and also do not define the term "unusual transaction," so that "reasonable grounds to suspect" could also arise where there are some doubts or where there is a vague feeling of unease or some other subjective feeling.

The obligation of reporting STRs to the AMLSCU is not limited to actual transactions, but also relates to attempted transactions.[142] This is in contrast to FLMLC 2002 which obliges the reporting of STRs just in case of actual transaction.[143] Hence, no criminal liability will be imposed

---

[136] This is compatible with the provision in Article 15 of FLMLC 2002, which does not require this.

[137] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 39.

This is unlike UK AML law, which requires that this is done as soon as is practicable, as shown in Chap. 8.

[138] This is what has been confirmed in the interviews with the banking sector in the UAE. Whilst it only takes up to one week in bank D, it takes one month in bank E. See Chap. 6. Chapter 10 provides recommendations to deal with this dilemma.

[139] Topic 8 of Addendum 2922/2008.

[140] Ibid.

[141] Ibid.

[142] Topic 7 of Addendum 2922/2008 introduces the obligation since no reference had been made to "attempted transactions" in CBR 24/2000. For further information, see 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 79.

[143] Article 15 of FLMLC 2002 (n 611).

if a compliance officer did not submit an STR about an attempted transaction, even though the regulation requires that a submission should be made.[144] This is because FLMLC 2002 only imposes criminal liability for failing to submit an STR about an actual transaction.[145]

The Prohibition of Tipping Off

This prohibition was added in Addendum 2922/2008 after the UAE MER indicated that there was no tipping off offence in relation to third parties or other persons than the one undertaking the transaction (as discussed above). The regulation thus proscribes banks and other financial institutions from tipping off any person, including the customer, that his or her transactions are being scrutinised for potential ML.[146]

However, the provision may conflict with another regulation (mentioned above),[147] which requires that the concerned customer provides documents in order to prove that the funds are lawful. This requirement definitely alerts the concerned customer to the fact that his or her transaction is being treated as suspicious. The provision conflicts further with the provisions pertaining to criminal liability contained in FLMLC 2002 and which will be critically evaluated in the following part.

Penalties in Case of a Failure to Comply with the Requirements

The regulation stipulates that any bank or other financial institution will be subject to penalties as contained in prevailing laws and regulations if a bank or financial institution fails to comply with the procedures outlined in CBR 24/2000 and its Addendum 2922/2008.[148]

---

[144] Topic 7 of Addendum 2922/2008.

[145] Article 15 of FLMLC 2002 (n 611).

[146] Topic 9 of Addendum 2922/2008.

[147] Article 15 (6) of CBR 24/2000 (n 624).

[148] Topic 11 of Addendum 2922/2008.

Significant Results

For the purpose of criminalising ML, the expression "prevailing laws," contained in CBR 24/2000 and its Addendum 2922/2008,[149] refers to FLMLC 2002. Nonetheless, we can make three significant observations here.

The Basis of STRs

The regulation obliges all banks and other financial institutions, including their board members, managers and employees, to submit STRs about ML to the AMLSCU if there are reasonable grounds for suspicion that the funds are derived from criminal activity.[150] On the other hand, FLMLC 2002 imposes criminal liability on persons simply for "having known" that the funds are derived from criminal activity and for refraining to report it;[151] it does not criminalise persons in cases where they only have "reasonable grounds to suspect." Thus, the regulations address "reasonable grounds to suspect," whilst FLMLC 2002 addresses actual knowledge.[152] In other words, under FLMLC 2002, the basis for submitting STRs is subjective, whilst under CBR 24/2000 it is objective.[153] Accordingly, no criminal liability will be imposed if a compliance officer did not fulfil the requirement in CBR 24/2000.

Criminal Liability in Tipping Off Cases

The regulation proscribes banks and other financial institutions from tipping off any person, including the customer, that his or her transactions are being scrutinised for potential ML.[154] However, FLMLC 2002 does not impose criminal liability for tipping off another person other

[149] Ibid.

[150] Topic 6 of Addendum 2922/2008 (n 650).

[151] Article 15 of FLMLC 2002 (n 611).

[152] The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 79.

[153] The term "subjective basis" will be examined in Chap. 7 and the term "objective basis" will be analysed in Chap. 8.

[154] Topic 9 of Addendum 2922/2008 (n 665).

than the concerned customer. As a result, the prohibition of tipping off in CBR 24/2000 is useless in practice. This is because criminal liability under FLMLC 2002 will only be imposed in case the customer, who undertakes the transaction, is tipped off.[155]

No Power to Impose Financial Penalties

The Central Bank has no legal power to impose financial penalties on banks or other financial institutions in case they breach AML/STR requirements.[156] Indeed, the Central Bank and all supervisory/regulatory authorities, such as ESCA in the UAE, should be able to impose financial penalties on relevant reporting entities which do not adopt internal AML procedures and which fail to adhere to the SARs requirements set out in FLMLC 2002 and other regulations, such as CDD, ECDD, record keeping and appointing a compliance officer. This would ensure that all reporting entities fully appreciate that they will be subject to a penalty(ies), if they do not discharge their duties. This would also require supervisory/regulatory authorities to examine regularly the reporting entities' internal AML/STRs procedures with a view to ensuring that they keep abreast of the latest AML/STRs requirements.

The Legal Framework of the AMLSCU to Combat ML

Articles 7 and 8 of FLMLC 2002 deal with the establishment and the functions of the AMLSCU. FLMLC 2002 stipulates that the Financial Information Unit (FIU) should be established within the Central Bank.[157] The unit is responsible for receiving STRs from all reporting entities, such as banks and other financial institutions. The duties of the AMLSCU require "studying" STRs and then notifying the public prosecution to take necessary actions.[158] FLMLC 2002 further requires that the AMLSCU makes all its information available to

[155] Article 16 of FLMLC 2002.

[156] This is unlike the FCA in the UK, which can impose financial sanctions, as shown in Chap. 7.

[157] Article 7 of FLMLC 2002.

[158] Article 8 (1) of FLMLC 2002.

the LEAs[159] for them to be able to carry out further investigations.[160] Despite the lack of sources available to the AMLSCU, this subsection critically assesses its functions for dealing with AML, particularly STRs, its independence from the UAE Central Bank, and its staff and training. This subsection is therefore essential to evaluate critically the functions of the AMLSCU within the STRs regime and the relationship which the AMLSCU has with the reporting entities and the LEAs.

The AMLSCU's Functions

As mentioned in the previous chapter, there are core and non-core functions for standard FIUs in the AML process.

The functions pertain to receiving, analysing and then disseminating STRs to the competent authority for further investigation or prosecution. Articles 7 and 8 of FLMLC 2002 state that the AMLSCU must receive STRs from the reporting entities[161] and must after "studying" the STRs notify them to the office of public prosecution, so that they can then take all of the necessary actions.[162] FLMLC 2002 does not mention the analytical function of the AMLSCU, but instead employs the expression "studying."[163] Apart from the above mentioned elements, FLMLC 2002 does not state anything further about the functions of AMLSCU in counteracting ML at the national level.

[159] The term "LEAs" is defined in Article 33 of the Federal Penal Procedures Code 35/1992 and its amendment 29/2005 and includes "Public Prosecutor's Office, police officers, border guard officials, airport officers, sea port and airport officers, civil defense officers, municipality inspectors, ministry of social affairs inspectors, health ministry inspectors and officials authorised to act as law enforcement officials according to laws, decrees and resolutions in force."

[160] In addition, Article 7 of FLMLC 2002 states that information can be exchanged with the UAE FIU's counterparts in other countries in accordance with international treaties and the principle of reciprocity. The UAE is the first of the Gulf countries which became a member of the Egmont Group in June 2002. The UAE is also a member of MENAFATF.

[161] Article 7 of FLMLC 2002.

[162] Article 8 (1) of FLMLC 2002.

[163] Ibid.

Receiving STRs

The CBR and other regulatory entities, such as ESCA and the Insurance Authority, contain the requirements and procedures which are imposed on reporting entities in relation to the transmission of STRs to the AMLSCU. However, it appears that there is a conflict between FLMLC 2002 and the regulations in relation to the form used for STRs. On the one hand, FLMLC 2002 stipulates that the NAMLC has the authority to design the form, which all reporting entities have to use, as well as the method for sending them to the AMLSCU.[164] On the other hand, CBR 24/2000 requires banks, finance companies, money exchange bureaus and other financial institutions to adopt a specific form attached to its regulation.[165] In addition, an ESCA Regulation requires all markets, companies and institutions, which are licensed by it, to adopt a specific form.[166] Hence, there is a lack of clarity as to whether reporting entities should adopt the NAMLC's form or the form of their particular regulatory authorities. More importantly, the NAMLC has not produced any STRs forms to date. The current practice by reporting entities to use the Central Bank and the ESCA STRs forms therefore conflicts with FLMLC 2002. This is because FLMLC 2002 is primary legislation and has thus priority over regulations issued by the Central Bank and ESCA.

Analysing STRs

FLMLC 2002 does not explicitly mention the term "analysing," but instead mentions the expression "studying"[167] without clarifying its meaning. Accordingly, the analytical function is vague in FLMLC 2002, although it forms the most important function of any FIU. Furthermore, FLMLC 2002 does not spell out which qualifications or experience the AMLSCU's staff should possess, despite them being responsible for conducting the "studying" function regarding STRs. The CBR also does not

[164] Article 7 of FLMLC 2002.

[165] (N 650).

[166] Article 8 of ESCA Regulation 17/2010 and its amendment.

[167] Article 8 (1) of FLMLC 2002.

provide information in this regard. The Central Bank is responsible for issuing AML regulations, which have to be adopted by the entities it supervises. Whilst the AMLSCU is not subjected to Central Bank supervision, it is nevertheless located in it. The UAE MER also mentions the AMLSCU analytical function and notes that, in practice, the letter represents the national centre for analysing STRs, although FLMLC 2002 does not explicitly authorise it to conduct such task.[168] The report further explains that the analytical process of the AMLSCU lacked a developed software analysing mechanism.[169] The analytical function was limited to a simple mechanism where staff could conduct a basic search in order to ascertain whether "both full name and near-name were matching," and this process was performed via a search of the AMLSCU database of STRs.[170] Indeed, it is pertinent that the AMLSCU adopts a sophisticated software analysing mechanism, notably in the light of the increasing number of STRs.

More importantly, no information is available about the nature and the components of the AMLSCU's analytical function. Even FLMLC 2002 does not add any useful elements. In the following chapter we therefore analyse the findings from interviews with employees from the AMLSCU in order to get information about the analytical function, which the AMLSCU fulfils, all with a view to assessing its function. In addition, the AMLSCU does not provide the reporting entities with bulletins and guidelines, despite this being important for increasing the quality and remedying deficiencies of STRs.[171] It is crucial that reporting entities are provided with guidelines for two main reasons. Firstly, this increases the quality of the submitted STRs. Secondly, and more importantly, this improves the analytical function of the AMLSCU since higher quality STRs are submitted by the reporting entities, which, in turn, makes it easier for the AMLSCU to fulfil its analytical function.

Banking supervision employees of the BSED used to conduct the analytical process of most STRs, despite them not being members of the

[168] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 38.

[169] Ibid 40.

[170] Ibid.

[171] This is unlike the UK FIU, which does so, as evaluated in Chap. 9.

AMLSCU.[172] This practice also raises doubts about the analytical skills and findings. The employees are not specialised in analysing STRs and do not have the required skills/experience to deal with them. This practice also highlights that the AMLSCU is not independent, as shown below.

Gaining Additional Information on STRs

Undoubtedly, gaining additional information from the reporting entity in relation to a specific STR is one of the essential mechanisms for properly conducting the analytical function. Nevertheless, FLMLC 2002 does not grant this power to the AMLSCU which negatively affects the quality of the analytical function. In contrast, LEAs might hold information which could be useful for the AMLSCU in analysing a specific STR. The AMLSCU does not have legal powers to order the LEAs to provide it with information, which could be helpful in relation to a specific STR which could assist the analytical process and thus increase the quality. Instead, FLMLC 2002 grants such power to the AMLSCU only in cases where an information exchange takes place with counterparts outside the country.[173] The AMLSCU should have the legal power to compel the reporting entities and the LEAs to furnish additional information since such a power positively enhances its analytical function.

Disseminating STRs

FLMLC 2002 states that the AMLSCU should, after studying the STRs, notify the public prosecutors to take the necessary actions.[174] It has also to make all information available, which it holds, so that the LEAs can undertake their investigation.[175] This means that the AMLSCU cannot disseminate information about STRs to any entity other than the

[172] It has been mentioned in the report that this practice had ceased. See 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 678) 41.

[173] Article 7 of the FLMLC 2002.

[174] Article 8 (1) of the FLMLC 2002.

[175] Article 7 of the FLMLC 2002.

LEAs.[176] However, the AMLSCU has disseminated information about STRs to the BSED and other supervisory agencies in order for them to follow up with the reporting entities.[177] This is despite these supervisory agencies not being an LEA. Hence, this is incompatible with the requirements contained in FLMLC 2002, which can raise doubts about the AMLSCU's independence.

The Absence of a Requirement to Store STRs

It is important to emphasise that FLMLC 2002 does not explicitly require the AMLSCU to store STRs, which are received from the reporting entities. However, such a procedure is crucial and assists the AMLSCU to discharge its analytical function since additional information can be obtained from old STRs, which could assist with identifying links between previous and current STRs and ML activity or recognising common ML patterns, which can then also lead to the promulgation of more robust requirements for the reporting entities for particular transactions. This is unlike the UK AML system and the CCA 2013, which explicitly require the NCA, the UK FIU, to store STRs which have been received from the reporting entities.

Statistics on STRs and the Role of the Compliance Officer

The information available about the number of received and disseminated STRs about ML are limited; however, in 2008 alone, 13,101 STRs about ML were reported to the AMLSCU.[178] Between June 2002 and May 2009, the AMLSCU received 80,592 STRs about ML from the reporting entities.[179] Despite this large number, only 285 STRs were transmitted

[176] For the meaning of the term "LEAs" in the UAE system, see (n 678).

[177] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 41.

[178] Sara Hamdan, 'Suspect funds on the rise' *The National*, Jun 23 2009, available online at: http://www.thenational.ae/business/banking/suspect-funds-on-the-rise (accessed on 19th February 2015).

[179] Ibid.

to the public prosecution office.[180] In light of the absence of justifications from the AMLSCU, it is crucial to stress that the reason behind the huge difference between the number received and the number transmitted to the Public Prosecution Office is open to several interpretations.

The discrepancy could be because the reporting entities have adopted a defensive approach.[181] For example, they may send all transactions cases which just appear "unusual" without taking into account any reasonable grounds for suspecting that there is ML. The reporting entities might adopt such an approach simply to ensure that they are safe and will not be subjected to the offences contained in FLMLC 2002.[182] The question then arises as to whether the current role of the compliance officers in the reporting entities is effective. Another issue is whether compliance officers have sufficient knowledge/experience to deal with STRs. This aspect recalls the fact that the AMLSCU must arrange training courses and workshops periodically for compliance officers at all reporting entities, instead of the Central Bank.

Another interpretation of the noticeable discrepancy between these two numbers is that the reporting entities do not clearly understand the basis of STRs. This could be because FLMLC 2002 requires "actual knowledge" that ML activity is involved in the transaction,[183] whilst CBR 24/2000 only requires "reasonable grounds to suspect."[184]

The large disparity between these two numbers could be attributed to the AMLSCU not having the legal power to obtain additional information from the reporting entities and the LEAs. The AMLSCU may therefore conclude that there is no evidence in the majority of STRs cases, not because it discharged its analytical function properly, but because it was unable to get additional information to undertake its function properly. In addition, as mentioned above, the AMLSCU does not provide the reporting entities with bulletins and guidelines with a view to ensuring

[180] Ibid.

[181] Jayesh D'Souza, *Terrorist financing, money laundering and tax evasion – Examining the performance of Financial Intelligence Unit* (Taylor & Francis Group, LLC 2012), 162.

[182] Article 15 of FLMLC 2002.

[183] Article 15 of the FLMLC 2002.

[184] Topic 6 of Addendum 2922/2008.

that the quality of their STRs is improved—which has not happened and has ultimately led to the large disparity.

Hence, the precise reason behind the large disparity between these two numbers is unclear. It is arguable that all the aforementioned reasons led to the large disparity. It is also noteworthy that the Public Prosecutions Office only sent 20, out of the 285 STRs which it received from the AMLSCU, to the courts. In addition, only 7 %, out of the 20 STRs resulted in an actual conviction.[185] These statistics on received/transmitted STRs and the large disparity between those received and transmitted by the AMLSCU require justification; in the following chapter therefore we will analyse how the AMLSCU and the Public Prosecution Office in the UAE have explained this disparity when being interviewed by the researcher.

Supporting Cases

The compliance officer of the banks or other reporting entities played no role. The cases were often commenced as a result of reports or because of judicial assistance requests from outside the UAE.

Case 1

In the case of *HSBC Bank v Other*,[186] the regional director of the Anti-Fraud section of the HSBC bank branch in Dubai Media City reported to the Dubai police that the HSBC bank in Bond Street, London, was exposed to a fraud. Gangsters had managed to steal a total amount of AED10,500,000[187] from the Malaysian Airline's bank account. They transferred the stolen funds into the bank accounts of the 11 defendants in three different banks in the UAE. On 18 June 2006 the Dubai Court, Criminal Division, convicted the defendants to one year imprisonment

[185] Alkaabi, Ali and others, 'A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA' [January 20, 2010] Finance and Corporate Governance Conference 2010 Paper 1, 8. Available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539843 (accessed on 13th November 2014).

[186] Dubai Court Judgment, Criminal Division, case No. 2901/2005.

[187] Which is about £1,810,345.

and fined each of them AED30,000[188] as they had acquired/transferred proceeds derived from a fraud offence contained in FLMLC 2002. The judgment mentioned the role of AMLSCU in verifying that the defendants had received the illegal proceeds in their bank accounts at three different banks in the UAE. The UAE Central Bank also managed to freeze half of the illegal proceeds, though the other half was dissipated by the defendants. The question arose as to what role the compliance officers had played in these three banks in the UAE. Why did they not manage to discover/suspect the illegal proceeds in the defendants' accounts? This ML case would not have been discovered if the regional director of the Anti-Fraud section at the HSBC bank branch in Dubai had not reported the case.

Case 2

Another case happened on 13 July 2007 when Dubai's Public Prosecution Office received a judicial assistance request No. 54/2007 from the Dutch judicial authority stating that the first defendant was a member of a criminal gang which was trafficking drugs in the Netherlands. The defendant laundered the funds and illegal proceeds by depositing them in his account at Bank E in Dubai. The judicial assistance request stated that the second defendant was an employee at Bank E and was assisting the first defendant in laundering the illegal proceeds. The second defendant was a director of the cards section of Bank E and she assisted the first defendant with opening his account at the bank. She also accepted the illegal funds in cash several times from the first defendant without asking him about the origin and the source of the funds. Through her assistance, the first defendant was able to transfer the illegal proceeds from his account to others outside the UAE, namely Thailand and Hong Kong, and to another account at a different bank in the UAE. The first defendant managed to launder more than AED20,000,000[189] through his account in Bank E. The second defendant, who was assisting him, received a commission of 1.5 % of the total amount of each transfer and

[188] Which is about £5175.

[189] Which is about £3,448,276.

earned in total AED300,000.[190] During the investigations, the Dubai Public Prosecution decided to form a committee composed of employees of the AMLSCU and the AML section of the Dubai Police. The mission of the committee was to provide the Dubai Public Prosecution with a report about the facts of the case and to inform about the first defendant's account movements. After receiving the report, the Dubai Public Prosecution sent the case file to the Court. On 12 May 2009, the Dubai Court, Criminal Division, convicted the first defendant to three years' imprisonment and imposed a fine of AED300,000 and fined the second defendant AED100,000[191] and also confiscated the funds, pursuant to FLMLC 2002.[192]

The question arises as to what the role was of the compliance officer at Bank E. Why did he not manage to discover/suspect that these huge amounts came from illegal proceeds? This ML case would not have been discovered if the Dubai Public Prosecution Office had not received the judicial assistance request from the Netherlands. Although the AMLSCU's and the Dubai Police's report assisted the judge to reach the decision, the report was only made after the judicial assistance request was received from Holland. This is because at that time there was no compliance officer role at Bank E, just as in Case 1.

The Absence of the Compliance Officers' Role

The above two cases clearly confirm that the compliance officers played no role in detecting STRs at their banks. There are three main reasons for this. Firstly, as shown above, the conflict between FLMLC 2002 and CBR 24/2000 about the STRs leads to the compliance officers not appreciating whether to adopt the basis contained in the legislation or in the regulations. Secondly, the compliance officers may suffer from lack of knowledge/experience to deal with STRs. This is because they do not receive good quality training courses and workshops on a periodic basis. The AMLSCU is not responsible for providing these courses, despite

[190] Which is about £51,725.

[191] Which is about £17,245.

[192] *Attorney general v Others*, Dubai Court Judgment, Criminal Division, case No. 370/2008.

being specialised in dealing with STRs. Instead, the Central Bank provides these courses, but without being specialised in dealing with STRs. The reporting entities are mainly responsible for providing these courses for their compliance officers and the relevant employees. However, no financial penalties will be imposed on the reporting entities for not adhering to this requirement. Lastly, and more importantly, no financial penalties will be imposed on the reporting entities for not appointing a compliance officer. It is unclear in the two cases whether there were actually compliance officers at the banks. In addition, it is unclear whether those banks have adopted the internal procedures on STRs/ML contained in CBR 24/2000, such as CDD measures. This is because the Central Bank has no legal power to impose financial penalties on banks when they fail to adhere to the AML/STR requirements.

Formation of the Dubai Police Committee

The Dubai Police committee, formed in the second case above, raised several questions, especially about the basis of the formation of the committee and the AMLSCU's independence when performing its functions as required by FLMLC 2002. This is because FLMLC 2002 requires that these types of cases are studied just by the AMLSCU.[193] Accordingly, the formation of the committee could conflict with FLMLC 2002, or at least the practice is without any legal basis. In addition, the formation of the committee conflicts with the methodology mandated by FATF and negatively affects the independence of the AMLSCU.[194]

The formation of the committee could undermine the AMLSCU's mandate in these types of cases. It also raises further questions about the effectiveness and efficiency of the AMLSCU in performing its functions

[193] Articles 7 and 8 (2) of FLMLC 2002.

[194] The methodology provides that the FIU should have "the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or forward or disseminate specific information." FATF Reference Document, 'Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems' February 2013, 74.

Available on the FATF website at: www.fatf-gafi.org (accessed on 13th April 2015). See also Chap. 4 (n 496).

as required under FLMLC 2002. The justification for the formation of the committee could be that the AMLSUC does not have experts and that the Dubai Public Prosecution decided to utilise the experts from the Dubai Police through the formation of the committee. Nevertheless, the Dubai Court, Criminal Division,[195] did not indicate in its judgment, directly or indirectly, that the formation of the committee lacked a legal base, but instead relied on the committee's report when reaching its decision.

FLMLC 2002 does not spell out the non-core functions of the AMLSCU. It just emphasises that the Public Prosecution Office has to take the necessary action after consulting with the AMLSCU if the STR has been directly reported to the public prosecution office.[196]

Providing General Feedback and Case by Case Feedback to the Reporting Entities

FLMLC 2002 does not entitle the AMLSCU to provide general feedback or case related feedback to the reporting entities for the purposes of increasing the quality of STRs about ML. Equipping the AMLSCU with such power would indeed be essential since the quality of STRs will otherwise not increase if the AMLSCU cannot point out deficiencies of previous STRs. Thus, this role is no less important than analysing STRs. Chapter 10 provides recommendations about how the AMLSCU should provide feedback to the reporting entities.

Providing Guidance to the Reporting Entities

FLMLC 2002 also does not require the AMLSCU to provide any guidance to reporting entities in relation to STRs. Since its inception in 2002, the AMLSCU has not published statistics about its functions on STRs.[197] Obviously, reports or statistics on the AMLSCU's functions are essential,

[195] *Attorney general v Others*, Dubai Court Judgment, case No. 370/2008 (n 528).

[196] Article 8 (2) of FLMLC 2002.

[197] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 42.

especially to gauge the effectiveness of AML laws and regulations in comparison with international standards.

The Responsibility for Taking the Decision

FLMLC 2002 does not state who is responsible for taking the decision at the AMLSCU when it comes to whether or not to transmit an STR to the Public Prosecution Office. The UAE MER explains that after an STR is analysed and recorded in the AMLSCU database, recommendations about relevant STRs are sent by letter to the Governor of the Central Bank who then decides whether to take further actions.[198] Indeed, this procedure can adversely affect the independence of the AMLSCU, which will be critically assessed in the following subsection.

The AMLSCU's Independence

The AMLSCU is located in the UAE's Central Bank building,[199] but has its own separate section.[200] It is considered to be an administrative section (as detailed in the previous chapter). The Head of the AMLSCU is also an Assistant Executive Director of the Central Bank, who also reports to the Governor of the Central Bank[201] and is responsible for appointing the head of the AMLSCU.[202] A number of issues could cast doubts over the independence of the AMLSCU from the Central Bank. For example, the vast majority of STRs are received by the AMLSCU, but are analysed by the banking supervision employees in the BSED.[203] This practice negatively affects the analytical function of the AMLSCU since employees are inexperienced at analysing STRs. This practice

[198] Ibid 43.

[199] Article 7 of FLMLC 2002.

[200] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 37.

[201] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 37.

[202] Ibid 43.

[203] Ibid 41.

could also explain the large disparity during the period from June 2002 to May 2009 between the number of STRs received by the AMLSCU and the number of STRs transmitted to the Public Prosecution Office. These employees may have concluded that there was no evidence in the majority of STRs and therefore did not transmit them to the competent authority because they were unable to carry out the analytical function properly due to their lack of experience. In addition, this practice conflicts with FATF Recommendation 29 and with the methodology issued by FATF, which require that the employees of the FIU must conduct the analytical function. This, in turn, negatively affects the independence of the AMLSCU to take decisions freely.After the STRs have been analysed, the Governor of the Central Bank decides whether to take further action,[204] although he is not a member of staff of the AMLSCU. This raises the question whether the current AMLSCU type of person—the administrative type—is the best choice for carrying out the AMLSCU's tasks in the AML process. The Interpretative Note to the 2012 FATF Recommendations 29 stresses that the FIU's core functions must be separate from those of other authorities if it is created as part of an existing authority.[205]

Indeed, the above mentioned practices illustrate that the AMLSCU is operationally dependent on the Central Bank. This situation confirms that the AMLSCU does not adhere to the relevant international requirements that the FIU is operationally independent.[206]

AMLSCU's Staff and Training

Employees of the AMLSCU are considered employees of the Central Bank.[207] FLMLC 2002 does not state how many staff the AMLSCU should have and also does not clarify what qualifications they should

[204] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 41.

[205] Interpretative Note to FATF Recommendation 29.

[206] Chapter 10 provides recommendations to ensure the operational independence of the AMLSCU.

[207] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 37.

possess and how much experience or training they should have. The administrative model for the AMLSCU or its sections is also not described.

Number of Staff

The available information is limited and can only be found in the UAE MER. As of March 2007, there were 13 employees working at the AMLSCU.[208] Only three of them analysed STRs.[209] The same number of employees followed up matters not arising from STRs, for example, matters in relation to the prosecution office or court orders. Apart from the head of the AMLSCU, two employees worked in the administration section and the same number undertook data entry work for hard copy reports.[210] One staff was responsible for legal advice, whilst another dealt with international cooperation.[211] Undoubtedly, the number of staff is too low, especially in the areas of analysing STRs and of data entry of hard copy reports when, in 2006, 965 STRs were received by the AMLSCU from reporting entities.[212] The vast number of these were processed by only three AMLSCU analysts.[213] The low number of AMLSCU employees negatively affects the quality of analysis of STRs. It can also explain why there is such a huge difference between the number of STRs received by the AMLSCU and the number which are transmitted to the Public Prosecutions Office during the period June 2002 and May 2009. Hence, work pressure could have resulted in AMLSCU employees not paying sufficient attention to the majority of the STRs they received. Similarly, it can also account for the huge variation between the numbers of STRs sent to the Public Prosecution Office and the number which were prosecuted through the courts. Hence, AMLSCU's employees

[208] Ibid 43.

[209] Ibid.

[210] Ibid.

[211] Ibid.

[212] Which means around 20 STRs per week.

[213] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 43.

may have been under pressure because of the vast numbers of STRs and could thus not provide sufficient evidence about ML suspicions and this, in turn, resulted in fewer prosecutions through the courts. It is assumed that AMLSCU employees possess sufficient knowledge, experience and skills in order to be able to analyse STRs and to find evidence, since police officers and prosecutors usually do not have the qualifications and experience for these types of cases, especially since financial transactions are involved.[214]

Training Courses and Workshops

The ALMSCU employees attended various workshops, seminars and conferences about AML and thus received training. They have also attended training courses about STR analysis.[215] However, they could also be sent to other regional FIUs or a country with rapid growth in its financial sector in order to learn further skills, increase their experience and to develop more practical procedures.[216]

In addition, the AMLSCU should provide training for financial institutions and other reporting entities, so that the quality of the STRs are improved and should also periodically publish typologies and guidance based on the received STRs. This is because the AMLSCU has professional knowledge and skills and it is in an ideal position to gather valuable data on STRs,[217] which make it possible to identify deficiencies contained in those received from reporting entities.

[214] Chapter 6 discusses interviews with employees of the AMLSCU and identifies how many employees currently work for the AMLSCU.

[215] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528) 43.

[216] Chapter 10 provides recommendations to improve the quality of training courses and workshops, inside/and outside the UAE, with a view to enhancing the skills and analytical function of analysts working for the AMLSCU.

[217] Anna Simonova, 'The risk-based approach to anti-money laundering: problems and solutions' (2011) 14 (4) Journal of Money Laundering Control 346, 355 & 356.

Confidentiality Matters

All employees of the Central Bank, including the AMLSCU, have to adhere to the confidentiality provisions contained in Article 106 of the Union Law No. 10 of 1980 Concerning the Central Bank, the Monetary System and Organisation of Banking. The Article provides that all information, which is submitted to the Central Bank, is confidential, except those used for statistical purposes which can be published on an aggregate basis. Furthermore, the AMLSCU has also to adhere to the confidentiality provision in Article 12 of FLMLC 2002.[218]

Compliance with the FATF Recommendation

UAE AML laws and regulations and the AMLSCU are rated as "partly compliant" with the 2003 FATF's Recommendation 26 in relation to the requirements of the FIU.[219] In addition, the UAE's MER indicated that it was difficult to gauge the level of success of the UAE's AML system due to the absence of significant statistics.[220] Currently, after the revision of FATF Recommendations, the UAE's AML laws and regulations do not comply with 2012 FATF Recommendation 29. As shown in the previous chapter, the 2012 FATF Recommendation 29 grants explicit powers to the FIUs, so that they can obtain additional information from the reporting entities and other sources, such as financial and law enforcement information. In addition, the Interpretative Note to the 2012 FATF Recommendation 29 emphasises that the FIU should be operationally independent when fulfilling its functions and responsibilities towards AML. The Recommendation also points out the importance of

[218] See (n 608).

[219] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 528)45.

In contrast, tar FIU and the Saudi Arabia FIU (SAFIU) were rated as "largely compliant" with the 2003 FATF's Recommendation 26, see 'QATAR Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism as produced by the FATF on 9 April 2008, 53–60. In addition, see 'Kingdom of Saudi Arabia Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF on 25 June 2010, 51–61.

[220] Ibid 13.

the analytical function of the FIU, including operational and strategic analysis with regard to the STRs since these functions present the most important task for preventing and detecting ML.

All of the above international requirements and powers, which an FIU should possess, are not yet contained in FLMLC 2002 and the AMLSCU's functions and responsibilities, nor are they clearly defined by legislation or in any of the regulations.

Conclusion

Undoubtedly, the UAE government has made great effort to improve AML controls and regulations, especially after issuing its MER. These efforts are evidenced by a number of regulations, for example the ESCA Regulation 17/2010 and its amendment, the Insurance Authority Regulation 1/2009 and the Central Bank Addendum 2922/2008. This Addendum addresses a number of issues, such as CDD and ECDD procedures, beneficial ownership, shell banks and companies, and correspondent banks. The UAE MER had made the criticism that there were insufficient provisions, but this was remedied. Nevertheless, FLMLC 2002 and its regulations still lack clarity in relation to the role of the AMLSCU in counteracting ML, including the STRs requirements. This may be evidenced in a number of aspects.

Firstly, in relation to the AMLSCU functions, FLMLC 2002 does not clearly spell out the tasks and powers of this entity. It also does not state which principal functions have to be carried out by the AMLSCU in order to counteract ML properly, especially when it comes to analysing STRs, which form the crucial stage in detecting and preventing ML activity. FLMLC 2002 does not even require the AMLSCU to store STRs, which have been received from the reporting entities, yet this is crucial for it to discharge fully its analytical function. In addition, it also does not state which additional roles the AMLSCU should fulfil, for example, to provide general feedback or case related feedback to the reporting entities in order to improve the quality of STRs in the future.

Secondly, FLMLC 2002 and CBR 24/2000 are inconsistent in relation to the basis for submitting STRs. The regulations require all banks and

other financial institutions, including their board members, managers and employees to submit STRs to the AMLSCU if there are reasonable grounds for suspicion that the funds are derived from criminal activity. In contrast, FLMLC 2002 imposes criminal liability only if the aforementioned persons "have known" that the funds derived from criminal activity and that they refrained from submitting STRs to the AMLSCU. This means that no criminal liability is incurred, for example if a banker failed to submit an STR to the AMLSCU, despite him or her having reasonable grounds for knowing or suspecting that a transaction was involved in ML.

A compliance officer and the relevant employees in the financial institutions will benefit much more from training courses if AMLSCU's staff provided these, as they have more knowledge/experience about STRs requirements. This will improve the quality of future STRs, which are being submitted by the reporting entities.

Thirdly, the Central Bank and all other supervisory/regulatory authorities in the UAE, such as ESCA, should be able to impose financial penalties on relevant reporting entities which do not adopt internal AML procedures and adhere to the SARs' requirements contained in FLMLC 2002 and regulations. Such a mechanism would put pressure on all reporting entities to adhere to AML/STRs requirements.

Lastly, differences pertaining to the definition of ML contained in FLMLC 2002 and CBR 24/2000, the low number of staff at the AMLSCU compared to the number of STRs received, and issues relating to the independence of the AMLSCU from the Central Bank are all matters which should be addressed. These problems could also partly explain the huge difference in the numbers of STRs received by the AMLSCU and the number transmitted to the Public Prosecutions Office in relation to the period June 2002 and May 2009.

In light of the 2012 revision of the FATF Recommendations, there is an urgent need to amend/revise the current rules, as contained in legislation and regulations, which govern the function of the AMLSCU, so that they are compatible with the FATF Recommendations in this regard. These revisions comprise a number of matters, such as granting explicit powers to the AMLSCU for the purpose of analysing STRs, gaining additional information from reporting entities and other sources, and providing general/case-by-case feedback to the reporting entities.

The revision also requires ensuring that any ambiguity surrounding the operational independence about the AMLSCU is resolved.

The following chapter is based on interviews with a number of relevant entities, including the AMLSCU, in order to evaluate critically the role which the AMLSCU plays in the AML process and when dealing with STRs, notably after the publishing of the UAE MER in April 2008. These interviews provide valuable data about the AMLSCU and its relationship with the reporting entities and the LEAs, especially in light of the limited information about the role, which the AMLSCU plays in the AML process, as well as the absence of annual reports and precise statistics about STRs.

6

Empirical Investigation in Relation to the AMLSCU

Introduction

As mentioned at the end of the previous chapter, there are insufficient data and information available about the functions of the AMLSCU to fight ML and to deal with STRs in particular. This information is important for removing any ambiguities and vagueness and to analyse critically the functions of the AMLSCU. No UAE case law exists to clarify or interpret the statutory responsibilities of the AMLSCU, the basis of STRs or even the role which compliance officers at reporting entities play within the STRs regime. Moreover, in order to analyse the negative consequences of the AMLSCU's current functions, it is necessary to examine whether the current model is an ideal type, which enables it to carry on its functions to deal with STRs properly. For these reasons, in the present chapter I adopt an empirical approach which makes use of the qualitative method in order to analyse the outcomes highlighted in the previous chapter and to evaluate the functions and legal powers of the AMLSCU when dealing with STRs.

A number of employees at various sectors in the UAE were interviewed for the purpose of the empirical investigation and to provide more in-depth information and statistics, both directly and indirectly, about the

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_6

task of the AMLSCU and the STRs regime. Four sectors have been chosen: (1) the AMLSCU, (2) the banking sector, (3) the Public Prosecution Office and (4) the police from the period between March and May 2012.

The reason for selecting these sectors is that the AMLSCU is best placed for providing data and information about its responsibilities and annual statistics about STRs. The banking sector, especially compliance officers, have been selected as it is likely that the majority of STRs are submitted by these officers to the AMLSCU. In 2011, banks in the UAE submitted 83 % out of the total STRs which were passed to the AMLSCU by the reporting entities.[1] Indeed, the empirical investigation aims at utilising the experience of specialist bankers, compliance officers, so that information on the functions of the AMLSCU and its responsibilities in the field of counteracting ML can be provided. The third sector chosen is the Public Prosecution Office as it receives STRs from the AMLSCU.[2] As the public prosecutor has extensive experience in investigating these cases, he also knows about the functions and responsibilities of the AMLSCU. The last sector is the Dubai Police, chosen simply because they established a specialised Section for AML and Financial Crimes in its General Department of Criminal Investigations (GDCI). This Section is not found in any other police department in the UAE.[3] Dubai City is also the international financial and commercial centre in the Middle East and thus it could be an attractive place for money launderers. The previous chapter outlined the set up of the committee, which is composed of employees of the AMLSCU and the AML Section of the Dubai Police during an ML investigation.[4]

---

[1] According to Mrs Angeli Pereira, who is an AML Officer at the AMLSCU. She presented a paper on the subject of "The role of AMLSCU in the recovery of proceeds emanating from money laundering, terrorist financing and related financial crimes" at the Conference on Recovery of Proceeds of Crime and Asset Sharing.

The conference was held in Dubai (Intercontinental Dubai Festival City) on 9 and 10 May 2012.

The conference was organised by the AMLSCU in cooperation with the Crown Prosecution Service (CPS) and Her Majesty's Revenue and Customs (HMRC) in the UK.

[2] If the AMLSCU concludes that there is suspicious ML activity involved in the particular STR.

[3] As in addition to the Federal Police in the UAE which is embodied in the Ministry of Interior, Abu Dhabi, Dubai and Ras Al Khaimah have their own local police departments.

[4] *Attorney general v Others* (n 711) of Chap. 5.

All information and data gathered through the interviews will be evaluated with a view to analysing the current functions and responsibilities of the AMLSCU to deal with STRs. The interview questions were sent in advance to the interviewees, so that they could have some opportunity to reflect on the questions prior to the interviews. The information and data were recorded during the interviews through note taking, as the interviewees refused to allow any electronic means of recording.[5]

Section "Interviewing Within the Relevant Sectors" of this chapter deals with interviews within the relevant sectors. Section "Analysing the Data and Information from the Interviews" critically analyses the information and data which have been gathered through the interviews. This is crucial so as to identify in which aspects the AMLSCU does not fully discharge its required functions and to analyse problems within its legal powers in relation to the STR regime. These are all considered in Chap. 10 which provides various recommendations.

Interviewing Within the Relevant Sectors

This section encompasses four parts. The first deals with the AMLSCU employee interview; the second provides the interviews with two of the compliance officers of the banking sector; the third discusses the interview with the public prosecutor; and the fourth relates to the interview with a Dubai police officer.

The Interview with the AMLSCU Staff

This subsection describes the interview with Mr A, who works as a "Senior STR Analyst" in the AMLSCU. The purpose of interviewing him is to acquire data about the functions of the AMLSCU, its responsibilities to deal with STRs and to evaluate its relations with reporting entities and LEAs. The following 31 questions were asked:

[5] In addition, the interviewees refused permission for their names to be mentioned in this research.

1. What is the relationship between the AMLSCU and the Central Bank?
2. What is the organisational structure of the AMLSCU?
3. How many staff has the AMLSCU?
4. What are the qualifications of the staff of the AMLSCU?
5. Who is responsible for providing training courses for the staff of the AMLSCU?
6. How often do you provide training courses for the staff of the AMLSCU annually?
7. What are the components of these training courses?
8. Do you receive all STRs from the reporting entities directly or via a specific entity?
9. Who are the reporting entities that you receive STRs from?
10. Is there any entity which reports STRs to a specific entity other than the AMLSCU?
11. What are the procedures after receiving an STR?
12. Could you please explain the analytical function in relation to STRs?
13. In case an STR is received, who is responsible for stopping the relevant transaction?
14. Who is responsible for deciding whether or not to send an STR case to the prosecution?
15. Do you exchange information about STRs—upon request—with foreign FIUs? If so, are there any countries in particular with which the level of cooperation has been very good?
16. Do you provide general feedback to the reporting entities about their functions in relation to transmitting STRs?
17. Do you provide specific/case-by-case feedback to the concerned reporting entity about its STR?
18. Who is responsible for providing guidelines to the reporting entities about their duty to combat ML?
19. Are you entitled in law to obtain directly additional information about an STR from a particular reporting entity?
20. Are you entitled in law to punish any reporting entity for failing to obey a reporting system obligation?
21. Do you have a legal power in case of receiving STRs to freeze the illegal proceeds?

22. Is there an electronic link between the AMLSCU and all the reporting entities?
23. Is there an electronic link between the AMLSCU and the LEAs?
24. Do you issue periodic reports about your work? If yes, are these reports publicly available?
25. Do you hold any statistical information about the number of STRs which you receive annually? If yes, are these publicly available?
26. If the answer to the previous question is yes, how many STRs did you receive, from the reporting entities, in the last five years?
27. How many STRs did you transmit to the police or the Public Prosecution Office in the last five years?
28. What role does the AMLSCU play in relation to national AML other than receiving STRs?
29. Do you communicate with the NAMLC?
30. On the basis of reliable statistics that I have to hand (from January 2002 to May 2009), I would like to know why only 285 out of 80,592 STRs were referred to the Public Prosecution Office. (Why is the percentage so small?)
31. Would you like to add any other information?

Mr A started the interview by stating that the AMLSCU is an independent unit within the Central Bank of the UAE. The Executive Director of the Central Bank is also working as the head of the AMLSCU. Four sections make up the organisational structure of the AMLSCU, namely (1) the STR Analysis and STR Database Management Section,[6] (2)

[6] Mr A explained that this Section is responsible for a number of tasks, for example:
A. Receiving, reviewing and analysing all STRs from the reporting entities.
B. Initiating search and/or freeze instructions to all financial institutions and following up responses accordingly.
C. Registering STRs and suspicious cases in the AMLSCU database.
D. Developing the training unit for the staff of the AMLSCU and reporting entities, including DNFBPs.
E. Supervising the existing STR analysis system and proposing changes/modifications depending on the future needs of the AMLSCU.
F. Preparing typologies reports after identifying the existing ML trends.
G. Preparing statistics and an annual report for the AMLSCU.

the Cross-Authorities Cooperation Section,[7] (3) the International Cooperation Section[8] and (4) the Administrative Support Section.[9]

At the time of the interview,[10] Mr A stated that the AMLSCU had 25 staff and access to more than 80 examiners, from the Central Bank, in order to conduct examinations on behalf of the AMLSCU. Most of the staff hold bachelor degrees and some also have post-graduate degrees, including in banking, law and economics or business administration. A number of staff have also obtained professional diplomas in AML. AMLSCU staff take part in in-house courses, which are held by experienced and senior staff members. Staff also attend external training courses which are provided by the UAE Central Bank, which in turn employs reputable institutions and universities to provide the training. The training courses comprise (1) critical report writing and executive summaries on suspicious transactions, (2) building up a case by laying out the elements of suspicion, (3) AML compliance, (4) time management and (5) leadership skills. Nevertheless, all of those in-house and external training courses take place irregularly and are only given when required.

---

[7] Mr A stated that this Section has the following duties:
   A. Receiving enquiries or requests from LEAs, the Public Prosecution Office and courts and taking appropriate action.
   B. Preparing Memorandum of Understanding (MOU) on AML information exchange with other domestic authorities.
   C. Executing public prosecution and court orders in the UAE against defendants, judgement debtors and the deceased in relation to their investments and bank accounts.

[8] Mr A said that this Section deals with international affairs, particularly:
   A. Receiving requests from the UN and foreign governments and taking action accordingly.
   B. Receiving requests from foreign FIUs on STRs and forwarding reports to the requesting FIU. Initiating requests to foreign FIUs in relation to STRs.
   C. Preparing MOUs on AML information exchange with foreign FIUs and international organisations.
   D. Following up on the UAE's MER.
   E. Coordinating with concerned entities, so that FATF standards are implemented.

[9] According to Mr A, this last Section deals with administrative matters, such as
   A. Sending/receiving letters/responses to/from all financial institutions via an email system and recording them into the AMLSCU database.
   B. All secretarial commitments, for example diary management, scheduling meetings/conferences/workshops and handling correspondence.

[10] On 21 May 2012.

According to what Mr A said, the AMLSCU is the sole national centre for receiving, analysing and reviewing STRS from all reporting entities, which are financial, commercial and economic and operate in the UAE. The AMLSCU also receives STRs from all DNFBPs. The Governor of the Central Bank, who is also the Chairman of the NAMLC, can freeze any account in the UAE for up to seven days and thereafter has to refer the case to the Public Prosecutions Office, so that an extension can be sought as required pursuant to FLMLC 2002. Once an STR is received by the AMLSCU, it is assigned to an analyst for review and processing. The analyst screens the person, who is subjected to the STR, against all the AMLSCU databases and other public and intelligent search databases and starts the analysis. This means that information generated from STRs can lead to the identification of potential and actual ML activities. Each STR is therefore analysed in the STR Analysis and Database Management Section. The analysis function is based on the Five Ws and the One H, namely Who (Who is conducting the suspicious transaction?), What (What instruments or mechanisms are being used?), When (When did the suspicious activity/transaction take place?), Where (Where did the suspicious activity/transaction take place?), Why (Why does the reporting entity think that the activity is suspicious?) and How (How did the suspicious activity/transaction occur?). Moreover, the AMLSCU has power to gather additional information from the relevant reporting entity through the UAE Central Bank. The AMLSCU also provides general feedback and specific/case-by-case feedback to the reporting entities. Mr A declined to confirm that the statistics mentioned in question 30, on the basis of the STRs, referred to statistics that also include Cash Declaration Reports.[11] He stated that accurate statistics on STRs are included in the AMLSCU's annual report.

After the analytical function has been completed, the Executive Director of the Central Bank, the head of the AMLSCU, is in charge of deciding whether or not to send the details of the STR to the Public Prosecution Office. Mr A added that the particular regulatory authorities are responsible for providing AML guidelines to their regulated entities and noted that the AMLSCU provides support and guidance to the part-

[11] See Chap. 5 (n 629).

ner regulatory authorities in this regard and also conducts training for the implementation of these directives and guidelines. In addition, he said that if any reporting entity does not obey the reporting system obligations, Article 15 of FLMLC 2002, which specifies the penalty, will be applied.[12]

On the questions relating to electronic links between the AMLSCU and all the reporting entities, Mr A stated that only banks and money changers are linked via the on-line STR reporting system. There also exists a secure e-link with LEAs.

According to what Mr A stated, the AMLSCU participates in all NAMLC meetings and ensures compliance with FLMLC 2002 and regulations in the UAE. The AMLSCU started publishing its annual report in 2008, so that all its achievements throughout the year are published. He also noted that the annual report is provided to all Egmont FIUs. During the interview, Mr A showed the AMLSCU annual reports for 2009 and 2010. These reports contained important statistics on STRs and will be critically analysed in section "Analysing the Data and Information from the Interviews" of this chapter.

Significant Observations

The following observations can be made in relation to some of the answers which Mr A provided. Firstly, there is no doubt that the AMLSCU has made great efforts to combat ML, especially in relation to receiving and analysing STRs; however, the number of AMLSCU staff may not accommodate the responsibilities and commitments of the AMLSCU in this regard. The AMLSCU should increase both its administrative and technical staff to fully accommodate its tasks. The fact that it has access to more than 80 investigators in order to conduct examinations prejudices its operational independence.

Secondly, the training courses for AMLSCU staff should be held periodically, for instance on a semi-annual basis, in order to keep abreast of all existing/potential ML patterns and activities. In addition, it would

[12] Article 15 of FLMLC 2002, see Chap. 5 (n 611).

be good if these training courses could also take place in developed countries which experience sophisticated ML patterns and activities.[13] The AMLSCU may also sign a MOU with foreign FIUs in order to host these training courses. Such sophisticated/new patterns of ML could arise in a number of areas, such as exploiting the sport sector for ML activities[14] or the using of online payment methods, when purchasing goods/services for the purpose of crime.[15] Furthermore, the AMLSCU may arrange workshops and seminars for its staff. It could invite academic and LEAs to join such workshops/seminars, so that its staff gain different perspectives, outside its own environment, in relation to its responsibilities.[16]

Thirdly, it is true that the Central Bank has got the right to freeze suspected transactions/funds in financial institutions for up to seven days pursuant to Article 4 of FLMLC 2002. Mr A stated that FLMLC 2002 grants the right to the Central Bank to refer the case to the Public Prosecution Office after the termination of the seven days in order to extend the period of the freeze. However, such practice could conflict with CBR 24/2000 which states that if the supervisory authority in the transfer country did not respond within the seven days, the Central Bank should take the decision to lift the freeze.[17] More importantly, FLMLC 2002 does not indeed specify the procedure which should be followed after the expiry.

Fourthly, according to what Mr A explained in relation to the analytical function, it appears that the AMLSCU is unaware or at least does not pay great attention to strategic analysis or "strategic intelligence," which was discussed in Chap. 4. This type of analysis is crucial as all the collected and analysed information on STRs is employed in order to formulate a new/amended strategy for the future work of the AMLSCU.

---

[13] Chapter 10 provides recommendations for dealing with periodical training for AMLSCU staff.

[14] For further detail on such issue, see FATF Report, 'Money Laundering through the Football Sector' July 2009, available online at:http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20through%20the%20Football%20Sector.pdf (accessed on 20th August 2015).

[15] For further detail on such issue, see FATF Report, 'Money Laundering Using New Payment Methods' October 2010, available online at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf (accessed on 20th August 2015).

[16] Jayesh D'Souza, *Terrorist financing, money laundering and tax evasion – Examining the performance of Financial Intelligence Unit* (Taylor & Francis Group, LLC 2012), 177.

[17] Article 15 (6) of CBR 24/2000, see (n 633) of Chap. 5.

Fifthly, the AMLSCU does not directly gather additional information/documents from the reporting entities, but instead indirectly obtains them from the Central Bank. This practice also may prejudice the operational independence of the AMLSCU since it needs to be entirely independent, at least at the operational level. Thus, FLMLC 2002 should equip the AMLSCU with this power, so that it can directly require additional information/documents from the reporting entities. This removes any doubts about its operational independence and ensures that its responsibilities are properly discharged.

Lastly, Mr A said that the AMLSCU participates in all NAMLC meetings, but there appears to be no legal basis for this. As noted in the previous chapter, Article 9 of FLMLC 2002 omitted to require representative(s) from the AMLSCU to be members of the NAMLC; however, a representative(s) from the Central Bank is required. A representative(s) from the Central Bank is not necessarily a representative(s) of the AMLSCU, since the latter is supposed to be independent of the former.

Interviews Within the Banking Sector

Three banks were selected to participate in the interviews, which are described as Banks D, E and H. The first two banks are national banks, which operate in the UAE, and Bank H is a branch of a famous foreign bank, which also has a presence in the UAE. The reason for interviewing national and foreign banks is to evaluate whether they adopt the same internal controls for dealing with STRs. Whilst the national banks agreed to the interviews, the manager of the foreign bank H refused to take part since the subject was considered too sensitive.

Hence, the findings of the interviews only relate to the national banks D and E. Mr Z from Bank D and Mr S from Bank E were interviewed. Both interviewees have been working in the Group Compliance Section of their banks. Mr Z has worked for ten years in this particular field. Mr S has worked in this field for 15 years, the first 11 with other banks outside the UAE and for the last four years with Bank E.

Sixteen questions were prepared concerning the functions of the AMLSCU and banks in combating ML, especially STRs requirements.

The questions also tried to remove the ambiguity surrounding the current functions of the AMLSCU, which was highlighted in the previous chapter. The following questions were asked:

1. What is the relationship between you and the AMLSCU in the Central Bank?
2. Who is responsible for providing guidance and training for your work in relation to counteracting ML?
3. How often do you attend training courses annually?
4. What are the components of the training course?
5. Who provides you with the form of an STR?
6. How do you become aware of STRs? What is the basis for an STR? Do you base your suspicion on subjective or objective grounds, or both?
7. What procedures do you follow when you suspect ML?
8. Is there a specific timeframe from the moment "reasonable grounds" are raised to sending the STRs to the AMLSCU?
9. Do you receive general feedback from the AMLSCU about your work in relation to STRs on ML?
10. Do you receive any specific/case-by-case feedback from the AMLSCU about your work in relation to a specific STR?
11. Approximately, how many STRs do you transmit to the AMLSCU annually?
12. Is there an electronic link between the AMLSCU and your department?
13. Is there any other system that deals with AML, other than STRs, for example, a CTR system—if a transaction exceeds a fixed amount? If yes, to whom do you report this transaction?
14. What are the principal strengths and weaknesses of the AMLSCU?
15. How could the effectiveness of the AMLSCU be improved?
16. Would you like to add any other information?

This subsection comprises two parts which illustrate the experience of Mr Z and Mr S in relation to these questions.

The Interview with Mr Z

According to what Mr Z said, the relation between Bank D and the AMLSCU started in 2000 when CBR 24/2000 required all banks to report STRs to the FIU in the Central Bank. The basis of STRs is not a subjective, but rather an objective, test. During the last three years, all banks have adopted an internal electronic system. It reviews all the transactions which are conducted through the bank at the end of each day. The benefit of this system is that it alerts the employees of the bank on a daily basis to any unusual transactions. For example, if a natural person has a bank account in Bank D, and he or she does not have any income except a salary which is AED10,000 monthly, and suddenly his or her account is credited with AED1,000,000, then the electronic system will alert the bank about the transaction and the account. The competent employee will analyse and investigate the transaction and the account. This can be done through KYC procedures which comprise analysing the customer's information, such as his or her place of residence, occupation and whether he or she is a natural or corporate person located in the free zone. Subsequently, if the competent employee is not satisfied, he or she will ask the customer to provide additional information or supporting documents to prove that the transaction is legitimate. In case the customer failed to respond to the request, was uncooperative, the documents were unreachable[18] or he or she provided the required information/documents, but the compliance officer in the bank was not satisfied with them, the officer will then submit the STR to the AMLSCU. Sometimes before submitting the STR to the AMLSCU, the competent employee of Bank D requires his colleague's assistance from another branch and asks whether this other branch holds useful information about the customer and his or her account.

It is important to stress that in relation to the above mentioned electronic system, Mr Z explained that this system has a threshold amount, so that it will only alert the competent employee if the transaction exceeds a certain threshold. However, this does not necessarily mean

[18] Mr Z provided an example of such a situation when the customer says that he or she has the relevant documents, but that they are outside the UAE, and does not provide them.

that the particular transaction is treated as a "suspicious transaction," but it does mean that the employee has to analyse the transaction based on the customer's profile and KYC as mentioned above. This is simply because the financial movements of a bank account of a large company are totally different in terms of the pattern of the transaction and their amounts from the financial movements in the bank account of a natural person who does not have any income except his or her monthly salary.

Mr Z stated that the submission of STRs to the AMLSCU used to be done via post, but for the last two years submission has taken place online; however, the AMLSCU still responds by mail. In addition, the AMLSCU's response relates to the procedures which have been taken and which should be adopted by the bank, for example the bank may be requested to freeze an account. After receiving a response from the AMLSCU, the bank records the information about the concerned STR in its own database. However, it does not know what happens to the STR after this.

Under CBR 24/2000, the Central Bank provides the form for the STRs. The form has not been changed and is attached to CBR 24/2000 and is also available online. The AMLSCU's response often takes about one to two weeks from the date the STR has been submitted. Mr Z stated that the banks annually submit thousands of STRs to the AMLSCU. He stated that he personally, in his branch, submits annually around 20 STRs on ML.

CBR 24/2000 does not require a specific timeframe from when the "reasonable grounds" arise until when the bank has to submit STRs to the AMLSCU. Nevertheless, the bank submits them as soon as possible and on average within one week. The AMLSCU/Central Bank provides training courses for all banks and reporting entities from time to time. Training courses take place irregularly and sometimes more than one year passes without a further course taking place. They include theoretical and practical aspects, and case studies are also used to understand when and how to suspect that a customer or his or her account is being used for ML.

The AMLSCU does not provide Bank D with general or case specific feedback about an STR. Nor does it ask Bank D for additional information about a specific STR except in very rare cases; however, it sometimes

asks for additional information about STRs, which have been submitted by other reporting entities. This occurs through the "electronic messaging system." Mr Z noted that the Central Bank requires that the person writes the source of the money and his or her identity card number on the receipt if the deposit is in cash and is AED40,000 or more. Additionally, a declaration system exists for travellers, but this is not directed at banks.

Mr Z concluded the interview by stating that the AMLSCU does not provide him with the annual report about the functions of the AMLSCU or statistics of STRs. Furthermore, he noted that he would like to increase communication between the AMLSCU and all banks and he suggested that the AMLSCU should report whether a specific STR has been transmitted to the police or the prosecution or has been discontinued. Currently, the AMLSCU does not inform him after he submits the STR.

The Interview with Mr S

Mr S repeated what Mr Z had said about the relationship between the banks and the AMLSCU. He confirmed that all banks have adopted an internal electronic system in order to detect any unusual transactions which could be involved in ML activity. However, he stated that an STR is based on both objective and subjective grounds. For example, it could be a normal transaction if a large company's bank account received AED500,000. In contrast, the same amount would not constitute a usual transaction if it had been transferred to a normal person's bank account, which only receives the person's monthly salary of AED15,000. If the electronic system flags up the unusual transaction, the employee will analyse the particular transaction and will ask the "relationship manager" to provide additional information about the customer. Moreover, the relationship manager will arrange a meeting with the customer and will ask him or her to provide information or supporting documents which show that the transaction is legitimate. Subsequently, the relationship manager will provide Mr S with the results of the meeting and the required documents. Mr S stressed that this procedure is adopted in all banks in the UAE in order to avoid the tipping off offence. If the compliance group contacted the customer directly about the concerned transaction, the cus-

tomer would know or suspect that his or her transaction is being treated as a suspicious one. For this reason, the relationship manager meets the concerned customer and asks him or her some routine questions, such as: "We are updating your account, could you please provide us with documents about the source of this transaction?"

The bank's compliance group will complete an STR form when: it is not satisfied with the documents/information which have been provided by the concerned customer; the latter is uncooperative; or if the documents are not presented to the bank. Mr S said that the Central Bank provides the form for STRs, which is based on CBR 24/2000 and has not changed since 2000; however, since January 2011, he submits STRs online to the AMLSCU and prior to this sent them by mail. The form requires that information is provided about the particular customer, how long the account has been opened, the types of accounts he or she holds, the reasons which the customer has given about the transaction, and the reason why the bank treats the transaction as suspicious. CBR 24/2000 does not require a specific timeframe from when the "reasonable grounds" arise until when the bank submits the STRs to the AMLSCU; however, according to Bank's E internal procedure, up to one month is allowed. This is because the compliance group is often not satisfied with the results of the meeting between the relationship manager and the concerned customer, so the compliance group asks the manager to request further information or documents from the customer. Only after the one month has passed will the compliance group decide whether or not to submit the STR to the AMLSCU.

Mr S stated that, in 2010, Bank E, including its branches in the UAE, submitted more than 200 STRs on ML to the AMLSCU. In addition, in the same year, all banks, foreign and local, which operate in the UAE, submitted more than 20,000 STRs on ML to the AMLSCU. Except for arranging seminars from time to time, the AMLSCU or Central Bank does not provide training courses to banks. Seminars are held irregularly and cover case studies on ML, which are presented by guest lecturers, for example from the UK. The training courses are arranged by Bank E which is responsible for providing these courses for its employees, who work in the compliance group. The training courses are held annually and cover examples and ML cases, as required by CBR 24/2000.

In addition, the AMLSCU does not provide Bank E with general or specific/case-by-case feedback on STRs. Nevertheless, some AMLSCU seminars have highlighted some common inaccuracies among reporting entities in relation to STRs, for example the trading licence of the concerned company not being attached to the STR. Mr S confirmed that sometimes the AMLSCU asks Bank E to provide additional information or further supporting documents in relation to an STR which Bank E has submitted. The AMLSCU may also require Bank E to permit the transaction and to provide updated information about the account.

He said that the Central Bank requires the customer to write the source of the money and his identity card number on the receipt if he makes an AED40,000 or more cash deposit into the account. He concluded the interview by proposing that the AMLSCU should increase the seminars on STRs as these enhance cooperation between the reporting entities and the AMLSCU. He also suggested that during these seminars more information should be provided about common mistakes in relation STRs, so that the quality of future ones can be improved.

Significant Observations

After having outlined what Mr Z and Mr S explained in their interviews, it is important to highlight common features and differences in relation to the responses to the questions.

Firstly, the basis of STRs is still unclear. Mr Z stated that it is objective, whilst Mr S stated that it is both objective and subjective. One reason why ambiguity may exist is the conflict between CBR 24/2000 and FLMLC 2002.

Secondly, internal controls vary between Bank D and Bank E in relation to the time stipulated from when "reasonable grounds" arise until STRs are submitted to the AMLSCU. Whilst it only takes up to one week in Bank D, it takes one month in Bank E.[19]

Thirdly, both interviewees confirmed that the AMLSCU requires additional information or supporting documents on STRs which have

[19] Chapter 10 provides recommendations which deal with the timeframe in which reporting entities should submit STRs.

been submitted by them; however, as assessed in the previous chapter, the AMLSCU possesses no legal power to request additional information/documents. Thus, the current practice by the AMLSCU to require additional information from the reporting entities has no legal basis.

Fourthly, both interviewees agreed that the AMLSCU does not provide the banks with general feedback on STRs, nor specific/case-by-case feedback on a particular STR and this confirms what has been analysed in relation to this issue in the previous chapter.

Fifthly, both interviewees agreed that cooperation between the AMLSCU and the banks should be improved. Mr Z suggested that the AMLSCU should inform the particular reporting entity about whether or not an STR has been transmitted to the police or to the prosecution or whether it has been stopped. Mr S suggested that the AMLSCU should hold more seminars and during these common errors should be pointed out in relation to STRs, so that the quality could be improved in the future.

Sixthly, both interviewees confirmed that the Central Bank provides the form for the STRs which means that the current practice of providing the form from the supervisory authorities, such as the Central Bank and the ESCA, is inconsistent with Article 7 of FLMLC 2002 which grants such authority to the NAMLC, as ascertained in Chap. 5.[20] Indeed, neither the NAMLC nor the supervisory authorities are in a position to provide all reporting entities with the STRs form. However, the AMLSCU is better placed to prepare it since it is the sole entity which deals with STRs.

Lastly, Mr Z mentioned several times the Central Bank when in fact he meant the AMLSCU. The interviewer asked him about the confusion and he answered that the Central Bank means the AMLSCU. Indeed this situation raises the question whether the AMLSCU is really operationally independent from the Central Bank. The AMLSCU should remove any doubt in reporting entities' minds and prove that it is also, in practice, entirely independent in its operations from the Central Bank.

[20] Article 7 of FLMLC 2002, see (n 683) of Chap. 5.

The Interview with the Public Prosecutor

In this subsection, it is important to illustrate briefly that the judicial system in the UAE is based on prosecution and court. In addition to the federal judicial system which is embodied in the Ministry of Justice[21] and is applied to four cities, namely Sharjah, Ajman, Umm Alquwain and Fujairah, there are three cities which have their own judicial system, namely Abu Dhabi,[22] Dubai[23] and Ras Al Khaimah[24] and which thus have their own prosecutions and courts since the UAE's constitution grants such right to the cities to establish their own judicial system.[25] However, the constitution stipulates that the federal judicial system and the UAE Union Supreme Court shall have jurisdiction in a number of matters which affect on the interests of the Federation.[26]

---

[21] See www.ejustice.gov.ae (accessed on 9th September 2015).

[22] Abu Dhabi Judicial Department, see www.adjd.gov.ae (accessed on 9th September 2015).

[23] Dubai Courts, see www.dubaicourts.gov.ae and Dubai Public Prosecution see www.dxbpp.gov.ae (accessed on 9th April 2015).

[24] RAK Courts Department, see www.rak.ae (accessed on 9th April 2014).

[25] The Constitution came into effect on 2 December 1971 and was permanently accepted in May 1996.

> Article 104 of the UAE's Constitution stipulates that:"The local judicial authorities in each Emirate shall have jurisdiction in all judicial matters not assigned to the Union judicature in accordance with this Constitution."

In addition, Section V of Chapter IV of the Constitution deals with the Judiciary in the Union and the Emirates.

[26] Article 99 of the Constitution states that:"The Union Supreme Court shall have jurisdiction in the following matters:

1. Various disputes between member Emirates in the Union, or between any one Emirate or more and the Union Government, whenever such disputes are submitted to the Court on the request of any of the interested parties.
2. Examination of the constitutionality of Union laws, if they are challenged by one or more of the Emirates on the grounds of violating the Constitution of the Union. Examination of the constitutionality of legislations promulgated by one of the Emirates, if they are challenged by one of the Union authorities on the grounds of violation of the Constitution of the Union or of Union laws.
3. Examination of the constitutionality of laws, legislations and regulations in general, if such request is referred to it by any Court in the country during a pending case before it. The aforesaid Court shall be bound to accept the ruling of the Union Supreme Court rendered in this connection.

This subsection describes the interview with the Dubai Public Prosecutor. Thirteen questions were designed for Mr L, the chief prosecutor. He answered a number of these questions, although his response to a few was "no comment." The following questions were asked:

1. What is the role of the AMLSCU at the Central Bank in relation to counteracting ML?
2. Are there any STRs that you investigated, which were reported by a financial institution operating in the UAE to the ALMSCU?
3. Are there any STRs that you investigated, which were reported by a bank operating in the UAE to the ALMSCU?
4. During the investigation of an ML case, do you request additional information from the AMLSCU?
5. Do you have any statistics about the number of STRs which you annually received from the AMLSCU?
6. Do you hold any statistical information about the number of STRs which you annually received from the AMLSCU and the number of cases which you prosecute in court?
7. Do you hold any statistical information about the number of ML cases which you brought to the court and how many of them have resulted in a conviction?
8. On the basis of reliable statistics which I have to hand (from January 2002 to May 2009), I would like to know why only 285 out of

4. Interpretation of the provisions of the Constitution, when so requested by any Union authority or by the Government of any Emirate. Any such interpretation shall be considered binding on all.
5. Trial of Ministers and senior officials of the Union appointed by decree regarding their actions in carrying out their official duties on tile demand of the Supreme Council and in accordance with the relevant law.
6. Crimes directly affecting the interests of the Union, such as crimes relating to its internal or external security, forgery of the official records or seals of any of the Union authorities and counterfeiting of currency.
7. Conflict of jurisdiction between the Union judicial authorities and the local judicial authorities in the Emirates.
8. Conflict of jurisdiction between the judicial authority in one Emirate and the judicial authority in another Emirate. The rules relating thereof shall be regulated by a Union Law.
9. Any other jurisdiction stipulated in this Constitution, or which may be assigned to it by a Union law.'

80,592 STRs were referred to the public prosecution. (Why is the percentage so small?)
9. What is the procedure which is followed if you—in the course of investigating any crime—suspect that there is ML involved?
10. Is there an electronic link between the prosecution and the AMLSCU?
11. In some ML cases, what is the reason for establishing a committee composed of employees of the AMLSCU and the AML Section of the Dubai Police?
12. How could the effectiveness of the AMLSCU be improved?
13. Would you like to add any other information?

Mr L started answering the questions by saying that Articles 7 and 8 of FLMLC 2002 govern the role of the AMLSCU. Article 7 provides that the AMLSCU receives STRs. Article 8 entitles the AMLSCU to study STRs and then to notify the Public Prosecution Office about particular STRs. Mr L did not answer question 2 and 3; however, he noted that the Public Prosecution Office, when investigating a case, often requests additional information about an STR and that it takes on average between three to four months to get a response from the AMLSCU. Furthermore, there is no electronic link between the Public Prosecution Office and the AMLSCU.

Table 6.1 shows the statistics provided by Mr L in relation to questions 5, 6 and 7.

Mr L declined to answer question 8 and suggested that it be directed to the AMLSCU. He stated that if in the course of a crime investigation the Public Prosecution Office suspects that there is ML, the AML and Financial Crime Section of the Dubai Police will be asked to gather evidence.

Table 6.1 STRs 2007–2011

Year	Number of STRs on ML	Number of STRs sent to the court	Convictions
2011	3	–	–
2010	2	–	–
2009	3	1	1
2008	1	–	–
2007	2	–	–

The Public Prosecution Office decides whether or not to establish a committee composed of employees of the AMLSCU and the AML Section of the Dubai Police in order to provide a case report. He added that the reason for establishing a committee is that it is often necessary to inspect relevant documents and computers/laptops at the bank or other entity. This task is usually carried out by the Dubai Police as it has experts in these fields. Thus, for this reason, the Public Prosecution Office decides whether or not to establish a committee to coordinate the work between the Dubai Police and the AMLSCU and to provide a technical case report. Mr L did not want to answer question 12.

Significant Observations

Four observations can be made about the interview. Firstly, the statistics, which Mr L provided, clearly demonstrate that for the period 2007 to 2011 the Dubai Public Prosecution Office received 11 STRs files on ML; however, only one case was sent to the Court and resulted in a conviction. The statistics, which were provided by Mr L, may be inaccurate, as they show that in 2007 no ML cases were sent to the Court; nevertheless, in the previous chapter we noted that the Dubai Public Prosecutor sent one case to the Court and that this resulted in the conviction of both defendants.[27]

Secondly, when the Public Prosecution Office asks AMLSCU for additional information, it takes between three and four months to get a response. This period is too long, notably in ML cases which require that action is taken promptly, especially when organised criminals are involved in cross-border transactions. This long duration could lead to evidence being lost. There are several reasons for this delay, for example, the AMLSCU lacks human resources and there is also no electronic link between the Public Prosecution Office and the AMLSCU.

Thirdly, there is no legal provision which permits that a committee composed of employees of the AMLSCU and the AML section of the Dubai Police can be established in order to provide a technical report

[27] *Attorney general v Others* Dubai Court Judgment, Criminal Division, case No. 370/2008, see (n 711) of Chap. 5.

in ML cases.[28] The AMLSCU is the only entity with authority to analyse STRs and to provide technical reports in ML cases. This is because Articles 7 and 8 of FLMLC 2002 state that STRs can only be received and studied (analysed) by the AMLSCU. The AMLSCU should therefore have sufficient human resources and experts to ensure that this is duly complied with. Hence, this practice prejudices the operational independence of the AMLSCU.

Lastly, whilst Mr L could have provided further information in relation to the questions, he preferred not to.

The Interview with the Dubai Police Officer

A number of questions were designed for the interview with Mr N, who had been working as an officer for more than ten years in the AML and Financial Crime Section at the Dubai Police. The following questions were asked:

1. What is the relationship between you and the AMLSCU at the Central Bank?
2. What do you do when you become aware of ML?
3. What is the difference between your function and the function of the AMLSCU?
4. Is there an electronic link between your Section and the AMLSCU?
5. How could the effectiveness of the AMLSCU be improved?
6. In some ML cases, what is the reason for establishing a committee composed of AMLSCU employees and employees who work for the AML Section at the Dubai Police?
7. Would you like to add any other information?

Mr N started answering the questions by stating that the relationship between the AML Section at the Dubai Police and the AMLSCU is based on two factors. FLMLC 2002 provides that the AMLSCU has the right to obtain assistance from LEAs when conducting its functions

[28] As happened in the case of *Attorney general v Others*, ibid.

and that the Dubai Police is one of these LEAs in the UAE. In addition, an MOU has been signed between the Dubai Police and the governor of the Central Bank, as he is the chief of the NAMLC and the National Committee to Combat Terrorism (NCCT). The reason for the MOU is that Dubai City represents a vital financial and commercial centre in the world and especially for the Middle East, and is the location for many national and foreign banks. This renders Dubai much more vulnerable to ML than other cities in the UAE.

Mr N stated that a suspicion about ML can arise when the AML Section receives information that ML activity has taken place or is going to take place. After verifying that the information is reliable, Mr N then informs the AMLSCU and the Public Prosecution Office. Alternatively, the AML Section receives an STR file on ML from the AMLSCU. The STR file contains an analytical report, which includes information and data provided by the reporting entity and states why the reporting entity considers the transaction suspicious. The AMLSCU then asks the AML Section to investigate the case, which then takes statements from parties and provides the AMLSCU with an analytical report and a recommendation, for example to close the particular bank account. The role of the AML Section finishes at this stage.

In case the AML Section requires additional information/documents from the reporting entity when investigating the STR file, Mr N stated that it does not request this directly from the entity, but via the AMLSCU. Mr N justified this long winded procedure by explaining that the AML Section is not equipped with any legal power entitling it to request directly the reporting entity to provide additional information/documents. However, he admitted that this long procedure causes delay. He stated that, in practice, the AML Section often directly asks the reporting entity, whilst at the same time requesting the AMLSCU to ask for the additional information/documents. This ensures that the AML Section receives information/documents much quicker, as the data is sent straight to the it, instead of via the AMLSCU. Mr N admitted that this practice is not in line with applicable laws, but more effective.

Mr N stated that no electronic information exchange link exists with the AMLSCU. However, he receives STRs via email and also responds by email. In relation to the question about the formation of a committee

composed of employees of the AMLSCU and the AML Section, Mr N explained that the Dubai Public Prosecution Office orders the formation of the committee during its investigation because the AMLSCU does not have employees from strategic partners, such as the police. The formation of the committee utilises the experience of other strategic partners, such as the AML Section.

Mr N concluded the interview by stating that the current model of the AMLSCU is an administrative one and that it may not have enough or adequately trained staff. He suggested that the overall efficiency of the AMLSCU could be improved through better human resource management. He suggested that strategic partners from a number of LEAs, such as the police, customs authority and public prosecution, could join the AMLSCU.

Significant Observations

When considering Mr N's answers, three observations can be made. Firstly, Mr N noted that FLMLC 2002 states that the AMLSCU has the right to seek assistance from LEAs in order to conduct its functions; however, this is inaccurate. Article 7 states that the AMLSCU "shall make the information obtained by it available to the Law Enforcement Agencies for their investigations."

Hence, FLMLC 2002 does not grant the AMLSCU the right to seek assistance from LEAs. As shown in the previous chapter,[29] it is legally obliged to assist LEAs in their investigations by providing them with relevant information.

Secondly, Mr N noted that the AML Section sends an analytical report and a recommendation to the AMLSCU about an STR. However, this practice lacks any legal basis and, more importantly, it actually breaches the provisions of FLMLC 2002 since the Act does not grant any such right to the police or to any LEAs. The FIU, the AMLSCU, is the sole entity which has the right to analyse STRs and to write subsequently analytical reports and then to transmit the STR file to the police or prosecution, so

[29] Article 7 of FLMLC 2002, see (n 694) of Chap. 5.

that these entities can carry out further investigations or commence prosecution. This is attributed to the fact that, pursuant to the FATF standards and FLMLC 2002, the FIU, the AMLSCU, is supposed to have a sufficient number of qualified experts capable of analysing STRs and is thus the sole national entity specialised in this particular task. Moreover, the police, or any of the LEAs, do not have the right to influence the AMLSCU when it comes to it discharging its functions, whether through directions or recommendations. Any other practice prejudices the operational independence of the AMLSCU. Indeed, LEAs, such as the police and the prosecution, can investigate ML cases and take certain decisions; however, this has to be done without undermining the authority of the FIU. The AMLSCU is the national entity which can analyse STRs and this represents the backbone of the FIUs' functions in general, and the AMLSCU's functions in particular.

Lastly, FLMLC 2002 does not equip the police or LEAs with a power to request additional information or supporting documents directly from reporting entities. Hence, the current practice of the AML Section is inconsistent with FLMLC 2002. Even the AMLSCU does not have this power, as shown in the previous chapter.

Analysing the Data and Information from the Interviews

Figure 6.1 shows the number of STRs which were received by the AMLSCU during the period 2002–2011.[30]

Reporting entities submitted more STRs in the UAE and there was an increase from a total of 1750 in 2009 to 2781 in 2010, which is a 59 % increase, and a 137 % increase if one compares the figures against 2008. However, there was a slight decline from 2781 in 2010 to 2576 in 2011. In general, during the period 2002 to 2011 the number of STRs submitted to the AMLSCU increased more than 100 %. This is due to one of two reasons. Firstly, the increase could be a result of the AMLSCU's efforts

[30] These statistics are taken from the "AMLSCU Annual Reports—2009" and the "AMLSCU Annual Reports—2010" as produced by the AMLSCU and Mrs Angeli Pereira (n 740).

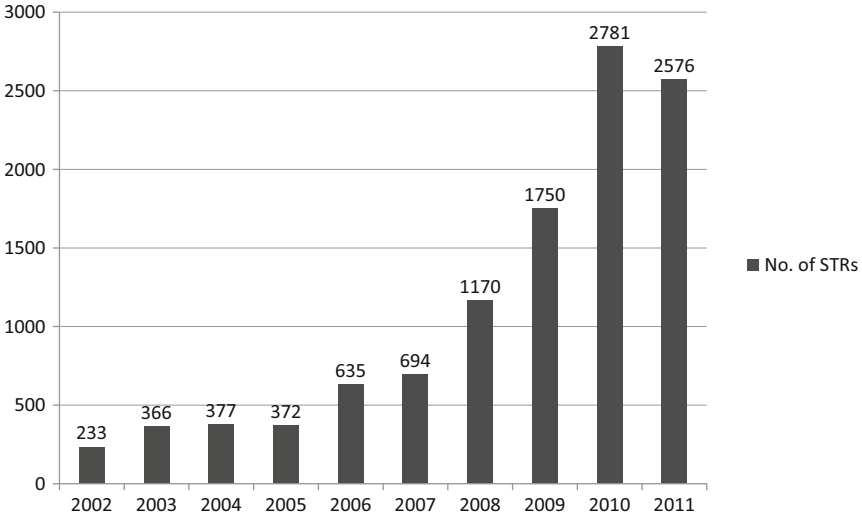

Fig. 6.1 STRs statistics 2002–2011

to enhance awareness amongst reporting entities about STR obligations. Secondly, reporting entities may have adopted a defensive approach and thus submitted all transactions which appear "unusual," but without taking into account whether reasonable grounds exist to suspect that there is ML. Hence, they may simply adopt such an approach to ensure that they are safe and not subject to any of the penalties contained in FLMLC 2002.

Figure 6.2 shows that banks submitted the majority of the STRs to the AMLSCU. For instance, in 2010, banks submitted 2465 out of 2871 STRs, which is 88.7 %.[31] The remaining STRs were submitted by other reporting entities, for example money changers and investment companies.

At the micro-level, 38 from a total of 55 banks within the UAE, that is 69 % of the banks in the UAE, submitted STRs.[32] Moreover, in 2009, 34

[31] AMLSCU Annual Report –2010 (n 769) 22.
[32] Ibid.

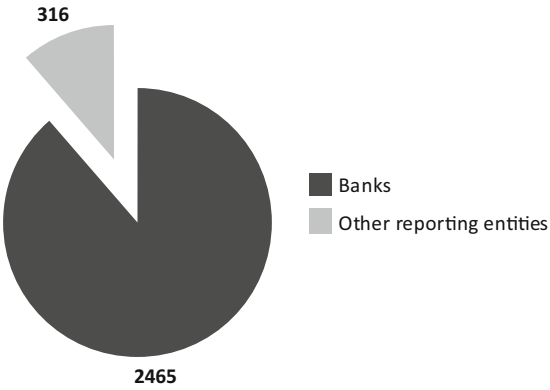

Fig. 6.2 Submission of STRs by banks and other reporting entities—2010

out of 55 banks in the UAE submitted 1445 out of a total of 1750 STRs to the AMLSCU[33] (see Fig. 6.3).

During 2011, banks submitted 2133 out of 2576 STRs to the AMLSCU, that is 83 % of the total numbers of submitted STRs[34] (see Fig. 6.4).

Hence, Figs. 6.2, 6.3 and 6.4 show that banks have submitted the vast majority of STRs out of the total number which have been submitted to the AMLSCU. Banks may be more vulnerable to ML activities/transactions than other reporting entities. Nevertheless, the AMLSCU annual reports do not provide accurate statistics about STRs on ML since the current statistics only show the annual number of STRs on ML, TF and other financial crimes,[35] such as fraud. Hence, despite crucial information and statistics being contained in the AMLSCU's annual reports, statistics about STRs on ML submitted are still vague, though according

[33] 'AMLSCU Annual Report—2009' (n 769) 18.

[34] Mrs Angeli Pereira (n 740).

[35] There is no statutory or case law definition for the term "financial crime." Yet in the UK, this term has been clearly defined. See (n 433) of Chap. 4 and (n 862) of Chap. 7.

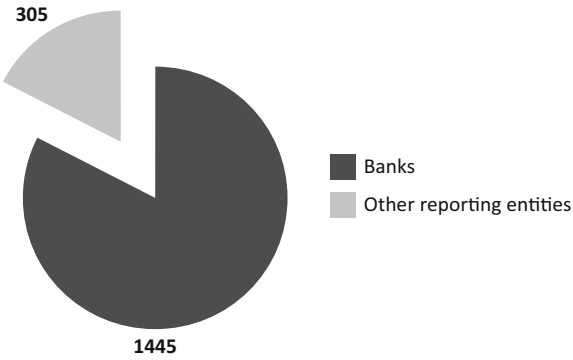

Fig. 6.3 Submission of STRs by banks and other reporting entities—2009

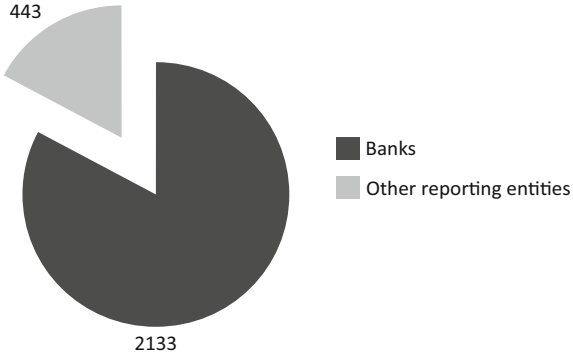

Fig. 6.4 Submission of STRs by banks and other reporting entities—2011

to the statistics for 2010, most of the STRs submitted involved suspected cases of ML and other types of financial crimes.[36]

Figure 6.5 shows that the AMLSCU passed on 1229 out of a total of 2871 STRs in 2010 compared with only 161 out of 1750 STRs in 2009 to the LEAs, so that they could carry out further investigations. The sharp

[36] AMLSCU Annual Report – 2010 (n 769) 24.

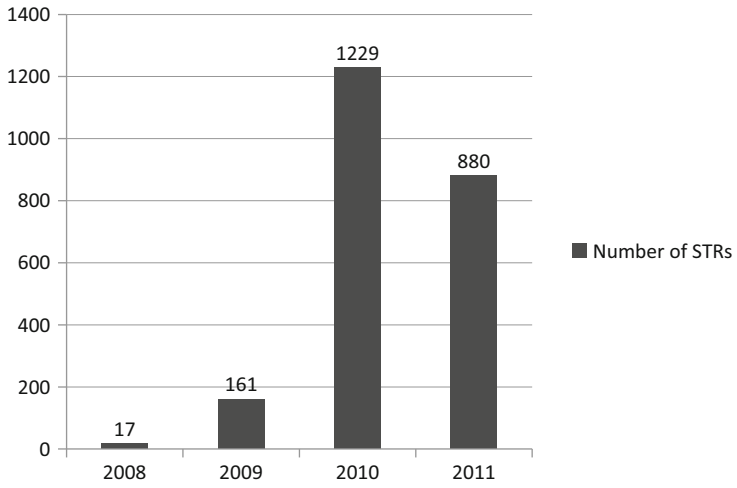

Fig. 6.5 STRs referred to the LEAs 2008–2011

increase, more than 75 %, could be the result of an increase in the quality and quantity of STRs submitted by the reporting entities during 2010.[37]

On the other hand, the number of STRs decreased to 880, out of 2576, in 2011, although there was no big difference between the number submitted by the reporting entities in 2010 and 2011, as illustrated in Fig. 6.1. Figure 6.6 is illustrative in relation to the function of the AMLSCU during 2011.

As mentioned above, the AMLSCU received 2576 STRs from the reporting entities in 2011. When analysing such a statistic, it may be noted that the AMLSCU disseminated 880 STRs to the LEAs for further investigation, whilst deciding there were no reasonable grounds for suspicion in relation to 883 STRs. In addition, it required that ECDD and monitoring be employed in relation to 458 STRs.[38]

Indeed, the number of STRs which were transmitted to LEAs decreased in 2011 in comparison with 2010; nevertheless, there was no big difference in terms of the number submitted by the reporting entities during these two years. This marked decline could be attributed to the fact

[37] Ibid.

[38] Mrs Angeli Pereira (n 740).

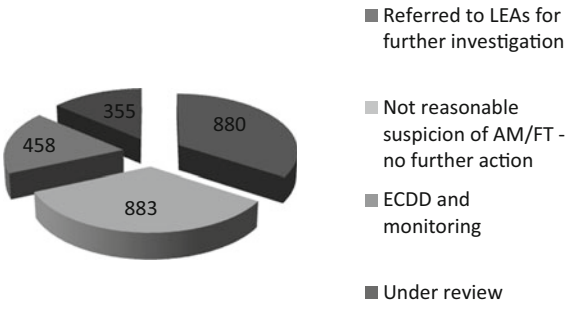

Fig. 6.6 Outcome of STRs and cases—2011

that the reporting entities may adopt a defensive approach, as mentioned above.

More importantly, the AMLSCU referred just 4 out of 1750 STRs to the Public Prosecution Office in 2009. Furthermore, despite a sharp increase in the number of submitted STRs in 2010, the AMLSCU referred only 3 out of 2871 to the Public Prosecution Office in 2010.[39] These huge variations between the number of STRs received by the AMLSCU and the number referred to the Public Prosecution Office could be attributed to one of two reasons, or both. Firstly, the AMLSCU has not sufficient employees and thus cannot properly fulfil its commitments when analysing suspicious transactions/activities. Analysing STRs represents the backbone of the AMLSCU's functions. Secondly, the reporting entities may have adopted a defensive approach. They may send all transactions cases which just appear "unusual" without taking into account whether there are reasonable grounds to suspect that there is ML. If this is the case, the question arises concerning the role/responsibility of the Central Bank or even the AMLSCU in issuing guidance and directing the reporting entities in order to avoid such a "defensive" approach, so that the quality of future STRs can be improved.

The number of STRs, which were referred to the Public Prosecution Office during 2011, is still unclear. The outcome of the interviews in

[39] These STRs involve one natural and two juridical persons. See AMLSCU Annual Report – 2010 (n 769) 25.

these different sectors confirms a number of issues which were analysed in the previous chapter.

Firstly, the reporting entities do not fully understand the basis for STRs, whether it should be subjective or objective, or both. In addition, CBR 24/2000 does not require a specific timeframe from when the "reasonable grounds" of suspicion arise until the bank has to submit STRs to the AMLSCU. This, in turn, has resulted in banks adopting internal banking procedures, which permit on average one week to pass; however, another bank even allowed up to one month.[40] More importantly, according to Mr A, Article 15 of FLMLC 2002 applies when a reporting entity does not obey the STRs requirement, which confirms that the Central Bank currently has no power to impose financial penalties on banks or other financial institutions when they fail to meet the requirement. This is because Article 15 does not state that non-compliance results in penalties, but instead only deals with failing to report STRs to the AMLSCU.[41] Without the Central Bank and all supervisory/regulatory authorities having a power to impose financial penalties for non-compliance, reporting entities may not consider it necessary to adopt internal AML/STRs requirements.

Secondly, the current practice of the AMLSCU in requiring additional information/documents from the reporting entities or even from LEAs in relation to analysing STRs lacks a legal basis. FLMLC 2002 does not explicitly state that the AMLSCU is permitted to do this.

Thirdly, the current online STRs reporting system is available only to banks and money changers. However, it should be available to all reporting entities in order to save valuable time. The percentage of STRs submitted via the online system and the percentage of STRs submitted manually (by paper) are still not included in the AMLSCU's annual reports. Nevertheless, it was expected that the percentage of STRs submitted via online STRs would reach over 90 %.[42] Indeed, the AMLSCU should make greater efforts to increase this percentage since submitting

[40] Chapter 10 provides recommendations to deal with the timeframe in which reporting entities should submit STRs.

[41] Article 15 of FLMLC 2002, see Chap. 5 (n 611).

[42] AMLSCU Annual Report –2010 (n 769) 31.

STRs electronically has a number of advantages, which will be examined in Chap. 9. Furthermore, an electronic link should exist between the AMLSCU and all LEAs, including the Public Prosecution Office, so that information about STRs can be exchanged.

Fourthly, the AMLSCU should provide semi-annual training courses to its staff, so that they are kept abreast of newly emerging complex patterns suggestive of ML transactions/activities. These training courses should also take place in countries which experience sophisticated ML patterns and activities. The AMLSCU may also sign an MOU with foreign FIUs in order to host training courses for its staff. Moreover, it should provide intensive courses for particular employees in the reporting entities, as they are the partners of the AMLSCU.

Fifthly, although Mr A, from the AMLSCU, said that the AMLSCU provides general feedback and specific/case-by-case feedback to the reporting entities about STRs, Mr Z and Mr S, from the banking sector, stated that the AMLSCU does not provide any feedback to the banks.

Sixthly, it seems that the AMLSCU does not provide any of its annual reports to the reporting entities, and Mr Z clearly stated this. In addition, both Mr Z and Mr S, from the banking sector, concluded their interview by stating that they wished that communication/cooperation between the AMLSCU and all banks could be increased. The AMLSCU's annual reports are also not available online and are not publicly available.

Lastly, FLMLC 2002 does not contain any provisions about the procedures of asset recovery and confiscations where those proceeds are derived from ML. In addition, it does not contain any provisions concerning the authority which is tasked with doing so. One of the ambiguities that arises as a result of the absence of provisions in this regard concerns those cases where the laundered proceeds have to be returned to the government. For instance, where an employee who works in a government has embezzled AED500,000 and used it in purchasing a house. In this case, if such proceeds are located outside the UAE, the international cooperation and ratified treaties will be applied.[43] However, after the court's judgment, what is the process for recovery/confiscation of such proceeds, in the interest of the government, if they are located in the UAE? Which

[43] Articles 21 and 22 of FLMLC 2002.

is the competent authority responsible for dealing with such issues and implementing the judgment? There is no provision for dealing with such a situation.

Conclusion

Despite the important information and statistics which are contained in the AMLSCU annual reports, it is still unclear how accurate about STRs on ML, which have been submitted to the AMLSCU, they really are. The current statistics show the annual number of STRs on ML, TF and other financial crimes, such as fraud. Hence, the AMLSCU annual reports do not provide accurate statistics solely in relation to STRs on ML. The annual reports should show accurate statistics, including how many STRs have been transmitted to the court and have resulted in convictions. These statistics are crucial in order to evaluate the annual performance of the reporting entities in relation to understanding STRs requirements. Only this type of statistic informs how efficiently the AMLSCU fulfils its functions, especially in relation to analysing STRs.

When one compares the number of STRs, which are received by the AMLSCU annually, with the number of AMLSCU staff, it emerges that it is difficult for the AMLSCU to discharge fully its responsibilities and commitments. Hence, the AMLSCU should employ more administrative, as well as technical, staff in order to ensure that all tasks are duly taken care of; notably that the AMLSCU does not just receive STRs from the reporting entities, but also receives requests and orders from a number of national and foreign entities. In 2010, it received 7524 search requests and 3508 freeze requests from the court in the UAE. It also received 268 requests from law enforcement and other domestic authorities. Moreover, it received 177 requests from foreign FIUs in 2010. In contrast, it submitted eight requests to foreign FIUs.[44] The AMLSCU should have employees from strategic partners who could be recruited from a number of LEAs, such as the police, the customs authority and the Public Prosecution Office.

[44] For further information about the statistics, see AMLSCU Annual Report – 2010 (n 769) 38–50.

The AMLSCU does not pay much attention to strategic analysis and intelligence. This type of analysis is crucial, as all the collected and analysed information on STRs is employed in order to formulate a new/amended strategy for the future work of the AMLSCU. More importantly, it is questionable whether it is operationally independent from the Central Bank. It should therefore ensure that any doubt that its operations are not separate from the Central Bank is removed. FLMLC 2002 should further bestow more independence on the AMLSCU.

In addition, CBR 24/2000 does not require a specific timeframe from when the "reasonable grounds" of suspicion arise until the bank has to submit STRs to the AMLSCU. This has led to the internal procedures in some banks that allow on average one week to pass, whereas in others bank a whole month may pass. Of course, it is difficult, if not impossible, to require reporting entities to submit STRs within a specific timeframe since the facts of each case are different. Nevertheless, they should be required to report the matter as soon as possible, so that the AMLSCU can carry out its duties and reach a decision promptly.

In light of the current functions of the AMLSCU and its achievements, a crucial question is whether the current administrative type is an ideal model for the AMLSCU or whether another would be better. Thus, the following three chapters deal with the UK's AML system and in particular with SOCA, now the NCA, which is an alternative model; we will examine this model's law enforcement with a view to understanding and answering this particular question.

7

The UK's AML Legislation and System

Introduction

Before an examination of the requirements contained in the UK SARs regime and the role of the SOCA, now the NCA, in relation to it, it is crucial to study how the UK legal system combats ML. The system is firstly based on POCA 2002, as amended by SOCPA 2005, the SCA 2007 and recently the CCA 2013.[1] In addition, MLR 2007 plays a vital role for the UK's AML system.[2] However, a number of secondary regulations exist, for example guidance and rules issued by the FCA and the Joint Money Laundering Steering Group (JMLSG).

[1] Prior to this, a number of ML offences were contained in different statutes, for example in s.24 of the Drug Trafficking Offences Act 1986, the Criminal Justice Act 1988 and Drug Trafficking Act 1994. For detailed information on the history of the UK's AML, see Robin Booth and others, *Money Laundering Law and Regulation*: *A Practical Guide* (First Published, Oxford University Press 2011), 14–16.

See also, Arun Srivastava, 'UK Part II: UK law and practice' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 27 at 29 & 30.

[2] Karen Harrison and Nicholas Ryder, *The Law Relating to Financial Crime in the United Kingdom* (Ashgate Publishing Limited 2013), 162.

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_7

The main objective of the current chapter is it to evaluate the key obligations, spelled out in MLR 2007, which are imposed upon banks and other financial institutions in the UK in order to detect SARs. In addition, the chapter discusses the first group of offences in relation to ML contained in part 7 of POCA 2002. This requires an assessment of three elements, namely criminal property, knowledge and suspicion, since they are directly related to the SARs regime and the offences of failing to report ML cases.

MLR 2007 is discussed in section "MLR 2007". The section evaluates MLR 2007 requirements, which banks and other reporting entities have to adhere to in order to protect themselves against ML activities. These requirements constitute the internal procedures which banks and other reporting entities have to adopt, namely CDD procedures, record keeping and training. In addition, there are commitments imposed on the supervisory authorities. The section also examines the positive role which the FCA and the JMLSG play in enhancing the understanding of the SARs and MLR 2007 requirements among the reporting entities, especially the power of the FCA to impose financial penalties on reporting entities which do not fulfil the SARs requirements. Section "POCA 2002" discusses the principal ML offences in POCA 2002. More importantly, the concepts of criminal property, knowledge and suspicion for the principal ML offences will be critically evaluated. These three terms constitute the main elements which trigger the duty to submit SARs.

The reason for starting the chapter with MLR 2007 is that its obligations have to be taken into account by banks and other financial institutions before SARs are submitted to the competent authority. The implementation of these obligations by financial institutions assists them in making the right decisions in relation to the submission of SARs to the competent authority. In other words, without the adoption of these obligations, banks and other financial institutions could not fulfil the requirements of the SARs regime set out in POCA 2002. Compliance with the SARs regime under POCA 2002 thus necessarily firstly entails adopting the relevant obligations under MLR 2007.

MLR 2007

Imposing civil and criminal responsibility for financial institutions is one of the most successful approaches to prevent ML and other illicit acts.[3] MLR 2007, as amended by the Money Laundering (Amended) Regulations 2012, entered into force on 15 December 2007 and replaced MLR 2003. MLR 2007 was adopted in compliance with the European Union (EU) Third Money Laundering Directive on the prevention of the use of the financial system for the purpose of ML and TF.[4] The regulations define the term "ML" as "an act which falls within section 340(11) of the Proceeds of Crime Act 2002."[5]

The aim of MLR 2007 is to impose criteria which control conduct and are best summed up as KYC (CDD) regulation. The purpose is to adopt a rule which monitors a customer's conduct. The "relevant persons" can thus provide any required documents in the case of prosecution or investigation,[6] which prevents money launderers from accessing not just the financial institutions, but also entities outside the financial sector.[7]

MLR 2007 applies to "relevant persons"[8] in the UK and this encompasses eight categories, namely: (1) credit institutions,[9] (2) financial institutions,[10] (3) auditors,[11] insolvency practitioners,[12] external accountants[13] and tax advisers,[14] (4) independent legal

[3] Janet Ulph and Michael Tugendhath, *Commercial Fraud. Civil Liability, Human Rights and Money Laundering* (First Edition, Oxford University Press 2006), 133.

[4] Directive 2005/06/EC of the European Parliament and of the Council of 26 October 2005. It should be noted that these requirements have been implemented in all EU Member States.

[5] MLR 2007, reg.2 (1).

[6] Alastair Hudson, *The Law of Finance* (Second Edition, Sweet & Maxwell 2013), 434.

[7] William Blair and Richard Brent, 'Regulatory Responsibilities' in William Blair and Richard Brent (eds), *Banks and Financial Crime: The International Law of Tainted Money* (Oxford University Press 2008), 241 at 244.

[8] MLR 2007, reg.3.

[9] MLR 2007, reg.3 (2).

[10] MLR 2007, reg.3 (3).

[11] MLR 2007, reg.3 (4).

[12] MLR 2007, reg.3 (6).

[13] MLR 2007, reg.3 (7).

[14] MLR 2007, reg.3 (8).

professionals,[15] (5) trust or company service providers,[16] (6) estate agents,[17] (7) high value dealers[18] and (8) casinos.[19] These relevant persons are also known as "regulated persons."[20] Accordingly, these bodies must comply with the obligations laid out in MLR 2007 in order to monitor and prevent ML.

Before the main features of MLR 2007 are analysed, it should be noted that the regulations emphasise that firms have to appoint a "nominated officer,"[21] who is usually a Money Laundering Reporting Officer (MLRO),[22] to receive internal reports about suspicious ML cases[23] and who can decide whether or not to submit a SAR to the NCA. There are three fundamental requirements, contained in MLR 2007, which assist with the AML process, especially detecting SARs, namely with regard to CDD procedures, record keeping and training, and supervision. Each of these is analysed in detail below.

CDD Procedures

This part deals with the meaning and the levels of CDD.

The Meaning of CDD

In general, CDD[24] can be defined as an ordinary investigation process which aims at evaluating possible risks which can occur during business relations.

---

[15] MLR 2007, reg.3 (9).

[16] MLR 2007, reg.3 (10).

[17] MLR 2007, reg.3 (11-11A).

[18] MLR 2007, reg.3 (12).

[19] MLR 2007, reg.3 (13).

[20] Alastair Hudson (n 789) 435.

[21] "Nominated officer" means "a person who is nominated to receive disclosures under Part 7 of the Proceeds of Crime Act 2002 (money laundering) or Part 3 of the Terrorism Act 2000 (terrorist property)," MLR 2007, reg.2 (1).

[22] POCA 2002 uses the term "nominated officer" and the FCA uses the term "MLRO." A nominated officer/MLRO is equal to a compliance officer in the UAE.

[23] MLR 2007, reg.20.

[24] There are detailed provisions in regulations 5 to 17 of MLR 2007 with regard to CDD procedures.

The background of the client is important and the investigation is performed by financial institutions. CDD should take place prior to any business agreement being entered into with a new customer.[25]

Unlike the Regulations in the UAE,[26] MLR 2007 defines CDD procedures as comprising the identification of the customer, or any beneficial owner of the customer and verification of the identity, or to obtain information in order to understand the commercial relationship and its intended nature.[27] MLR 2007 emphasises that a "relevant person"[28] must adopt CDD procedures if he or she: (1) creates a business relationship; (2) performs an occasional transaction;[29] (3) has a suspicion that ML is taking place; and (4) has a suspicion about the veracity of the information, which was previously obtained for the purpose of CDD.

A relevant person has to apply CDD procedures in other suitable situations to current clients if there is a "risk sensitive basis."[30] Generally, the verification of the client's identity and any beneficial owner should be undertaken prior to the establishment of a business relationship or before occasional transactions are conducted;[31] how-

[25] For a comparative analysis, see Tang Jun and Lishan Ai, 'The international standards of criminal due diligence and Chinese practice' (2009) 12 (4) Journal of Money Laundering Control 406, 407.

[26] See Chap. 5.

[27] Reg.5 of MLR 2007 defines CDD procedures as follows:

> (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
> (b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
> (c) obtaining information on the purpose and intended nature of the business relationship.

For the purposes of this section, the beneficial owner has different meanings according to the type of customer, reg.6 of MLR 2007.

[28] MLR 2007, reg.3 (n 791).

[29] "Occasional transaction" means "a transaction (carried out other than as part of a business relationship) amounting to 15,000 euro or more, whether the transaction is carried out in a single operation or several operations which appear to be linked." MLR 2007, reg.2 (1).

[30] MLR 2007, reg.7(1–2).

[31] MLR 2007, reg.9 (2).

ever, the verification may be concluded during the establishment of a business relationship in case this is necessary so as not to disrupt the normal course of business and there is no concern about the likelihood of ML.[32]

Indeed, CDD depends on the level or degree of the ML risk. MLR 2007 adopts a three-level risk-based method in respect of CDD. The respective level depends on how much a customer represents a risk of ML. The three levels are: (1) standard CDD, (2) simplified CDD and (3) ECDD. All of these will be assessed in detail below.

The Levels of CDD

The Standard Approach

Standard CDD checks are a mandatory requirement, which should be performed in all situations except that the simplified or enhanced method is being employed. It may be helpful to mention such an approach again, that it comprises: (1) identifying the customer and verifying his or her identity; (2) identifying the beneficial owner, where appropriate, and verifying the beneficial owner's identity; and (3) gaining information about the aim and intended nature of the commercial relationship.[33]

Relevant persons have also to monitor their clients during the course of the business relationship and not only at the beginning. Hence, "ongoing monitoring" is mandated and should be done in the following two ways:

---

[32] MLR 2007, reg.9 (3).

In addition, reg.9 (4–5) of MLR 2007 states that:
(4) The verification of the identity of the beneficiary under a life insurance policy may take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy.
(5) The verification of the identity of a bank account holder may take place after the bank account has been opened provided that there are adequate safeguards in place to ensure that
(a) the account is not closed; and
(b) transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder), before verification has been completed.

[33] Reg.5 of MLR 2007 (n 810).

1. the relevant persons must scrutinise the transactions during the business relationship, in order to ensure that the transactions are harmonious with the relevant person's knowledge about the client, his business and his risk profile.
2. firms[34] are required to maintain information, documents and data which have been gained for the aim of CDD procedures and to keep them updated.[35]

As such, the term "monitoring" comprises less stringency in comparison with CDD procedures.[36] It is important to mention that a relevant person, who is unable to adopt standard CDD procedures, will be prohibited from establishing a business relationship or carrying out an occasional transaction with the respective customer.[37]

---

[34] Firm means "any entity, whether or not a legal person, that is not an individual and includes a body corporate and a partnership or other unincorporated association": MLR 2007, reg.2 (1).

[35] MLR 2007, reg.8.

[36] William Blair and Richard Brent (n 790) 249.

[37] Reg.11 of MLR 2007 states that:

> (1) Where, in relation to any customer, a relevant person is unable to apply customer due diligence measures in accordance with the provisions of this Part, he
> (a) must not carry out a transaction with or for the customer through a bank account;
> (b) must not establish a business relationship or carry out an occasional transaction with the customer;
> (c) must terminate any existing business relationship with the customer;
> (d) must consider whether he is required to make a disclosure by Part 7 of the Proceeds of Crime Act 2002 or Part 3 of the Terrorism Act 2000.
> (2) Paragraph (1) does not apply where a lawyer or other professional adviser is in the course of ascertaining the legal position for his client or performing his task of defending or representing that client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings.
> (3) In paragraph (2), 'other professional adviser' means an auditor, accountant or tax adviser who is a member of a professional body which is established for any such persons and which makes provision for
> (a) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and
> (b) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards"

Moreover, bond trustees are exempted from adopting CDD procedures contained in reg.5 (b) of MLR 2007. MLR 2007, reg.12.

The Simplified Approach

In certain circumstances, there are exceptions to the requirement to undertake CDD procedures, and simplified due diligence means that it is not mandated to carry out CDD procedures. Hence, there is no need to identify the client or to verify his identity, to identify the beneficial owner or, where relevant, to verify his identity, or even to gain information about the aim and intended nature of the commercial relationship.[38]

MLR 2007 allows for such cases in exceptional circumstances. For example, relevant persons do not have to undertake CDD procedures when there are reasonable grounds to believe that the customer is a public authority in the UK or a financial institution under the EU Third Money Laundering Directive.[39] However, MLR 2007 limits these exceptional cases. In addition, even where there is an exceptional case, it is still essential for relevant persons to adopt "ongoing monitoring"[40] in respect of their business relationships in order to detect SARs.[41]

The Enhanced Approach

The relevant persons must perform ECDD and enhanced ongoing monitoring in particular situations, which are set out in MLR 2007. There are three particular situations where such an approach is adopted, namely where the customer has not been physically present for identification purposes, there is a corresponding banking relationships/business relationship with a respondent institution from the non-European Economic Area (EEA) or the transaction is with a PEP.[42] In such circumstances, ECDD and enhanced ongoing monitoring have to be undertaken by the relevant persons. These circumstances will be discussed in detail below.

---

[38] Kathleen A Scott and Rebecca Stephenson, 'Enhanced customer due diligence for banks in the UK and the US' (2008) 23 (2) Journal of International Banking and Financial Law 89.

[39] MLR 2007, reg.13.

[40] MLR 2007, reg.8 (n 818).

[41] Arun Srivastava (n 784) 77.

[42] MLR 2007, reg.14 (2–4).

Where the customer is not actually present for the purpose of identification, a relevant person is bound to conduct particular and appropriate procedures in order to recompense for the higher risk of ML. The regulations have stipulated several methods, which can be adopted by a relevant person with a view to achieving this target.[43]

For non- EEA[44] clients, the ECDD method will be applied if a credit institution[45] (the correspondent) has or proposes to enter into a correspondent banking relationship with a respondent institution (the respondent) from a non-EEA state. In such a case, there are rafts of commitments to be performed by a relevant person.[46]

ECDD will be applied in the event that a customer is a PEP. The meaning of a PEP is defined by regulations as including individuals who are or have at any time in the preceding year been entrusted with a prominent public function by a state outside the UK, a Community institution or an international body.[47] Moreover, the regulations also provide that other persons have to be considered a PEP, for instance members of parliament, members

[43] Reg.14 (2) of MLR 2007 imposes the following procedures:
A. Obtaining additional information, data, or documents with the purpose of verifying the client's identity.
B. Making use of confirmatory certification requirements from credit or financial institutions, which are subject to the EU Third Money Laundering Directive, or undertaking assistance procedures to verify or certify provided documents.
C. Verifying that the first payment is made via an account opened in the client's name with a credit institution.

[44] A "non-EEA state" means a state that is not an EEA state. MLR 2007, reg.2 (1).

[45] MLR 2007, reg.3 (2) (n 792).

[46] Reg.14 (3) of MLR 2007 requires the following commitments:
A. Adequate information about the respondent must be collected in order to completely understand the nature of the respondent's business.
B. Recognising the status of the respondent and the nature of its reputation and supervision. This can be done through publicly available information.
C. Evaluating the respondent's controls in respect of AML.
D. An approval from senior management must be obtained. This should be done prior to establishing a new correspondent banking relationship.
E. Documenting the responsibilities of both respondent and correspondent.
F. Where the respondent's customers have direct access to accounts of the correspondent, the relevant person has to be satisfied that the respondent:
(i) has verified the identity of those customers and performs ongoing monitoring of them; and
(ii) is able to supply to the correspondent, upon request, the documents, data or information obtained from the CDD checks and the ongoing monitoring.

[47] MLR 2007, reg.14 (5)(a).

of the Supreme Court and heads of states.[48] In addition, an "immediate family member" of a PEP and a "known close associate" of a PEP will be also deemed to fall into this category.[49] There are a number of procedures that must be adopted by a relevant person if he or she proposes to enter into a business relationship or perform an occasional transaction with a PEP.[50]

Other Situations Representing a Higher Risk of ML

It is critical to appreciate that in addition to the aforementioned three cases of ECDD measures,[51] measures will also be imposed on a relevant person "in any other situation which by its nature can present a higher risk

---

[48] The following persons are considered PEPs:
"(i) heads of state, heads of government, ministers and deputy or assistant ministers;
(ii) members of parliaments;
(iii) members of supreme courts, of constitutional courts or of other high-level judicial bodies, whose decisions are not generally subject to further appeal, other than in exceptional circumstances;
(iv) members of courts of auditors or of the boards of central banks;
(v) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; and
(vi) members of the administrative, management or supervisory bodies of state-owned enterprises." MLR 2007, sch.2 para 4 (1)(a).

[49] MLR 2007, reg.14 (5)(b)(c).

"Immediate family members" comprise parents, one's partner, spouse, children and their spouses or partners. MLR 2007, sch.2 para 4 (1)(c).

"Persons known to be close associates" encompass two cases:
"(i) any individual who is known to have joint beneficial ownership of a legal entity or a legal arrangement, or any other close business relations with a PEP; and
(ii) any individual who has sole beneficial ownership of a legal entity or legal arrangement, which is known to have been set up for the benefit of a PEP." MLR 2007, sch.2 para 4 (1)(d).

[50] Reg.14 (4) of MLR 2007 states that a relevant person must:
A. obtain approval from suitable senior management in order to create the business relationship with a PEP;
B. take appropriate measures to determine the sources of wealth and funds, which are utilised in the proposed business relationship or occasional transaction,
C. perform enhanced ongoing monitoring of the relationship after the business relationship is entered into, and
D. conduct adequate risk-based measures in order to decide whether or not a client is a PEP.

See Kathleen A Scott and Rebecca Stephenson (n 821) 89.

[51] Which are (1) clients not physically present, (2) non-EEA clients and (3) PEPs. Reg.14 (2–4) of MLR 2007 (n 825).

of money laundering."[52] Accordingly, a relevant person ought to maintain adequate documents, data or information about the conditions and business of his or her clients for two reasons: (1) to increase the chance of detecting the use of client's services and products for ML through observing client and client's business activity and (2) to report its risk evaluation procedure and thereby successfully to reduce the risk of customers laundering money.[53]

In response to the FATF's public statement on high-risk and non-cooperative jurisdictions published on 19 October 2012,[54] HM Treasury issued an Advisory Notice in which it advised firms to apply ECDD measures in accordance with the particular risk when dealing with identified jurisdictions.[55] Although MLR 2007 does not give examples of situations where a higher risk may be present, a number of circumstances can be identified: (1) non-citizen clients; (2) customers who are carrying out transactions in or through countries with known high levels of drug production, ML, human trafficking, corruption or organised crime in general; (3) situations where customers are providing insufficient identification evidence, or are reluctant to provide identification evidence; and (4) customers or groups of customers who often deal with the same person or group of persons.[56]

Indeed, the term "any other situation which by its nature can present a higher risk of money laundering"[57] is a broad term.[58] Any business relationship or transaction could be covered since there is no criterion, indication or guidance that can be followed to decide whether or not a business relationship presents a "higher risk of money laundering."

---

[52] MLR 2007, reg.14 (1)(b).

[53] Kathleen A Scott and Rebecca Stephenson (n 821) 89.

[54] FATF Public Statement, 'High-risk and non-cooperative jurisdictions' published by the FATF on 19 October 2012, available online at: http://www.fatf-gafi.org/media/fatf/documents/FATF%20Public%20Statement%2019%20October%202012.pdf (accessed on 20th December 2014).

[55] For further details about the Advisory Notice, see 'Advisory Notice on Money Laundering and Terrorist Financing controls in Overseas Jurisdictions' issued by the HM Treasury, available online at: http://www.hm-treasury.gov.uk/d/advisory_notice_moneylaundering_nov2012.pdf (accessed on 20th December 2014).

[56] Christ Stott and Zai Ullah, 'Money Laundering Regulations 2007: Part 1' (2008) 23 (3) Journal of International Banking Law and Regulation 175, 177.

[57] MLR 2007, reg.14 (1)(b) (n 835).

[58] Christ Stott and Zai Ullah (n 839) 177.

The term is so wide and exceeds all of the three above circumstances.[59] The term "higher risk" should be narrowly interpreted and should be limited to the above examples[60] for two main reasons. Firstly, there is a risk that the term is being mis-utilised for subjective purposes. For example, if there is a quarrel between a banker and a client, the banker can annoy the client and obstruct his transaction by adopting ECDD procedures on the basis that there is a "higher risk of money laundering," even when this is not the case. This is due to MLR 2002 not limiting the term to certain circumstances. Secondly, the term "higher risk of money laundering" is wide enough to accommodate the three above ECDD circumstances,[61] which render these three circumstances redundant.[62]

Record Keeping and Training

The relevant person is also required to maintain adequate records.[63] The aim of this is to ensure that records and procedures, which are taken by the relevant person, comply with CDD measures.[64] Relevant persons are obligated to keep records for at least five years starting

[59] Which are (1) clients not physically present, (2) non-EEA clients and (3) PEPs. Reg.14 (2–4) of MLR 2007 (n 825).

[60] Christ Stott and Zai Ullah (n 839).

[61] Which are (1) clients not physically present, (2) non-EEA clients and (3) PEPs. Reg.14 (2–4) of MLR 2007 (n 825).

[62] In addition, relevant persons are under an obligation not to establish or carry on a correspondent banking relationship with a shell bank or a corresponding banking relationship with a bank, which is known to permit its accounts to be used by a shell bank. A "shell bank" means "a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction, which has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate or third-country financial conglomerate." MLR 2007, reg.16 (5).

Moreover, reg.16 (1–3) of MLR 2007 states that setting up an unknown passbook or an anonymous account for any existing or new client by a credit or financial institution is prohibited. This is because these situations could be easily used for ML purposes and would render it difficult to identify the person(s) who is/are managing such kind of banks and unknown accounts. See Alastair Hudson (n 789) 436.

[63] Detailed provisions with regard to record keeping, procedures and training in regulations are contained in reg.19–21 of MLR 2007. Reg.19 (2) provides a definition for "records" for the purpose of this issue.

[64] Christ Stott and Zai Ullah (n 839) 178.

from the expiration of the business relationship or when the last dealing was completed.[65]

The relevant persons have also to adopt and retain "appropriate and risk-sensitive" policies and procedures[66] with regard to a number of matters, such as CDD measures, ongoing monitoring and record keeping[67] for the purposes of detecting SARs. Record keeping and adopting and retaining "appropriate and risk-sensitive" policies and procedures require that the relevant person has well trained employees,[68] who are well versed with regard to their respective duties. These training courses must be provided on a regular basis and should focus on SARs on ML.[69] Hence, it is explicitly required that relevant persons provide training to their employees on a regular basis. However, UAE CBR 24/2000 does not require this, as shown in Chaps. 5 and 6.

---

[65] MLR 2007, reg.19 (3).

[66] These policies encompass procedures:

(a) which provide for the identification and scrutiny of
(i) complex or unusually large transactions;
(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and
(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;
(b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity;
(c) to determine whether a customer is a politically exposed person;
(d) under which
(i) an individual in the relevant person's organisation is a nominated officer under Part 7 of the Proceeds of Crime Act 2002 and Part 3 of the Terrorism Act 2000;
(ii) anyone in the organisation to whom information or other matter comes in the course of the business as a result of which he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing is required to comply with Part 7 of the Proceeds of Crime Act 2002 or, as the case may be, Part 3 of the Terrorism Act 2000; and
(iii) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing. MLR 2007, reg.20 (2).

[67] MLR 2007, reg.20 (1).

[68] MLR 2007, reg.21.

[69] Ibid.

Supervision

Pursuant to MLR 2007, each type of relevant person is supervised by a specific agency.[70] The objective of this is to ensure that every relevant person keeps records in a proper way and also to guarantee that the procedures are compatible with MLR 2007.[71] Two main commitments are imposed on supervisory authorities. Firstly, a supervisory authority must efficiently observe relevant persons and must implement adequate internal procedures and policies. This is done in order to ensure due compliance with the requirements of MLR 2007. Secondly, it must immediately inform SOCA, now the NCA, if it knows or suspects that any person is involved in ML.[72] The regulations also contain provisions enabling officers of designated authorities[73] to obligate relevant persons to provide information, to produce documents and to answer questions in certain circumstances.[74]

FCA

In addition to MLR 2007 and POCA 2002, the FSA played an important role in fighting ML pursuant to Part 1 of the Financial Services and Markets Act 2000 (FSMA 2000).[75] It regulated most financial services markets, exchanges and firms. Moreover, it authorised and supervised most financial

[70] There are detailed provisions with regard to supervision and registration set out in Part 4 of MLR 2007.

[71] Alastair Hudson (n 789) 436.

[72] MLR 2007, reg.24 (1–2).

[73] "Officer" means:

> (a) an officer of the Authority, including a member of the Authority's staff or an agent of the Authority;
> (b) an officer of Revenue and Customs; or
> (c) a relevant officer.

"Designated authority" means:

> (a) the Authority; and
> (b) the Commissioners. MLR 2007, reg.36.

[74] MLR 2007, reg.37–41. It should be noted that if the relevant person does not obey the officers of the designated authorities, civil or criminal sanctions can be imposed, reg.42 & 45 of MLR 2007.

[75] Part 1 of FSMA 2000 has been abolished by the Financial Services Act 2012.

institutions. Those firms which were regulated by the FSA were subjected to further obligations, in addition to MLR 2007 and POCA 2002, as detailed in the FSA Handbook.[76] The FSA monitored financial institutions and ensured that they adhered to its AML requirements[77] and could also prosecute breaches of MLR 2007.[78] One of its key goals was to prevent financial businesses being used to commit financial crimes,[79] notably ML, and for this purpose it imposed a number of administrative sanctions and financial penalties.[80]

In this context, it is important to point out that the FSA imposed a financial penalty of £140,000 on 5 May 2010 on Alpari (UK) Ltd,[81] since it did not manage to adopt appropriate AML systems and controls, failed to conduct adequate CDD measures at the account opening stage and also did not monitor its accounts sufficiently. Furthermore, its customer relationship was not operated on a face-to-face basis. In addition, Alpari did not implement appropriate systems to check customers against UK and global sanction lists and did not ascertain which customers were PEPs.[82]

On 26 July 2012, the FSA imposed a financial penalty of £294,000 on Turkish Bank (UK) Ltd (TBUK) for breaching MLR 2007.[83] Between 15 December 2007 and 3 July 2010, TBUK failed to obey MLR 2007 in relation to the following three aspects:

---

[76] The FSA Handbook contained rules and guidance.

[77] For further information, see Andrew Campbell, 'The Financial Services Authority and the Prevention of Money Laundering' (2000) 4 (1) Journal of Money Laundering Control 7.

[78] For the investigative and enforcement powers of the FSA in detail, see Nicholas Ryder 'The Financial Services Authority and money laundering: a game of cat and mouse' (2008) 67 (3) Cambridge Law Journal 635, 646 & 647.

[79] Charles Proctor (n 924) 147.

In addition, s.1H (3) of FSMA 2000, as amended by the Financial Services Act 2012, defines the term "financial crime" to include any offence involving:

(a) fraud or dishonesty,
(b) misconduct in, or misuse of information relating to, a financial market,
(c) handling the proceeds of crime, or
(d) the financing of terrorism.

[80] Under MLR 2007, reg.42.

[81] Alpari is an online provider of foreign exchange services for speculative trading.

[82] Available online on FSA's website at: http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/077.shtml (accessed on 4th May 2015)

[83] Available online on FSA's website at: http://www.fsa.gov.uk/static/pubs/final/turkish-bank.pdf (accessed on 13th May 2015).

1. not establishing appropriate and risk-sensitive measures for its correspondent banking relationships;[84]
2. not adopting adequate CDD measures and ongoing monitoring whether the firm's customers acted as respondent banks and not reconsidering these relationships;[85] and
3. not maintaining adequate records in relation to the aforementioned issues.

On 1 April 2013, the FSA dismantled and renamed itself 'FCA' in accordance with the Financial Services Act 2012.[86] That Act introduced a new financial services regulatory regime. FSMA 2000, as amended by the Financial Services Act 2012, introduces the Prudential Regulation Authority (PRA)[87] and the FCA.[88] The PRA[89] forms part of the Bank of England and is responsible for the prudential regulation and supervision of banks, credit unions, building societies, insurers and investment firms.[90] It sets standards and supervises financial institutions for individual firms and enhances the safety and soundness of PRA-authorised persons.[91]

Most importantly, the FCA authorises firms[92] and regulates the financial services industry in the UK. It also supervises the autho-

[84] Under MLR 2007, reg.14 (1).

[85] Under MLR 2007, reg.14 (3) (n 829).

[86] S.1A of FSMA 2000 as amended by the Financial Services Act 2012.

[87] S.2A of FSMA 2000.

[88] S.1A of FSMA 2000.

[89] See http://www.bankofengland.co.uk/PRA/Pages/default.aspx (accessed on 26th May 2015).

[90] Sch.9 (2) para 4 of POCA 2002 defines the supervisory authorities as follows:

(1) The following bodies are supervisory authorities
(a) the Commissioners for Her Majesty's Revenue and Customs;
(b) the Department of Enterprise, Trade and Investment in Northern Ireland;
(c) Financial Conduct Authority;
(d) the Gambling Commission;
(e) the Office of Fair Trading;
(ea) Prudential Regulation Authority;
(f) the Secretary of State; and
(g) the professional bodies listed in sub-paragraph (2).

[91] S.2B (2) of FSMA 2000.

For further information about the PRA, see Alastair Hudson (n 789) 220–222.

[92] S.19 of FSMA 2000.

rised persons.[93] Every firm, which is authorised by the FCA, has to meet the standards set out in the FCA Handbook.[94] Among various objectives, the FCA aims to protect and enhance the integrity of the UK financial system,[95] prevent firms from being used for financial crime,[96] and detect and prevent ML. Firms have therefore to comply with the applicable ML rules, which are issued by the FCA and are referred to as "Senior Management Arrangements Systems and Controls" (SYSC).[97] The SYSC requires firms to appoint an MLRO[98] and to ensure that as part of their internal controls appropriate AML training is provided to their employees.[99]

The FCA is equipped with broad enforcement powers and can thus pursue criminal, civil and regulatory actions against firms or individuals which/who do not meet the applicable standards. For instance, it can withdraw a firm's authorisation, impose financial penalties on firms or individuals which/who breach the rules or commit market abuse[100] and bring criminal prosecutions against those who commit financial crimes. On 8 August 2013, the FCA imposed a financial penalty of £525,000 on Guaranty Trust Bank UK Limited (GTBUK) because it failed to take reasonable care to establish and maintain effective internal AML systems and controls in relation to customers who posed a higher ML risk under MLR 2007, including those customers deemed to be PEPs.[101]

While the FCA can impose financial penalties on reporting entities which do not fulfil SAR/AML requirements, the UAE Central Bank

---

[93] S.1 L of FSMA 2000.

[94] The FCA Handbook replaces the FSA Handbook. The FCA Handbook is available on the FCA's website at: www.fca.org.uk (accessed on 24th October 2014).

[95] The term "UK financial system" means (a) financial markets and exchanges, (b) regulated activities and (c) other activities connected with financial markets and exchanges. S.1I of FSMA 2000.

[96] S.1D (2)(b) of FSMA 2000.

[97] SYSC is available on the FCA's website at: www.fca.org.uk (accessed on 24 October 2014).

[98] SYSC 3.2.6I.

[99] SYSC 3.2.6G.

[100] Under MLR 2007, reg.42.

[101] Available on the FCA's website at: http://www.fca.org.uk/your-fca/documents/final-notices/2013/guaranty-trust-bank-uk-limited (accessed on 29th October 2014).

does not have such power, as shown in Chap. 5. However, such power results in the adoption of internal AML/SAR requirements since reporting entities will naturally want to avoid financial penalties.

JMLSG

The JMLSG provides useful guidance to assist the understanding of MLR 2007 requirements. It consists of the leading UK trade associations in the financial services industry.[102] It provides good practice guidance on counteracting ML and for interpreting MLR 2007.[103] It periodically reviews its guidance,[104] which is mainly for FCA regulated business and firms represented by JMLSG's member bodies.[105] However, firms which are outside the regulated sector and subject to MLR 2007 can also utilise the guidance. The guidance has a number of objectives, for example to interpret the regulations and relevant law on ML,[106] so that firms can properly implement them in practice. The guidance also aims at providing assistance to firms by adopting internal controls with a view to reducing the risk of being exploited by money launderers.[107]

Overall, MLR 2007 imposes a great number of regulatory commitments on financial bodies in general. The regulations maybe complex and tough; however, relevant persons ought to understand accurately how these regulations affect their business. Accordingly, adequate rules ought to be put in place in order to ensure that the regulations are obeyed,[108] as

[102] The JMLSGs members consists of 18 associations, for example the Association of British Insurers (ABI), Association of British Credit Unions Ltd (ABCUL) and Association of Financial Mutuals (AFM). See www.jmlsg.org.uk (accessed on 2nd December 2014).

[103] Karen Harrison and Nicholas Ryder (n 785) 28.

[104] The guidance was introduced in 1990 and has been subjected to a number of reviews, also to accommodate changes introduced by POCA 2002 and MLR 2007.

[105] Detailed information on the JMLSG and its guidance are available online on the JMLSG website at: www.jmlsg.org.uk (accessed on 2 December 2014).

[106] Nicholas Ryder, *Money Laundering – An Endless Cycle*? (First Published, Routledge Cavendish 2012), 84.

[107] Ibid.

[108] Christ Stott and Zai Ullah (n 839) 178.

otherwise there is a high risk that relevant persons will expose themselves to civil penalties, as well as criminal liability.[109]

Furthermore, the determination of the degree of ECDD is generally dependent on the ML risk evaluation which could arise in any of the three above situations.[110] Obviously, the risk evaluation will be undertaken by the relevant person. Relevant persons are therefore best advised to document the basis for any evaluation and to retain information and data since these elements are pertinent for any evaluation.[111]

POCA 2002

This section examines the offences in relation to ML, which are contained in Part 7 of POCA 2002, which entered into force on 24 February 2003. POCA 2002 defines ML as an act which falls into one of four categories: (1) an offence under section 327, 328 or 329 of POCA 2002; (2) attempting, conspiracy or inciting the commission of any of the offences in category (1); (3) aiding, abetting, counselling or procuring any of the offences in category (1); or (4) would constitute any of the offences, mentioned in the previous three categories, if it occurred in the UK.[112]

The definition of ML in MLR 2007[113] is compatible with the above definition. This is unlike the UAE AML system where there is a difference in the ML definition between FLMLC 2002 and CBR 24/2000, as shown in Chap. 5. These crimes, which constitute ML under POCA 2002, can be classified into two principal types: (1) general crimes and (2) crimes relating to the "regulated sector."[114] The criminal offences can be also divided into three groups: (1) the principal offences relating to

[109] Reg.42 & 45 of MLR 2007 (n 857).

[110] Which are (1) clients not physically present, (2) non-EEA clients and (3) PEPs. Reg.14 (2–4) of MLR 2007.

[111] Kathleen A Scott and Rebecca Stephenson (n 821) 89.

[112] S.340 (11) of POCA 2002.

[113] MLR 2007, reg.2 (1) (n 788).

[114] John Wright, 'Introduction to amended guideline 12 (the Proceeds of Crime Act) and new Guideline on the Formalities for Drafting an Award' (2010) 76 (2) Arbitration 291, 294.

The term "regulated sector" will be explained in Chap. 8.

ML, (2) the offences relating to the failure to report ML cases and (3) the tipping off offences.

There are three major goals of Part 7 of POCA 2002, which are: (1) to convict anybody accepting, by whatever means, any profit from "criminal property;" (2) to require that particular types of transaction are divulged to the authorities; and (3) to convict those who tip off money launderers.[115]

This section discusses the first group of offences and their essential elements, namely the notion of criminal property, knowledge and suspicion. Analysing these three elements is essential since they are directly related to the UK SARs regime and the basis of SARs. In other words, the critical evaluation of the UK SARs regime and the basis of SARs require an analysis of the above three elements. The second and third group of offences are analysed in the following chapter since they are directly associated with the SARs regime.

The Principal Offences Contained in Part 7 of POCA 2002

The Act contains three principal ML offences, which are the concealing offence, the arranging offence and the acquisition, use and possession offence. These offences are also commonly known as the "substantive money laundering offences"[116] since they are subjectively based on knowledge or suspicion, as discussed later. Furthermore, such offences may be committed by any persons regardless of whether or not he/she works in the "regulated sector.".[117]

[115] Alastair Hudson (n 789) 414—415.

[116] Stephen Gentle, 'Proceeds of Crime Act 2002: update' (2008) 56 (May) Compliance Officer Bulletin 1, 14.

[117] Nicholas Ryder, *Financial Crime in the 21st Century*: *Law and Policy* (Edward Elgar Publishing Limited 2011), 35.

The Concealing Offence

This offence is established if a person conceals, disguises, converts, transfers or removes "criminal property" from the UK.[118] Three main conditions must be met for the concealing offence. Firstly, a person charged must have committed one or more of the five listed activities of (1) concealing, (2) disguising, (3) converting, (4) transferring and/or (5) removing. Secondly, the subject of the specific activity must be centred on a "criminal property." Thirdly, a person charged must commit the activity in the UK. Indeed, the Act broadly interprets the terms "concealing or disguising" criminal property so that it can encompass concealing or disguising its source, disposition, nature, movement, location or ownership or any rights in relation to it.[119]

An example of concealing criminal property would be if a person hands over money, which he has stolen from a jewellery shop, to his wife in order to conceal it in the loft. If his wife puts the money in the loft behind the cupboard, she would consequently commit the crime of "concealing." She would be guilty of "disguising" and "concealing" the money, if for example she separates the money and places banknotes behind her clothes in her wardrobe. She would commit the offence of "removing" the money from the jurisdiction, if she packed it inside her handbag when going on a vacation. She would commit the offence of "converting" the criminal property if she tried to exchange the stolen sterling banknotes into euros when she is abroad.[120] Another example of "converting" criminal property is if a person permits another to use his bank account to deposit stolen money.[121] The crime of "transferring" criminal property will be com-

[118] S. 327(1) of POCA 2002 states that a person commits an offence if he or she:

(a) conceals criminal property;
(b) disguises criminal property;
(c) converts criminal property;
(d) transfers criminal property;
(e) removes criminal property from England and Wales or from Scotland or from Northern Ireland.

[119] POCA 2002, s.327 (3).

[120] Alastair Hudson (n 789) 416.

[121] *R v Fazal* (*Mohammed Yassen*), [2009] EWCA Crim 1697.

mitted if the wife deposited the money into her bank account and then transferred it to a bank account in France.[122]

In *Ahmad* (*Mohammad*) *v HM Advocate*,[123] the defendant was the secretary, director and 50/50 shareholder together with another person of a company trading in Glasgow under the name Makkah Travel. The company was set up in 2002 to operate as a travel agency and a money services bureau. The defendant was convicted of transferring and removing criminal property from Scotland, namely £2,256,646 of cash money by paying it into the National Westminster Bank plc and transmitting the value to Pakistan, the UAE and China.[124]

For the purpose of establishing the concealing offence, three elements have to be established, by the prosecution. Firstly, the prosecution has to prove that the property constitutes the proceeds of illegal activity.[125] In the case of *R v Montila*,[126] the court stated that: "[it] was necessary for the Crown to prove that the property," which had been converted, was in fact the proceeds of crime.[127]

Secondly, the prosecution has to prove that the person, who is charged, knew or suspected[128] that the property was criminal property. Thirdly, the prosecution must prove that the person charged acted in order to conceal or disguise the source, nature, movement, disposition, location or ownership or any rights with respect to the property.[129]

There are three main defences available to avoid being charged for the concealing offence: (1) authorised disclosure,[130] (2) the relevant crimi-

---

[122] Alastair Hudson (n 789) 416.

[123] [2009] HCJAC 60.

[124] Contrary to POCA 2002, s. 327(1)(d) and (e).

[125] Rudi Fortson, 'Money Laundering Offences under POCA 2002' in William Blair and Richard Brent (eds), *Banks and Financial Crime*: *The International Law of Tainted Money* (Oxford University Press 2008), 155 at 177.

[126] [2004] UKHL 50.

[127] Ibid para 23.

[128] Rudi Fortson (n 908) 177.

[129] Evan Bell, 'Concealing and disguising the criminal property' (2009) 12 (3) Journal of Money Laundering Control 268, 269.

[130] The authorised disclosure defence is also applied to all principal ML offences. S.327 (2) of POCA 2002 provides that a person will be exempt from the concealing offence if one of the fol-

nal conduct takes place outside the UK[131] and (3) being a deposit-taking body.[132]

The Arranging Offence

This offence catches any person who enters into or is otherwise involved in an arrangement to prepare, through any means, the acquisition, retention, use or control of criminal property, either by himself or on behalf of another person.[133] However, the property in question has to come or

---

lowing three circumstances is satisfied, namely if he (1) made an authorised disclosure under s.338 of POCA 2002 before he committed the prohibited act, namely any act listed in section 327 (1), 328 (1) or 329 (1) of POCA 2002, and he had the appropriate consent; (2) did not make authorised disclosure because of a reasonable excuse; or (3) did the act to enforce a statutory provision.

In order to avoid repetition, the authorised disclosure, along with the term "appropriate consent," will be thoroughly analysed in the following chapter in relation to the types of ML disclosure. An example of defence (3) mentioned above is where the police are performing their official duties and deposit cash derived from criminal activity in a bank account in order to ensure that it is kept in a safe place. In such circumstances, the relevant bank can invoke the defence. See Doug Hopton, *Money Laundering*, *A Concise Guide for All Business* (Second Edition, Gower Publishing Limited 2009), 55.

[131] S.327 (2A)(a) of POCA 2002 provides that a person does not commit the offence if he had reasonable grounds to know or believe that the "relevant criminal conduct" occurred outside the UK. However, criminal conduct takes place when property is being removed from the UK to another jurisdiction, as it is taken across the border. See Alastair Hudson (n 908) 425.

S.327 (2B) of POCA 2002 states that the term "relevant criminal conduct" means "criminal conduct by reference to which the property concerned is criminal property."

S.327 (2A)(b) of POCA 2002 imposes the following two requirements for the defence to be evoked:

> (b) the relevant criminal conduct
> (i) was not, at the time it occurred, unlawful under the criminal law then applying in that country or territory, and
> (ii) is not of a description prescribed by an order made by the Secretary of State.

[132] "Deposit-taking body" means:

> (a) a business which engages in the activity of accepting deposits, or
> (b) the National Savings Bank'. POCA s.340 (14).

Deposit-taking banks are the most likely organisations to conduct transferring and converting criminal property and the defence relates to transferring and converting criminal property. Under s.327 (2c) of POCA 2002, these bodies will not commit the transferring and converting offences if (1) the body did the act to operate an account, which it maintained; and (2) the value of the relevant criminal property was less than £250. This threshold is spelled out in s.339A (2) of POCA 2002.

[133] POCA 2002, s.328 (1).

represent the benefits from illegal activity and the person charged must know or at least suspect that this is the case.[134]

As regards this particular offence, difficulties arise from the term "arrangement." What does such a term mean? Although the Act has not given a proper definition of the term, the Court of Appeal stated in *Bowman v Fels*[135] that: "[the] proper interpretation of section 328 is that it is not intended to cover or affect the ordinary conduct of litigation by legal professionals."[136]

Hence, a solicitor does not commit an arranging offence if he discovers, in the course of his work on advising his client regarding legal proceedings, that his client is involved with criminal property. The justification for this is that this offence does not apply to the ordinary conduct of lawyers dealing with litigation. The decision of the Court in *Fels*[137] therefore represents a fundamental guarantee that the legislation does not violate the human rights of defendants to criminal proceedings.[138]

Obviously, the term "arrangement" does not apply to procedures taking place before any transaction or contract is completed, hence it excludes "what is done [to] facilitate the acquisition or control of criminal property."[139] In this context, it has to be proven, by the prosecution, that the person charged enters into or becomes involved with an arrangement. In addition, the prosecution has to prove that the person charged for such an arrangement knows or at least suspects that he facilitates the acquisition, retention, use, or control of criminal conduct either by himself or on behalf of another person.[140]

---

[134] Angela Leong, *The Disruption of International Organised Crime*: *An Analysis of Legal and Non-Legal Strategies* (Ashgate Publishing Limited 2007), 154.

[135] [2005] EWCA Civ 226.

[136] Ibid para 83.

[137] (N 918).

[138] Alastair Hudson (n 789) 427.

[139] Stephen Gentle (n 899) 15.

[140] 'Proceeds of Crime Act 2002 Part 7—Money Laundering Offences' (updated 15 September 10), available online at: http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/ (accessed on 31st January 2015).

Indeed, this offence is directed at those who work in the banking sector and who may not directly benefit from criminal property.[141] Thus, such offence can comprise cases where a bank passes money via its accounts, especially in circumstances where its employees have a suspicion that the money could constitute criminal property. The offence of "retention" can arise if money, which constitutes criminal property, is held in an account.[142] Moreover, the example of a "use" offence can take place if such money has been converted into foreign currency.[143] The offence with regard to "control" can for example occur if such money has been paid into an account over which the criminal is a trustee.[144] If a trustee then disposes of trust property by way of a settlement, a further "arrangement" offence will be committed and those involved may become "concerned in" that arrangement via facilitating the settlement, if they know or at least suspect that the dispute between the parties relates to the recovery or attempted recovery of property, which one party has gained from illegal activity.[145] On the other hand, if a bank seeks to recover money stolen in an armed robbery through legal proceedings, this does not constitute an "arrangement" for the purpose of the offence, although the money constitutes criminal property since it emanated from criminal activity, namely armed robbery.[146] This is due to the bank being the victim and there thus being no collusion.

The defences for this offence are in fact the same as those for the concealing offence mentioned above.[147]

---

[141] Charles Proctor, *The Law and Practice of International Banking* (Oxford University Press 2010), 157.

[142] Alastair Hudson (n 789) 426.

[143] Ibid.

[144] Ibid.

[145] John Wright (n 897) 294.

[146] Charles Proctor (n 924) 158.

[147] POCA 2002, s.328 (2)(3)(5).

The Acquisition, Use and Possession Offence

This offence will be committed if a defendant acquires, uses or possesses criminal property.[148] For the purpose of this crime, it is crucial that the prosecution proves the acquisition, use or possession of criminal property, as well as that the person charged knew or suspected that the property in question represents a profit from criminal activity.[149]

Possession means physically holding criminal property.[150] In the case of *Warner v Metropolitan Police Commissioner*,[151] the court noted that an individual cannot possess a thing if he is unaware of its existence and accordingly a person cannot be in possession of anything planted on him without his awareness or knowledge. In the case of *R v Tat Venh Fay*,[152] the police officers conducted a search of the defendant's home and found cash totaling £55,460, as well as drugs. The defendant pleaded guilty for possessing criminal property, namely cash from illegal drugs sales.[153]

An example of an acquisition of criminal property is that where a person buys a house with the knowledge or suspicion that it emanated from criminal activity, for example if he or she buys the house from a well-known drug dealer.[154] If a person borrows a car from another person with the knowledge or suspicion that it emanated from criminal activity in order to use it for social activities, the person will commit the offence of using criminal property.

The defences for this offence are in fact the same as those for the concealing and arranging offences mentioned above.[155] However, there is one additional defence, which can be invoked for this crime and pursuant to which this offence will not be committed if a person acquires,

---

[148] POCA 2002, s.329 (1).

[149] Rudi Fortson (n 908) 186.

[150] 'Proceeds Of Crime Act 2002 Part 7—Money Laundering Offences' (n 923).

[151] [1969] 2A.C. 256.

[152] [2012] EWCA Crim 367.

[153] In addition, he pleaded guilty for possession of controlled drugs with intent to supply. Ibid.

[154] *R v Griffiths* (*Philip*), [2006] EWCA Crim 2155.

[155] POCA 2002, s.329 (2)(2A-2C).

uses, or possesses criminal property for "adequate considerations."[156] More importantly, the common feature in relation to these three principal ML offences is the term "criminal property" and it is crucial to analyse what this term precisely denotes.

The Notion of "Criminal Property"

POCA 2002 provides the following definition:

---

[156] "Proceeds Of Crime Act 2002 Part 7—Money Laundering Offences" (n 923).

S.329 (3) of the POCA 2002 defines "inadequate considerations" as follows:

> For the purposes of this section
> (a) a person acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property;
> (b) a person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of the use or possession;
> (c) the provision by a person of goods or services which he knows or suspects may help another to carry out criminal conduct is not consideration.

This defence can be relied on in particular by tradesmen, accountants and solicitors. Hence, traders are not obliged to ask about the origin of the money when they are paid for services and consumable goods in money which come from the offence. See Doug Hopton (n 913) 55.

The defence is also available to professional advisors, such as accountants or solicitors, when they are paid on account for expenses either from the customer or from another person on behalf of the customer.

In the case of *R v Gibson* [2000] Crim. L.R. 479, the defendant was accused of holding £28,000 of criminal proceeds for another person. At the trial, he argued that on returning the money he added an additional £500 and this extra fund embodied adequate consideration. The Criminal Division of the Court of Appeal stated that:

> When he acquired that property, the appellant had given no consideration for it. Nor was there any express or implied promise or obligation on his part to pay for its use. In our view between 9th February and 8th March he gave no consideration for use of the £28,000. When he paid the cheque into his bank account, he had done an act which amounted to having possession of it. He had thus committed the offence. para 23.

Therefore, in the case of *R v Kausar* (*Rahila*) [2009] EWCA Crim 2242, the Criminal Division of the Court of Appeal stated that:

> One of the issues that may arise under section 329 is whether the property in question was acquired for inadequate consideration. If it was not so acquired, no offence under it is committed ((2)(c)), and that is so even if the person who acquires it knows or suspects the property to be criminal property. para 8.

S.334 (1) of POCA 2002 states that a person guilty of any of the principal ML offences mentioned above can be liable to receive up to 14 years' imprisonment and/or a fine and subject himself to civil recovery or a confiscation order. See Doug Hopton (n 913) 5.

(3) Property is criminal property if
(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and
(b) the alleged offender knows or suspects that it constitutes or represents such a benefit.[157]

Elements of Criminal Property

This definition contains two conditions. Firstly, the property has to constitute a person's profit from criminal activity or represents such a profit. In this context, the term "benefit" encompasses three aspects: (1) any (benefit in kind) which results from that criminal act, (2) any (gain) which is due directly to that criminal act and (3) anything which represents such a profit.[158] The property in this regard comprises a wide range, including: money; all types of property, real or personal, heritable or moveable; or things in action and other intangible or incorporeal property.[159] In addition, the property has to come from "criminal conduct,"[160] which means any offence committed in the UK, or that would constitute an offence in the UK if it occurred there.[161] This is regardless of who benefited from such "criminal conduct," who carried it out and whether it occurred before or after the passing of POCA 2002.[162]

Based on the definition of a "criminal conduct" and for the purpose of applying the term to the principal ML offences, any crime in any

[157] POCA 2002, s.340 (3).

[158] Alastair Hudson (n 789) 418.

[159] POCA 2002, s.340 (9).

[160] Charles Proctor (n 924) 154.

[161] S 340(2) of POCA 2002 states that:

(2) Criminal conduct is conduct which
(a) constitutes an offence in any part of the United Kingdom, or
(b) would constitute an offence in any part of the United Kingdom if it occurred there.

S.102 of SOCPA 2005 creates a defence for the principal ML offences, namely the relevant criminal conduct takes place outside the UK (already illustrated above) (n 914). The defence also applies to the three offences relating to failing to report ML cases, analysed in the following chapter.

[162] POCA 2002, s.340 (4).

part of the UK is covered. This is irrespective of the seriousness of the crime or the value of a transaction,[163] except in case of a deposit-taking institution if the two above conditions are satisfied.[164] There is no closed list of predicate offence to ML, but rather POCA 2002 adopts an "all crimes" basis to ML.[165] This is different to FLMLC 2002 in the UAE, which adopts a closed list of predicate offences to ML.

Secondly, the person charged has to know or at least suspect the first condition. This means that in order to establish one of the three principal ML offences, the person charged must know or suspect that the property constitutes a person's profit from criminal activity or represent such a profit.[166] Thus, the second limb of the definition of criminal property consists of two parts: knowledge or suspicion. In other words, a subjective test is applied in relation to the principal ML offences; nevertheless, the provisions of such offences do not require it, but it is applied by virtue of s.340 (3) of POCA 2002. Accordingly, the prosecution has to prove in relation to the principal ML offences that the person charged knew or suspected that the property in question was criminal property.

The Elements Which Have to Be Proven

In the case of *R v Anwoir and others*,[167] the Court of Appeal established that there are two ways for the Crown to prove the relevant property is criminal property:

> (a) by showing that it derives from conduct of a specific kind or kinds and that conduct of that kind or those kinds is unlawful, or (b) by evidence of the circumstances in which the property is handled which are such as to

[163] Arun Srivastava (n 784) 77.

[164] See (n 915).

[165] Robert Stokes and Anu Arora, 'The duty to report under the money laundering legislation within the United Kingdom' [2004 May] Journal of Business Law 332, 340. See also Chap. 4 (n 319).

[166] Doug Hopton (n 913) 47.

[167] [2008] EWCA Crim 1354.

> give rise to the irresistible inference that it can only be derived from crime.[168]

Another case which followed this approach is *Ahmad* (*Mohammad*) *v HM Advocate*,[169] in which the Court of Appeal stated that "there is nothing, it appears to us, in the language of section 340 (2)(a) which suggests or requires,"[170] that it is necessary to prove that the criminal property derived from a specific offence or offences. The Court further added that "we accept that that is right. If, of course, known offences can be identified, then all well and good. If known offenders can be identified, all well and good."[171]

Hence, the Crown does not have to prove the specific offence which generated the illicit proceeds, though it is sufficient for it to prove the circumstances which could result in the jury, concluding that the proceeds are criminal property derived from criminal conduct.[172] This can be established in a number of ways, for example accomplice evidence or where forensic evidence indicates that bank notes contain traces of drugs, suggesting that the money is criminal property, which emanated from drug trafficking.[173]

Furthermore, according to the above, property will be considered criminal property in three cases. The first case is mixed property, which means that the property emanates partly from a lawful activity/source and partly from a criminal activity. In this case all the property is considered to be a benefit from criminal conduct and is considered criminal property.[174] The second case is indirect criminal property.[175]

---

[168] Ibid para 21.

[169] (N 906).

[170] Ibid para 12.

[171] Ibid para 15.

[172] David McCluskey, 'Money laundering: the disappearing predicate' (2009) 10 Criminal Law Review 719.

[173] 'Proceeds Of Crime Act 2002 Part 7—Money Laundering Offences' (n 923).

[174] Robin Booth and others (n 923) 35 & 36.
S.340 (7) of the POCA 2002 provides that:
"References to property or a pecuniary advantage obtained in connection with conduct include references to property or a pecuniary advantage obtained in both that connection and some other."

[175] S.340 (3)(a) of the POCA 2002.

Any asset attributed to crime is criminal property;[176] for instance, if the proceeds of drug trafficking have been deposited in a number of bank accounts and subsequently the illicit proceeds have been used to purchase a house, it will be deemed criminal property. The third case does not limit criminal property to property gained as a result of criminal conduct, but also extends it to property gained in connection with it;[177] for instance, if a drug dealer intended to sell a car purchased from drug trafficking and offers a TV LCD to the buyer as a gift. In this case, the criminal property is not limited to the car, but also extends to the TV.

The Concept of "Knowledge"

The first part of the second condition of the definition of criminal property requires that "the alleged offender knows ... that it constitutes or represents such a benefit."[178] Obviously, knowledge in this context means actual knowledge generally, namely that the person charged had actual knowledge[179] of the criminal conduct, though "constructive knowledge"[180] is also sufficient.[181]

The Notion of "Suspicion"

The second part of the second condition of the definition of criminal property requires, if the knowledge is unavailable, that "the alleged offender ... suspects that it constitutes or represents such a benefit."[182] In this context, "suspicion" is the central mental ingredient for the

[176] Robin Booth and others (n 923) 37.

[177] Ibid.

[178] POCA 2002, s.340 (3) (n 940).

[179] For example, when a customer physically deposits cash into his bank account and admits in the course of his conversation with a banker that this cash is the result of drug trafficking. In this case, the banker has actual knowledge that this cash constitutes criminal property since it emanates from criminal conduct.

[180] That a reasonable person would have known or the person charged ought to have known.

[181] Doug Hopton (n 913) 61.

[182] POCA 2002, s.340 (3) (n 940).

three principal ML offences, which is a subjective and personal threshold.[183]

Suspicion Means the Possibility

There is no definition for "suspicion" in the Act; however, in *R v Da Silva*,[184] Longmore LJ in the Criminal Division of the Court of Appeal explained that:

> The essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be "clear" or "firmly grounded and targeted on specific facts" or based upon "reasonable grounds." To require the prosecution to satisfy such criteria as to the strength of the suspicion would, in our view, be putting a gloss on the section.[185]

The most important sentence for defining a "suspicion" in the above paragraph is "there is a possibility, which is more than fanciful, that the relevant facts exist."[186] The Court of Appeal in this case has illustrated the meaning of "suspicion" as contained in s.93A (1)(a) of the Criminal Justice Act 1988.[187] Such an interpretation could be applied to the offences under POCA 2002. This is what happened when the Civil Division of the Court of Appeal applied the interpretation of "suspicion" in the *Da Silva*[188] case to POCA 2002 in *K Ltd v Natwest Bank PLC.*[189]

---

[183] Jonathan Fisher, 'The anti-money laundering disclosure regime and the collection of revenue in the United Kingdom' (2010) 3 British Tax Review 235, 237.

[184] [2006] EWCA Crim 1654.

[185] Ibid para 16.

[186] Ibid.

[187] Which was repealed by POCA 2002, sch.12 para 1.

[188] (N 967).

[189] [2006] EWCA Civ 1039.

In fact, an assessment of whether likelihood is fanciful involves a value judgment and every case will be different.[190]

Suspicion Must Be Based on Specific Facts

Lord Scott has taken a different approach in relation to "suspicion," in a civil context, when he opined in *Manifest Shipping CO Ltd. v Uni-Polaris insurance CO Ltd* ("*the star sea*")[191] that:

> Suspicion is a word that can be used to describe a state of mind that may, at one extreme, be no more than a vague feeling of unease and, at the other extreme, reflect a firm belief in the existence of the relevant facts ... the suspicion must be firmly grounded and targeted on specific facts.[192]

Indeed, such an approach is not suitable for interpreting the term "suspicion" under POCA 2002 for two reasons. Firstly, the expression of "vague feeling of unease" or "inkling" is insufficient to appreciate the meaning of "suspicion" under POCA 2002[193] since "suspicion" denotes a higher degree than these terms do. Therefore, at the trial of *Da Silva*,[194] in order to find the meaning of "suspecting," the judge directed the jury to the *Chambers English Dictionary* which defines "suspicion" as "the imagining of something without evidence or on slender evidence; inkling: mistrust."[195] Accordingly, the judge stated that "any inkling or fleeting thought" that the other person had engaged in criminal conduct sufficed for the offence.[196]

In contrast, the Criminal Division of the Court of Appeal rejected such an approach and stated that:

---

[190] Jonathan Fisher (n 966) 238.
[191] [2001] UKHL 1.
[192] Ibid para 116.
[193] Robin Booth and others (n 784) 47.
[194] (N 967).
[195] *Chambers English Dictionary*, (Cambridge 1988).
[196] (N 967).

> The judge could not, in our judgment, have been criticised if he had declined to define the word "suspecting" further than by saying it was an ordinary English word and the jury should apply their own understanding of it. Of course, the danger with saying nothing is that the jury might actually ask for assistance about its meaning and, if they did, the judge would have to assist as best he can … Using words such as "inkling" or "fleeting thought" is liable to mislead.[197]

The Court of Appeal added further that if the judge felt it appropriate to assist the jury, he should direct them that:

> The prosecution must prove that the defendant's acts of facilitating another person's retention or control of the proceeds of criminal conduct were done by a defendant who thought that there was a possibility … that the other person was or had been engaged in or had benefited from criminal conduct.[198]

Secondly, POCA 2002[199] does not require that a "suspicion" must be reasonable or relate to specific facts for the purpose of the definition of criminal property. As a result, in *Da Silva*,[200] the Court stated that:

> This court could not, even if it wished to, imply a word such as "reasonable" into this statutory provision. To do so would be to make a material change in the statutory provision for which there is no warrant.[201]

Moreover, the Court of Appeal in the *K Ltd*[202] case emphasised that "the existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion."[203]

---

[197] Ibid paras 12 & 19.
[198] Ibid para 16.
[199] S.340 (3)(b) of POCA 2002.
[200] (N 967).
[201] Ibid para 8.
[202] (N 972).
[203] Ibid para 21.

The Proper Definition for "Suspicion"

As such, the Court of Appeal in *Da Silva*[204] appears to have properly clarified the term "suspicion" in the context of POCA 2002, which means that there is a "possibility" that relevant facts exist and that this possibility is more than fanciful. Certainly, a "possibility" anticipates that an event has occurred or is going to occur. However, even though they do not reach a belief, the anticipation should be based on some grounds.[205]

This approach does not necessarily conflict with the fact that the meaning of "suspicion" has to be settled. For example, due to his training, a banker may suspect that a large cash deposit could involve ML activities. However, such suspicion could be mitigated in the case where the banker finds out from the bank's records that the relevant customer has a "cash-based business."[206]

Nevertheless, recently the Court of Appeal in *Shah v HSBC Private Bank (UK) Ltd*[207] adopted a totally a different approach in relation to interpreting "suspicion." This recent approach will be critically evaluated along with its legal implications in the course of studying the offences relating to the failure to report ML cases and the consent regime in Chap. 9.

Conclusion

MLR 2007 imposes a great number of regulatory commitments on financial bodies in general. Such commitments are crucial to assist the banks and other reporting entities in understanding and taking the right decision as to whether to submit a SAR to the competent authority.[208]

---

[204] (N 967).

[205] Commonwealth Secretariat, *Combating Money Laundering and Terrorist Financing*: *A Model of Best Practice for the Financial Sector, the Professions and other Designated Businesses* (Second Edition, Commonwealth Secretariat 2006), 138.

[206] Robin Booth and others (n 784) 49.

[207] [2010] EWCA Civ 31.

[208] The basis of submitting a SAR will be critically analysed in Chap. 8.

The regulations explicitly require banks and other reporting entities to provide regular training for relevant employees. In addition, these training courses have to focus on SARs on ML. However, CBR 24/2000 in the UAE does not require that training courses are provided on a regular basis.[209]

Similarly, unlike CBR 24/2000 in the UAE, MLR 2007 suitably defines CDD procedures and levels. Another positive aspect is that the definition of ML contained in MLR 2007 is the same as in Part 7 of POCA 2002, unlike in the UAE where it is contained in FLMLC 2002 and is different from that contained in CBR 24/2000.[210]

More importantly, in addition to the three situations where they should be applied,[211] ECDD procedures and measures must be applied to relevant persons "in any other situation which by its nature can present a higher risk of money laundering."[212] However, MLR 2007 does not give examples of when a higher risk may be present. This term is overly broad and should be given a narrow interpretation for two reasons. Firstly, there is a risk that the term is being mis-utilised for subjective purposes. Secondly, the term is wide enough to accommodate the above three ECDD circumstances, which render these three circumstances redundant.

The FCA plays an important role in ensuring that AML/SAR requirements are being adopted by reporting entities since it can impose financial penalties on those that don't. However, the UAE Central Bank has no such power. This has negatively impacted on the adoption of the STRs requirements by the reporting entities in the UAE, especially the role of compliance officer in banks.[213]

The principal ML offences contained in POCA 2002 are subjectively based, namely on knowledge or suspicion. The Act does not define the term "suspicion," though the Court of Appeal in *Da Silva*[214] appears

[209] As analysed in Chaps. 5 and 6.

[210] As critically analysed in Chap. 5.

[211] Namely (1) clients not physically present, (2) non-EEA clients and (3) PEPs.

[212] MLR 2007, reg.14 (1)(b) (n 835).

[213] The two cases, analysed in Chap. 5, clearly confirm that the compliance officers played no role in detecting STRs at their banks.

[214] (N 967).

to have properly clarified the term in the context of POCA 2002. Nevertheless, recently the Court of Appeal in *Shah v HSBC Private Bank (UK) Ltd*[215] adopted a totally different approach, which could affect the number of SARs submitted by the reporting entities, and which will be critically assessed in Chap. 9. Before this, however, it is crucial that we examine the legal basis for submitting SARs in the UK and the legal consequences if a reporting entity fails to submit a SAR to the competent authority. This we do in the next chapter.

[215] (N 990).

8

The UK's SARs Regime on ML

Introduction

This chapter is pivotal in terms of the UK's AML system since it examines the SAR requirements, which are imposed on reporting entities. One of the principal objectives of the SAR requirements is to protect the reputation and integrity of the financial system.[1] The SARs system aims at preventing and detecting ML activities or at least mitigating its consequences by prohibiting the use of illicit proceeds. The main objective of the current chapter is to critically analyse the legal basis for SARs and the types of disclosure, which are required under the SARs regime and the complicated requirements, which can, in practice, overlap with each other. The required, authorised and protected disclosures are evaluated to appreciate the legal consequences. In case of non-compliance, one of the three offences

[1] SOCA, 'FAQ and Definitions', available online on SOCA's website at: www.soca.gov.uk (last accessed on 13th September 2014).

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_8

of failing to report SARs can be committed, namely the second group of ML offences contained in Part 7 of the POCA 2002.

All types of disclosure are lawful, if the respective conditions are fulfilled. On the other hand, disclosures can be unlawful or prohibited under part 7 of the POCA 2002 in relation to the tipping off offences, which constitute the third group of ML offences spelled out by the Act. The offences of prohibited disclosures are directly related to the SARs regime since the first type of these offences necessarily requires that a SAR has been submitted to the competent authority, before the commission of the offence.

It is essential to critically assess the UK SARs regime before analysing the UK's FIU since the success of the SARs regime positively affects the functions of the FIU, especially its analytical function. The deficiencies of the UAE FIU cannot be entirely attributed to the lack of legal powers, but rather deficiencies within the UAE's STRs regime, such as the basis for STRs, CDD procedures, training courses for compliance officers and the absence of penalties for reporting entities which do not fulfil the STRs requirements.[2] Indeed, these deficiencies negatively affect the functions of the UAE FIU.

This chapter consists of two main sections. The first section critically analyses the legal basis for submitting SARs. All the elements of the failing to disclose offences are therefore analysed. More importantly, the section evaluates the three types of disclosures, which are essential to avoid committing the failing to report offence(s) or the principal ML offence(s). The section also analyses the practical and legal consequences for each type of disclosure, especially if a SAR involves more than one type of disclosure.

The second section discusses the tipping off offences and their relationship to SARs. These offences will be committed if a disclosure relating to a ML have been made. The disclosures in these cases are unlawful since they are deemed as an exception to the duty to disclose ML cases which are analysed in the first section.

[2] As critically analysed in Chap. 5 and confirmed in Chap. 6.

The Legal Basis for Adherence to the Requirements of SARs

The legal basis of the SARs is based on the second group of ML offences contained in part 7 of the POCA 2002, namely the three offences of failing to report.[3] In addition, although the POCA 2002 and its amendments do not explicitly oblige firms in the regulated sector to appoint a nominated officer,[4] the MLR 2007 obliges firms to appoint a nominated officer in order to receive internal SARs from employees in his firm.[5] After SARs are internally received, the nominated officer[6] must evaluate and decide, based on his experience and authority, whether a SAR should be passed on to the NCA or not.[7] The nominated officer could be accused of committing the second type of failing to report offences for failing to fulfil his commitments and which is analysed below.

As clarified below, the offences of failing to report also means failing to disclose specific information/matters to the relevant authority. Consequently, these offences occur where there is a failure to report and where there is a failure to disclose specific information/matters. However, both terms, "report" and "disclosure," achieve the same result since failing

[3] It is worth noting that in addition to the SARs regime, there are Cash Declaration rules, which were adopted by the European Parliament and Council according to Regulation No 1889/2005. The Regulation came into effect in all EU Members States on 15 June 2007. Hence, a passenger who enters the UK from a non-EU country or departs the UK to a non-EU country must declare to HMRC if he carries 10,000 Euros or more (or the equivalent in another currency). Cash is not confined to currency notes and coins, but also banker's drafts and cheques, including travellers' cheques. A passenger who fails to make the declaration or provides false declaration could face a penalty of up £5000 pursuant to the Control of Cash (Penalties) Regulations 2007. Form C9011 is dedicated for the declaration and all information on how to declare the cash and the form can be found on the website of HMRC at: www.hmrc.gov.uk (accessed on 25th November 2014). The declaration is not required if the passenger is travelling between EU countries.

[4] Doug Hopton, *Money Laundering, A Concise Guide for All Business* (Second Edition, Gower Publishing Limited 2009), 65.

[5] MLR 2007, reg.2 (1).

[6] MLR 2007, reg.20 (2)(d).

[7] If a firm does not obey the MLR 2007 in appointing a nominated officer and fulfilling the regulations in this regard, this will result in committing a criminal offence which is punishable of imprisonment for a term not exceeding two years, a fine or to both in addition to the possibility of civil penalties. MLR 2007, reg.42 & 45.

to report necessarily entails failing to disclose specific information/matters to the relevant authority. In practice, the SARs under the POCA 2002 are applied to all types of disclosure contained in the same Act.[8] This section therefore consists of two subsections. The first subsection investigates the offences of failing to report/disclose ML cases. The second subsection evaluates types of disclosure under the POCA 2002 and their consequences.

The Offences of Failing to Report ML Cases Under Part 7 of POCA 2002

Introduction

This subsection is dedicated to critically analyse the second group of offences under part 7 of the Act. These offences relate to failing to report ML cases in circumstances where the person charged knows, suspects or at least has reasonable grounds to believe that ML is occurring or is going to occur.[9] This group of offences consists of three types of offences:

- the crime of regulated sector employees failing to report,
- the crime of regulated sector nominated officers failing to report,
- the crime of other nominated officers failing to report.

Before focus is placed on these three crimes, it is important to mention that the common feature of all these three types of offences is that they are not just related to failing to disclose actual ML activities, but also failing to disclose possible ML activities.[10] In addition, the common feature between the first and the second type of criminal offence is that they apply solely to employees, who work in the "regulated sector" and both of them can be committed on a mere negligence basis.[11] This means that it is sufficient to prove that a person, who works in the regulated sector, has failed

[8] Robin Booth and others, *Money Laundering Law and Regulation*: *A Practical Guide* (First Published, Oxford University Press 2011), 104.

[9] Alastair Hudson, *The Law of Finance* (Second Edition, Sweet & Maxwell 2013), 427.

[10] *Ahmad* (*Mohammad*) *v HM Advocate*, [2009] HCJAC 60, paras 30 & 37.

[11] Angela Leong, *The Disruption of International Organised Crime: An Analysis of Legal and Non-Legal Strategies* (Ashgate Publishing Limited 2007), 155.

to report, had suspicion/knowledge or there were reasonable grounds for suspicion/knowledge for any of these two offences to be committed.[12]

The Crime of Employees in the Regulated Sector Failing to Report

This crime will be committed if the following four requirements are met:

1) The person must subjectively or objectively consider that another person (the money launderer) is involved in ML.
2) The information must come to him in the course of his work in the regulated sector.
3) He either can identify the money launderer or the whereabouts of the laundered property or he believes that the information, which has come to him, may help identifying the money launderer or the whereabouts of the laundered property.
4) He failed to make the required disclosure to the competent authority.[13]

---

[12] George Brown and Tania Evans, 'The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicious activities' (2008) 23 (5) Journal of International Banking Law and Regulation 274, 275.

[13] S. 330(1)— (4) of the POCA 2002 provides that:

'(1) A person commits an offence if the conditions in s (2) to (4) are satisfied

(2) The first condition is that he

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.

(3) The second condition is that the information or other matter

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector.

(3 A) The third condition is

(a) that he can identify the other person mentioned in (2) or the whereabouts of any of the laundered property, or

(b) that he believes, or it is reasonable to expect him to believe, that the information or other matter mentioned in (3) will or may assist in identifying that other person or the whereabouts of any of the laundered property.

(4) The fourth condition is that he does not make the required disclosure to

(a) a nominated officer, or

Before investigating these conditions, it is helpful to explain the term "regulated sector" since the crime only applies to employees who work in this sector. The Act defines businesses in the regulated sector[14] as comprising all businesses in the financial sector, such as banks, and also estate agents, tax advisers, auditors and lawyers.[15] Moreover, a dealer in goods, whose single transaction or group of associated transactions involves accepting money in cash in excess of €15,000, is also considered to be someone of the regulated sector.[16] Broadly speaking, the "regulated sector" does not encompass just banks/credit institutions, but also covers the majority of businesses,[17] which can be exploited for ML activities.

Conditions for the Offence

A failure to report crime can cause massive issues to those working in the financial sector, as well as professionals,[18] but what is the basis for this? Indeed, the offence will not be committed, unless the aforementioned four elements are satisfied.

Objective or Subjective Basis

The first condition stipulates that anyone who works in the regulated sector could be committed this crime if he "knows," "suspects" or if there are "reasonable grounds" to know or suspect that another person is engaged in ML.[19] This means that either a subjective basis for knowledge

(b) a person authorised for the purposes of this Part by the Director General of the National Crime Agency, as soon as is practicable after the information or other matter mentioned in (3) comes to him.'

[14] Sch.9 (1) of the POCA 2002 defines businesses in the regulated sector and excluded activities.

[15] Jonathan Fisher, 'The anti-money laundering disclosure regime and the collection of revenue in the United Kingdom' (2010) 3 British Tax Review 235, 237.

[16] Doug Hopton (n 1002) 57.

See also Chap. 7 (n 787 & 812).

[17] Alastair Hudson (n 1007) 428.

[18] Stephen Gentle, 'Proceeds of Crime Act 2002: update' (2008) 56 (May) Compliance Officer Bulletin 1, 16.

[19] POCA 2002, s. 330(2).

or suspicion or an objective basis for reasonable grounds for knowledge or suspicion is applied. Nevertheless, the subjective basis, especially mere suspicion, raises a number of dilemmas in relation to the offences of failing to report since the Act does not require that the suspicion is based on reasonable grounds.[20] This means that a mere suspicion is enough to meet the first condition. The serious consequences, which flow from this, will be critically evaluated in the following chapter.

An objective basis means that reasonable grounds for knowing or suspecting ML are enough.[21] An objective test is applied with regard to the first condition. This is in contrast with the subjective test, which is applied in relation to the principal ML offences,[22] discussed in the previous chapter. However, what does "reasonable grounds" or an objective test for knowledge or suspicion mean in this context? This simply means that the offence can be committed on the basis of a person, in the regulated sector, simply not taking into account grounds, which a reasonable professional ought to have known or suspected.[23] The justification for this is that a CDD is required in the regulated sector under the AML system.[24] Unlike businesses outside the regulated sector, employees and the nominated officers, who work in the regulated sector, have to adhere to the highest level of CDD when they deal with clients' transactions.[25] Thus, following training, a person, who works in the regulated sector, has to pay great attention to the information gained through CDD measures, as the information could inform him that there are reasonable grounds to know or suspect that another person/firm is engaged in ML activity.[26]

---

[20] Robert Stokes and Anu Arora, 'The duty to report under the money laundering legislation within the United Kingdom' [2004 May] Journal of Business Law 332, 345.

[21] Charles Proctor, *The Law and Practice of International Banking* (Oxford University Press 2010), 159.

[22] Jonathan Fisher (n 1013) 239.

[23] Doug Hopton (n 1002) 62.

[24] 'Proceeds of Crime Act 2002 Part 7— Money Laundering Offences' (Updated 15/09/10), available online at: http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/ (accessed on 31st January 2015).

[25] Arun Srivastava, 'UK Part II: UK law and practice' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 27 at 41.

[26] Robin Booth and others (n 1006) 49.

The case of *R v Phillip Griffiths and Leslie Dennis Pattison*[27] clearly illustrates the difference between knowledge and suspicion, which is a subjective test, and "having reasonable grounds for knowledge or suspicion," which is an objective test. In this case the defendant was acquitted of the principal ML offence, which is based on knowledge or suspicion. On the other hand, he was convicted for failing to disclose the ML offence, which is based on knowledge, suspicion or having reasonable grounds for the knowledge or suspicion. The Court of Appeal stated that:

> Most significantly, he [the defendant] was acquitted of the more serious offences based on knowledge and suspicion and was convicted of failing to disclose to the authorities when he had reasonable grounds for knowing or suspecting that this transaction involved money laundering.[28]

Another example of the offence is the conviction by Preston Crown Court in 2007 of two senior managers at Lloyds STB, who failed to report that they operated an account at their branch for one of their customers, who operated a brothel.[29] Judge Andrew Blake stated that there was no evidence that they had actual knowledge about the details of the illegal business or that they received any sexual favour in order to operate the customer's bank account. Nevertheless, both senior managers received fines, as they did not report their suspicion/knowledge or reasonable suspicion/knowledge that the customer was managing an illegal business.[30]

In *Ahmad* (*Mohammad*) *v HM Advocate*,[31] the defendant was the secretary and director of a company trading as Makkah Travel in Glasgow. He was convicted of failing to disclose his knowledge, suspicion or reasonable grounds for knowledge or suspicion that William Anthony Gurie was engaged in ML,[32]

---

[27] [2006] EWCA Crim 2155.

[28] Ibid para 12.

[29] This case is not a reported case and it is mentioned in George Brown and Tania Evans (n 1010) 275. In addition, this case has been published on the BBC website at: http://news.bbc.co.uk/1/hi/england/lancashire/6647473.stm (accessed on 13st May 2015).

[30] Ibid.

[31] (N 1008).

[32] Contrary to the POCA 2002, s.330.

> namely repeated visits to [him] by William Anthony Gurie to deposit large, unexplained quantities of cash for transmission to a jurisdiction with which he had no legitimate connection known to [him].[33]

Although there is no comprehensive guidance about the notion of "reasonable grounds," there are three fundamental circumstances, which require a MLRO (nominated officer) to have reasonable grounds to know or suspect. Firstly, where complex transfers of monies are carried out across jurisdictions, especially when AML legislation has been repeatedly disobeyed; for instance, transfers, which are carried out through countries on the FATF high-risk and non cooperative jurisdictions.[34] Secondly, where it appears that there is no economic justification for the money dealings.[35] In addition, massive cash amounts provide reasonable grounds to know or suspect ML,[36] particularly if the relevant customer declined to provide the required information/documents without any reasonable justification[37] or if he provided information/documents, but they did not satisfy the expectation of the relevant employee. Thirdly, when OFCs'[38] services are widely used and the economic needs of the customers do not appear to necessitate this.[39] It may be worth noting that the term "objective test" or "reasonable grounds" or "negligence test" all denote the same.[40]

---

[33] (N 1008) para 1.

[34] See (n 364) of Chap. 4.

[35] Stephen Gentle (n 1016) 16.

[36] Ibid.

[37] Commonwealth Secretariat, *Combating Money Laundering and Terrorist Financing*: *A Model of Best Practice for the Financial Sector*, *the Professions and other Designated Businesses* (Second Edition, Commonwealth Secretariat 2006), 139.

[38] An OFC can be defined as any jurisdiction, which exclusively adopts a system in order to promote business, legal and financial infrastructures, including those infrastructures, which display a higher degree of flexibility for the demands of foreign investors than traditional infrastructures in onshore. This means that an OFC is a jurisdiction, which accommodates an enormous number of financial services to customers, such as banking and insurance, who are non-resident, compared to the quantity of sourced business at the domestic level.

For further detail, see, Rose-Marie Antoine, *Confidentiality in Offshore Financial L*aw (First published, Oxford University Press 2002), 7.

See also, Richard Hay, 'Offshore financial centres: the supranational initiatives' (2001) 2 Private Client Business 75, 76.

[39] Commonwealth Secretariat, (n 1035) 139.

[40] Doug Hopton (n 1002) 62.

The Information Must Come to the Person During the Course of Business in the Regulated Sector

The second condition is that the information or matters, mentioned in relation to the first condition, must have come to the employee's knowledge in the course of his work in the regulated sector.[41] Accordingly, if the information/matters came to him outside his work in the regulated sector, the employee will not commit the offence of failing to report since he must receive information/matters in the manner specified under the second condition mentioned above.[42] This is unlike the UAE AML system, which does not require this condition. This condition is crucial as it determines the scope of SARs and without this condition the scope of SARs will be wide, as critically analysed in Chap. 5.

Identifying the Money Launderer or the Whereabouts of the Laundered Property

The third condition requires that a person in the regulated sector is able to (1) identify the money launderer or (2) the location of any "laundered property"[43] or (3) the information with which he could help to identify the money launderer or the location of the "laundered property".[44]

Failing to Inform the Competent Authority

The last condition necessitates that a person in the regulated sector fails to disclose "as soon as is practicable" a required disclosure to the nominated officer or to provide the financial report to the NCA.[45] However,

---

[41] POCA 2002, s.330 (3).

[42] Ibid.

[43] The "laundered property" is 'the property forming the subject-matter of the money laundering that he knows or suspects, or has reasonable grounds for knowing or suspecting, that other person to be engaged in.' POCA 2002, s.330 (5 A).

[44] POCA 2002, s.330 (3 A).

[45] POCA 2002, s.330 (4).
In addition, s.340 (12)(13) of the POCA 2002 provides that:

in practice, an employee, in the regulated sector, will make such required disclosure to the nominated officer, in his institution.[46] Three elements must be established in relation to the required disclosure: (1) the identity of the money launderer mentioned in the first condition of the offence, if he knows it, (2) the whereabouts of the laundered property, so far as he knows it and (3) the information or other matter mentioned in the second condition of the offence.[47]

Furthermore, an employee should make more than one required disclosure to the nominated officer in case the same client requests separate transactions and the conditions for the offence are met for all transactions.[48] Thus, the nominated officer, who is usually the MLRO in the regulated sector, has to study the "required disclosure" and consider the possibility of passing it on to the NCA. The same situation can also give rise to the commission of another offence under the Act, namely the offence of regulated sector nominated officers failing to report ML cases and this is analysed in the following subheading. In addition, the duty of disclosure applies irrespective of the amount at stake or the sort of criminal conduct, which has generated the criminal property and also applies in cases of attempted ML, regardless of whether the relevant business/transaction has been rejected or completed.[49]

The Defences to the Crime of Employees in the Regulated Sector Failing to Report

A person in the regulated sector does not commit the offence of failing to report if any one of the four defences applies:

'(12) For the purposes of a disclosure to a nominated officer

(a) references to a person's employer include any body, association or organisation (including a voluntary organisation) in connection with whose activities the person exercises a function (whether or not for gain or reward), and

(b) references to employment must be construed accordingly.

(13) References to a constable include references to a person authorised for the purposes of this Part by the Director General of the National Crime Agency'.

[46] Arun Srivastava (n 1023) 43.

[47] POCA 2002, s.330 (5).

[48] Paul Hynes, Nathaniel Rudolf and Richard Furlong, *International Money Laundering and Terrorist Financing*: *A UK Perspective* (First Edition, Sweet & Maxwell/Thomson Reuters 2009), 225.

[49] Stephen Gentle (n 1016) 19.

1) If he has a "reasonable excuse" for not divulging information of other matter.[50] Indeed, the most difficult issue with this defence is the notion of "reasonable excuse." No judicial direction or interpretation exists with regard to what constitutes a "reasonable excuse"[51]; however, two elements must be established by the employee. For the first element, he must prove a sufficient justification for not divulging the information and for the second element, he has to prove his intention to make a report.[52] Indeed, the excuse(s), provided by the employee, is scrutinised by the court and the court at its discretion can decide whether the justification is reasonable or not in light of the particular facts of the case.
2) He is a professional legal adviser or "relevant professional adviser"[53] and the information or other matter came to him under "privileged circumstances."[54]
3) He did not know or suspect that another person is engaged in ML and had not been provided with training by his employer.[55] This means that if the employee was not provided with training, he will invoke the defence. This demonstrates how important training courses are. In addition, reporting entities, notably banks, are required to provide training courses since they are keen to protect their reputation being tarnished by allegations of facilitating ML.

---

[50] POCA 2002, s.330 (6)(a).

[51] Doug Hopton (n 1002) 66.

[52] Charles Proctor (n 1019) 162.

[53] "A relevant professional adviser" is 'an accountant, auditor or tax adviser who is a member of a professional body which is established for accountants, auditors or tax advisers (as the case may be) and which makes provision for

(a) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and
(b) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards.' POCA 2002, s.330 (14).

[54] POCA 2002, s.330 (6)(b).
S.330 (10) defines the term "privileged circumstances" as:
'Information or other matter comes to a professional legal adviser or relevant professional adviser in privileged circumstances if it is communicated or given to him

(a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client,
(b) by (or by a representative of) a person seeking legal advice from the adviser, or
(c) by a person in connection with legal proceedings or contemplated legal proceedings.'

[55] POCA 2002, s.330 (7).

4) He knows or reasonably believes that the ML is taking place outside the UK and that the activity was not illicit under the criminal law applicable in that country or territory and "is not of a description prescribed in an order made by the Secretary of State."[56]

The Crime of a Nominated Officer in the Regulated Sector Failing to Report

The link between this offence and the aforementioned offence is clear. The statutory provisions for this offence apply to the nominated officer, who receives the disclosure (as set out in s.330 of the POCA 2002) from employees of firms in the regulated sector, and who does not comply with his duties in passing on this information to the SOCA,[57] and now to the NCA.

A nominated officer receiving a disclosure from a person in his firm, in the regulated sector, will commit this crime, if the following four conditions are met:

1) He subjectively or objectively considers that another person (the money launderer) is involved in ML.
2) An employee from his firm must inform him about the internal SAR during the course of his work in the regulated sector.
3) He either can identify the money launderer or the whereabouts of the laundered property,[58] or he believes that the information, which came to him, may help identifying the money launderer or the whereabouts of the laundered property.
4) He failed to make the required disclosure to the competent authority.[59]

---

[56] POCA 2002, s.330 (7 A). Furthermore, s.330 (8) of the Act provides "In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant guidance which was at the time concerned
(a) issued by a supervisory authority or any other appropriate body,
(b) approved by the Treasury, and
(c) published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it."

[57] Jonathan Fisher (n 1013) 237.

[58] The laundered property has been given the same definition as in the first offence of failing to report. S.331 (5 A) of the POCA2002, see also (n 1041).

[59] S.331 (1–4) of the POCA provides that:
'(1) A person nominated to receive disclosures under section 330 commits an offence if the conditions in s (2) to (4) are satisfied (2) The first condition is that he

Conditions for the Offence

Indeed, these conditions and their interpretation are quite similar to those for the previous offence, namely the crime of failure to report for employees in the regulated sector. Nevertheless, these conditions are applied when a nominated officer receives the required disclosure, pursuant to the provisions contained under the first offence of failure to report, from an employee in his firm in the regulated sector. Suppose that an employee in a firm in the regulated sector suspects that a client is engaged in ML and this employee then makes a report, a required disclosure, about this suspicion to a nominated officer in order to avoid criminal liability under the first type of failing to report offence.[60] The nominated officer has to then decide on the basis of his experience and the available information which next step to take. In such a case, if he knew, suspected or had reasonable causes for knowing or suspecting, namely that there were objective grounds that another person is engaged in ML, he must report the required disclosure to the NCA.[61]

(a) knows or suspects, or
(b) has reasonable grounds for knowing or suspecting,
that another person is engaged in money laundering.
(3) The second condition is that the information or other matter
(a) on which his knowledge or suspicion is based, or
(b) which gives reasonable grounds for such knowledge or suspicion,
came to him in consequence of a disclosure made under section 330.
(3 A) The third condition is
(a) that he knows the identity of the other person mentioned in (2), or the whereabouts of any of the laundered property, as a result of a disclosure made under section 330,
(b) that that other person, or the whereabouts of any of the laundered property, can be identified from the information or other matter mentioned in (3), or
(c) that he believes, or it is reasonable to expect him to believe, that the information or other matter will or may assist in identifying that other person or the whereabouts of any of the laundered property.
(4) The fourth condition is that he does not make the required disclosure to a person authorised for the purposes of this Part by the Director General of the National Crime Agency as soon as is practicable after the information or other matter mentioned in (3) comes to him.'

[60] POCA 2002, s.330.

[61] Nicholas Ryder 'The Financial Services Authority and money laundering: a game of cat and mouse' (2008) 67 (3) Cambridge Law Journal 635, 648.

Components of the Required Disclosure

Three elements must be contained in the required disclosure, namely (1) the identity of the money launderer mentioned under the first condition of the offence, if disclosed to him pursuant to the provisions under the first offence of failure to report, (2) the whereabouts of the laundered property, so far as disclosed to him under the provisions of the first offence of failure to report and (3) the information or other matter mentioned in the second condition of this offence.[62] However, a nominated officer can also on the basis of his experience or due to his greater access to client information decide that there are no reasonable grounds for suspicion and not make the disclosure to the NCA,[63] but again there has to be adherence to the objective test.

Nevertheless, what is the position where the decision of a nominated officer has been wrong? In other words, if a nominated officer decided that there are no reasonable causes for suspecting ML according to an objective test, and he did not make a required disclosure to the NCA, but it later emerges that the decision was not right. Can criminal liability nevertheless be established?[64] As mentioned in respect of the first offence, employees of the regulated sector, who fail to report can commit the offence also on a mere negligence basis. The nominated officer should record and retain in detail all internal SARs (disclosures) that he receives from his firm's employees, even if he reached the decision that there is no suspicion, knowledge or reasonable grounds for suspicion/knowledge and decided not to pass a SAR to the NCA. This procedure is fundamental, so that he can review the SAR, which he decided not to submit to the NCA, in cases where further/additional information/matters emerge in the future, which could give reasonable grounds to suspect/know ML and which ultimately leads to the decision of submitting the SAR to the NCA. Accordingly, such a nominated officer avoids taking a wrong decision of not submitting the SAR to the NCA.

[62] POCA 2002, s.331 (5).

[63] Doug Hopton (n 1002) 66.

[64] Stephen Gentle (n 1016) 17.

The Common Condition for the First and Second Offence

It is necessary to recall that for the purposes of establishing the first and second offences of failing to report, it is enough to prove the existence of reasonable causes for suspicion. In *Ahmad v HM Advocate*,[65] the court mentioned that to prove the existence of reasonable grounds for suspicion and that a person in the regulated sector should have divulged to the SOCA, now the NCA, solely requires that the prosecution establishes the offence of failing to disclose and this is regardless of whether the money constitutes the proceeds of the defendant or another person's illegal act.

In addition, it is crucial to note that the nominated officer does not commit the offence if he receives information/matters for the purpose of consultation by a professional legal advisor or relevant professional advisor. The disclosure in such a case is made for the purpose of consultation and the person who discloses does not intend the disclosure to be a disclosure under the provisions of the first offence of failing to report.[66] In other words, in order to establish the second offence of a nominated officer failing to report, it is crucial that he must receive a disclosure specified under the provisions of the first offence of failing to report.[67] This situation illustrates a clear and direct relationship between such offence and the first offence of failure to report, as mentioned above.

Indeed, this offence clearly illustrates the vital AML role, which the nominated officer plays in firms[68] since he receives all internal SARs on ML. A nominated officer can be described as a filter channel for all SARs between the reporting entities and the NCA/UK FIU.[69]

---

[65] (N 1008).

[66] POCA 2002, s.330 (9 A).

[67] POCA 2002, s.331 (3).

[68] Doug Hopton (n 1002) 65.

[69] A nominated officer is required to also produce a report to the firm's senior management at least once a year. SYSC 3.2.6G stipulates that:

'A firm should ensure that the systems and controls include:

(2) appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's money laundering reporting officer (MLRO) on the operation and effectiveness of those systems and controls.'

The report should evaluate the current firm's system and controls in relation to counteracting ML and propose any amendments/additional controls. See Mark Simpson and Nicole Smith, 'UK Part III: Practical implementation of Regulations and Rules' in Mark Simpson, Nicole Smith and Arun

The Defences to the Crime of Failure to Report for a Nominated Officer in the Regulated Sector

There are two defences available in relation to this type of crime. The first defence exists if the nominated officer has a reasonable excuse for not divulging information or other matters.[70] As mentioned above, there is no clear guidance available with regard to the meaning of reasonable excuse. This can lead to the nominated officers disclosing all cases to NCA and adopting cautionary methods solely to avoid the imposition of criminal responsibility and to stay away from the offence of failing to disclose. This is because a nominated officer would otherwise be susceptible to criminal responsibility at any time, if he does not divulge information or other matters to the NCA, even if he took his decision on an objective basis.[71]

The second defence is available if he knows or reasonably believes that ML is taking place outside the UK and that it was not illicit under the criminal law of that country or territory and "is not of a description prescribed in an order made by the Secretary of State."[72]

The Crime of Other Nominated Officers Failing to Report

As mentioned above, the link between the first two offences of failing to report is direct and clear since the second offence deals with the "required disclosure" contained in the first offence.[73] In contrast, the third offence of failing to report does not show a clear and direct relationship with these offences. This is due to two reasons. Firstly, the offence catches any person who works as a nominated officer irrespective of whether in the regulated sector or outside,[74] so long as he receives internal disclosures (SARs) from

Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 95 at 107. See also in this regard in detail, Doug Hopton (n 1002) 123–129.

[70] POCA 2002, s.331 (6).

[71] Doug Hopton (n 1002) 66 & 67.

[72] POCA 2002, s.331 (6 A).

[73] Robin Booth and others (n 1006) 133.

[74] Paul Hynes, Nathaniel Rudolf and Richard Furlong (n 1046) 229.

another person in that firm, which causes him to suspect/know that another person is involved in ML and he fails to disclose that suspicion/knowledge to the NCA.[75] Secondly, unlike the first two failing to report offences, which deal with just one type of SARs, namely "required disclosure," the subject of such offence is two types of SARs, namely "protected disclosure" and "authorised disclosure,"[76] assessed in the following subsection. A nominated officer who is outside the regulated sector will therefore not deal with the "required disclosure," simply because his organisation falls outside the sector and will thus not be obliged to adhere to the type of disclosure under the first offence of failing to report,[77] namely s.330 of POCA 2002.

Generally, the conditions for this offence are similar to the conditions relating to the second failing to report offences, except that "reasonable grounds for knowledge or suspicion" are not required. Hence, this crime cannot be committed on a mere negligence basis, which means that an objective test is not required for the purpose of establishing this offence. This may be because the offence applies to all nominated officers who work inside and outside the regulated sector.[78] Although, it may be helpful if an objective test was required for establishing the conditions of the offence since a nominated officer should adhere to the highest level of CDD when dealing with clients' transactions for the purpose of detecting or preventing ML. A nominated officer supposes to possess greater experience on ML activities and patterns than other persons in his organisation. Hence, even if a nominated officer is outside the regulated sector, so long as he receives internal SARs from another person in that firm, the same ought to apply to him.

A nominated officer who receives a "protected disclosure"[79] or an "authorised disclosure"[80] will commit the offence if the following four conditions are met:

1) He subjectively considers that another person (the money launderer) is involved in ML.

[75] Jonathan Fisher (n 1013) 237.
[76] Robin Booth and others (n 1006) 136.
[77] Ibid.
[78] Robin Booth and others (n 1006) 137.
[79] S.337 of the POCA 2002.
[80] S.338 of the POCA 2002.

2) An employee of his firm must have informed him about the internal SAR, so that there is a "protected disclosure" or "authorised disclosure."
3) He either can identify the money launderer or the whereabouts of the laundered property,[81] or he believes that the information, which came to him, may help identifying the money launderer or the whereabouts of the laundered property.
4) He failed to make the required disclosure to the competent authority.[82]

From the aforementioned conditions, two key points emerge. Firstly, the conditions are applied where a nominated officer receives a "protected disclosure" or an "authorised disclosure" from employees/persons in his organisation, inside and outside the regulated sector. Secondly, the last condition, namely failing to make a required disclosure to the NCA, will not be fulfilled unless the first three conditions are met. In other words, if one/or more of the first three conditions are not present, the nominated officer is not required to make a required disclosure to the NCA. There is no issue when applying the conditions to the "protected disclosure." Ambiguity only arises when conditions are applied to the "authorised disclosure," especially

[81] For the purpose of this offence, the laundered property is "the property forming the subject-matter of the money laundering that he knows or suspects that other person to be engaged in," s.332 (5 A). The definition is same as the definition given to laundered property for the first two offences of failure to report, except in relation to "grounds for knowing or suspecting." This is due to the objective basis not applying for the purpose of the offence.

[82] S.332 (1–4) of the POCA 2002 provides that:

'(1) A person nominated to receive disclosures under section 337 or 338 commits an offence if the conditions in s (2) to (4) are satisfied.

(2) The first condition is that he knows or suspects that another person is engaged in money laundering.

(3) The second condition is that the information or other matter on which his knowledge or suspicion is based came to him in consequence of a protected disclosure or authorised disclosure.

(3 A) The third condition is

(a) that he knows the identity of the other person mentioned in (2), or the whereabouts of any of the laundered property, in consequence of a [protected disclosure or authorised disclosure],

(b) that that other person, or the whereabouts of any of the laundered property, can be identified from the information or other matter mentioned in (3), or

(c) that he believes, or it is reasonable to expect him to believe, that the information or other matter will or may assist in identifying that other person or the whereabouts of any of the laundered property.

(4) The fourth condition is that he does not make the required disclosure to a person authorised for the purposes of this Part by the Director General of the National Crime Agency as soon as is practicable after the information or other matter mentioned in (3) comes to him.'

the first condition. As discussed in the following subsection, the subject of the authorised disclosure is not a person who is engaged in ML, but rather criminal property. Nevertheless, the first condition of this offence is "he knows or suspects that another person is engaged in money laundering"[83] which is totally different from the subject of an authorised disclosure. Thus, a nominated officer can receive a disclosure in his organisation, which could result in him not fulfilling the first condition of the offence, despite the subject of the disclosure being a property and not a person. This, in turn, results in the nominated officer not having to make a required disclosure to the NCA under the fourth condition of the offence.[84]

However, in addition to the information about the criminal property, it is very likely that an authorised disclosure includes information about the person, who is suspected to be involved in ML. Hence, in such case a nominated officer is obliged to make a required disclosure to the NCA since the first three conditions of the offence are met.[85]

Moreover, as discussed below, a nominated officer has to obtain consent from the NCA to proceed with the transaction if he received an authorised disclosure from an employee/person in his organisation. This is entirely different from the required disclosure. It is therefore also likely that the SAR submitted by the nominated officer to the NCA constitutes both required disclosure to avoid criminal liability under the third offence of failing to report and at the same time authorised disclosure to the NCA in order to obtain consent to proceed with the relevant transaction.[86]

Internal SARs and the Writing Requirement

It is worth noting that neither the POCA 2002 nor the MLR 2007 requires the reporters, employees/persons inside and outside the regu-

[83] S.332 (2) of the POCA 2002.

[84] Robin Booth and others (n 1006) 139.

[85] Ibid.

In addition, Three elements are important for the required disclosure, namely (1) the identity of the other person mentioned in the first condition of the offence, if disclosed to him under the protected disclosure or authorised disclosure, (2) the whereabouts of the laundered property, so far as disclosed to him under the protected disclosure or authorised disclosure and (3) the information or other matter mentioned in the second condition of the offence. POCA 2002, s.332 (5).

[86] Robin Booth and others (n 1006) 140.

lated sector, to send internal disclosures (SARs) to the nominated officer in a written form. However, it is advisable that reporters document their disclosures in detail electronically for two reasons. Firstly, to prove that they adhered to the conditions and requirements contained in the offences of failure to report. Secondly and most importantly, to assist the nominated officer in carrying out his work of evaluating and studying all internal disclosures to decide whether to pass on any of them to the NCA. Nevertheless, nominated officers alone have to record the information/matters contained in internal disclosures in writing or electronically in case they received them orally.[87]

The Defences to the Crime of Other Nominated Officer Failing to Report

There are two defences available in relation to this offence, which are the same as the ones available to the crime of a nominated officer in the regulated sector failing to report.[88]

The situations and circumstances in relation to the third offence of failing to report clearly show that the SARs do not involve one type of disclosure, but there are three types of disclosure, which can be authorised, required or protected. Hence, in order to simplify the issue, the following subsection deals with the types of disclosure in relation to ML.

Types of Disclosure Under the POCA 2002 and Their Consequences

There are basically three types of disclosure for ML set out in the POCA 2002, namely required, authorised and protected disclosure. However, a protected disclosure cannot be treated as a separate type of disclosure,[89] as discussed below. There are therefore two different major types of dis-

[87] Mark Simpson and Nicole Smith (n 1067) 130 & 131.

[88] POCA 2002, s.332 (6–7).

A person, who is found guilty of any the three offences relating to failing to report ML cases, can be sentenced for up to Fiveyears' imprisonment and/or a fine. POCA 2002, s.334 (2).

[89] Robin Booth and others (n 1006) 96.

closure which are required and authorised and which are likely to overlap with each other in practice. In addition, all these disclosures are applied to the term SAR. Indeed, the POCA 2002 does not use the term SAR, but instead uses the term disclosure, nevertheless, the SOCA, now the NCA, as the UK FIU, uses the term SAR as a more comprehensive term and includes all types of disclosure[90] since it receives all disclosures on ML. However, this does not mean that the NCA receives all disclosures made to the nominated officers since this officer evaluates and studies all internal disclosures and decides which disclosures need to be submitted to the NCA. This subsection critically evaluates the types of disclosure and their features, also with a view to appreciating the legal consequences.

Required Disclosure

This type of disclosure must be made in order to avoid criminal liability for the three offences of failing to report, analysed above. Hence, the required disclosure is directly linked to these three offences. Circumstances differ depending on the offence,[91] but its nature does not differ in all the three offences and remains the same. The disclosure is about another person, who is known or suspected, to be involved in ML. Furthermore, failure to make the disclosure results in the commission of an offence, namely one of the three failing to report offences.[92]

There are therefore three cases in relation to who must make the required disclosure and to whom it must be made. Firstly, the required disclosure is mandatory and has to be made by employees of the regulated sector in order to avoid committing the first failing to report offence.[93] The recipient of the required disclosure in this case could be a nominated officer or the NCA.[94] However, as mentioned above, in practice, an employee in the regulated sector will make the required disclosure to the nominated officer in his institution. Secondly, the disclosure must be

[90] Robin Booth and others (n 1006) 104.
[91] POCA 2002, s.330 (5), s.331 (5) or s.332 (5).
[92] Robin Booth and others (n 1006) 98.
[93] S.330 of the POCA 2002.
[94] S.330 (4) of the POCA 2002.

made by the nominated officer in the regulated sector in order to avoid committing the second offence of failing to report.[95] The recipient of the required disclosure is the NCA.[96] Thirdly and lastly, the disclosure has to be also made by the nominated officer whether inside or outside the regulated sector in order to avoid the commission of the third offence of failing to report.[97] The recipient of the disclosure is also the NCA.[98] As a result, in all cases the NCA, as the UK FIU, is the place which receives the required disclosure if the nominated officer decided to pass it on.

Authorised Disclosure

Unlike the previous disclosure, the subject of the authorised disclosure is the property, criminal property, which generally represents a person's benefit from criminal conduct. The disclosure is not obligatory and any person can make it, regardless of whether he works in the regulated sector or not. This is since the purpose of the disclosure is to avoid that a prohibited act[99] is committed, which constitutes one of the three principal ML offences, which apply to both inside and outside the regulated sector. Hence, any person (alleged offender),[100] who is at risk of committing one/more of these principal offences can make a disclosure to obtain appropriate consent in order to avoid committing the offence.[101] On the other hand, the disclosure has to be made to one of three persons, namely (1) a constable (including the NCA), (2) a customs officer[102] or (3) a nominated officer.[103]

---

[95] S.331 of the POCA 2002.

[96] S.331 (4) of the POCA 2002.

[97] S.332 of the POCA 2002.

[98] S.332 (4) of the POCA 2002.

[99] The term "prohibited act" means any act listed in section 327 (1), 328 (1) or 329 (1) of the POCA 2002.

[100] S.338 (1)(a) of the POCA 2002.
The term "alleged offender" means any person at risk of committing principal ML offence(s).

[101] Arun Srivastava (n 1023) 43.

[102] An officer of HMRC, s.6 of Commissioners of Revenue and Customs Act 2002.

[103] S.338 (1)(a) of the POCA 2002.

Accordingly, the authorised disclosure can be made directly to the NCA, through an external disclosure, or to the nominated officer, through an internal disclosure. An internal disclosure in the regulated sector or even outside the sector can be made if an organisation has appointed a nominated officer to receive internal disclosures.[104] In practice, authorised disclosures are normally made to the nominated officer who seeks consent from the NCA[105] in order to perform the transaction/prohibited act.

Conditions for the Authorised Disclosure

One of three conditions must be satisfied for the disclosure and which relate to the timing of the disclosure, which could be (1) before, (2) after or (3) whilst prohibited act is conducted.[106]

The first case arises if the disclosure is made before the alleged offender does the prohibited act. The alleged offender has to therefore make the disclosure before the prohibited act occurs, as long as he knows or suspects that the property represents a person's benefit from criminal conduct. In this case, he must seek to obtain appropriate consent to do the act.

The second case is if the disclosure is made at the same time the prohibited act takes place. Three elements must be met (1) before carrying out the prohibited act, the alleged offender must not know or suspect that the property constitutes or represents a person's benefit from crimi-

---

[104] S.338 (5) of the POCA 2002.

[105] Arun Srivastava (n 1023) 33.

[106] S.338 (2–3) of the POCA 2002 provides that:

'(2) The first condition is that the disclosure is made before the alleged offender does the prohibited act.

(2 A) The second condition is that

(a) the disclosure is made while the alleged offender is doing the prohibited act,

(b) he began to do the act at a time when, because he did not then know or suspect that the property constituted or represented a person's benefit from criminal conduct, the act was not a prohibited act, and

(c) the disclosure is made on his own initiative and as soon as is practicable after he first knows or suspects that the property constitutes or represents a person's benefit from criminal conduct.

(3) The third condition is that

(a) the disclosure is made after the alleged offender does the prohibited act,

(b) he has a reasonable excuse for his failure to make the disclosure before he did the act, and

(c) the disclosure is made on his own initiative and as soon as it is practicable for him to make it.'

nal conduct, (2) he must make the disclosure about the relevant property and (3) the decision to make a disclosure must be taken on his own initiative.[107]

The third case is when a disclosure is made after the prohibited act has been committed and the alleged offender must have had a reasonable justification for why he did not manage to divulge the information prior to the commission of the prohibited act and he must also on his own initiative make the disclosure as soon as it is practicable for him to make it.[108] The POCA 2002 does not define the term "reasonable excuse" and there is currently no judicial interpretation for it. This could potentially lead to the defence being misused,[109] as anybody could rely on this defence if the disclosure is made after the commission of the prohibited act. However, it is up to the Court to decide whether there is a reasonable excuse and this should be interpreted narrowly for obvious reasons.[110]

Differences Between the Required Disclosure and Authorised Disclosure

The required disclosure and authorised disclosure have the following differences:

1) The required disclosure is a mandatory disclosure, whilst the authorised disclosure is not mandatory. However, any person (alleged offender), who is at risk of committing the principal ML offence(s) can make the authorised disclosure in order to avoid criminal liability. The required disclosure ensures that the failing to report offence(s) can be avoided.
2) The required disclosure must be made by those who work in the regulated sector and by the nominated officer, inside/outside the regulated sector, whilst any person can make the authorised disclosure.

[107] POCA 2002, s.338 (2 A).
[108] POCA 2002, s.338 (3).
[109] Doug Hopton (n 1002) 55.
[110] Robin Booth and others (n 1006) 145.

3) The required disclosure must be made to the nominated officer or the NCA, depending on the conditions of each case illustrated above, whilst the authorised disclosure can be made to a constable (including the NCA), a customs officer or a nominated officer.
4) The required disclosure is about a person who is known or suspected to be involved in ML, whilst the authorised disclosure is about criminal property. However, it is very likely that an authorised disclosure includes also information about the person who is suspected to be involved in ML. In this case, the SAR, made by the nominated officer to the NCA, constitutes both the required disclosure and requested consent (external authorised disclosure). On the other hand, if the internally required disclosure is made to the nominated officer, he must ask himself whether it is necessary to request consent and if so the SAR constitutes both the externally required disclosure and requested consent (external authorised disclosure).

The Authorised Disclosure and the Meaning of Appropriate Consent

The authorised disclosure is directly related to the appropriate consent. This situation arises if the disclosure is made before the prohibited act is undertaken. In other words, the alleged offender cannot do the prohibited act even if he made the authorised disclosure, but he must wait to receive consent to do so. An appropriate consent simply means consent to do the prohibited act. This, in turn, necessarily supposes that the authorised disclosure was made along with a consent request, prior to the prohibited act taking place, since consent cannot be granted after the act has occurred.[111] Consent cab be given by a nominated officer if the disclosure is made to him, by a constable (including the NCA) if the disclosure is made to him or by a customs officer if the disclosure is made to him.[112]

The consent can be either actual or deemed consent. Actual consent means explicit consent, whilst there can be deemed consent in two situ-

[111] Paul Hynes, Nathaniel Rudolf and Richard Furlong (n 1046) 65.
[112] S.335 (1) of the POCA 2002.

ations. In case the alleged offender made the disclosure to a constable or customs officer, consent will be implied, so long as the requested consent was not refused by a constable or customs officer during the notice period. There will also be deemed consent if the alleged offender received from a constable or customs officer a refusal within the notice period, but the moratorium period has expired[113] and no action, such as the form of a restraining order, has been taken. The notice period is 7 working days from the day after the alleged offender makes the disclosure, whilst the moratorium period is 31 days from the day on which the alleged offender receives notice that consent is refused.[114]

The objective of the notice period is to give time to the NCA and other LEAs to evaluate the information/matters contained in the disclosure with a view to considering whether or not to grant or refuse the consent to perform the prohibited act.[115] Indeed, the notice period is essential to give analysts of the UK FIU enough time to analyse STRs (consent requests) and to decide whether to grant or refuse consent. The notice period is therefore important for the UK FIU to fulfil its analytical function.

The purpose of the moratorium period is to give time to the relevant LEAs to investigate information/matters contained in the disclosure in order to consider taking necessary actions, for example to make an appli-

[113] S.335 (2–4) of the POCA 2002 provides that:
'(2) A person must be treated as having the appropriate consent if
(a) he makes an authorised disclosure to a constable or a customs officer, and
(b) the condition in (3) or the condition in (4) is satisfied.
(3) The condition is that before the end of the notice period he does not receive notice from a constable or customs officer that consent to the doing of the act is refused.
(4) The condition is that
(a) before the end of the notice period he receives notice from a constable or customs officer that consent to the doing of the act is refused, and
(b) the moratorium period has expired.'

[114] S.335 (5–7) of the POCA 2002 provides that:
'(5) The notice period is the period of seven working days starting with the first working day after the person makes the disclosure.
(6) The moratorium period is the period of 31 days starting with the day on which the person receives notice that consent to the doing of the act is refused.
(7) A working day is a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in the part of the United Kingdom in which the person is when he makes the disclosure.'

[115] Robin Booth and others (n 1006) 147.

cation to the Crown Court[116] for a restraining order.[117] The moratorium period is longer than the notice period. This is because investigations carried out by the LEAs take more time than the UK FIU discharging its analytical function. In other words, the moratorium period is important for the investigation stage and to decide whether to grant requested consent and to take any action(s).

These circumstances arise when the alleged offender makes a disclosure either to a constable (including the NCA) or to a customs officer. Nevertheless, what is the situation if the alleged offender makes the disclosure to the nominated officer, inside/outside the regulated sector? This situation has a separate section in the POCA 2002 since his duties and responsibilities are vital in this regard and, in practice, most authorised disclosures are made to him.

Although the POCA 2002 grants the right to the nominated officer to give consent to the "discloser"[118] in his organisation to do the prohibited act, if he received it,[119] he cannot do so unless he receives actual consent from the NCA or there is deemed consent. Indeed, actual consent and deemed consent circumstances and conditions are the same as discussed above, nevertheless, such a case differs in two respects. Firstly, when the nominated officer receives an internal authorised disclosure, he must pass on the disclosure (about the criminal property) to the NCA to receive consent to do the prohibited act.[120]

---

[116] S.41 of the POCA 2002.

[117] Robin Booth and others (n 1006) 148.

[118] The term "discloser" means the person who makes the disclosure.

[119] S.335 (1) of the POCA 2002.

[120] S.336 (1–4) of the POCA 2002 provides that:

'(1) A nominated officer must not give the appropriate consent to the doing of a prohibited act unless the condition in (2), the condition in (3) or the condition in (4) is satisfied.

(2) The condition is that

(a) he makes a disclosure that property is criminal property to a person authorised for the purposes of this Part by the Director General of the National Crime Agency, and

(b) such a person gives consent to the doing of the act.

(3) The condition is that

(a) he makes a disclosure that property is criminal property to a person authorised for the purposes of this Part by the Director General of the National Crime Agency, and

(b) before the end of the notice period he does not receive notice from such a person that consent to the doing of the act is refused.

(4) The condition is that

(a) he makes a disclosure that property is criminal property to a person authorised for the purposes of this Part by the Director General of the National Crime Agency,

Secondly, he will commit an offence if he grants consent to do the prohibited act, although he knows or suspects that he has to obtain actual consent from the NCA or deemed consent.[121] More importantly, if the nominated officer receives an internal authorised disclosure and it contains information/matters about a person who is suspected or known to be involved in ML, in addition to the information about the criminal property, the SAR to the NCA can consists of both an externally required disclosure[122] and a consent request to do the prohibited act in order to avoid the commission of the aforementioned offence.[123] The duration of the notice period and the moratorium period are the same as described above.[124]

Protected Disclosures

This disclosure has a separate section in the POCA 2002 and in fact is not a real additional type of disclosure, but rather reflects the protection given to several types of disclosure.[125] Protection means that the

(b) before the end of the notice period he receives notice from such a person that consent to the doing of the act is refused, and

(c) the moratorium period has expired.'

[121] S.336 (5–6) of the POCA 2002 provides that:

'(5) A person who is a nominated officer commits an offence if

(a) he gives consent to a prohibited act in circumstances where none of the conditions in s (2), (3) and (4) is satisfied, and

(b) he knows or suspects that the act is a prohibited act.

(6) A person guilty of such an offence is liable

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.'

[122] To avoid committing the third failure to report offence if the conditions contained in s.332 of the POCA 2002 are met.

[123] S.336 (5–6) of the POCA 2002 (n 1119).

[124] S.336 (7–9) of the POCA 2002 provides that:

'(7) The notice period is the period of seven working days starting with the first working day after the nominated officer makes the disclosure.

(8) The moratorium period is the period of 31 days starting with the day on which the nominated officer is given notice that consent to the doing of the act is refused.

(9) A working day is a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in the part of the United Kingdom in which the nominated officer is when he gives the appropriate consent.'

[125] Robin Booth and others (n 1006) 96.

disclosure will not result in a breach of the limitations imposed on the disclosure of information, however imposed,[126] such as banking confidentiality imposed upon a banker, as analysed in Chap. 3. There are three conditions for the disclosure to be deemed protected and to be given the protection:

1) The information/matter came to the discloser in the course of his business, within/outside the regulated sector.
2) The discloser, based on the information/matter mentioned above, knows/suspects or has reasonable grounds to know/suspect that another person is engaged in ML. This condition illustrates the close link with disclosure in relation to the three failing to report offences, analysed above.[127]
3) The disclosure must be made to a constable, a customs officer or a nominated officer. In addition, it must be made as soon as practicable. Accordingly, this condition applies to internal disclosures made to the nominated officer and to external disclosures made to a constable (including the NCA) and a customs officer.[128]

All Disclosures Lead to Immunity

In addition, protection is also given to information contained in the required disclosure.[129] Protection given to the disclosures is broad and covers the

[126] S.337 (1) of the POCA 2002. Article 20 of the UAE FLMLC 2002 also provides this immunity, see (n 623) of Chap. 5.

[127] Namely s.330 (2), s.331 (2) and s.332 (2) of the POCA 2002.

[128] S.337 (2–4) of the POCA 2002 provides that:
'(2) The first condition is that the information or other matter disclosed came to the person making the disclosure (the discloser) in the course of his trade, profession, business or employment.
(3) The second condition is that the information or other matter
(a) causes the discloser to know or suspect, or
(b) gives him reasonable grounds for knowing or suspecting,
that another person is engaged in money laundering.
(4) The third condition is that the disclosure is made to a constable, a customs officer or a nominated officer as soon as is practicable after the information or other matter comes to the discloser.'

[129] Disclosures contained in s.330 (5), s.331 (5) and s.332 (5) of the POCA 2002.
S.337 (4 A) of the POCA 2002 provides that:
'Where a disclosure consists of a disclosure protected under (1) and a disclosure of either or both of
(a) the identity of the other person mentioned in (3), and

required disclosures contained under the three offences of failing to report,[130] as well as voluntary disclosures on ML by those who work outside the regulated sector in order to support those making such disclosures.[131]

As a result, all disclosures have been given protection by the POCA 2002, including the authorised disclosure.[132] However, the scope of protection is limit to the information/matters contained in the disclosure and additional information if requested.[133] Moreover, protection given to authorised disclosures is less than to other disclosures since it is connected with the principal ML offences, which have a subjective basis. Instead, protection given to protected disclosures is wider since they are initially connected to the three offences of failing to disclose, which have a subjective/objective basis.[134]

Furthermore, it is important to clarify whether protection is given to the nominated officer when making disclosure about criminal property to the NCA (externally authorised disclosure). Indeed, this type of disclosure happens often and, in practice, also includes information about a person who is suspected or known to be involved in ML. As a result, this disclosure will also be protected.[135] Accordingly, all types of disclosure are lawful disclosures, if the conditions are fulfilled. Nevertheless, in practice, most cases of lawful disclosures are authorised disclosure[136] and required disclosure.[137]

(b) the whereabouts of property forming the subject-matter of the money laundering that the discloser knows or suspects, or has reasonable grounds for knowing or suspecting, that other person to be engaged in, the disclosure of the thing mentioned in paragraph (a) or (b) (as well as the disclosure protected under (1)) is not to be taken to breach any restriction on the disclosure of information (however imposed).'

[130] Robin Booth and others (n 1006) 151.

[131] E. P. Ellinger, Eva Lomnicka and C.V.M Hare, *Ellinger's Modern Banking Law* (Fifth Edition, Oxford University Press 2011), 104.

[132] S.338 (4) of the POCA 2002 provides that:

"An authorised disclosure is not to be taken to breach any restriction on the disclosure of information (however imposed)."

In addition, s.7 (1) of the CCA 2013 provides protection, provided that the disclosure is made for the purpose of discharging the functions of the NCA in counteracting serious and organised crime.

[133] Under s.339 (2–4) of the POCA 2002.

[134] Arun Srivastava (n 1023) 50.

[135] Robin Booth and others (n 1006) 152.

[136] To avoid committing any of the three principal ML offences.

[137] To avoid committing any of the three offences of failing to report.

It is worth noting that the UK's disclosures system on ML is rated as "compliant" with the 2003 FATF's Recommendations in relation to the requirements of the SAR on ML.[138] On the other hand, there are disclosures deemed unlawful or prohibited under the POCA 2002. Theses prohibited disclosures will be discussed in the following section.

The Tipping off Crimes

These offences only apply to persons, who work in the regulated sector. This group of crimes encompasses two types. Firstly, tipping off disclosing SARs on ML. Secondly, tipping off ML investigations.[139]

The Tipping off Crime Relating to Disclosing ML

This type of crime requires a person, who works in a regulated sector, to divulge to a third party that a disclosure of ML, under part 7 of POCA 2002, has been made. This offence requires the following three conditions to be satisfied for a person to be charged:

i. A person must divulge any information to another party that a disclosure about ML has been made to a constable, an officer of the Revenue and Customs, a nominated officer or the NCA.[140]
ii. The disclosure, under the first condition, of any information probably harms any investigation, which might take place subsequent to the disclosure.[141]
iii. The disclosure, under the first condition, has to be based upon information which the defendant obtained during the course of business in the regulated sector.[142]

---

[138] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF 29 June 2007, 148.

[139] Stephen Gentle (n 1016) 17.

[140] POCA 2002, s.333 A (1)(a).

[141] POCA 2002, s.333 A (1)(b).

[142] POCA 2002, s.333 A (1)(c).

The first condition necessarily requires that a ML disclosure[143] has been made prior to this disclosure being divulged to a third party by a defendant. In addition, there is no limit in relation to the extent of the disclosure and both unintentional, as well as intentional disclosures are covered.[144] The second condition requires that the disclosure may harm the investigation which could be a criminal investigation (confiscation investigation) or a civil investigation (civil recovery investigation).[145] This does not mean that the disclosure has to cause actual prejudice to the investigation, but potential prejudice is sufficient. The third condition requires that the information, which is the subject of the disclosure, must be obtained in the course of the defendant's business. This means that if the defendant obtained information outside of his business in the regulated sector, for example, in a private social occasion, this case will not be subjected to the statutory provisions of this offence. This is because divulged information has been obtained outside the regulated sector and therefore falls outside the third aforementioned condition of the offence.

The Crime of Tipping off Relating to ML Investigations

The second type of tipping off crime requires that a person, who works in a regulated sector, divulges to a third party that a ML investigation is either being expected or underway.[146] Consequently, a person will not be committing this crime, unless the following three conditions are met:

[143] POCA 2002, s.333 A (2) has provided that:
'The matters are that the person or another person has made a disclosure under this Part
(a) to a constable,
(b) to an officer of Revenue and Customs,
(c) to a nominated officer, or
(d) to a National Crime Agency officer authorised for the purposes of this Part by the Director General of that Agency, of information that came to that person in the course of a business in the regulated sector.'

[144] Doug Hopton (n 1002) 70.

[145] Robin Booth and others (n 1006) 177.

[146] Stephen Gentle (n 1016) 17.

i. A person must divulge the fact that an investigation in relation to ML is being expected or underway.[147]
ii. The disclosure of any information, mentioned in the first condition, probably harms the investigation.[148]
iii. The disclosure, mentioned in the first condition, is based upon information, which the defendant gained in the course of business in the regulated sector.[149]

The second and third conditions are the same as for the first type of offence. This means that it is sufficient that the disclosure, mentioned in the first condition, potentially prejudices the investigation. In addition, the information divulged by the defendant must be obtained in the course of his business. However, a nominated officer, who works outside the regulated sector, should be subjected to the statutory provisions of the tipping off offences if he received an internal SAR from another person in his firm. He also has ML experience and should therefore know that the customer should not be alerted that the transaction has been treated as a SAR.

More importantly, the tipping off offences covers the prohibition of divulging information to any person, not just to the person undertaking the transaction. The statutory provisions in the POCA 2002 are very wide and do not confine the prohibition of disclosure to the person undertaking the transaction, but to any person. However, in the UAE, Article 16 of the FLMLC 2002 is very narrow and only outlaws making a disclosure to the person undertaking the transaction. Hence, no offence will be committed if the person informed a third party, who is related to or associated with the person undertaking the transaction, that the transaction is being checked or investigated for potential ML, as critically analysed in Chap. 5. This situation can lead to the relevant customer/third party changing facts/documents[150] and evidence(s) being destroyed and this can affect the quality of the analytical function of the AMLSCU and can

[147] POCA 2002, s.333 A (3)(a).
[148] POCA 2002, s.333 A (3)(b).
[149] POCA 2002, s.333 A (3)(c).
[150] With a view to removing the suspicion of ML from his transaction.

hamper the investigation by the LEAs and any subsequent prosecution. Indeed, the aims of the tipping off offences are not to prejudice actual or potential ML investigations and not to alert the relevant customer that his transaction/activity is suspected of being a SAR.[151]

Tipping off crimes can cause a strained relationship between individuals (customers) and institutions or firms. In particular, this will be the case when a disclosure of a SAR, coupled with a consent request, has been made to the NCA and the firm has to await the response. During this time, a customer may ask the firm to proceed with transaction, but a firm is neither able to continue the transaction or the activity, nor can it inform the client that the transaction is suspected of constituting ML since otherwise the firm will open itself up to criminal liability for tipping off. A firm may also not want to continue with a transaction where a ML investigation is underway.[152]

---

[151] There are a wide range of defences available to the tipping off offences. Firstly, s.333D (3–4) of the POCA 2002 provides that these offences will not be committed if the defendant does not know or suspect that the disclosure probably harms the investigation. Secondly, under s.333B (1) of the Act, no crime takes place when an employee, officer or partner of an undertaking discloses any information to an employee, officer or partner of the same undertaking. Thirdly, under s.333B (2) of the Act, if a disclosure relates to a customer and has been made in the context of a transaction associated with both institutions, it is lawful to disclose it amongst credit or financial institutions or within entities of the same group. In addition, s.333B (4) of the Act stipulates that this defence extends to professional legal advisers and relevant professional advisers. Fourthly, under s.333D (1) of the Act, the disclosure is allowed when it has been made vis-a-vis a supervisory authority or done in compliance with the provisions of the Act. Lastly, there is a defence, under s.333D (2) of the Act, for professional legal advisers and relevant professional advisers. This relates to the disclosure, which he makes, so long as it is made to the 'adviser's client and for the purpose of dissuading the client from engaging in conduct amounting to an offence.'

A person guilty of any tipping off offences, mentioned above, can be liable for up to two years' imprisonment and/or a fine. POCA 2002, s.333 A (4).

[152] Stephen Gentle (n 1016) 18.

There is another offence of prejudicing investigation contained in Part 8 of the POCA 2002, namely s.342 (2)(a) provides that:

'(1) This section applies if a person knows or suspects that an appropriate officer or (in Scotland) a proper person is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation, an exploitation proceeds investigation or a money laundering investigation which is being or is about to be conducted.

(2) The person commits an offence if

(a) he makes a disclosure which is likely to prejudice the investigation.' S.342 (3) of the POCA 2002 provides defences to such offence.

Conclusion

The SARs regime in the UK is innovative since it includes various types of disclosure. The second group of ML offenses, namely failing to report/disclose ML offences contained in part 7 of the POCA 2002 spells out the legal basis for adhering to the SARs' requirements. The conditions for the last type group of offences, namely the offence of other nominated officers failing to report, do not require an objective test for the purpose of establishing this offence. However, the adoption of an objective test may assist in establishing the conditions for the offence since a nominated officer should adhere to the highest level of CDD when dealing with clients' transactions for the purpose of detecting or preventing ML. A nominated officer is supposed to possess greater experience in identifying ML activities and patterns than other persons in his/her organisation. Hence, even if a nominated officer works outside the regulated sector, so long as he/she receives internal SARs from another person in that firm, the same ought to apply to him. In addition, submitting a SAR to the UK FIU, on the basis of a mere suspicion, has serious consequences for both the relevant customer and the reporting entity, especially if the reporting entity is a bank, as critically analysed in the following chapter.

There are basically three types of disclosure for ML set out in the POCA 2002, namely required, authorised and protected disclosure in relation to SARs. Indeed, the Act does not use the term "SAR," but instead speaks of disclosure. Nevertheless, the NCA, as the UK FIU, uses the term "SAR" as a more comprehensive term and includes all types of disclosure. More importantly, despite required disclosure and authorised disclosure being entirely different; they can overlap, in practice, and form the subject of a SAR. A required disclosure is about a person who is known or suspected to be involved in ML, whilst an authorised disclosure is about criminal property. However, it is very likely that an authorised disclosure includes also information about the person, who is suspected to be involved in ML. In this case, the SAR, made by the nominated officer to the NCA, constitutes both the required disclosure and requested consent (external authorised disclosure. On the other hand, if the internally required disclosure is made to the nominated officer, he must ask himself whether

it is necessary to request consent and if so the SAR constitutes both the externally required disclosure and requested consent (external authorised disclosure).

The purpose behind the required disclosure is to avoid the commission of the failing to disclose offence(s), whilst the purpose of the authorised disclosure is to avoid the commission of the principal ML offence(s). Otherwise, a prohibited disclosure will be made to a third party if the requisite legal conditions are met. This ensures that any actual or potential ML investigation is not harmed and that no customer is alerted that his transaction/activity is being suspected of ML. The statutory provisions of the tipping off offences only apply to those, who work in the regulated sector, though a nominated officer, who works outside the regulated sector, should also not commit the tipping off offences when he knows about ML activities.

In practice, all types of lawful disclosures are received by the NCA as external disclosures (SARs). In other words, all roads lead to the NCA. In these cases, NCA deals with SARs on ML. The following chapter analyses this unique UK FIU organisation in terms of its structure, responsibilities and authorities in relation to the SARs.

9

The Role of the SOCA, Now the NCA, in the SARs Regime

Introduction

The objective of this chapter is to critically evaluate the functions of the SOCA, now the NCA, as the UK's FIU law enforcement model and to assess this model in terms of its ability and power to handle SARs received from the reporting entities. This is essential in order to evaluate in the final chapter the chances of the UAE successfully adopting this model. In addition, this chapter critically analyses the efficiency of the consent regime in relation to the SARs and the practical problems associated with the grounds for submitting SARs to the NCA.

This chapter thus consists of three sections. The first section deals with the SOCA, now the NCA, as the UK FIU law enforcement model. This section analyses the core and non-core functions of the UK FIU in respect to SARs. The section also assesses its constructive relationship with the reporting entities and the LEAs (the end users of the SARs). The second section critically evaluates what role the SARs Regime Committee plays in terms of annual reports and discusses the statistics, which it has published. An analysis of the figures is crucial to assess the effectiveness

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_9

of the SARs regime and the UK FIU model. The third section critically analyses the consent procedures in the SARs regime and more importantly the practical problems when SARs are submitted to the NCA when there is a mere suspicion.

SOCA and NCA

In October 2013, the NCA replaced the SOCA, as a result of the adoption of the CCA 2013, so that the UK FIU is no longer situated within the SOCA, but the NCA. However, this shift does not affect the UK FIU since its core and non-core functions in relation to the SARs remain the same. Yet, it is essential to explain the SOCA and its functions as the UK FIU, also since the 2013 Act emphasises that its abolition does not affect the validity of anything the SOCA did before,[1] including its annual plans, reports, bulletins and guidance notes during its operational life, as discussed below.

The Situation with the SOCA

The SOCA had been established by the SOCPA 2005.[2] It replaced the NCIS, which was enacted as the UK FIU and the NCS.[3] In addition, the SOCA undertook "the investigative and intelligence work of the Her Majesty's Customs and Excise (HMCE) on serious drug trafficking and the recovery of related criminal assets and the Home Office's responsibilities for organised immigration crime."[4] It started its functions on 1 April

[1] The CCA 2013, Sch.8 (1) para 6.

[2] SOCA's staff consisted of 3700 full-time employees. They worked from around 50 sites in the UK and 40 sites abroad. It was divided into three major business groups, namely (1) Strategy and Prevention, (2) Operational Delivery and (3) Capability and Service Delivery. Detailed information about these groups is available on its website at: www.soca.gov.uk (last accessed on 13th September 2013).

[3] S.1 (3) of the SOCPA 2005, which is repealed by the CCA 2013, Sch.8 (2) para 158.

[4] 'One Step Ahead—A 21st Century Strategy to Defeat Organised Crime' as produced by the Home Office in March 2004, 1, available online at: www.soca.gov.uk/about-soca/library/doc…/67-one-step-ahead (last accessed on 11th November 2014).

2006. The SOCA was sponsored by the Home Office, but was operationally independent.[5] It dealt with serious organised crimes, which affected national security and harmed the UK's economic and social welfare,[6] for example human trafficking, fraud, drugs and ML. Part 1 of the SOCPA 2005, which is now defunct under the CCA 2013, created the SOCA and spelled out the powers and functions in relation to serious organised crime, whilst Schedule 1 of the Act contained provisions about the Director General and staff.[7]

The SOCA was responsible for three principal functions. Firstly, it was responsible for preventing and detecting organised crime and reducing its consequences.[8] Secondly, it could recover assets.[9] Lastly and most relevant to this study, it was responsible for gathering/receiving, analysing and disseminating information,[10] hence SOCA acted as a FIU. In addition to the normal investigative powers, which most LEAs have, the SOCA acted as the UK's FIU in relation to SARs

[5] It was a Home Office Non-Departmental Government Body, see 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF 29 June 2007, 84.

[6] Ben Bowling and James Ross, 'The Serious Organised Crime Agency—should we be afraid?' [2006 Dec] Criminal Law Review 1019, 1019.

[7] The SOCA Board included the Chair, the Director-General, who were both appointed by the Home Secretary and ordinary members, as well as ex-officio members appointed by the Director-General in consultation with the Chair. See Clive Harfield, 'SOCA: a paradigm shift in British policing' (2006) 46 (4) British Journal of Criminology 743, 750.

Further information on the Board of SOCA is available on the SOCA's website at: www.soca.gov.uk (last accessed on 13th September 2013).

Moreover, under s.43 (1) of the SOCPA 2005, which is repealed by sch.8 (2) para 158 of the CCA 2013, the Director General was responsible for designating officers' powers which can be one/more of the following:

(a) a person having the powers of a constable, England and Wales, Scotland and /or Northern Ireland;

(b) a person having the customs powers of an officer of Revenue and Customs;

(c) a person having the powers of an immigration officer.

[8] S.2 (1) of the SOCPA 2005, which is repealed by the CCA 2013, Sch.8 (2) para 158.

[9] S.2 A of the SOCPA 2005, which is repealed by the CCA 2013, Sch.8 (2) para 158.

S.74 of the SCA 2007 abolished the Assets Recovery Agency (ARA) and Sch.8 (2) of the Act equipped SOCA and now NCA with civil recovery powers. The decision of merging ARA with the SOCA was due to the underachievement of the ARA and to enhance the effectiveness of the civil confiscation regime. See Nicholas Ryder, *Financial Crime in the 21st Century*: *Law and Policy* (Edward Elgar Publishing Limited 2011), 208.

[10] S. 3(1) of the SOCPA 2005, which is repealed by the CCA 2013, Sch.8 (2) para 158.

on ML. This means that the function of SOCA was similar to a policing unit[11] and represented a FIU law enforcement model; however, it was not a police organisation.[12]

The Situation with the NCA

After seven years, the SOCA was abolished and replaced by the NCA.[13] In 2011, the Home Office announced that it was going to introduce a new strategy to fight crime by establishing the NCA, as "an integral part of the UK law enforcement with a senior Chief Constable at its head."[14] In addition, The SARs regime committee facilitated the transition, so that the "NCA [could] take over responsibility for the UK FIU from SOCA in October 2013.".[15]

The Reason for the Creation of the NCA

The main reason for this shift and the establishment of the NCA is the global nature of organised and serious crime, which threatens the UK's national security and economy.[16] The NCA has been established

[11] Sabrina Fiona Preller, 'Comparing AML legislation of the UK, Switzerland and Germany' (2008) 11 (3) Journal of Money Laundering Control 234, 236.

[12] Clive Harfield (n 1157) 743.

[13] See www.nationalcrimeagency.gov.uk (accessed on 20th April 2015).

[14] Home Office Report, 'The National Crime Agency- A plan for the creation of a national crime-fighting capability', Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty (HM), June 2011, available on the Home Office website at: www.homeoffice.gov.uk (accessed on 25th November 2014).

[15] 'Suspicious Activity Reports Regime, Annual Report 2011' as produced by the SOCA, 42, and 'Suspicious Activity Reports Regime, Annual Report 2012' as produced by the SOCA, 41.

[16] The National Security Strategy defines organised crime as significant and persistent threat to UK citizens, the economy and business. See HM Government Report, 'A Strong Britain in an Age of Uncertainty: The National Security Strategy', Presented to Parliament by the by the Prime Minister by Command of HM, October 2010, available online at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (accessed on 23rd October 2014).
Organised crime costs the UK between £20 billion and £40 billion yearly and is expected to rise during the next five years, notably in light of increasing globalisation, facilitated through the internet, which assists criminals to commit crimes more easily. See 'SOCA annual Plan 2013/14' as produced by the SOCA on 28 March 2013, 8 & 9.

to act as an operational crime fighting agency to (1) combat organised crime, (2) safeguard the UK's borders, (3) fight cyber crime and to (4) protect children and young people from sexual exploitation and abuse.[17]

The NCA's Strategies and Independence

NCA has been established under the CCA 2013[18] and it became operational on 7 October 2013. Part 1 and Schedule 1 of the 2013 Act create the NCA and spell out its powers and functions, including of its officers and the Director General, and how accountability is achieved. The Director General of the NCA[19] is appointed by the Home Secretary and he is also accountable to the Home Secretary[20]; however, the Director General is operationally independent from the Home Secretary in relation to the NCA activities.[21] In addition, the Home Secretary is responsible for determining strategic priorities for the NCA after consultation with the strategic partners[22] and

[17] Karen Harrison and Nicholas Ryder, *The Law Relating to Financial Crime in the United Kingdom* (Ashgate Publishing Limited 2013), 25 & 26.

[18] The CCA 2013 received Royal Assent on 25 April 2013.
In addition, the National Policing Improvement Agency (NPIA) has been replaced by the NCA.

[19] The current Board of the NCA comprises (1) Keith Bristow- Director General (Chair), (2) Phil Gormley- Deputy Director General, (3) David Armond Director- Border Policing Command, (4) Peter Davies Director- CEOP Command, (5) Gordon Meldrum Director- Organised Crime Command, (6) Gary Chatfield- Director of Operations (Temporary), (7) Tim Symington- Director of Intelligence, (8) Stephen Webb- Director Corporate Services (Interim) and (9) Trevor Pearce Director- Economic Crime Command (Interim).
For further information about the members of the NCA, see 'NCA Annual Plan 2013–14', as produced by the NCA in October 2013, 10 & 11.

[20] And through the Home Secretary to Parliament.
In addition, s.11 of the CCA 2013 requires Her Majesty's Inspectors of Constabulary (HMIC) to carry out inspections of the NCA and to report to the Secretary of State on the NCA's efficiency and effectiveness.

[21] 'NCA Annual Plan 2013–14' (n 1169) 10.

[22] The term "strategic partners" means:
'(a) the Scottish Ministers;
(b) the Department of Justice in Northern Ireland;
(c) such persons as appear to the Secretary of State to represent the views of local policing bodies;
(d) such persons as appear to the Secretary of State to represent the views of the chief officers of England and Wales police forces;
(e) the chief constable of the Police Service of Scotland;

the Director General of the NCA.[23] The Home Secretary has set a number of strategic priorities for the NCA, for example to (1) prosecute and disturb people engaged in serious and organised crime, (2) prevent people from committing such crime, (3) enhance safeguards and (4) to decrease the impact of serious and organised crime.[24]

The NCA has 4500 staff in the UK and 120 staff in 40 countries and its budget is £463 million.[25] Its officers have the powers of a constable, a customs officer and an immigration officer.[26] It fulfils two core functions. Firstly, it fights organised and serious crime.[27] Secondly, it analyses and disseminates criminal intelligence relating to serious and organised crime.[28] This means that the NCA acts as a FIU.

The NCA's Units

The NCA has four units to fulfil its responsibilities, namely (1) the Organised Crime Command (OCC), (2) the Border Policing Command (BPC), (3) the Economic Crime Command (ECC) and (4) the Child

(f) the Chief Constable of the Police Service of Northern Ireland;
(g) the Commissioners for Her Majesty's Revenue and Customs;
(h) the Director of the Serious Fraud Office.' S.16 of the CCA 2013.

The functions of the NCA extend to Scotland and Northern Ireland, but specific arrangements have been adopted since police and criminal justice are devolved matters in Scotland and Northern Ireland. The NCA is co-located with the police in Scotland and other partners at the Scottish Crime Campus in Gartcosh and the NCA carries out its operations in collaboration with the police in Scotland. In Northern Ireland, the NCA's functions cover tackling serious and organised crime, customs offences, immigration crime and some asset recovery; however, NCA officers are not given the powers of a constable. The NCA works with the Police Service of Northern Ireland and other Northern Ireland enforcement partners. For the NCA's functions in Scotland and Northern Ireland in detail, see 'NCA Annual Plan 2013–14' (n 1169) 11, and 'SOCA annual Plan 2013/14' (n 1166) 10.

[23] S.3 of the CCA 2013.

[24] More details about the strategic priorities can be found in the 'NCA Annual Plan 2013–14' (n 1169) 6.

[25] Philip Johnston, 'The National Crime Agency: Does Britain need an FBI?' *The Telegraph*, 7 October 2013.

[26] S.10 (1) of the CCA 2013.

[27] S.1 (4) of the CCA 2013.

[28] S.1 (5) of the CCA 2013.

Exploitation and Online Protection Centre (CEOP).[29] The OCC is responsible for fighting and reducing serious and organised crime and thus takes over the activities of the SOCA. As the SOCA was the largest body, which has been moved into the NCA, its budget and staff still form the core of the NCA. The NCA builds upon SOCA's capabilities in order to deliver a stronger, more integrated and better co-ordinated national response to serious and organised criminality. As a result, the NCA, among other responsibilities, is now responsible for receiving, analysing and disseminating SARs.[30] The abolition of the SOCA does not affect the validity of the functions and procedures it carried out prior to its abolition.[31]

The SOCA, now the NCA, as the UK FIU

As mentioned above, amongst other responsibilities, the SOCA, now the NCA, plays a crucial role in relation to the SARs. The responsibility stems from firstly the POCA 2002 which obliges firms in the regulated sector to disclose information about any potential ML activity, SARs, to the NCA,[32] as critically analysed in the previous chapter. Nominated officers outside the regulated sector can also be required to disclose SARs to the NCA.[33] Secondly, the CCA 2013 bestows the NCA with the power to act as the UK FIU in relation to gathering, analysing and disseminating SARs,[34] however, the Act does not explicitly mention the term "FIU".[35] The UK FIU was situated within the SOCA, namely in the Proceeds of

[29] For more details about the commands, see 'NCA Annual Plan 2013–14' (n 1169) 12–14.

[30] Emma Radmore, 'Deferred Prosecution Agreements—for more enforcement action?' May 2013 Financial Regulation International 1. Available online at:
http://www.dentons.com/insights/articles/2013/june/18/deferred-prosecution-agreements-for-more-enforcement-action (accessed on 25th August 2015).

[31] The CCA 2013, Sch.8 (1) para 6.

[32] S.104 of the SOCPA 2005.

[33] S.332 of the POCA 2002.

[34] S.5 (1) of the CCA 2013.

[35] Even Part 1 of the SOCPA 2005, before it was abolished, did not explicitly mention the term "FIU."

It is worth noting that the EU Third Money Laundering Directive requires all member state to create a FIU as a national unite specialised in receiving, analysing and disseminating SARs. Article 21 of the Directive provides that:

Crime Department[36] and is now located within the International Hub[37] of the NCA. The internal policies of the SOCA, now the NCA, require that the UK FIU is the only place, which deals with all aspects of the SARs.[38] This comprises the core functions of a standard FIU, namely receiving, analysing and disseminating SARs. In addition, it is dealing with other non-core functions, as evaluated below.

In 2006, the UK's SARs regime was reviewed by Sir Stephen Lander[39] in light of the creation of the SOCA and its functions as the UK FIU in order to assess the effectiveness of the regime in terms of its weaknesses, strengths and benefits and to provide necessary recommendations.[40] The review gave 24 recommendations, which can be classified into four groups, namely (1) 9 recommendations dealing with the SOCA as the UK FIU, (2) 3 recommendations addressing the reporting entities, (3) 11 recommendations about exploiting the SARs by LEAs and (4) 1 recommendation in relation to the implementation of the recommendations.[41]

'1. Each Member State shall establish a FIU in order effectively to combat money laundering and terrorist financing.

2. That FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation. It shall be provided with adequate resources in order to fulfil its tasks.

3. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks.'

Directive 2005/06/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[36] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 78.

[37] 'Suspicious Activity Reports Regime, Annual Report 2013' as produced by the NCA, 4.

It is worth noting that although the SARs annual report 2013 is produced by the NCA, it refers to the reporting year under the management of SOCA, as the NCA replaced the SOCA in October 2013.

[38] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 78.

[39] The review was commissioned in July 2005. Sir Stephen Lander, 'Review of the suspicious activity reports regime' as produced by the SOCA in March 2006, available on the SOCA's website at: www.soca.gov.uk (last accessed on 13th November 2012).

[40] Angela Leong, *The Disruption of International Organised Crime* : *An Analysis of Legal and Non-Legal Strategies*,(Ashgate Publishing Limited 2007), 209.

[41] For details about the 24 recommendations, see Sir Stephen Lander (n 1189).

The UK FIU has adopted the recommendations.[42] Indeed, the review has taken into account all stakeholders which participate in the SARs regime, namely the UK FIU, reporting entities and LEAs. The SARs regime can only be effective if all these entities cooperate with each other. Higher quality SARs improves the analytical function of the NCA. The most important recommendations by Sir Stephen Lander are that all reporting entities should attend quarterly seminars about their tasks and a continuous dialogue should be established between all entities to enable them to overcome practical difficulties.[43]

The UK FIU was funded through the budget of the SOCA and now the NCA; however, it is operationally independent,[44] as it has its own management structure which comprises the five departments. Theses departments are (1) SARs Administration and Control,[45] (2) Consent,[46] (3) Sector Dialogue Team,[47] (4) Intelligence,[48] (5) HMRC Team[49] and (6) International.[50]

---

[42] Jayesh D'Souza, *Terrorist financing, money laundering and tax evasion- Examining the performance of Financial Intelligence Unit* (Taylor and Francis Group, LLC 2012), 159 & 160.

[43] Sir Stephen Lander (n 1189), recommendations 2, 7 and 11.

[44] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 29.

[45] This department manages the SARs regime and processes the SARs from the reporting entities. It is also responsible for creating best practice for ELMER use and its feedback. In addition, it preserves control over IT support. Jayesh D'Souza (n 1192) 161.

[46] This department has two major functions. Firstly, it collects, collates and disseminates consent-derived intelligence. Secondly, it works as an intervention device between LEAs and reporting entities with a view to ensuring best practice and to develop the use of consent. Ibid.

[47] This team is the link between the UK FIU and entities affected by the SARs regime, including reporting entities, regulators and LEAs. This team also provides individual feedback to the aforementioned entities about the SARs regime and vice versa. Ibid.

[48] This department analyses SAR-derived intelligence for tactical and strategic evaluation purposes and to enhance the utilisation of SARs in accordance with the UK's and international requirements. Ibid.

[49] The team is responsible for analysing and disseminating SARs on certain crimes to appropriate HMRC investigation teams. These SARs deal with VAT fraud, ML, tax credit, tax evasion, cash/foreign currency intelligence, arms proliferation and excise fraud. Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 81.

[50] The role of this department is to ensure that the UK FIU complies with the Egmont Group by providing financial intelligence to the UK LEAs and foreign FIUs upon request. Jayesh D'Souza (n 1192) 161.

In addition, there are a number of other departments, such as the TF Team and PEPs. 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 81–87.

The UK FIU was a founding member of the Egmont Group and was given full membership status in June 1995.[51] This section only analyses the key features of the functions of the UK FIU in relation to the SARs. The CCA 2013 has given the NCA the right to receive, analyse and disseminate these SARs. S.1 (3)(b) of the Act provides that the NCA is to have "The functions conferred by the Proceeds of Crime Act 2002." In addition, s.1 (5) of the Act provides that the NCA has to gather/receive, store, analyse and disseminate criminal intelligence about SARs.[52]

Although the core functions and non-core functions of a FIU have been discussed in detail in Chap. 4, it is important to critically assess these functions from the UK FIU's perspective.

Receiving SARs

A great number of institutions, especially large and medium firms, have adopted Intelligent Transactional Monitoring Systems (ITMS)[53] as an internal procedure in order to monitor transactions, which involve potential ML. The system cannot identify which transaction is involved in ML; however, it alerts the nominated officer of the firm about transactions which appear unusual.[54] In turn, the nominated officer has to

---

[51] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 85.

[52] S.1 (5) of the CCA 2013 provides that:

'(5) The NCA is to have the function (the "criminal intelligence function") of gathering, storing, processing, analysing, and disseminating information that is relevant to any of the following

(a) activities to combat organised crime or serious crime;

(b) activities to combat any other kind of crime;

(c) exploitation proceeds investigations (within the meaning of section 341(5) of the Proceeds of Crime Act 2002), exploitation proceeds orders (within the meaning of Part 7 of the Coroners and Justice Act 2009), and applications for such orders.'

[53] This is similar to the internal electronic system, which is used by banks in the UAE, as illustrated in the course of interviewing Mr. Z. See Chap. 6.

[54] Doug Hopton, *Money Laundering, A Concise Guide for All Business* (Second Edition, Gower Publishing Limited 2009), 119.

study the relevant transaction according to his experience, CDD procedures, updated profiles of the relevant parties and the circumstances surrounding the relevant transactions. If all the aforementioned procedures lead the nominated officer to know/suspect or give him reasonable grounds for knowledge/suspicion about potential ML, he has to report the case on a SAR form[55] to the NCA. For the ITMS to be properly operated, the system has to be linked and full access has to be given to all the firm's records, national and international results and other intelligence available.[56] It is crucial that the links between the employee, who suspects or knows potential ML, and the nominated officer are short and direct in order to save time.[57]

In all cases, the SARs must be reported to the NCA as soon as the person knows/suspects or has reasonable grounds for knowledge/suspicion that another person is involved in ML[58] and this could be before, during or after the transaction has occurred. The role of the NCA, as the UK FIU, at this stage is to receive and gather these SARs from the reporting entities, as required under the CCA 2013. The submission of the SARs to the NCA can be made either in hard copy or electronically. The reporting entities can send the SARs in hard copy by post or fax to the UK FIU.[59] Reporting entity should use the NCA's Preferred Paper SAR Form,[60] though submitting the SARs in hard copy is not favoured by the

[55] The SAR, in this case, comprises one/more type(s) of disclosure, as analysed in the previous chapter.

[56] Doug Hopton (n 1204)119.

[57] Ibid 120.

[58] UK FIU Guidance Note, 'Introduction to Suspicious Activity Reports (SARs)' as produced by the NCA in October 2013, available on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 25th October 2014).

[59] The address of the UK FIU and the number of its Fax are available on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 25th October 2014)

[60] 'Frequently Asked Questions' (FAQs) as produced by the SOCA and available on its website at: www.soca.gov.uk (last accessed on 15th November 2012). The NCA Preferred Paper SAR Form can be downloaded also from the NCA's website.

NCA and SARs should be submitted electronically via one of three ways, namely (1) MoneyWeb,[61] (2) SAR Online[62] or (3) Encrypted email.[63]

The NCA highly recommends submitting SARs via SAR Online, as it has a number of advantages, namely (1) it is a free and secure system, (2) which is available 24 hours a day, 7 days a week, (3) enables quicker dissemination of a SAR to the relevant LEA and reduces administrative tasks and (4) more importantly, the reporter receives a reference number (ELMER reference number) along with acknowledgement, in his email account, once he has completed the submission of the SAR via SAR Online.[64] The reference number of the report is essential since it can be used as evidence, especially by the nominated officer, to avoid committing the failing to report offence.[65]

SARs Form

The UK FIU has a modular report form, available through SAR Online.[66] In addition, the NCA Standard Form, in cases of manual SAR reporting,

[61] This is a secure electronic reporting system for entities which report a large volume (more than 250) of SARs a year. 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 82.

[62] The NCA prefers this method to submit SARs. The system enables all persons, regardless of whether they work in the regulated sector or outside it, to report SARs to the NCA electronically and securely, but the person/entity has to register for the system to work. This only entails downloading and completing the registration form from the NCA website and only requires a working email account, which is used for SAR Online user identification. Robin Booth and others, *Money Laundering Law and Regulation*: *A Practical Guide* (First Published, Oxford University Press 2011), 105.

The email account can be used by only one user. The SAR Online can be easily accessed from the NCA website. In 2012, the system was used by more than 4000 reporting entities. 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 18.

[63] This is a secure electronic system for submitting SARs, as reporters have encrypted emails to submit SARs. 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 82.

[64] UK FIU Guidance Note, 'Reporting via SAR Online' as produced by the NCA in October 2013, available on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 24th October 2014).

[65] S.331 and s.332 of the POCA 2002. See Chap. 8.

[66] However, the POCA 2002 gives the right to the Home Office to prescribe the form and manner of the required disclosure and authorised disclosure. At present, the government has decided not to proceed with the prescribed form after the Home Office issued a consultation document in July

comprises seven separate models.[67] The reporting entities have to use the correct SAR glossary code[68] when they complete a SAR, whether electronically or manually, in order to render the submission more useful for law enforcement officers. Thus, if a nominated officer rings the police and divulges his knowledge or suspicion about potential ML, this will not be sufficient under the Act. This is because the disclosure and submission of the SARs must be in accordance with the method adopted by the Director General of the NCA.[69]

The Vital Role of the UK FIU During the Receiving SARs Stage

Indeed, the UK FIU plays vital role at this stage since it provides the reporting entities with guidance on how to improve the quality of their SARs and what should be contained in them. For instance, it recommends that reporting entities should consider the 5 Ws and 1 H questions when they complete the SAR form. The questions are (1) who, (2) what, (3) where, (4) when, (5) why and (6) how.[70] In addition, the UK FIU recommends that SARs should include as much information as

2007 on this issue and published, in February 2008, a summary of responses to the consultation exercise. See Robin Booth and others (n 1212) 152–153.

[67] These models are (1) a Source Registration Document which needs to completed when the reporting entity reports its first SAR to the UK FIU, (2) Report Details (cover sheet), (3) Subject Details, (4) Additional Details, (5) Transaction Details in case the reporting entity is a financial institution, such as a bank, (6) Reason for Suspicion and Limited Intelligence Value (LIV) SAR and (7) Reason for Suspicion Continuation which allows the reporter/discloser to write, in his own words, why the transaction is unusual or why he has reasons for suspicion and it includes "tick boxes" for the suspected offences, such as drugs. In relation to model no.5, namely Transaction Details, the reporter, bank, has to fill out this module about the known/suspected customer, for example, account(s) number, sort code(s) and balance of the account. For further details about the NCA Standard Form, see FAQs (n 1210).

[68] For example, code XXS1XX requires immediate attention from law enforcement officers when reporters do not seek consent for the purposes of s.335 of the POCA 2002, whilst code XXS99XX denotes that appropriate consent has been sought under the POCA 2002. All SAR Glossary Codes are available on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 24th October 2014).

[69] Doug Hopton (n 1204) 61 & 67.

[70] It is crucial to note that these questions are the elements of the analytical function of the UAE FIU, as Mr. A, from the AMLSCU staff, stated in Chap. 6.

possible about the relevant transaction.[71] The information assists the relevant LEA at a later stage in accessing other important information about the relevant customer.[72] More importantly, the UK FIU continually publishes bulletins on aspects of SARs, such as the procedure after submitting SARs, the legal basis for SARs, FAQs and case studies on SARs for training purposes All of these bulletins and guidance notes are published in order to increase the quality of the SARs and were available on the SOCA website and can now be found on the NCA website. Indeed, these guidelines vitally assist the reporting entities to avoid deficiencies contained in their previous SARs. The UK FIU is aware that its analytical function will not be improved, unless the quality of SARs, submitted by the reporting entities, is increased. This is unlike the UAE FIU, which does not issue these bulletins and guidelines. This aspect has negatively affected the quality of the STRs and consequently the analytical function of the UAE FIU. This is evidenced by the large disparity between submitted STRs by the reporting entities and the disseminated STRs, which the AMLSCU has passed to the prosecutor between June 2002 and May 2009, as critically analysed in Chap. 5.[73]

Storing, Analysing and Disseminating SARs

Storing and Analysing SARs

After receiving SARs from the reporting entities, the SARs Administration and Control department of the UK FIU[74] processes and categorises them into certain groups in order to have them analysed by specialised FIU teams.

[71] Such as the date of the activity, type of product or service and the reason for suspicion. Moreover, information about the relevant parties, such as his full name, date of birth, his occupation and his account/policy number (if appropriate) and information about the relevant company, such as full legal name, registration number and address. See, UK FIU bulletin, 'Compliance and the Consent Regime' as produced by the UK FIU in February 2011, available on the SOCA's website at: www.soca.gov.uk (last accessed on 15th November 2012)

[72] Mark Simpson and Nicole Smith, 'UK Part III: Practical implementation of Regulations and Rules' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 95 at 132.

[73] The AMLSCU received 80,592 STRs from the reporting entities and only 285 STRs were transmitted to the Public Prosecution Office.

[74] See (n 1195).

A tactical analysis[75] is employed and databases are searched, for example criminal databases and the FIU's database known as (ELMER),[76] communication takes place with LEAs and data mining searches are carried out.[77]

The Consent Team of the UK FIU[78] analyses SARs involving consent requests and passes the requests to the relevant LEA for consultation on the consent decision.[79] In some cases, although a SAR involves known/suspected ML, consent may be given for an operational analysis,[80] such as to track the movement of the money.[81] The Consent Team usually informs the reporter via telephone about the consent decision in consultation with the relevant LEA within the 7 days notice period and also sends a confirmation letter by post.[82]

The SOCA, now the NCA, has recently established a new web based portal called "DISCOVER" to assist with searches via the NCA system, thereby enhancing operational intelligence gathering. The main objective of the DISCOVER system is that financial investigators of NCA improve their knowledge/understanding about the crime by searching more data on the various NCA systems in order to gather lots of details,[83] which can thus be used for strategic and tactical analyses.[84]

The Importance of ELMAR

All SARs are stored electronically on ELMER. This database serves two main objectives. Firstly, apart from it being used for tactical analysis purposes, it

[75] The term of "tactical analysis" has been analysed in Chap. 4.

[76] ELMAR is an Internal UK FIU database, which stores all SARs, which have been received from the reporting entities.

[77] The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 79–80.

[78] See (n 1196).

[79] UK FIU bulletin, 'Compliance and the Consent Regime' (n 1221).

[80] The term "operational analysis" has been analysed in Chap. 4.

[81] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 80.

[82] FAQs (n 1210).

[83] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 39.

[84] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 39.
The term of "strategic analysis" has been analysed in Chap. 4.

is also used for strategic analysis. This type of analysis is usually done by the Intelligence Department of the UK FIU[85] in order to identify groups of SARs, which are linked with each other in terms of the subject and the time period. Persons can therefore be linked to the same type of crime and the relevant LEA can take the appropriate decision/action and an example is SARs records on Chinese organised crime in the UK.[86] This type of analysis also assists with identifying whether there is any specific geographical area for ML and how criminals operate and whether they exploit certain businesses or financial products/services for their criminal activities.[87] Secondly, ELMER provides maximum dissemination of SARs data to LEAs and thereby adds great value and supports any existing/future SAR investigation.[88] Officers of LEAs can easily access ELMER via MoneyWeb.[89] In December 2011, the database was simplified by the removal of unnecessary functions[90] and SARs are also only stored on ELMER for up to 6 years and all SARs which are stored longer than this will be deleted.[91]

Disseminating SARs

Recently, the SOCA, now the NCA, established a sophisticated internet system for analysing SARs and extracting intelligence from them.

[85] See (n 1198).

[86] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 80–81.

[87] FAQs (n 1210).

[88] However, SARs on sensitive subjects, such as terrorism, are not available for LEAs via ELMER. Ibid.

[89] Furthermore, the SOCA, now the NCA, has published criteria for direct access to SARs on ELMER via Money Web and ARENA for LEAs or other relevant government bodies. The criteria apply from October 2011 onwards and are included in Annex G of 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165).

[90] 'Suspicious Activity Reports Regime, Annual Report 2010' as produced by the SOCA.

[91] Moreover, all SARs which are not related to criminal activity are also being deleted. SOCA, now the NCA, has issued this policy following a consultation with the Information Commissioner. For further information, see, 'UK FIU Updates, New retention and deletion policy for Suspicious Activity Reports (SARs)', available on the SOCA's website at: www.soca.gov.uk (last accessed on 17th November 2012). Accordingly, 745,203 SARs have been removed from ELMER. 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 21.

Currently there are about 1.38 million SARs on ELMER. This number has been obtained from the SOCA's website at: www.soca.gov.uk (last accessed on 17th November 2012).

This innovative system is called "ARENA." Unlike the ELMER database, which displays the results of a SARs search as a list, the ARENA system can be exploited by "end users of SARs,"[92] who wish to conduct large number of searches on SARs in terms of people and entities. In other words, by ARENA allows that a great number of SARs can be searched and provides a clear image and links SARs' parties, for example people, subjects, locations, companies and other relevant information.

This system provides common links and themes between SARs and thereby establishes links between suspected person(s) via a simplified vision of the funds movements.[93] Hence, the ARENA system assists LEAs with identifying relevant intelligence and enabling them to take appropriate decision/action without spending too much time on conducting research.[94] As such, the NCA, as the UK FIU, plays a vital role in assisting relevant LEAs with investigating SARs. The UK FIU has the authority to disseminate SARs to UK police force,[95] special police force[96] or LEAs[97] for investigation or action.[98] SARs are only analysed by UK FIU staff whilst the decision of disseminating a SAR to the LEAs and other

[92] SOCA, now the NCA, uses the term "end users of SARs," which means LEAs and other relevant government bodies, which are current or potential users of SARs.

[93] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 24.

[94] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 47 & 48.

[95] The UK police force means:
'(a) an England and Wales police force;
(b) the Police Service of Scotland;
(c) the Police Service of Northern Ireland;
(d) a special police force.' S.16 (1) of the CCA 2013.

[96] Special police force means:
"(a) the British Transport Police;
(b) the Civil Nuclear Constabulary;
(c) the Ministry of Defence Police." S.16 (1) of the CCA 2013.

[97] UK LEAs means:
'(a) the Commissioners for Her Majesty's Revenue and Customs;
(b) the Director of the Serious Fraud Office;
(c) the Director of Border Revenue;
(d) the Scottish Administration;
(e) a Northern Ireland department;
(f) any other person operating in England, Scotland, Northern Ireland or Wales charged with the duty of investigating or prosecuting offences (apart from a UK police force).' S.16 (1) of the CCA 2013.

[98] In addition, sch.3 (2) of the CCA 2013 deals with exchange of information.

government bodies lies with the head of the UK FIU.[99] Furthermore, the use of SARs by end users is confidential and subject to the terms of the Home Office Circular.[100]

Explicit Requirement for Storing SARs

It is crucial to note that the CCA 2013 explicitly requires that the NCA stores all SARs.[101] The FATF does not explicitly require this in its Recommendations, not even in the 2012 FATF's Recommendations. However, the Interpretative Note to FATF Recommendation 29 briefly refers to the storage of information held by the FIU, as analysed in Chap. 4. Even the EU Third Money Laundering Directive[102] does not explicitly require FIUs to store SARs. It is thus arguable that the UK requirements are superior to the FATF Recommendations and the EU Directive in this particular regard. In addition, the FLMLC 2002 in the UAE does not require the AMLSCU to store STRs, which it receives from reporting entities, as analysed in Chap. 5. However, the AMLSCU stores STRs on its database, but no legal requirement has been adopted, which provides for this.

Feedback on the SARs

Providing feedback is one of the most important tools for improving the quality of the SARs, which the reporting entities submit. In this context, feedback has two limbs, namely providing and receiving feedback.

---

[99] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 84.

[100] Home Office Circular 53/2005: 'Money laundering: the confidentiality and sensitivity of Suspicious Activity Report (SARs) and the identity of those who make them', available on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 27th October 2014)

[101] S.1 (5) of the CCA 2013, and even s.3 (1) of the SOCPA 2005, which is abolished now, required the SOCA to do so.

[102] (N 1185).

Providing Feedback

Feedback has to be provided to the reporting entities by the UK FIU. This feedback could be general or case-by-case based, as analysed in Chap. 4.[103] Very often general feedback is given to reporting entities, as opposed to rather specific feedback since, in practice, it is likely that the relevant law enforcement officers will contact the reporting entity before the end of the case or the trial and if this communication does not affect any investigation.[104] Nevertheless, in some cases the UK FIU provides specific feedback to the reporting entity about the SAR, which has been submitted.[105] For instance, any new reporting entity, which registers on SAR Online, receives from the UK FIU case-by-case feedback of its SARs 1 month and 6 months after registration.[106]

General feedback about SARs can be provided in various ways, for example through continuous feedback to the largest volume reporters of SARs,[107] the publication of case studies on SARs for training purposes and SOCA, now the NCA, alerts which warn reporting entities about existing threats on specific issues affecting their businesses.[108] In addition, general feedback can be given at conferences organised by the UK FIU for small and medium businesses, such as solicitor's firms and accountants where the importance of the SARs regime is stressed and vulnerabilities of their businesses are addressed in respect of ML and financial crime.[109] In 2011, the UK FIU arranged 50 conferences and events for reporting entities and 12 conferences and events for

[103] See also (n 502).

[104] Sabrina Fiona Preller (n 1161), 235.

[105] FAQs (n 1210).

[106] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 16.

[107] Ibid 44.

[108] Between October 2010 and the end of September 2012, the reporting entities submitted 1212 STRs as a direct result of SOCA alerts. These alerts increased their awareness about particular issues. Moreover, between October 2012 and the end of September 2013, they submitted 581 SARs as a direct result of SOCA alerts. See, 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 17, 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 18 and 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 15.

[109] Jayesh D'Souza (n 1192) 154.

regulators and national and foreign LEAs.[110] Furthermore, in 2013, the UK FIU attended more than 232 presentations, conferences and events, which were directed at stakeholders of the SARs regime, namely reporting entities and the LEAs.[111] The UK FIU also runs quarterly seminars for MLROs on the issues of reporting SARs and threats they face.[112] General feedback can also emanate from meetings of the "Vetted Group," which consists of representatives of reporting entities, LEAs and key policy departments. Hence, the Vetted Group is chaired by the UK FIU and meetings take place regularly to discuss sensitive issues on SARs. The objective of the Vetted Group meetings is to provide advice to the UK FIU on policy and disseminations to the reporting entities and LEAs.[113]

Receiving Feedback

Feedback is received from end users of the SARs every 6 months in the form of Twice Yearly Feedback Questionnaire (TYFQ). All end users receive this questionnaire from the UK FIU and this mechanism allows statistics to be generated and feedback to be received about their use of the SARs in the preceding 6 months.[114] In addition, the TYFQ asks end users to provide examples on how they used SARs. The results of the

[110] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 17.

[111] This comprised 94 events for reporting entities, 102 for LEAs and 36 supervisor/professional body/trade association visits. The numbers thus almost doubled compared to 2012, which saw 128 events. 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 9.

[112] Jayesh D'Souza (n 1192) 154.

[113] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 41.

For instance, in 2009, the Vettel Group reviewed the SARs submitted by the accountancy sector in order to produce material to assist the sector with improving the quality of their SARs. As a result, the UK FIU has published a bulletin, 'Suspicious Activity Reports (SARs)—Top Ten Tips for the Accountancy Sector 'in April 2011, available on the SOCA's website at: www.soca.gov.uk (last accessed on 20th November 2012)

[114] The end users of SARs are obliged to respond to the TYFQ pursuant to the criteria for direct access to the SARs on ELMER via MoneyWeb and ARENA (n 1239).

criterion 3(2) provides that:

'The organisation must submit comprehensive and timely Twice Yearly Feedback Questionnaires (TYFQs) and adequately detail their use of SARs.

The organisation must provide case studies outlining how a SAR(s) was used in a particular investigation and the assets recovered, if appropriate.'

TYFQ are contained in a summary document with a view to improving best practice between the reporting entities and the end users and to provide feedback to the UK FIU on the SARs regime at the operational level. Examples of how the use of SARs by end users are utilised by the UK FIU can be found in the published SARs annual report, which contains numerous case studies for training purposes that is if authorisation has been granted by the reporting entity and the end user and the case is not sub judice.[115]

Indeed, the main objective for providing feedback to the reporting entities is to increase the quality of the SARs, which are submitted to the UK FIU, since providing feedback assists the UK FIU with fulfilling its analytical function. In addition, the main objective of the TYFQ is to invite end users of the SARs to provide their knowledge/experience to the UK FIU on the operation of the SARs regime which thereby helps provides important feedback to the reporting entities.[116] Both limbs of feedback are crucial for the UK FIU's endeavor to develop and increase the efficiency of the SARs regime since each limb completes the other. This is unlike the UAE FIU, which does not provide feedback to the reporting entities, as critically analysed in Chap. 5 and confirmed in Chap. 6. \.

Additional Information and Exchange of Information

The UK FIU has direct and indirect access to additional financial, commercial, administrative and law enforcement information, for example HMRC's and the Driver Vehicle Licensing Authority's (DVLA)[117] databases. In addition, it can directly require additional information from the relevant reporting entity about a SAR, which has been submitted, especially in cases where the SARs involve consent requests.[118] The power

[115] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 22.

[116] Ibid 22 & 48.

[117] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 83.

[118] However, a court order is required in case the FIU requires additional information, but the additional information in this case does not directly relate to a specific activity/transaction contained in the SAR. Ibid.

to request additional information is crucial since it positively assists the UK FIU to discharge its analytical function. This is unlike the UAE FIU, which is not legally equipped with this power, as critically analysed in Chap. 5 and confirmed in Chap. 6. The UK FIU can also exchange information with national partners, for example LEAs and regulators and with foreign partners, for example foreign FIUs.[119]

SARs Regime Committee

This committee was located within the SOCA and is situated within the NCA in order to further develop the SARs regime. It includes representatives from government bodies, LEAs and the private sector, thereby ensuring that all decisions about the UK FIU are agreed by all stakeholders.[120] The committee evaluates the SARs regime and produces its annual report to the Home Office and Treasury Ministers. It published its annual report for the first time in 2007.[121] In 2009, the committee introduced its three-year strategy about the SARs regime and the following SARs annual reports have followed this strategy. The strategy focuses on the following four principal aims: (1) all reporting entities have to submit appropriate SARs, (2) use the information, which is being generated by the SARs, as much as possible to prevent and detect crime and to recover illegal assets,[122] (3) improve the technical capabilities and

[119] S.33 and s.34 of the SOCPA 2005.

[120] As of September 2013, the membership of the SARs Regime Committee was comprised of the SOCA Executive Director (the NCA Director) (Chair), the Association of Chief Police Officers, the British Bankers' Association, the FCA, HM Revenue and Customs, HM Treasury, the Home Office, the Institute of Chartered Accountants in England and Wales, the Law society of England and Wales, the Metropolitan Police Service, the National Terrorist Financial Investigation Unit (NTFIU), the Office for Security and Counter-Terrorism and the SOCA, now the NCA. From October 2012, the SOCA replaced by the NCA. See, 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) annex B.

[121] All of the annual reports were publically available on the SOCA's website at: www.soca.gov.uk and can now be found on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 15th December 2014)

[122] For the role, which the SOCA plays in confiscating the proceeds of crime and recovering assets, see Nicholas Ryder, *Money Laundering—An Endless Cycle?* (First Published, Routledge Cavendish 2012), 95–99.

experience of all SARs regime stakeholders, including the reporting entities and LEAs and (4) enhance the governance and transparency of the SARs regime.[123] Moreover, the aim and role of the UK FIU has to be considered when developing the SARs regime,[124] as recommended by Sir Stephen Lander.[125]

The SARs Annual Report

Generally, the SARs annual report comprises two main parts. The first part focuses on the performance of the SARs regime during the reporting year[126] and the second part sets out an action plan for the next year and spells out strategic aims. SARs annual reports generally explain key factors for increasing the effectiveness of the SARs regime. These include feedback methods provided to the reporting entities by the UK FIU, the results of TYFQ, case studies about submitted SARs, which have been provided in the TYFQ[127] and recently, also examples on how to exploit ARENA in practice.[128] SARs annual reports highlight negative practical aspects, for example, the SARs annual report 2010 indicated that a high number of unnecessary SARs had been submitted by some sectors; especially SARs containing consent requests, although these SARs appear did not in fact to fall under the POCA 2002 provisions. The report noted that the practice may have been because relevant reporting entities submitted SARs without applying appropriate CDD procedures or submitted consent requests as standard SAR.[129] The SARs annual report of 2011 therefore indicated that a number of SARs, which had been submitted by the law and accountancy sectors, were reviewed by the UK FIU and selected

[123] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 4.

[124] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 10.

[125] (N 1189).

[126] The reporting year means the period from October to September of the next year.

[127] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 23–28 and 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 22–28.

[128] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 37.

[129] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 14.

relevant practitioners in order to reduce these unnecessary SARs. The guidance, which had been provided to these sectors were reviewed and a structured reporting model in relation to consent requests was developed.[130] In 2011, The UK FIU conducted a review of SARs submitted by a number of firms in the legal sector and provided specific feedback to the legal sector. The feedback includes good practice guidance and tips on how to improve the quality of SARs submitted by firms in the legal sector.[131]

Key Statistics on SARs

The SARs annual report further includes key statistics about SARs. Figure 9.1 below shows the percentage of SARs, which were submitted by the reporting sectors, for the reporting years October 2007 to September 2010.

The aforementioned chart clearly shows that the banking sector has submitted the majority of the SARs[132] over this period, namely 78.31 % of all SARs, while just 21.69 % of all SARs were submitted by other

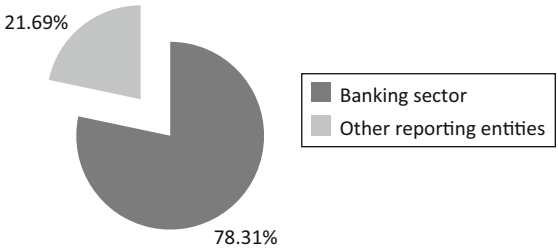

Fig. 9.1 SARs by sector Oct. 2007–Sep. 2010

[130] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 5–6.

[131] Ibid 6.

[132] SARs in this regard are not confined to ML, but cover other crimes, such as TF, fraud and other financial crime.

entities, such as accountants, gambling[133] and Money Services Businesses (MSBs).[134] At the same time, the top 10 reporting entities consisted of 8 banks, 1 money transmitter and 1 bookmaker which have submitted 56.9 % of all SARs over this period. More than half, namely 52 %, of all SARs were submitted by four banks, which hold 83 % of all current accounts in the UK.[135] Fig. 9.1 highlights how important the banking sector is for the SARs regime, as it is more vulnerable than any other sector when it comes to ML activities/transactions and financial crime. This is attributable to responses to regulatory actions within the global financial sector.[136] Such situation is same as the situation in the UAE, as discussed in Chap. 6.[137]

The banking sector has remained the largest reporting sector in relation to submitting SARs in 2011, 2012 and 2013. In 2011, banks situated in the UK submitted 77.70 % of all SARs, whilst the second largest reporting sector was MSBs, which submitted 9.46 % of all SARs during the same period, as shown in Fig. 9.2 below.[138]

Whilst in 2012, banks submitted 78.24 % of all SARs and as in previous year, MSBs were the second largest reporting sector, which submitted 8.40 % of all SARs, as shown in Fig. 9.3 below.[139]

The situation has remained the same in 2013. Banks submitted 79.40 % of all SARs and MSBs were the second largest reporting sector, which submitted 6.74 % of all SARs, as shown in Fig. 9.4 below.[140]

---

[133] It should be noted that gambling is an illegal activity in the UAE.

[134] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 13.
MSBs includes money transmitters, bureaux de change and cheque cashers, 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 157.

[135] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 14. The report did not mention the name of the four banks.

[136] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 7.

[137] See charts 2, 3 and 4 in Chap. 6.

[138] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 14.

[139] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 14.

[140] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 8.

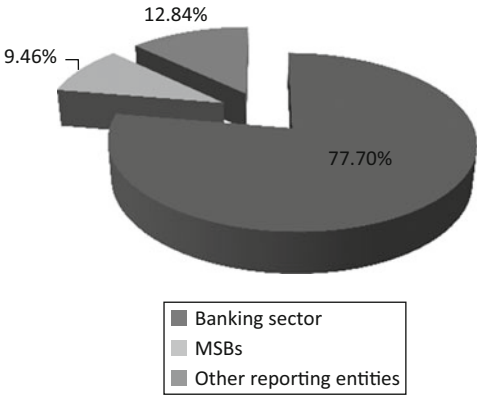

Fig. 9.2 SARs by sector Oct. 2010–Sep. 2011

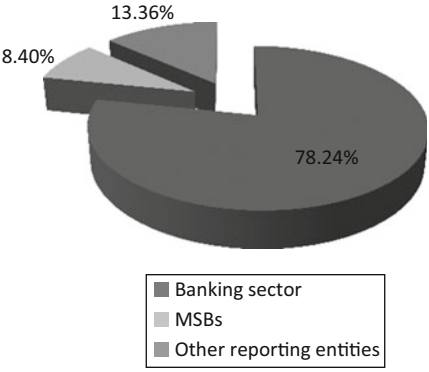

Fig. 9.3 SARs by sector Oct. 2011–Sep. 2012

The top 10 reporting entities in 2011 consisted of 8 banks and 2 MSBs.[141] The number of SARs submitted by the gambling sector declined to 0.39 % of all submitted SARs in 2011 and to 0.34 % of all submitted SARs in 2012[142] and 2013,[143] compared to 2.38 %

[141] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 14.
[142] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 14.
[143] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 8.

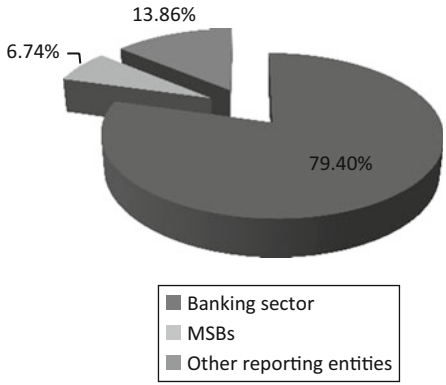

Fig. 9.4 SARs by sector Oct. 2012–Sep. 2013

of all submitted SARs in the reporting years from 2007 to 2010.[144] In fact, high numbers of submitted SARs may indicate that the relevant reporting entity/sector is aware about the reporting requirements and has adopted an appropriate internal system to detect suspicious activities/transactions. However, it could also indicate that the relevant entity/sector adopts a defensive approach,[145] just to avoid criminal liability under the POCA 2002 and other relevant Acts, and that appropriate CDD procedures were not followed before submission of the SARs, whilst low numbers of submitted SARs may suggest that the relevant entity/sector is unaware about the reporting requirements.[146] The 2011 SARs annual report indicated that the UK FIU will explore the reason for the decline in submitted SARs from the gambling sector in 2011[147] in the following annual report; nevertheless, the 2012 SARs annual report did not explore the reason(s) for such a decline in the gambling sector.

[144] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 14.
[145] Nicholas Ryder (n 1272) 93.
[146] 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 14.
[147] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 14.

Table 9.1 Statistics on SARs between 2009 and 2013

Key statistics	Reporting year (2009)	Reporting year (2010)	Reporting year (2011)	Reporting year (2012)	Reporting year (2013)
Total SARs submitted by the reporting entities	228,834	240,582	247,601	278,665	316,527
Total consent requests	13,618	14,334	13,662	12,915	14,103
Percentage submitted electronically	96 %	97 %	98 %	98.87 %	99.25 %
Percentage submitted manually (by paper)	4 %	3 %	2 %	1.13 %	0.75 %
Breaches of SARs confidentiality	2	0	1	0	2

Table 9.1 below provides statistics about submitted SARs between 2009 and 2013 from different perspectives.[148]

The table above shows that the number of SARs submitted to the UK FIU has continued to increase over this period,[149] especially 2013 witnessed an increase of almost 38,000 SARs from the previous year. This reflects that certain reporting entities/sectors follow the requirements of the SARs regime, have adopted appropriate internal procedures to detect suspicious transactions/activities and generally pay a great deal attention to the SARs regime, even though the number of SARs submitted by a number of other entities, for example the gambling sector declined in 2011 and 2012, as mentioned above. The increase could also be attributed to the increase in the number of reporting entities, as there were

[148] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 10, 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240) 11, 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 12 and 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 6.

[149] The SARs annual reports contain SARs, including consent requests, by industry sector as appendix.

5228 new SARs online registrations from October 2010 to September 2012.[150] The year 2013 alone saw 2677 new SARs online registrations.[151]

Decrease in the Number of Consent Requests

In addition, the number of total consent requests decreased to 13,662 in 2011[152] and to 12,915 in 2012,[153] compared to 14,334 in 2010. This decline could be attributed to the UK FIU's endeavor to reduce unnecessary consent requests, as discussed above. Hence, it is arguable that the UK FIU has succeeded in relation to this aspect. More importantly, it is arguable that this decrease is attributed to the decision in *Shah v HSBC Private Bank (UK) Ltd.*,[154] analysed in the following section. However, the number of total consent requests increased to 14,103 in 2013, but this is attributable to the increase in the number of reporting entities, as mentioned above.[155]

The table further shows that the percentage of electronically submitted SARs[156] has increased from 96 % in 2009 to more than 99 % in 2013 due to the advantages of this method, as mentioned above.

---

[150] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 12 & 13.

[151] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 7.

[152] In 2011, the UK FIU refused 2197 (16.08 %) consents requests within 7 days and 164 (7.46 %) consents requests, which had been refused were subsequently granted during the moratorium period when it appeared that the relevant investigating agencies were unlikely to obtain restraint orders.

'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 20.

[153] In 2012, the UK FIU refused 1229 (9.05 %) consents requests within 7 days, whilst 169 (13.75 %) consents requests, which had been initially refused, were subsequently granted during the moratorium period when it appeared that the relevant investigating agencies were unlikely to obtain restraint orders.

'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 30.

[154] [2010] EWCA Civ 31.

[155] Where the UK FIU refused 1387 (9.08 %) consents requests within 7 days, whilst 266 (19.02 %) consents requests, which had been initially refused, were subsequently granted during the moratorium period when it appeared that the relevant investigating agencies were unlikely to obtain restraint orders.

'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 19.

[156] This includes all electronic methods, such as SAR Online and encrypted email.

Main Observations Regarding SARs Annual Report

Two main observations can be made in relation to the SARs annual report. Firstly, it should be noted that the annual report is completely different from the NCA annual report and plan which the CCA 2013 requires.[157] Secondly and more importantly, the SARs annual report contains important statistics about SARs on ML in detail, which have been submitted by the reporting entities.[158] This is because the POCA 2002 adopts an "all crimes" basis to ML and predicate offences to ML are not subject to a closed list. Hence, it is not necessary under the legislation to know what the predicate offence is in order to prosecute for ML, although this appears preferable.[159] Moreover, the SARs annual report contains information about the exchange information and information requests from foreign FIUs; nevertheless, it does not include statistics about the number of SARs out of all SARS received, which the UK FIU has disseminated to LEAs and other government bodies. The annual report also does not indicate the number of SARs out of all SARS received, which the UK FIU after its analysis decided to delete due to there being no suspected/known ML or financial crime. In addition, the SARs annual report does not state how many SARs have resulted in a conviction. Indeed, these statistics are crucial to gauge the effectiveness of the SARs regime, to assess the analytical function of the UK FIU and to appreciate the volume of crime, which takes place through reporting entities.

---

[157] S.4 (3) and Sch.2 (2) para 7 of the CCA 2013 require the NCA at the beginning of each financial year to issue a plan setting out how it intends to exercise its functions during that year and to issue a report at the end of each financial year about the exercise of its functions during that year. All these annual reports and plans were available on the SOCA's website at: www.soca.gov.uk and can now be found on the NCA's website at: www.nationalcrimeagency.gov.uk (accessed on 15th December 2014)

[158] Annexes C and D of the 'Suspicious Activity Reports Regime, Annual Report 2010' (n 1240), 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165), 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) and 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187).

Moreover, the SARs annual reports contain detailed statistics, by industry sector, about SARs on TF.

[159] As analysed in Chap. 7. This is unlike the UAE's legislation, which adopts a limited list of predicate offences to ML, as analysed in Chap. 5.

The SARs regime committee recently drew great attention to the 2012 FATF Recommendations, especially to Recommendation 29,[160] which deals with the core functions and powers of the FIU within a SARs regime at the national and international levels, as such revision forms the basis for future FATF MERs for countries in terms of their compliance with the revised Recommendations.[161] The UK FIU was rated as "lacking compliance" with the 2003 FATF's Recommendation 26 in relation to the requirements of the FIU.[162] However, after having evaluated its functions and powers, it is arguable that the current UK FIU is not only compliant with the 2012 FATF Recommendation 29, but indeed exceeds the FATF Recommendations.

Indeed, the SARs regime committee plays a vital role in enhancing and developing the SARs regime and the functions of the UK FIU in the regime. However, in the UAE, there is no STRs regime committee, which regularly evaluates the effectiveness of the STRs regime and the functions of the AMLSCU to keep abreast of developments in ML patterns. This hampers the evolution of the STRs regime and the functions of the AMLSCU. It is essential for the UAE AML system to have a STRs regime committee, which should be comprised of members from the public and private sector. The committee should regularly evaluate the STRs regime and review the strategies and priorities of the AMLSCU in dealing with STRs. The following chapter evaluates such a committee mechanism, discusses who should be the members and the responsibilities, which such a committee should discharge.

After analysing the UK FIU's role in the SARs regime and its achievements, along with its constructive relationship with the reporting entities and the LEAs, it is important to critically evaluate the consent regime and more importantly the practical problems associated with submitting STRs when there is only a subjective belief, which can threaten the entire success of the SARs regime.

---

[160] FATF Recommendation 29 has been analysed in Chap. 4.

[161] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 35.

[162] 'The United Kingdom Third Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' (n 1155) 88.

The Consent Regime and Practical Problems

Waiting to receive consent from the UK FIU

The UK FIU has up to 40 days to consider whether or not to grant consent to proceed with a transaction, which consists of a notice period and a moratorium period, as illustrated in the previous chapter.[163] The problem in the case of the reporter, for example a bank, is that the customer's transaction has to be suspended until actual consent or deemed consent is received from the UK FIU. At the same time, the relevant customer could be harmed from the suspension (freezing) of his transaction, notably if the consent request is rejected within the 7 working days notice period and the banker wait for the entire 31 day moratorium period to receive consent. However, the UK FIU is aware of this issue and tries to deal with the SARs, which contain consent requests, as soon as possible. Statistics show that during 2011, the UK FIU has turned around[164] 41 % of all consent requests on the day of receipt or the next working day. In addition, it has turned around the rest of the consent requests by the third day of receipt.[165] Thus, the average turnaround time was 2.5 days in 2011, compared to 2.8 days in 2010.[166] However, the average has slightly increased to 3.1 days in 2012.[167] The SARs regime committee attributed the increase to staff changes in the UK FIU, which have now been resolved.[168] Similarly, the average has slightly increased to 3.5 days in 2013 and the SARs regime committee attributed the increase to two factors.[169] Firstly, the increase in volume and quality of the SARs. Secondly, a great number of SARs cases were allocated to LEAs for their consultation.[170]

[163] See Chap. 8 (n 1122).
[164] The UK FIU consults the relevant LEA before granting or refusing consent.
[165] 'Suspicious Activity Reports Regime, Annual Report 2011' (n 1165) 20.
[166] Ibid.
[167] 'Suspicious Activity Reports Regime, Annual Report 2012' (n 1165) 29.
[168] Ibid.
[169] 'Suspicious Activity Reports Regime, Annual Report 2013' (n 1187) 20.
[170] Ibid.

The UK FIU has to take into account these issues in order to overcome the dilemma

Furthermore, in order to mitigate the consequences of the aforementioned dilemma, the UK FIU must not refuse consent without reasonable reasons. It must review its refusal decision during the moratorium period and should grant consent when there are no good reasons to refuse consent,[171] although the POCA 2002, the SOCPA 2005 or the CCA 2013 does not provide for this. In the case of *UMBS Online Ltd. v SOCA*,[172] Ward L.J. in the Civil Division of the Court of Appeal stated that:

> I am prepared to accept that SOCA [the UK FIU] should not withhold consent without good reason. This is no more than good administration … SOCA is an immensely powerful statutory body whose decisions have the consequence of imperilling private and business banking activity based, initially at least, on no more than a reported suspicion of money laundering. If the proper balance is to be struck between undue interference with personal liberties and the need constantly to fight crime, then the least that can be demanded of SOCA is that they do not withhold consent without good reason.[173]

Ward L.J. added further that:

> Since it is accepted by SOCA that they must keep the matter under review, they must give the bank consent when there is no longer any good reason for withholding it… The bank has done its duty by reporting its suspicion and now it may simply sit on its hands and take care not to operate the account until the expiry of the moratorium. It is not directly affected but its customer is and the customers of the customer are. They are entitled to ask SOCA to review the matter and SOCA are obliged to do so.[174]

Most importantly, the Home Office issued a Circular which provides guidance and criteria, which have to be taken into account when decid-

[171] Arun Srivastava, 'UK Part II: UK law and practice' in Mark Simpson, Nicole Smith and Arun Srivastava (eds), *International Guide to Money Laundering Law and Practice* (Third Edition, Bloomsbury Professional 2010), 27 at 44.

[172] [2007] EWCA Civ 406.

[173] Ibid para 36.

[174] Ibid para 52.

ing whether or not to grant or refuse consent.[175] The 'Consent Policy' is attached to the circular and must be followed by the LEAs since the UK FIU consults the relevant LEA before granting or refusing consent. The 'Consent Policy' emphasises proportionality, which means that interests are balanced when considering whether or not to grant or refuse consent. The balance includes "the public interest of the impact on crime… the private rights of those involved in the activity which is subject to the consent request and those of the reporter."[176] In other words, if the SAR, which contains a consent request, does not in reality involve ML, a decision to refuse consent will cause serious consequences to the individuals, for example significant financial loss.[177]

In practice, it is arguable that the serious consequences of the consent regime are mitigated because of three reasons mentioned above, namely (1) the UK FIU deals with consent requests as soon as possible, (2) the refusal of consent must be reasonable and the UK FIU must review its refusal decision during the moratorium period and (3) the Home Office's Circular along with its 'Public Policy' provides additional guidance.

The risk of submitting SARs on mere suspicion

However, legal and practical problems arise not only with the consent regime, but also with the SARs regime as a whole. The risk is because a subjective basis, namely suspicion or knowledge, is enough for submitting all SARs on ML, including authorised disclosure and protected disclosure.[178] There is no harm where the SAR is based on actual knowledge, but vagueness arises since mere suspicion is enough for submitting a SAR and no legal requirement is contained in the POCA 2002, which requires that the suspicion must be firmly justified. On the other hand, if the banker, a nominated officer, has just a suspicion that the transaction involves ML, he is

[175] Circular 029/2008, 'Proceeds of Crime Act 2002: obligations to report money laundering—the consent regime', which released on 5th December 2005, available on the Home Office website at: www.homeoffice.gov.uk (accessed on 28th November 2014).

[176] See 'Consent Policy' which is attached to the Circular 029/2008, ibid.

[177] Ibid.

[178] Where an authorised disclosure is based on a subjective basis, the first two offences of failing to report are based on either a subjective basis or objective basis and the third offence of failing to report is based on a subjective basis, as critically analysed in the previous chapter.

legally obliged to submit his suspicion on a SAR form to the NCA. Serious consequences can flow from this, especially for the customer's rights and reputation or even the bank if it was the reporter. The case of *Squirrell Ltd. v National Westminster Bank plc*[179] illustrates this situation. *Squirrell Ltd.* was established in 2002 under another name and traded in mobile phones and other goods. It opened an account with the National Westminster Bank plc. In March 2005, the bank froze the account. Mr. Khan, who was the managing director of the firm, did not receive any explanation or notification from the bank. The managing director sought to discuss the reason for this with employees at the bank, but did not manage to get any information from them, instead was prevented from accessing the company's account and did not receive any notification. As no funds could be accessed, the company could not instruct a solicitor, but instead the managing director himself had to act as counsel for the company. The case demonstrates the serious impact, which SARs can have upon a customer of a bank, particularly since a customer who has not got any evidence, which has been forwarded to establish a *prima facie* case, has also not been charged with any particular crime. Laddie J. opined in *Squirrell*'s[180] case that:

> … [I] should say that I have some sympathy for parties in Squirrell's position. It is not proved or indeed alleged that it or any of its associates has committed any offence. It, like me, has been shown no evidence raising even a prima facie case that it or any of its associates has done anything wrong. For all I know it may be entirely innocent of any wrongdoing.[181]

The change in the judicial interpretation of the term "suspicion"

The notion of suspicion has been analysed in Chap. 7, the Court of Appeal in the case of *Da Silva*[182] interpreted this notion and the Court of Appeal in *K Ltd.*[183] provided that the POCA 2002 does not require that a suspicion has to be based on reasonable grounds. Nevertheless, recently,

[179] [2005] EWHC 664 (Ch).

[180] Ibid.

[181] Ibid para 7.

[182] [2006] EWCA Crim 1654. See Chap. 7.

[183] [2006] EWCA Civ 1039. See of Chap. 7.

the Court of Appeal in the case of *Shah v HSBC Private Bank (UK) Ltd.*[184] differently interpreted the notion of suspicion. In summary the facts of the case are that the defendant bank suspected that the claimant was a money launderer and accordingly submitted a SAR[185] to the SOCA, now the NCA, requesting consent to proceed with the claimant's instructions in relation to a transfer of funds out of accounts he held with the bank. SOCA granted consent and the bank carried out the claimant's transfer request. The claimant alleged that he lost $331 million[186] in interest as a result of the SAR, which the defendant bank had made. Moreover, he asked the bank to prove the reason for its suspicion and argued that the suspicion was irrational. However, he did not argue that the bank made the SAR in bad faith. The judge stated that the only way to challenge these cases is by alleging bad faith; accordingly he rejected the claimant's allegations. In contrast, Longmore L.J. in the Civil Division of the Court of Appeal explained that:

> I cannot see why… Mr Shah cannot require the bank to prove its case that it had the relevant suspicion and be entitled to pursue the case to trial so that the bank can make good its contention in this respect.[187]

The solicitor of the bank provided details of the procedures used to deal with suspicions and which affirmed that a suspicion existed via a witness statement, although the Court of Appeal considered the witness statement insufficient and stated that:

> No reason why the bank should not be required to prove the important fact of suspicion in the ordinary way at trial by first making relevant disclosure and then calling either primary or secondary evidence from relevant witnesses.[188]

---

[184] (N 1304).

[185] Under s.338 of the POCA 2002 (authorised disclosure), see Chap. 8.

[186] Which is about £206 million.

[187] (N 1304) para 22.

[188] Ibid para 25.

According to the Court of Appeal, the relevant person/customer has the right to ask for the reasons behind the suspicion and the defendant bank must divulge the basis and nature of its suspicion. In other words, if the suspicion was not based on reasonable grounds or the defendant failed to prove the grounds, the SAR will be deemed illegal.[189] Furthermore, if the reporter/bank did not justify its suspicion, the relevant customer could claim that the bank breached its contract and claim damages for any financial loss.[190]

Consequences of the change and a possible solution

It is not easy to analyse and justify the dramatic change in the interpretation of the notion of suspicion from the perspective of Court of Appeal. The Court's interpretation exceeds what is required for a suspicion to be made out. There is no legal requirement contained in the POCA 2002 that a suspicion has to be based on reasonable grounds. Furthermore, in relation to some SARs, the POCA 2002 provides alternative conditions for the basis of SARs, such as in the case of the first two offences of failing to report,[191] which are based on either a subjective or objective basis. Thus, if a mere suspicion has to be based on reasonable grounds, as required by the Court of Appeal in the case of *Shah*,[192] an objective basis rendered redundant. Consequently, the court's interpretation of the notion of suspicion may be incompatible with the provisions of the Act. The significant result of interpreting "suspicion" by the Court of Appeal in the case of *Shah*[193] is that the number of submitted SARs will indeed largely decrease in the near future.[194] This is evidenced by statistics, in Table 9.1 above, which highlight that the SARs that contained consent requests, submitted by the reporting entities, has decreased in the years 2011 and 2012,[195] compared to 2010. The reporting entities are aware

[189] Paul Marshall, 'Does Shah v HSBC Private Bank Ltd. make the anti-money laundering consent regime unworkable?' (2010) 25 (5) Journal of International Banking and Financial Law 287, 288.

[190] Keith Stanton, 'Money laundering: a limited remedy for clients' (2010) 26 (1) Professional Negligence 56, 58.

[191] S.330 and s.331 of the POCA 2002, as critically analysed in Chap. 8.

[192] (N 1304).

[193] Ibid.

[194] Paul Marshall (n 1339) 287.

[195] However, the number of total SARs with consent requests increased in 2013, but this is attributable to the increase in the number of reporting entities.

that the Court of Appeal in the case of *Shah*[196] requires a suspicion to be based on grounds or facts.

In reality, the notion of suspicion causes a number of dilemmas when it comes to the SARs on ML, especially for the customer's financial affairs and reputation, even if his transaction is not suspended, but a SAR is only submitted which informs that his account is suspected to be involved in ML, as clearly this could harm his reputation seriously, especially if the customer is a famous firm or publically known. On the other hand, the situation could also badly affect the reporter's reputation, notably if the reporter is a bank. Financial institutions, including banks, are legally obliged to submit a SAR once they have a mere suspicion that a transaction could be involved in ML, as they will otherwise commit the crime of failing to report, as critically analysed in the previous chapter.[197] Accordingly, if it becomes publically known that a specific bank inconveniences their customers; it will lose its customers or at least will not attract further customers as a result of its bad reputation in dealing with its customers. These practical dilemmas may necessitate that "suspicion" is removed from the Act as a basis for SARs and there are two main reasons support such argument.

Firstly, the current practice may allow the submission of SARs to the NCA for revenge purposes. For example, if there is a quarrel between a banker and one of his customers, the banker can submit a SAR on the basis of a merely suspecting that the customer's account is involved in ML activity. Although the relevant customer can challenge the allegation of bad faith, it is difficult to prove bad faith since the Act requires the banker to submit a SAR on a mere suspicion.

Secondly, as mentioned above, the first two offences of failing to report are based on either subjective or objective, which means that the prosecution must prove one of three alternative elements, namely (1) knowledge, (2) suspicion and (3) reasonable grounds for knowledge or suspicion. As a result, the reasonable grounds element in this case seems a redundant alternative since this element is harder to prove than suspicion and

[196] (N 1304).

[197] S.330, s.331 and s.332 of the POCA 2002. See Chap. 8.

accordingly the prosecution prefers the suspicion element in order to avoid having to establish a more onerous case.[198]

Being able to submit a SAR on a mere suspicion may also be challenged by virtue of Article 8 of the 1950 European Convention on Human Rights (ECHR), as incorporated by the Human Rights Act 1998,[199] particularly if the divulgement has a serious impact on a person, as discussed above. Hence, for the aforementioned arguments, the basis for SARs should either be actual knowledge[200] or objective reasonable grounds for knowledge or suspicion in order to ensure fairness.[201]

Conclusion

The UK FIU law enforcement model within the NCA has a great number of powers under the SARs regime. The analytical function, including the three types, namely operational, tactical and strategic analysis are all carried out and it is also, in practice, operationally independent from the NCA. The UK model also pays great attention to both limbs required for a feedback loop, so that information is not only provided, but also received and this improves the quality of SARs and the SARs regime in

[198] Rudi Fortson, 'Money Laundering Offences under POCA 2002' in William Blair and Richard Brent (eds), *Banks and Financial crime*: *the International Law of Tainted Money* (Oxford University Press 2008), 155 at 170.

[199] Article 8 of sch.1 of the Human Rights Act 1998 provides that:

'1- Everyone has the right to respect for his private and family life, his home and his correspondence.

2- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. The content of this Article is same as Article 8 of the 1950 ECHR.

It seems that there is incompatibility between interference under Article 8 (2) (the minimum necessary degree to achieve the legitimate aim pursued) and suspicion as a basis for SARs and it may well be that the legitimate goal pursued, mentioned in Article 8 (2), is exceeded in this context which is counteracting ML. For additional detail on such issue, see Robert Stokes, 'The banker's duty of confidentiality, money laundering and the Human Rights Act' [2007 Aug] Journal of Business Law 502. See also Clive Harfield (n 1157) 753 & 754.

[200] For example, in the case where the customer explicitly confessed, in front of the banker, that the amount he received in his account is a result of drug trafficking.

[201] *R v Saik* [2006] UKHL 18.

general. At the same time, LEAs (end users of the SARs) are assisted with the investigation of SARs by the ELMER and ARENA databases. The DISCOVER system also assists the FIU's staff in enhancing their knowledge about crime.

In addition, it is arguable that the UK's SARs requirements are superior to the FATF Recommendations since the CCA 2013 explicitly requires that the NCA stores all SARs, which have been submitted by the reporting entities. The FATF Recommendations do not explicitly require FIUs to store STRs. Indeed, the requirement of storing STRs by FIUs improves the analytical function. The function of the UK FIU model achieves a great number of successes and appears to be effective in the SARs regime and in counteracting ML in general. However, the FLMLC 2002 in the UAE does not explicitly require the storage of all STRs. Moreover, unlike the successful UK FIU model, the UAE FIU model appears to be not as effective when it comes to dealing with STRs.

The SARs regime committee plays a vital role in developing the SARs regime and the functions of the UK FIU. It is also responsible for issuing annual reports and statistics about SARs. The existence of such committee is essential for developing the SARs regime since such a committee is composed of representatives from the public and private sector, who can work together with one aim, namely to detect SARs. On the other hand, in the UAE, there is no such committee.

However, there are two main problems with the UK's SARs regime. Firstly, the SARs annual report contains fundamental statistics about submitted SARs on ML, but it does not include statistics about the number of SARs out of all SARS received, which the UK FIU has disseminated to LEAs and other government bodies. The annual report also does not indicate the number of SARs out of all SARS received, which the UK FIU after its analysis decided to delete due to there being no suspected/known ML or financial crime. In addition, it is not stated how many SARs have resulted in a conviction. Such statistics are indeed essential since they provide a realistic assessment about the effectiveness of the SARs requirements imposed on the reporting entities on one hand, and the efficiency of the UK FIU, especially its analytical function, in dealing with the SARs on the other hand. The aforementioned elements should be included in the following SARs annual reports since such statistics are

crucial to gauge the effectiveness of the SARs regime and to appreciate the volume of crime taking place amongst reporting entities.

Secondly, the basis for submitting SARs, especially on a mere suspicion basis, raises a number of practical and legal problems. The decision of the Court of Appeal in the case of *Shah*[202] emphasises problems and has caused confusion about the notion of suspicion. Serious consequences can flow when a SAR is submitted to the NCA on a mere suspicion, especially for the customer's rights and reputation. As discloser, the bank may also gain a bad reputation and become known for annoying its customers by suspending their transactions/activities without reasonable justifications. The bank may even lose its customers or not attract new ones. Hence, in order to overcome such a dilemma, the basis of SARs should be on an objective basis, namely reasonable grounds for knowledge or suspicion and subjective basis, namely just actual knowledge. The mere "suspicion" must be removed from the basis of SARs since it is a broad term and can be used for revenge purposes. The following and last chapter deals with the recommendations and conclusion of this book.

[202] (N 1304).

10

Recommendations and Conclusion

Introduction

The analysis and critical evaluation in the previous chapters of this book have been undertaken with a view to proposing the optimal model for the UAE FIU in counteracting ML. The recommendations describe the optimal model for the UAE FIU, so that STRs can be dealt with more effectively and provide the key factors, which ensure the success of the proposed FIU model.

This chapter is therefore divided into nine parts. The first eight parts comprise eight categories of recommendations, which spell out an optimal model for the UAE FIU, both in terms of its core and non-core functions in counteracting ML. The last part provides the conclusion of this book. The recommendations are aimed at ensuring that (1) in practice, STRs are dealt with successfully and effectively, (2) the quality of submitted STRs to the AMLSCU is increased and (3) relevant international standards are adhered to. Indeed, a great number of these recommendations are derived from the empirical investigation, as detailed in Chap. 6, especially since no data or information exists about the role which the

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6_10

AMLSCU plays in fighting ML. In addition, these recommendations consider the positive aspects of the UK FIU law enforcement model, especially (1) its efficiency when dealing with SARs, (2) how to increase the quality of SARs received from the reporting entities and (3) the constructive relationship with the LEAs to successfully implement the SARs regime. The recommendations also take into account the vital role of the UK SARs Regime Committee to develop the SARs regime and the functions of the UK FIU within the regime.

Prior to thoroughly examining these recommendations, it is crucial to stress that a great number of the recommendations have been influenced by the UK FIU system and the UK SARs regime. However, the proposed recommendations have been adapted in a way, which does not conflict with the UAE's legal system to ensure that the recommendations are also feasible. These recommendations are mainly focused on the proposed UAE FIU model and STRs requirements. The recommendations also address the UAE FIU's organisational structure, its operational independence and accountability and its relationship with the reporting entities and the end users of the STRs, namely LEAs and the prosecution.

The Optimal Model for the UAE FIU

The Four Options

There are four options[1] to set up an optimal model for the AMLSCU in counteracting ML. Each model, along with its chances of success or failure, is examined below.

The Option of Retaining the Current Model (administrative model)

In the light of the current deficiencies and disadvantages of the AMLSCU in counteracting ML, it is difficult to retain the current model of the AMLSCU with its current situation. The current functions of the

[1] The four famous FIU models in the world are critically analysed in Chap. 4.

AMLSCU, along with deficiencies therein, have been critically evaluated in Chaps. 5 and 6. There is no harm in briefly recalling the following main deficiencies of the AMLSCU, which cause ambiguity, namely (1) its operational independence from the Central Bank, (2) its role in sufficiently analysing STRs on ML, (3) its human resources and their qualifications and skills in dealing with STRs received from the reporting entities, (4) its role in providing feedback to the reporting entities and increasing the quality of the STRs received from them, (5) its relationship with LEAs and (6) the absence of a strategic analysis[2] in order to formulate a strengthened strategy for its future work.

All of the aforementioned deficiencies, and others, are combined with the absence, or unclearness, of legal mechanisms[3] that should provide legal ground for its functions and authority in dealing with the STRs, the reporting entities and the LEAs. The likelihood of retaining the current model of the AMLSCU is low given its relative lack of success and non-compliance with FATF Recommendations.

The Option of Adopting the UK FIU Model (law enforcement model)

The Adoption of the Entire UK FIU Model

The previous chapter has evaluated the UK FIU law enforcement model as an innovative unit and has analysed its success in dealing with SARs, its vital role in increasing the quality of SARs received from the reporting entities and its constructive relationship with the reporting entities and the LEAs with a view to achieving a successful implementation of the SARs regime on ML. Such success would support the adoption of the same model for the AMLSCU in the UAE. However, it is not easy to adopt the UK FIU model entirely due to a one particular problem. The adoption of the entire UK FIU model would firstly require that a new national agency is established in the UAE, comparable to the SOCA, now

[2] The term "strategic analysis" has been analysed in Chap. 4.

[3] These deficiencies and the lack of legal mechanisms have been critically evaluated throughout Chaps. 5 and 6.

the NCA, in the UK, to deal with serious and organised crime, which threatens national security and areas, such as human trafficking, child exploitation and people smuggling. The AMLSCU would then have to be merged within such a national agency. It will be difficult to establish this agency within the UAE for two main reasons, as follows;

1) The establishment of such a new agency will cost the UAE government.
2) When considering the feasibility of establishing such a national agency and despite there being no statistics about serious and organised crime, these are not very common crimes in the UAE and therefore do not constitute a source of threat to UAE's national security or the financial system. As a result, there is no urgent need to establish such an agency.

Hence, the UK FIU model, as an innovative model, has emerged as a result of the own UK's circumstances and conditions. This does not necessarily mean that such a model will achieve the same success in another country, since the form of a FIU depends on the particular conditions and circumstances of individual countries, as mentioned in Chap. 4. Furthermore, there is no one FIU standard model suitable for all countries.[4] Nevertheless, there are a number of positive aspects and novel mechanisms contained in the UK FIU and the UK SARs regime and these have been taken into account when proposing the optimal model for the UAE FIU.

The Adoption of the Law Enforcement Model

There is another option of adopting the law enforcement model for the AMLSCU, namely within the police system of the UAE. One could argue that there is no need to establish a new agency since the police system already exists. Merging the AMLSCU within the police system does, however, produce a dilemma. As mentioned in Chap. 6,[5] in addition

[4] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Second Edition and Supplement on Special Recommendation IX, 2006 The World Bank), VII–18.

[5] See (n 742) of Chap. 6.

to the Federal Police in the UAE which is embodied in the Ministry of Interior, a number of cities have their own local police departments. Accordingly, if the AMLSCU is merged with the Ministry of Interior, this means that the AMLSCU will not receive STRs from the reporting entities which are located in Dubai, since it has its own police system and it is independent from the Ministry of Interior. Alternatively, more than one FIU, with its own organisational structure, in the UAE needs to be established to accommodate all police systems, which conflicts with FATF Recommendation 29 since the Recommendation requires that there is only one national agency, which deals with STRs.

As a result, it is not easy to adopt the entire UK FIU law enforcement model for the AMLSCU or the law enforcement model in general due to the UAE's circumstances and conditions which are different from the UK, especially when considered in light of the special nature of its police system.

The Option of Adopting Judicial Model

This option means that the AMLSCU will be within the UAE's judicial system, namely within the Prosecutor's Office. The main advantage of such a model, if adopted, is that the AMLSCU will enjoy a high level of independence, in contrast to the current administrative model. In addition, the AMLSCU would investigate and prosecute all STRs received from the reporting entities since it will have such powers. This, in turn, means that there is no need for the AMLSCU to transmit STRs, after analysing, to the LEAs or prosecution since it has the powers to take the proper action(s), and thereby saving time and take the decision(s)/action(s) promptly. Nevertheless, there are three main obstacles that are an impediment to adopting such a model for the AMLSCU.

Firstly, as mentioned in Chap. 4, such a model could be suitable for countries which have a small number of financial institutions. There are a great number of financial institutions, including banks,[6] within the UAE, which means a large number of STRs submitted by them annually. Such

[6] According to the 2010 statistics, there are 55 banks in the UAE. See Chap. 6.

In addition, the number of banks, in the UAE, in detail is available on the Central Bank website at: www.centralbank.ae (accessed on 11th April 2015).

a model will not be able to cope with a large number of STRs from the reporting entities.[7]

Secondly, this model is the least popular model,[8] which means that the AMLSCU, if it adopted such a model, will face difficulties when it comes to exchanging information with foreign FIUs, particularly because most foreign FIUs have not adopted this judicial model. Undoubtedly, co-operation between FIUs at international level is a vital mechanism in detecting and preventing ML. Therefore, there is a risk that if the AMLSCU adopted such model this could result in it not fulfilling the relevant FATF Recommendations in relation to international co-operation.[9]

Lastly and most importantly, as mentioned in Chap. 6, the judicial system in the UAE is based on Prosecution and Court. In addition to the Federal judicial system in the UAE, a number of cities have their own judicial systems and thus have their own Prosecutions and Courts. Hence, it is difficult to merge the AMLSCU within the UAE's judicial system since it will not receive all STRs from the reporting entities from the seven cities of the UAE. Alternatively, more than one FIU, with its own organisational structure, in the UAE needs to be established to accommodate all judicial systems, which conflicts with FATF Recommendation 29, as mentioned above. As a result, it is difficult, if not impossible, to adopt such model for the AMLSCU due to the judicial system within the UAE and international standards considerations.

The Option of Adopting Hybrid Model

As illustrated in Chap. 4, the hybrid model is based on merging the advantages of more than one of the aforementioned FIU models with a view to creating a pioneering FIU model that adapts with the circumstances and the legal system of a country. Thus, an optimal solution will be found if

[7] In 2011 alone, the reporting entities, in the UAE, submitted 2576 STRs to the AMLSCU. See chart.1 in Chap. 6.

[8] Where just 4 member states of the Egmont Group adopt the judicial/prosecutorial FIU model. See Chap. 4 (n 477).

[9] For the FATF Recommendations, which deal with international co-operation, see Chap. 4 (n 312).

the advantages of the UK FIU law enforcement model were combined with the administrative model in order to establish a new model for the UAE FIU, which comprises the advantages of both models. The main rational behind this option is that it utilises the advantages of the UK FIU model and endeavors to adapt them in a way so as not to conflict with the UAE's own circumstances and legal system. In addition, another objective of this model would be to establish a more effective UAE FIU, which can deal more successfully with STRs.

The current situation of the AMLSCU is that it is part of the Central Bank which has a regulatory and supervisory authority on the reporting entities, namely banks and other financial institution. Such a situation has negatively affected the AMLSCU in terms of its independence, its core functions in dealing with the STRs and its relationship with the reporting entities and LEAs.

In order to overcome the current situation, the AMLSCU should first be transferred to an entity that does not have any supervisory or regulatory authority on the reporting entities. Such a neutral entity could be the Ministry of Finance,[10] so that the AMLSCU is located within the Ministry, but with a high degree of operational independence and with the enjoyment the advantages of the UK FIU law enforcement model, as far as possible. The key justification, which supports the transfer of the AMLSCU to the Ministry of Finance, is that the Ministry does not have any supervisory or regulatory authority over the reporting entities, as the Central Bank, ESCA or the Insurance Authority has. There is further justification, which is no less important, and will be illustrated later in the course of providing recommendations for the AMLSCU's sections.

Nevertheless, the proposed UAE FIU hybrid model will not achieve success, or be effective in the STRs regime and fulfil the relevant FATF Recommendations, unless a number of amendments/revisions are made in relation to the statutory provisions, regulations and the organisational structure of the AMLSCU. Such amendments/revisions are discussed and evaluated in detail in the following parts.

[10] See www.mof.gov.ae (accessed on 24th April 2015).

General Recommendations

These recommendations deal with amendments/revisions to a number of aspects of the FLMLC 2002 and the CBR 24/2000 which have a direct/or indirect link to the STRs regime.

Predicate Offences to the ML Contained in the FLMLC 2002

The predicate offences set forth in the FLMLC 2002 do not meet the FATF standards since the FLMLC 2002 only currently covers six out of the 2003 FATF's 20 "designated categories of offences"[11] and now pursuant to the 2012 FATF Recommendations, the number of these offences has increased to 21 offences after tax crimes were added. Thus, the list of predicate offences should be extended to comprise the minimum list of offences as defined in the General Glossary of the FATF Recommendations[12] with a view to fulfilling the relevant FATF Recommendations in this regard. This is essential since the prosecution, in the UAE, has to prove the predicate offence in a ML case. This is because there is a closed list offences contained in Article 2 (2) of the FLMLC 2002, which constitute the predicate offences to ML. This is unlike the UK AML system, where the POCA 2002 adopts an "all crimes" basis for ML. The Crown therefore does not have to prove the specific offence, which generated the illicit proceeds, but it is sufficient for the Crown to prove circumstances, which could result in the jury concluding that the proceeds are criminal property derived from criminal conduct.

Amendments Proposed in Relation to the CBR 24/2000

Such amendments are crucial since they increase the ability of the banks and other reporting entities in detecting a STR before taking the proper

[11] See (n 320) of Chap. 4.

[12] 'The United Arab Emirates Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism' as produced by the FATF on 20 June 2008, 26.

decision whether to submit it to the AMLSCU. In addition, the amendments deal with the authority of the Central Bank in imposing sanctions/fines on the relevant financial institution that does not comply with regulations, such as CDD measures, record keeping and appointing a compliance officer. The amendments are related to three aspects, namely the definition of ML, CDD measures and sanctions/fines imposed by the Central Bank.

The Definition of ML

Unlike the definition of ML contained in ESCA Regulation 17/2010[13] and the Insurance Authority Regulation 1/2009,[14] the definition of ML contained in the CBR 24/2000 is different from that contained in the FLMLC 2002.[15] Such variation causes ambiguity and uncertainty for reporting entities; most notably for banks, since the CBR 24/2000 adds to the second part of the definition of ML that "This definition includes monies that are destined to finance terrorism or criminal acts." [16] This means that the definition of ML also covers money intended for financing terrorism or criminal acts. In other words, even money from legitimate business, but which is used for financing terrorism or criminal acts, is covered by the definition. However, such an interpretation confuses reporting entities and courts since the FLMLC 2002 provides that money/property must emanate from one or more of the predicate offences for ML listed in the Act.[17] Yet, the definition of ML in the FLMLC 2002 does not cover cases where money is derived from legitimate business, but is used to finance terrorism or criminal acts.

The definition of ML in the CBR 24/2000 conflicts with the definition in the FLMLC 2002. This is clearly evidenced when money, which is derived from legitimate business, is used to finance terrorism. This case falls within the definition of ML under the CBR 24/2000. However, it is

[13] See (n 580) of Chap. 5.

[14] See (n 588) of Chap. 5.

[15] Article 1 of the FLMLC 2002, see (n 597) of Chap. 5.

[16] Article 1 of CBR 24/2000, see (n 538) of Chap. 5.

[17] Article 2 (2) of the FLMLC 2002, see (n 600) of Chap. 5.

not considered ML under the FLMLC 2002, which requires that money has to be derived from one of the criminal activities (predicate offences), which are listed in the Act. Accordingly, no criminal liability arises in such a case and the judge cannot convict a person. The definition of ML in the FLMLC 2002 and the CBR 24/2002 have to be harmonised in order to avoid ambiguity among reporting entities and to ensure that courts can consistently apply the definition in relation to STRs.[18]

CDD Measures and Procedures

I would propose the following four changes in relation to the CDD measures since these measures assist banks and other reporting entities with detecting transactions for which STRs have to be submitted.

1) Although the term "CDD" is mentioned for the very first time in Addendum 2922/2008 of the CBR 24/2000, there is no clear definition, and the constituent elements of the term are also not clarified. The definition and the meaning of the term "CDD" along with its constituent elements must be clarified in the CBR 24/2000 since this component is vital for banks and other financial institutions in identifying STRs.[19]
2) The regulation requires banks and money exchange bureaus to have in place "effective risk based procedures"[20] in order to identify and handle the transfers in such cases in relation to inward transfers, especially where the originator's information in relation to the inward transfers is insufficient. However, Addendum 2922/2008 does not clarify the meaning of the term "effective risk based procedures" and also does not provide any examples for cases where there is a "lack in complete originator information."[21] The meaning and

[18] It is worth noting that the MLR 2007 defines the term "ML" in a way that does not conflict with the definition contained in the POCA 2002. See (n 788) of Chap. 7.

[19] The MLR 2007 provides a clear definition for the CDD procedures, as analysed in Chap. 7.

[20] Topic 3 of Addendum 2922/2008 which amended Article 5 (1) of Regulation 24/2000.

[21] Ibid.

the purpose of the term "effective risk based procedures" must be provided in the regulation and also examples of cases which "lack in complete originator information" must be provided for.

3) The term of "more strict CDD procedures"[22] which must be applied to businesses/individuals, such as dealers in real estate and auction houses, has been contained in the Addendum 2922/2008 without clarifying the meaning of such a term. The regulation should provide the meaning and examples of such "more strict CDD procedures" as applied in the aforementioned cases.
4) The ECDD procedures must be applied to a FPEP and his/her "immediate family members" and "close associates."[23] However, the Addendum 2922/2008 does not provide a definition or spell out its constituent elements, neither does it define the term "immediate family members," nor the term "close associates"[24] and this leads to uncertainties for banks and other financial institutions. Hence, the regulation should clarify to what level/extent such two terms must be subjected to the ECDD procedures.

Sanctions/Fines Imposed by the Central Bank

The CBR 24/2000 provides that a bank or financial institutions will be penalised in the case it fails to comply with any or all of the obligations and requirements in relation to combating ML,[25] such as CDD procedures, record keeping and appointing a compliance officer. Although, Addendum 2922/2008 does not clarify such sanctions or penalties, but just provides that such penalties are "in accordance with the prevailing laws and regulations." [26] In addition, Mr. A, from the AMLSCU, said that if any reporting entity does not obey the reporting system obligations, Article 15 of the FLMLC 2002, which specifies the penalty, will be

[22] Topic 4 (c) of Addendum 2922/2008.

[23] Topic 4 (a) of Addendum 2922/2008.

[24] While the MLR 2007 contains a clear definition and states the components for those two terms. See (n 832) of Chap. 7.

[25] Topic 11 of Addendum 2922/2008.

[26] Topic 11 of Addendum 2922/2008. See Chap. 5.

applied. Indeed, this Article does not deal with penalties imposed in cases of non-compliance with the requirements contained in the CBR 24/2000 but, rather, it deals with failing to report STRs to the AMLSCU.

As a result, there is not any authority, contained in the CBR 24/2000 and its Addendum 2922/2008, granted to the Central Bank in relation to impose penalty(s) on banks and other financial institutions in cases of non-compliance with the requirements contained in the CBR 24/2000.[27] Such a situation conflicts with the FATF Recommendation 27 which provides that supervisors should possess powers to punish financial institutions in case they fail to adopt and follow AML measures and procedures. Such penalties are crucial to ensure that the banks and other financial institutions comply with the requirements of AML contained in the regulation. The UAE Central Bank and all other UAE supervisory/regulatory authorities, such as the ESCA, should be able to impose financial penalties on relevant reporting entities, which do not adopt internal AML procedures and the SARs' requirements contained in the FLMLC 2002 and regulations, such as ECDD measures, record keeping and appointing a compliance officer. This ensures that all reporting entities appreciate that they will be subjected to penalties if they do not fulfil these requirements. This also requires that the supervisory/regulatory authorities regularly examine the internal AML/STRs procedures of reporting entities to ensure that they keep abreast of STRs requirements. There is an urgent need to grant such power to the Central Bank.

Recommendations Dealing with the STRs Regime

The following STR regime recommendations relate to (a) its basis and scope, (b) the STRs form, (c) the timeframe for submitting a STR and (d) the nationality of the compliance officer.

[27] This is in contrast to the UK's system where the FCA can impose financial penalties on reporting entities, which do not fulfil SAR/AML requirements. See Chap. 7.

The Basis and Scope of STRs

The Basis of STRs

There are three principal recommendations to deal with the basis of STRs.

Firstly, Article 15 of the FLMLC 2002 is the sole Article contained in the Act which governs STRs.[28] The Article imposes criminal liability on individuals who work in "financial institutions"[29] and "other financial, commercial and economic establishments"[30] if they fail to inform the AMLSCU of their actual knowledge about the occurrence of a ML offence in their institutions.

Hence, any persons outside the aforementioned entities, who have actual knowledge about the occurrence of a ML offence in any other entity, will not be subject to this provision. The FLMLC 2002 should include a further provision which imposes criminal liability on individuals, who work outside the aforementioned entities, if they fail to inform the AMLSCU about their actual knowledge of the occurrence of a ML offence in their entities. One such category should be notaries in UAE courts and lawyers. This is due to that the current situation that notaries in UAE courts[31] and lawyers[32] are obliged, by regulations issued by the Ministry of Justice, to inform the AMLSCU if they have reasonable grounds to suspect that ML has been perpetrated by their clients; nevertheless, there is no criminal liability imposed upon them if they fail to do so.

Secondly, currently Article 15 of the FLMLC 2002 is imposed upon the financial institutions' employees, including their compliance officers, which is equivalent to the nominated officer (MLRO) within the UK's system. There is no specific offence, contained in the FLMLC 2002, for the compliance officer if he has been informed by any employee in his

[28] This is in contrast to the UK's system where there are three sections contained in the POCA 2002, which govern the basis of SARs on ML, namely s.330, s.331 and s.332 of the POCA 2002. See Chap. 8.

[29] See (n 529) of Chap. 5

[30] See ((n 530) of Chap. 5.

[31] See (n 595) of Chap. 5.

[32] Ibid.

institution that the ML offence has been committed through the institution and he did not report this to the AMLSCU. His job, amongst other things, is to evaluate internal STRs, which are received from employees and to decide, based on his experience, whether or not to report a STR to the AMLSCU. Therefore, there should be a separate provision contained in the FLMLC 2002 that criminalises a compliance officer, if he fails to submit a STR to the AMLSCU. The punishment in such case should be more robust than is provided in Article 15. This is due to the fact that compliance officers are supposed to possess greater experience in ML transactions and patterns than fellow employees and they can almost be considered an internal FIU within their company.[33]

Thirdly and most importantly, the CBR 24/2000 obliges all banks and other financial institutions, including their Board Members, managers and employees to report STRs to the AMLSCU if there are reasonable grounds for suspicion that the funds are derived from criminal activity.[34] On the other hand, the FLMLC 2002 imposes criminal liability on persons simply for "having known" that the funds derived from criminal activity and have refrained from reporting STRs to the AMLSCU,[35] but it does not criminalise persons in cases where they have "reasonable grounds to suspect." Thus, the regulations address "reasonable grounds to suspect," whilst the FLMLC 2002 addresses actual knowledge. In other words, under the FLMLC 2002, the basis for submitting STRs is subjective, whilst under the CBR 24/2000 is objective. The significant result is that no criminal liability arises if a compliance officer in a bank or other financial institution did not fulfil the requirement contained in the CBR 24/2000 since the FLMLC 2002 criminalises cases where STRs have not been submitted, despite actual knowledge, but not when there are reasonable grounds of knowledge suspicion. This conflict between the FLMLC 2002 and the CBR 24/2000 has caused confusion amongst the banks on the basis of STRs, namely Mr. Z from bank D confirmed

[33] As analysed in Chap. 8, s.331 of the POCA 2002 criminalises a nominated officer in the regulated sector if he failed to submit a SAR to the NCA and s.332 criminalises other nominated officers in other circumstances.

[34] Topic 6 of Addendum 2922/2008, see (n 650) of Chap. 5.

[35] Article 15 of the FLMLC 2002. See Chap. 5.

that the basis is objective, whilst Mr. S from Bank E stated that it is both objective and subjective.

This situation has increased the unnecessary STRs, which have been submitted to the AMLSCU. This is further evidenced by the huge differences between the number of received STRs and the number of STRs, which were transmitted to the Public Prosecutions Office between June 2002 and May 2009.[36] This discrepancy is because the reporting entities are confused about the conflicting FLMLC 2002 provisions and AML regulations and have adopted a defensive approach. They may send all transactions which appear "unusual" without taking into account that actual knowledge or a reasonable ground for suspicion has to exist. The reporting entities may adopt such an approach simply to ensure that they are safe and are not subjected to any of the offences set out in the FLMLC 2002.

Rational Grounds for STRs

Moreover, the CBR 24/2000 obliges banks and other financial institutions to examine the background of any "unusual transaction" and its purpose, and to document their findings.[37] However, it does not contain any guidance and also does not define the term "unusual transaction;" so that "reasonable grounds to suspect" could also arise where there are some doubts or where there is a vague feeling of unease or some subjective feeling.

Therefore, there must be consistency between the FLMLC 2002 and the AML regulations on the basis of STRs, so that any ambiguity must be removed amongst the banks and the reporting entities in general. In this regard, it is arguable that the FLMLC 2002 and the regulations should adopt an objective basis, namely reasonable grounds for knowledge or suspicion and subjective basis, namely just actual knowledge. The term "suspicion" must not form the basis for a STR since it is too broad a term and can be used for revenge purposes.[38] It is true that Article 20

[36] The AMLSCU received 80,592 STRs about ML from the reporting entities. Despite this large number of STRs, only 285 STRs were transmitted to the Public Prosecution Office.

[37] Topic 8 of Addendum 2922/2008, see (n 658) of Chap. 5.

[38] Such issue has been critically analysed in Chap. 9.

of the FLMLC 2002 provides good faith immunity from any criminal/civil liability, including breach of contract, legislation, regulation or any other administrative provision for the reporting entities, which divulge STRs to the AMLSCU,[39] and Article 17 of the Act imposes criminal liability in cases of bad faith,[40] nevertheless, it is difficult to prove bad faith if the law/regulations require the banks and other reporting entities to submit a STR on a mere suspicion without reasonable grounds for it. Consequently, the basis for SARs should either be actual knowledge or objective reasonable grounds for knowledge or suspicion in order to ensure fairness.

The Scope of STRs

There are two recommendations in relation to the scope of STRs.

1) The absence of the term "in the course of his business"

Neither Article 15 of the FLMLC 2002, nor the CBR 24/2000 require that the information or matters, on which the employee's knowledge is based or which give reasonable grounds for suspicion, must have come to him in the course of his work in the banks or other reporting entities in general. This, in turn, means that if the information/matters came to him outside the course of his business, the employee will commit the offence of failing to report if he failed to do so. It is irrelevant whether or not the information came to him during the course of business or outside of it.[41]

Without such a requirement, the scope of a STR becomes too wide and it becomes too difficult to determine its scope. In other words, any person who works in a reporting entity is obliged to inform the AMLSCU about his knowledge/suspicion on a STR, even if it is outside of his company. Indeed, it is not easy to realise such a result which means that a person, who works in a reporting entity, will be confused about whether he needs to focus on transactions/activities in his company and outside of it.

[39] See (n 623) of Chap. 5.
In addition, the FATF Recommendation 21(a) provides such good faith immunity, see (n 346) of Chap. 4.

[40] Ibid.

[41] This is unlike to the UK's system which requires such requirement. See Chap. 8.

Therefore, in order to avoid the aforementioned confusion, the term "in the course of his business" should be implied in the FLMLC 2002.

2) STRs on the attempted ML transactions

The CBR 24/2000 obliges the banks and other financial institutions to submit STRs to the AMLSCU not just in the case of actual transactions, but also in cases of attempted transactions.[42] This is in contrast to the FLMLC 2002 which creates an obligation to report STRs to the AMLSCU just in the case of actual transactions.[43] This means that if a bank did not submit a STR, attempted ML transaction, to the AMLSCU, it will not be subject to any criminal liability. Thus, the FLMLC 2002 should be amended to include attempted transactions/activities, so that STRs have to be also submitted in relation to these attempts.

The Form of STRs

Article 7 of the FLMLC 2002 stipulates that the NAMLC has the authority to design the form for the STRs, which all reporting entities have to use, as well as the method for sending them to the AMLSCU.[44] On the other hand, the CBR 24/2000 requires banks and other financial institutions to adopt a specific form attached to its regulation.[45] In addition, ESCA Regulation 17/2010 requires all markets, companies and institutions, which are licensed by it to adopt a specific form attached in its Regulation.[46] Moreover, Mr. Z and Mr. S, from the Banking sector, confirmed that the Central Bank provides the form for the STRs. Hence, there is a conflict between the FLMLC 2002 and the regulations in relation to the form of STRs. This means that the current practice in providing the form of the STRs by the supervisory authorities, such as the Central Bank and the ESCA is inconsistent with Article 7 of the FLMLC 2002.

[42] Topic 7 of Addendum 2922/2008, see (n 661) of Chap. 5.

[43] Article 15 of the FLMLC 2002, as critically evaluated in Chap. 5.

[44] See (n 683) of Chap. 5.

[45] Form (CB9/200/6), see (n 650) of Chap. 5.

[46] Article 8 of ESCA Regulation 17/2010, see (n 685) of Chap. 5.

Indeed, neither the NAMLC nor the supervisory authorities the appropriate entities to provide all reporting entities the form of the STRs. This is simply because they do not receive and analyse submitted STRs from the reporting entities and therefore have insufficient knowledge to identify the essential components of STRs forms. Instead, the AMLSCU is the appropriate entity to provide such form since it is the sole entity which deals with the STRs, and thus it should have such authority and identify the form's components which will assist its core function in analysing STRs. In addition, the AMLSCU should devise a form according to the type of the sector. For example, the form of the STRs for the banking and financial institutions should be different, in its components, from that which is for insurance companies or companies which are licensed by the ESCA.[47] For the aforementioned reasons, the FLMLC 2002 should grant such power to the AMLSCU.

The Timeframe of Submitting STRs

The current situation is that neither the FLMLC 2002 nor the regulations require the reporting entities to make a decision whether or not to submit a STR to the AMLSCU in a specific timeframe from when reasonable grounds for knowledge/suspicion arose. The absence of such requirement has resulted in a huge discrepancy in internal banking procedures from one bank to another in this regard. For instance, bank D submits STRs to the AMLSCU on average within one week; however, it takes one month in bank E. It is true that it is difficult, if not impossible, to oblige the reporting entities to submit the STRs within a specific timeframe since each case has its own circumstances and conditions. Nevertheless, under the FLMLC 2002, there should be a requirement placed on the reporting entities to do so as soon as possible[48] in order to allow the AMLSCU to carry out its duties in the proper time and take the proper decision or

[47] The UK's SARs standard form comprises seven separate models, which are produced by the UK FIU. See Chap. 9.

[48] It is worth noting that the POCA 2002 provides the term "as soon as is practicable." See the conditions of s.330, s.331 and s.332 which have been analysed in Chap. 8.

to inform the competent authority to take the proper action promptly without losing time.

FATF Recommendations 30 and 31 provide that in situations of suspected criminal property, the country's competent authorities must be able to identify said property as soon as possible, monitor it and to start procedures to freeze or seize the relevant property.

The Nationality of the Compliance Officer

As analysed in Chap. 5, the Insurance Authority Regulation 1/2009 requires that compliance officers of insurance companies and professionals associated with insurance activities have to be UAE nationals. Due to the sensitive task of a compliance officer in evaluating all internal STRs in his company before submitting them to the AMLSCU, such a requirement is deemed rational. Hence, it is recommended that all regulations issued by the supervisory authorities, such as the Central Bank and the ESCA should require that the compliance officer in all reporting entities has to be a UAE national.

Nevertheless, it is difficult for the reporting entities to fulfil such requirement currently since a compliance officer has to possess a great amount of experience on ML transactions and patterns, as well as having analytical skills in dealing with an internal STR, things not associated with UAE nationals currently. However, such a requirement should exist as a strategic objective for all the reporting entities, so that they are obliged to achieve it within 5 years. Such a period is granted for the reporting entities in order to prepare UAE nationals, through training and courses, so as to be able to work as a compliance officer. The AMLSCU can also play a great role in assisting the reporting entities to fulfil such requirement by providing courses and seminars for the compliance officer candidates from the UAE.

Recommendations in Relation to Tipping Off Offences

Article 16 of the FLMLC 2002 is formulated in narrow terms and only covers circumstances where the disclosure is made to the person undertaking the transaction, which is checked or under investigation. There

is no offence if the person, who works in the reporting entity, informs a third party, who is related to or associated with the person undertaking the transaction, that the transaction is being checked or investigated for potential ML.[49] The absence of the term "third party" in the aforementioned provision may result in the person undertaking the transaction knowing through a "third party" that his transaction is being checked or investigated. The CBR 24/2000 provides the prohibition of tipping off "any person;"[50] however, there is not any criminal liability if such case occurs since the FLMLC 2002 does not impose criminal liability for tipping off another person other than the concerned customer. Therefore, Article 16 must be amended to criminalise the tipping off of another person other than the concerned customer.

On the other hand, Article 15 (6) of the CBR 24/2000 requires banks and other financial institutions, after they have submitted a STR to the AMLSCU, to inform the customer that the Central Bank has decided to freeze his transaction. In addition, the reporting entity has to request the affected customer to provide documents and information in order to prove that the transaction is lawful.[51] This requirement results in the customer being alerted to the fact that his transaction is being treated as suspicious. Indeed, such a requirement is inconsistent with the aforementioned Article 16 of the FLMLC 2002 and even with the aforementioned CBR 24/2000 about the prohibition of tipping off for "any person." Thus, Article 15 (6) of the CBR 24/2000 must be abolished to remove inconsistency with the FLMLC 2002 and the CBR 24/2000. Instead, it is suggested that the CBR 24/2000 includes a provision that banks and other financial institutions may, before submitting a STR to the AMLSCU, ask the relevant customer to provide documents and information which are related to his transaction. This must be done without stating that the transaction is suspected of being part of a ML scheme in order to avoid the commission of the tipping off offence, as Mr. S from bank E stated. Such a proposed provision can be deemed as an optional requirement for the reporting entities if the compliance officer, before submitting a STR

[49] This is unlike the UK's system which criminalises tipping off any person. See Chap. 8.

[50] Topic 9 of Addendum 2922/2008, see (n 665) of Chap. 5.

[51] Article 15 (6) of CBR 24/2000, see (n 624) of Chap. 5

to the AMLSCU, needs additional information/documents in order to consider whether the relevant transaction is a suspected transaction that involves ML.

Recommendations Regarding the Organisational Structure of the AMLSCU

These recommendations will focus on three aspects, namely the AMLSCU's sections, its human resources and the STRs regime committee. The appointment of the Head of the AMLSCU will be discussed later.

Sections of the AMLSCU

In addition to the current sections of the AMLSCU, which have been illustrated in Chap. 6, there are a number of recommendations that should be taken into account in this regard, namely (1) enhancing the AMLSCU's analytical functions, (2) keeping abreast of international standards, (3) training courses and (4) recovery of illegal proceeds.

Analytical Section

Analysing STRs is currently run by (the STR Analysis and STR Database Management Section). However, due to the importance of this function, as it constitutes the backbone of the AMLSCU's functions, there should be a separate section specialised in analysing STRs received from the reporting entities. In addition, this proposed section should conduct three elements of analysis, namely tactical, operational and strategic analysis. The analytical function has two important roles. Firstly, based on the analytical function, the AMLSCU decides whether there is a suspicion/knowledge about ML, and accordingly transmits a STR to the prosecution. Secondly, the strategic analysis plays a vital role in improving the work of the AMLSCU and is important, as currently the AMLSCU does not pay great attention to this type of analysis. Therefore, the analytical function should be transferred to the proposed section due to its great importance.

Paying Attention to International Standards

The International Cooperation Section, in the AMLSCU, which is responsible for following up on the UAE's MER and coordinating with concerned entities to ensure implementing the FATF Recommendations, should make greater efforts to ensure that the relevant FATF Recommendations are fulfilled, especially in the light of the 2012 FATF's Recommendations revision. The importance of such an issue is that fulfilling the relevant FATF Recommendations, Recommendations that deal with the FIU and the STRs requirements, will reflect positively on the compliance level of the UAE's FIU and STRs requirements and its compliance with the Forty Recommendations in general.

Training and Development Section

Developing and training the AMLSCU's staff is currently run by (the STR Analysis and STR Database Management Section). However, a Training and Development Section should be established at the AMLSCU due to existing deficiencies in relation to (1) the training of AMLSCU's staff and compliance officers at the reporting entities, (2) the quality of the STRs submitted by the reporting entities and (3) the quality of STRs analysis by the AMLSCU. This Training and Development Section should fulfil the following tasks:

1) Providing training courses and arranging seminars for the AMLSCU's staff, notably analysts who are responsible for analysing STRs,
2) Providing training courses and arranging workshops and seminars for the compliance officers who work in the banks and other reporting entities,
3) Providing general and case by case feedback to the reporting entities, and
4) Studying the results of the strategic analysis which is conducted by the proposed Analytical Section.

The first three tasks will be further explained below, while the task of studying the results of the strategic analysis is crucial with a view to proposing a new/amended AMLSCU's works in the future to keep pace with new developments in ML activities, especially in the light of the absence of such elements in the current AMLSCU situation. The Training and Development Section should periodically inform the Head of the AMLSCU about its proposals on the new/amended AMLSCU's works to ensure their implementation. In addition, the proposed section must be connected with the International Cooperation Section to be aware of any changes/amendments in the FATF Recommendations.

Assets Recovery Section

As illustrated in Chap. 6 the FLMLC 2002 does not contain any provisions about the procedures of asset recovery and confiscations where those proceeds are derived from predicate offence(s) for ML. In addition, the Act does not contain any provision on the authority which is tasked with doing so. One of the ambiguities that arises as a result of the absence of provisions in this regard is that in cases where the laundered proceeds have to be returned to the government. For instance, after the Court's judgment, what procedure should be adopted by the government to recover/confiscate proceeds if they are located within the UAE? Who is the competent authority responsible for dealing with such an issue and enforcing the judgment? Currently, no provisions exist to address these matters.

Therefore, a provision should be added in the FLMLC 2002 granting such responsibility to a separate section called the "Asset Recovery Section" in the AMLSCU and in coordination with the Ministry of Finance. In addition to other competencies, the Ministry of Finance is responsible for collecting and auditing federal government's revenues, identifying mechanisms of collecting federal government's revenues, developing its facilities, establishing a financial risk management unit and developing its associated controls.[52] The Ministry of Finance is the best place that can

[52] See www.mof.gov.ae (accessed on 16th April 2015).

cooperate with the AMLSCU on the issue of assets recovery, especially if laundered proceeds have to be returned to the government. Indeed, in addition to the justification mentioned above, this issue provides further justification for proposing the location of the AMLSCU to be within the Ministry of Finance. Nevertheless, the role of the AMLSCU in asset recovery in ML cases is another issue which is left out of the scope of this research and could be studied in further research, especially in the light of the absence of provisions, contained in the FLMLC 2002, which govern it.

The Human Resources

It is assumed that AMLSCU employees possess sufficient knowledge, experience and skills in order to be able to analyse STRs and to find evidence since police officers and prosecutors usually do not have the qualifications and experience for these types of cases, especially where financial transactions are involved. According to the latest update, Mr. A, from the AMLSCU, stated that the AMLSCU has got 25 staff members and access to more than 80 investigators, from the Central Bank, in order to conduct examinations on behalf of the AMLSCU. Indeed, using investigators from the Central Bank prejudices the operational independence of AMLSCU and recommendations to deal with this issue will be provided later. However, the current number of AMLSCU staff seems very low and does not accommodate its responsibilities. This aspect negatively impacts on its ability to effectively analyse STRs received from the reporting entities and the quality of analysing STRs.

Such negative consequences of the current AMLSCU's staffing numbers can be seen clearly in three aspects. Firstly, the huge difference between the number of STRs received by the AMLSCU and the number of STRs, which are transmitted to the Public Prosecutions Office during the period between June 2002 and May 2009.[53] Hence, work pressure could result in AMLSCU employees not paying great attention to the majority of the STRs they receive. Similarly, it can also account for the huge

[53] The AMLSCU received 80,592 STRs about ML from the reporting entities. Despite this large number of STRs, only 285 STRs were transmitted to the Public Prosecution Office.

variation between the numbers of STRs sent to the Public Prosecution Office and the number of STRs which were prosecuted through the courts.[54] Hence, AMLSCU's employees may have been under pressure because of the vast numbers of STRs and could thus not provide sufficient evidence about ML suspicious and this, in turn, resulted in fewer prosecutions through the courts. Secondly, a particularly long period, namely between 3 and 4 months, usually passes between the request for additional information from the Public Prosecution Office and the response from the AMLSCU, as Mr. L stated. Lastly, the formation of a committee composed of employees of the AMLSCU and AML Section of Dubai Police during the investigation by Dubai Public Prosecution Office.[55] The formation of such a committee is due to the fact that the AMLSCU does not have employees from strategic partners, such as the police, and thus it utilises the experience of other strategic partners, such as the AML Section at Dubai Police, as Mr. N stated. Therefore, in order to overcome these human resources problems, two recommendations should be taken into account, namely increasing the number of the AMLSCU's staff and periodical training and workshops.

Increasing the Number of the AMLSCU's Staff

The AMLSCU should have sufficient human resources and experts in order to accommodate its responsibilities and functions, particularly sufficient and qualified analysts in the proposed Analytical Section. In addition, strategic partners from a number of LEAs, such as the Police, Customs Authority and Public Prosecution, could join the AMLSCU in order that their experience be utilised. In this regard, it is important to mention that the proposed Training and Development Section will play a vital role, through its reports and studying the results of the strategic analysis, in amending the AMLSCU's works in the future, notably identifying the functional requirements and the number of the staff that the AMLSCU needs in the forthcoming year.

[54] Only 20 out of the 285 STRs received by the Public Prosecution Office were sent to the courts. In addition, only 7 % out of the 20 STRs resulted in a conviction.

[55] As occurred in *Attorney general v Others*, Dubai Court Judgment, Criminal Division, case No. 370/2008, see (n 711) of Chap. 5.

Periodical Training and Workshops

Due to the importance of continuous training, the AMLSCU, via the proposed Training and Development Section, should provide semi-annual training courses and workshops to its staff, so that they are kept abreast of new forms of sophisticated ML transactions/activities; for example, ML through the football sector[56] or new payment methods, such as prepaid cards and internet and mobile payment services.[57] These training courses should also take place in countries, such as Italy,[58] US,[59] Australia,[60] and France[61] which experience the above mentioned sophisticated ML patterns and activities. The AMLSCU may also sign a MOU with FIUs in these countries in order to utilise their experience on sophisticated ML patterns and to provide training courses for its staff. In addition, it could invite academic and LEAs to join workshops/seminars, so that the AMLSCU's staff gain different perspectives, outside the AMLSCU environment, in relation to the AMLSCU responsibilities.

The STRs Regime Committee

FATF Recommendation 33 requires the competent authorities of a country to keep comprehensive statistics about their work, such as statistics on the STRs, prosecutions and convictions. The AMLSCU

[56] FATF Report, 'Money Laundering through the Football Sector' July 2009, available online at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20through%20the%20Football%20Sector.pdf (accessed on 15th July 2015).

[57] FATF Report, 'Money Laundering Using New Payment Methods' October 2010, available online at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf (accessed on 15th July 2015).

[58] Which has experienced an attempt to launder money through the purchase of a famous Italian football team. For further details, see FATF Report, 'Money Laundering through the Football Sector' (n 1408) 20.

[59] Which has witnessed the laundering of illegal gambling proceeds through prepaid cards and illegal online steroid sales. For further details, see FATF Report, 'Money Laundering Using New Payment Methods' (n 1409) 37.

[60] Which has experienced the laundering of drug proceeds through prepaid cards. For further details, see FATF Report, 'Money Laundering Using New Payment Methods' (n 1409) 38.

[61] Which has witnessed the laundering of illegal proceeds from mis-utilised company assets to fund a football club. For further details, see FATF Report, 'Money Laundering through the Football Sector' (n 1408) 17.

started publishing its annual report in 2008 and it is the mission of (the STR Analysis and STR Database Management Section),[62] nevertheless, the AMLSCU annual reports do not provide accurate statistics in relation to STRs on ML since most of the STRs, which have been submitted to the AMLSCU, involved suspected cases of ML and other types of financial crimes, such as fraud. The AMLSCU annual reports should show accurate STRs statistics on ML, including how many STRs have been transmitted to the Court and have resulted in convictions. These statistics are crucial in order to evaluate the annual performance of the reporting entities in relation to understanding STRs requirements. In addition, only this type of statistics can inform how efficiently the AMLSCU fulfils its functions, especially in relation to analysing STRs.

In order to provide valuable and comprehensive STRs on ML statistics, preparing and issuing the annual reports should be the responsibility of a specific committee associated with the AMLSCU.[63] The membership of this committee should not be confined to the AMLSCU, but should also include members from strategic partners in the STRs regime, such as LEAs and the reporting entities. The STRs regime committee should comprise the Head of the AMLSCU (chair), the proposed AMLSCU's Training and Development Section, the Central Bank as a representative for banks and other financial institutions, the ESCA, the Customs Authority, the Insurance Authority, the Ministry of Interior and local police from Abu Dhabi, Dubai and Ras Al Khaimah. In its annual report, the committee should provide comprehensive STRs statistics on ML, set out identified deficiencies in the particular reporting year and address how these will be resolved and assessment solution(s) in the subsequent annual report. The committee has to spell out the strategic objectives in the short and long term for the AMLSCU and these should be periodically reviewed, particularly since this is not currently been done. In addition, the annual report should include statistics on assets recovery and their values since such statistics are not provided in the current AMLSCU's annual reports.

[62] See (n 745) of Chap. 6.

[63] Similar to the SARs Regime Committee in the UK, as analysed in Chap. 9.

There is a strong argument that AMLSCU does not provide annual reports to banks and other reporting entities,[64] so such annual reports should be provided to the banks and other reporting entities. More importantly, the AMLSCU should have its own website on the internet as currently there is little information available about it on the website of the Central Bank.[65] Further, the annual reports should be publically available via its website since they are not available publicly. This should be done with a view to increasing public awareness of the ML issue.

Recommendations to Enhance the Operational Independence of the AMLSCU and its Accountability

Enhancing the AMLSCU's Independence

In the light of the doubts surrounding the independence of the AMLSCU, as critically analysed in Chaps. 5 and 6, I would like to make a number of recommendations. Firstly, the recommendation, mentioned above, of transferring the AMLSCU from the Central Bank, which has a supervisory and regulatory authority on the banks and other financial institutions, to the Ministry of Finance, which does not have such characteristics. In this case, it should be stressed that the AMLSCU should have its own budget and human resources separate from the Ministry of Finance. Secondly, the recommendations, mentioned above, on the AMLSCU's human resources, will assist in enhancing the AMLSCU's independence. No employees outside the AMLSCU should carry out the AMLSCU's analytical function, as currently happens.[66] Thirdly, the current situation is that the Executive Director of the Central Bank is also working as the Head of the AMLSCU. Instead, it would be much better if the Head of the AMLSCU was appointed by the Ministry of Finance,

[64] This was confirmed by Mr. Z from the banking sector. See Chap. 6.

[65] See www.centralbank.ae (accessed on 16th April 2015).

[66] Mr. A. from the AMLSCU confirmed that the AMLSCU uses more than 80 examiners from the Central Bank in order to conduct its analytical function on behalf of the AMLSCU.

so long as the AMLSCU is located within this Ministry. Such appointment should be for 5 years period and can be renewable. However, the AMLSCU should not be accountable to the Ministry of Finance, but instead it should be accountable to another entity which can develop also the AMLSCU's policies, illustrated below.

Accountability of the AMLSCU

Article 10 of the FLMLC 2002 provides that the NAMLC has the responsibility for proposing AML regulations and controls in the UAE and facilitating information exchange between parties represented therein.[67] This committee is responsible for proposing AML regulations and controls, so the AMLSCU could be accountable to the NAMLC, notably Article 9 of the FLMLC 2002 provides that the Minister of Finance is responsible for establishing such a committee, under the chairmanship of the governor of the Central Bank, and it includes representatives of the following seven entities: (1) the Central Bank, (2) the Ministry of Interior, (3) the Ministry of Justice, (4) the Ministry of Finance and Industry, (5) the Ministry of Economic, (6) Authorities responsible for issuing trade and (7) industrial licences and the State Custom Board.[68]

By adopting this proposal, it is ensured that the AMLSCU is accountable to an independent body, which is specialised in AML affairs at the national level. This proposal entails that the AMLSCU should provide to the NAMLC its annual reports, conducted by the proposed STRs regime committee, as well as the reports which contain results of the strategic analysis, conducted by the proposed Training and Development Section. This will assist the NAMLC with evaluating the AMLSCU policy and proposing new work for the AMLSCU, so that it keeps pace with new trends within ML. In addition, it will ensure that the NAMLC plays a greater role than current role in AML at national level since one of its responsibilities is proposing AML regulations and controls.[69] Indeed, studying the STRs annual reports, received from the AMLSCU, will be a key element in assisting the NAMLC to propose AML regulations and controls.

[67] Article 10 of the FLMLC 2002, see (n 635) of Chap. 5.

[68] Article 9 of the FLMLC 2002, see (n 634) of Chap. 5.

[69] Article 10 of the FLMLC 2002.

This proposal requires that a representative from the AMLSCU is located at the NAMLC, as currently Article 9 of the FLMLC 2002 omits such a requirement. Hence, the Article should be amended to explicitly include the Head of the AMLSCU as a representative.

Recommendations in Relation to the Role of the AMLSCU in Dealing with the STRs

These recommendations aim at enhancing and improving the AMLCU's role in the STRs regime in terms of three aspects, namely its core functions, non-core functions and its authority to freeze suspicious transactions.

The AMLSCU's Core Functions

As analysed in Chap. 4, the core functions of a FIU are receiving, analysing and disseminating STRs.

Receiving STRs

Currently, only banks and money changers are electronically linked with the AMLSCU via the online STR system.[70] This means that only those entities can submit STRs to the AMSCU electronically. The percentage of STRs submitted via online STRs system and the percentage of STRs submitted manually (by paper) are still not included in the AMLSCU's annual reports. Nevertheless, it was expected that the percentage of STRs submitted via online STRs would reach over 90 %. Indeed, the online STRs system should be available to all reporting entities since such a mechanism has a number of advantages, for instance, STRs are received much quicker from the reporting entities. The AMLSCU should try its utmost to increase this percentage by (1) publishing bulletins for the reporting entities[71] and (2) arranging workshops for compliance officers with a view of clarifying how to register and submit STRs electronically.

[70] As Mr. A, from the AMLSCU, stated in Chap. 6.

[71] The UK FIU provides bulletins to the reporting entities. See Chap. 9.

Establishing a comprehensive online STRs system entails that the AMLSCU takes into account confidentiality matters, so that the compliance officers, in the reporting entities, should have a valid working email account, which is used for STR online user identification. Such an email account must be used by only one user. Moreover, a reference number should be provided to the reporter once he submits a STR electronically.[72] The reference number of the report is essential since it can be used as evidence, especially by the nominated officer, to avoid committing the failing to report offence.

In addition to receiving STRs, the FLMLC 2002 should explicitly require the AMLSCU to store all STRs, received from the reporting entities, on its own database, even if this requirement has not been explicitly required in the FATF Recommendations.[73] Storing STRs is currently run by (the STR Analysis and STR Database Management Section) within AMLSCU,[74] however, a legal provision should expressly provide for this.

Analysing STRs

Article 8 (1) of the FLMLC 2002 does not explicitly mention the term "analysing," but instead mentions the expression "studying"[75] without clarifying its meaning. Accordingly, the analytical function is vague in FLMLC 2002, although, it forms the most important function of any FIU. This Article should be amended to include the analytical function, so as to be compatible with FATF Recommendation 29.[76] The Act should also clarify that this function includes tactical, operational and strategic analysis. In addition, the FLMLC 2002 should require the AMLSCU to identify its strategic plan and objectives annually along with its future needs, such as additional IT staff or analysts. The AMLSCU will not manage to set up its strategic plan and objectives and its future needs, unless it conducts the strategic analysis.

---

[72] This is the same under the UK SARs regime. See Chap. 9.

[73] Interpretative Note to FATF Recommendation 29, see (n 514) of Chap. 4.

[74] See (n 745) of Chap. 6.

[75] Article 8 (1) of the FLMLC 2002, see (n 686) of Chap. 5.

[76] FATF Recommendation 29 has been critically analysed in Chap. 4.

In order to assist the AMLSCU's function in analysing STRs, received from the reporting entities, and to increase the quality of such analysis, the FLMLC 2002 should explicitly grant an authority to the AMLSCU to require additional information/document(s) from the relevant the reporting entity, if such information/document(s) assists it in analysing a STR. The Act should equally explicitly grant the AMLSCU the power to require additional information/document(s) from the LEAs. The current practice of the AMLSCU in requiring additional information/document(s) from the reporting entities or even from LEAs in relation to analysing STRs lacks a legal basis. Such authority must be contained in the Act in order to fulfil the FATF Recommendation 29.

Disseminating STRs

Article 8 (1) of the FLMLC 2002 states that the AMLSCU should, after studying the STRs, notify the public prosecutors to take necessary actions. In addition, Article 7 of the Act requires the AMLSCU to make all information, which it holds, available to LEAs for their investigations. This means that the AMLSCU cannot disseminate information about STRs to any entity other than LEAs. However, the AMLSCU has disseminated information about STRs to the BSED in the Central Bank and other supervisory agencies in order for them to follow-up with the reporting entities. This is despite these supervisory agencies not being a LEA. Indeed, such practice is incompatible with the requirements contained in the Act and can raise doubts about the AMLSCU's independence. Therefore, the AMLSCU should appreciate this issue and, in future, should not disseminate information about STRs to any agency other than LEAs.

The AMLSCU's Non-Core Functions

The FLMLC 2002 does not specify the non-core functions of the AMLSCU, such as providing feedback to reporting entities and participating in improving the national AML regulations and controls. Indeed, some non-core functions are no less important than the aforementioned core functions.

Providing Feedback on the STRs

FATF Recommendation 34 requires that the relevant authorities of a country should provide entities with guidelines and feedback about STRs in order to increase the quality of STRs submitted. The feedback encompasses general feedback and case by case feedback.[77] It is arguable that Recommendation 34 directly addresses national FIUs since the national FIU is best placed to provide this type of feedback as it has comprehensive knowledge and keeps statistics about STRs, which it has received from the reporting entities.

When applying the aforementioned requirement to the AMLSCU, the FLMLC 2002 does not entitle the AMLSCU to provide general feedback or case related feedback to the reporting entities. Mr. Z and Mr. S, from the banking sector, confirmed that the AMLSCU does not provide the banks with general feedback on STRs, nor specific/case by case feedback on a specific STR. Hence, there is an urgent need to amend the FLMLC 2002 to require the AMLSCU to provide the reporting entities such feedback and guidelines since the quality of STRs will otherwise not increase if the AMLSCU cannot point out the deficiencies of previous STRs.

On the other hand, the FLMLC 2002 should require the AMLSCU to provide LEAs, the end users of the STRs, with questionnaires in order to receive feedback on the STRs regime. Such questionnaires should be provided to the end users of the STRs at least once a year with a view to receiving notes/suggestions on the workings of the AMLSCU, the STRs files disseminated by the AMLSCU and whether there are any deficiencies in the STRs regime in general. The results of such feedback should be shown in the AMLSCU's annual reports.

Indeed, the adoption of these two feedback limbs has a number of advantages. The main objective of providing feedback to the reporting entities is to increase the quality of the STRs which are submitted to the AMLSCU, whilst the main objective of receiving feedback from the LEAs is to invite end users of the STRs to provide their knowledge/experience to the AMLSCU on the operation of the STRs regime which thereby helps in providing important feedback to the reporting entities.

[77] See (n 502) of Chap. 4.

As a result, both limbs of feedback are crucial for the functions of the AMLSCU since the reporting entities, the AMLSCU and the LEAs are all partners within the STRs regime.

Participating in developing the national AML regulations and controls

Such a role will be played by adopting the proposal that the AMLSCU should be accountable to the NAMLC, mentioned above. In addition, the AMLSCU can utilise its analytical function in order to provide the government/NAMLC with ideas about how to reform the STRs system. It can suggest that specific entities are more vulnerable and prone to exploitation by money launderers than others. Moreover, through its analysing STRs, the AMLSCU may assist the NAMLC in proposing a number of amendments in the national AML system, such as enhancing preventive measures because new patterns of ML have emerged in specific areas, such as the football or the sports sector in general.

The AMLSCU should also play a role in increasing public awareness of the ML issue via making its all annual reports available on its website.[78] In addition, there is another crucial non-core function of the AMLSCU, namely providing training courses to the reporting entities which is discussed in the last recommendations category.

The AMLSCU's Authority in Freezing Suspicious Transactions

The current situation is that the Central Bank has the right to freeze suspect criminal property within financial institutions for up to seven days. Public prosecutors have got the same right in relation to suspected property, proceeds or instruments. The competent court has the same right but can freeze assets for an unlimited period. Whilst the FLMLC 2002 stipulates the period for freezing assets for the Central Bank and competent courts, it does not spell out the period for public prosecutors. The FLMLC 2002 also does not set out what procedures apply at

[78] This is the same under the UK SARs regime where annual reports are publicly available on the NCA (UK FIU) website.

the end of the seven days in relation to assets which have been frozen by the Central Bank.

In order to overcome the aforementioned dilemma, the authority of freezing suspicious transaction should be given to the AMLSCU and more precisely to the proposed Analytical Section since it has the knowledge about the relevant STRs and it is the best place for practicing such authority. This authority is one of the advantages of the FIU law enforcement model.[79] Hence, the FLMLC 2002 should clarify the freezing system and take into account the following elements and procedures:

1) The reporting entities are obliged to submit a STR to the AMLSCU.
2) The nominated officer in the reporting entity must wait two working days, starting from the day after he submits the STR, in order to receive the AMLSCU's decision of freezing the transactions.
3) The nominated officer can proceed with the transaction, if he did not receive the freezing decision from the AMLSCU within the aforementioned two working days.
4) If the AMLSCU decided to freeze the transaction within the aforementioned two working days, it will have 15 working days from the time of the freezing decision.
5) The nominated officer cannot proceed with the transaction, unless the 15 working days have finished or he receives the AMLSCU's permission to proceed with the transaction.
6) If the AMLSCU decides that it needs a longer period for freezing other than the aforementioned 15 working days, it should request the Public Prosecution Office to extend the freezing period to 30 days, including holiday(s) day, before the end of the aforementioned 15 working days.
7) The nominated officer cannot proceed with the transaction if he is informed by the AMLSCU about the extension of the freezing decision for 30 days by the Public Prosecution Office.

[79] As critically evaluated in Chap. 4. Under UK FIU law enforcement model, it can freeze suspicious transactions, as critically analysed in Chap. 8.

8) If the AMLSCU or the Public Prosecution Office decides it needs an additional freezing period, the Public Prosecution Office should seek an extension from the competent Court for an unlimited period. In such a case, the compliance officer cannot proceed with the transaction, unless he receives the Court's permission.

The aforementioned procedures have a number of justifications. Firstly, the objective of the first two working days for the AMLSCU to decide whether to freeze the transaction is to allow it initially to distinguish between a real STR and a STR that does not fulfil the requirements contained in the Act and the relevant regulations. Secondly, the AMLSCU has the right to freeze for 15 working days, instead of the current 7 days. This allows the AMLSCU to properly analyse STRs, particularly when the AMLSCU requires additional information from the relevant reporting entity/or a LEA. Thirdly, the Public Prosecution Office has the right to freeze for 30 days, instead of the vague/unlimited period set out currently, something that could be misused and cause a number of problems for the concerned customer.[80] Fourthly, the Prosecution cannot extend the freezing period by its own decision, but should seek the extension from the competent Court. This means that the Court will supervise and observe all STRs and freezing periods decided by the AMLSCU and the Public Prosecution Office in the interests of fairness and to avoid undue freezing. Lastly and more importantly, the FLMLC 2002 should be amended, so that criminal liability is imposed on compliance officers or employees of banks and other reporting entities, who proceed with a transaction during the period when the transaction has been frozen, except when this has been authorised.[81] The current situation is that there is no offence if they proceed with the transaction during the freezing period.

[80] Examples of such problems have been analysed in the Chap. 9.

[81] Under the UK SARs regime, s.336 (5–6) of the POCA 2002 provides that a nominated officer will commit an offence if he granted consent to do the prohibited act, although he knows or suspects that he has to obtain actual consent from the NCA or deemed consent. See (n 1119) of Chap. 8.

Recommendations on the Relationship of the AMLSCU With the Reporting Entities, LEAs and the Prosecution

The Relationship of the AMLSCU with the Reporting Entities

Article 17 of the CBR 24/2000 provides that the Central Bank is responsible for running workshops for employees of banks and other financial institutions. A compliance officer and other relevant employees within the financial institutions have to attend training courses about STRs/AML, which are run by the Central Bank. Currently, the Central Bank runs irregular seminars on AML for the banks and other financial institutions. It has been noted that the compliance officers in the banks suffer from a lack of professional training; this was evidenced by the absence or the negative role of the compliance officers in the banks mentioned in the two cases analysed in Chap. 5.[82]

In order to provide periodical training courses, the AMLSCU should take the responsibility of providing these courses to the compliance officers and other relevant employees at banks and all reporting entities, such as insurance companies, which are supervised by the Insurance Authority, and companies and institutions which are licensed by the ESCA. The AMLSCU should also publish periodical typologies and guidance based on STRs received from the reporting entities. It should arrange workshops, seminars and training courses on a semi-annual basis according to the reporting sector. For instance, the training courses for the compliance officers who work in the banks and financial institutions should differ from training courses for those who work in the insurance companies. The AMLSCU has professional knowledge and skills and it is in ideal position to gather valuable data on STRs, which make it possible to identify deficiencies contained in STRs received from reporting entities. In such a way, the quality of STRs submitted by the reporting entities will be improved and it will be assured that the cooperation between the AMLSCU and the reporting entities is improved since all of them are working within the STRs regime on ML.

[82] Namely cases no. 2901/2005 and no. 370/2008 of Dubai Court Judgments, Criminal Division.

The Relationship of the AMLSCU with the LEAs and the Prosecution

The current situation is that there is no e-communication network between the AMLSCU and the Public Prosecution Office. There is also no e-communication network between the AMLSCU and the Police for information exchange. On the other hand, the FATF Recommendation 2 requires that policy-makers and all competent authorities, such as the FIU, LEAs and supervisors should domestically co-ordinate and co-operate with each other at the operational level. The absence of an e-communication network between the ALMSCU and the LEAs has resulted in decisions not having been taken promptly. This is highlighted by the fact that it normally takes 3–4 months when the Public Prosecution Office asks the AMLSCU for additional information.[83] Similarly, when a STR file is investigated, the police may require additional information from the AMLSCU, but it usually takes a very long time before a response is received.[84]

There is an urgent need to establish an encrypted e-communication network between the AMLSCU and the Public Prosecution Office and the LEAs, such as the Ministry of Interior and local police in the cities,[85] the Customs Authority and others. Such an encrypted e-communication network has a number of advantages in exchanging information between the AMLSCU and those entities and this saves time.

More importantly, the AMLSCU should utilise such an e-link to play a positive role in assisting the LEAs to investigate STRs disseminated by the AMLSCU. Therefore, the AMLSCU should establish a secure system, which stores all the results of the STRs analyses by the AMLSCU. The LEAs should have a secure access to this system so as to assist them when investigating STRs when they need specific information, such as that about a suspected person/property.[86] The LEAs can exploit the proposed program by identifying relevant intelligence, enabling them to take the

[83] As Mr. L stated in Chap. 6.

[84] As Mr. N stated in Chap. 6.

[85] Which are in Abu Dhabi, Dubai and Ras Al Khaimah.

[86] Similar to ARENA model in the UK's system.

appropriate decision/action without spending too much time on conducting research. The Cross-Authorities Cooperation Section,[87] in the AMLSCU, should take the responsibility of establishing such program.

Conclusion

The UAE government has made great efforts to improve AML controls and regulations, especially after issuing its MER. These efforts are evidenced by a number of regulations, for example, the Central Bank Addendum 2922/2008. This Addendum addresses a number of issues, such as CDD and ECDD procedures, beneficial ownership, shell banks and companies and correspondent banks. Nevertheless, the FLMLC 2002 and the AML regulations still lack clarity in relation to the role, which the AMLSCU plays in counteracting ML and the STRs requirements should be also further clarified, especially in light of the 2012 FATF Recommendations. The FLMLC 2002 does not address the AMLSCU's role sufficiently. Therefore, the current administrative model of the UAE FIU suffers from a large number of problems. Such problems are embodied in doubts on its independence, its role in analysing STRs efficiently and its human resources. In addition, there is a lack of legislation in relation to the authority of the AMLSCU in dealing with the STRs, such as its authority to obtain additional information/document(s) from the reporting entities and the LEAs. The AMLSCU also does not play a vital role in increasing the capability of banks and other reporting entities to detect STRs. Furthermore, it does not constructively participate in assisting LEAs and the Public Prosecution Office to investigate and prosecute STRs.

All of the aforementioned dilemmas and others[88] have negatively affected the effectiveness of the AMLSCU and hampered compliance with the FATF Recommendations. Therefore, it is difficult, if not impossible, to retain the current model of the UAE FIU without modification.

The UK FIU law enforcement model has been analysed in this research in order to utilise ideas from this innovative model and to

[87] See (n 746) of Chap. 6.

[88] Which have been analysed throughout Chaps. 5 and 6.

consider the chances of success if the same model was adopted for the UAE FIU. Indeed, the UK FIU has achieved great success in dealing with SARs, its vital role in increasing the quality of SARs received from the reporting entities and its constructive relationship with the reporting entities and the LEAs. This success gives impetus to the idea of adopting the same model for the AMLSCU in the UAE. However, it is not easy to adopt the UK FIU model entirely due to major problem. Although the model has been a success within the UK, it does not necessarily mean that the model will achieve the same success in another country, since the form of a FIU depends on the particular conditions and circumstances of individual countries. Therefore, it is difficult to adopt the entire UK FIU law enforcement model for the AMLSCU or the law enforcement model in general due to the UAE's circumstances and conditions, which are different from the UK. Moreover, the special nature of the UAE's police system makes it difficult to adopt the law enforcement model since in addition to the Federal Police (the Ministry of Interior) which is in charge of a number of cities; there are a number of other cities, which have their own local police departments, such as Dubai. If the AMLSCU was merged with the Ministry of Interior, then the AMLSCU will not receive STRs from the reporting entities which are located in Dubai, since Dubai has its own police system and operates independently from the Ministry of Interior. Alternatively, more than one FIU would have to be established in the UAE in order to accommodate all police systems, which conflicts with FATF Recommendation 29.

On the other hand, when considering the judicial FIU model, it is difficult to adopt such a model for the AMLSCU due to the nature of the UAE's judicial system and international standards considerations. The judicial system in the UAE is based on prosecution and courts proceedings. In addition to the federal judicial system, which is applied to a number of cities, some cities also have their own judicial systems and thus have their own office of prosecution and courts. Hence, it is difficult to merge the AMLSCU within the UAE's judicial system since it would not receive all STRs from the reporting entities from the seven cities of the UAE. Alternatively more than one FIU in the UAE would have to be established in order to accommodate all judicial systems, which also conflicts with FATF Recommendation 29.

As a result, one option remains, namely adopting the hybrid FIU model which could achieve success. This option is based on utilising the benefits of the UK FIU law enforcement model and combining it with the administrative model in order to establish a new model for the UAE FIU that comprises the advantages of both models in a way, which does not conflict with the UAE's situation and legal system. Indeed, the core of the proposal is that the AMLSCU should be transferred to the Ministry of Finance. Two key justifications support this proposal. Firstly, the Ministry of Finance (unlike the Central Bank) does not have any supervisory or regulatory authority over the reporting entities. The current situation, namely that the AMLSCU is based within the Central Bank, has negatively affected the AMLSCU in terms of its independence. This is because most STRs have been analysed by banking supervision employees of the BSED in the Central Bank, despite them not being members of the AMLSCU. Central Bank's employees were thus given the authority to analyse STRs; however this breaches Article 8 of the FLMLC 2002, which only confers this power on AMLSCU's staff. In addition, those employees do not possess the required skills and experience to analyse STRs and this has negatively affected the analytical function of the AMLSCU. Secondly, the Ministry of Finance is the best institute to cooperate with the AMLSCU on the issue of asset recovery, especially if a laundered property has to be returned to the government. However, the proposed UAE FIU hybrid model suggests that it should have its own budget separate from the Ministry of Finance. In addition, it should be accountable to the NAMLC.

The proposed UAE FIU hybrid model will not achieve success, be effective in the STRs regime and fulfil the relevant FATF Recommendations, unless a number of amendments/revisions are made in relation to the statutory provisions, regulations and the organisational structure of the AMLSCU.

Firstly, the definition of ML contained in the CBR 24/2000 is different from that contained in the FLMLC 2002. This causes uncertainty for the reporting entities; most notably for banks and courts. The definition of ML, contained in CBR 24/2000, covers money which is intended to be used for FT or criminal acts, even if this money comes from legitimate business activities. However, a judge cannot hold a person criminally

responsible in such a case. This is because the FLMLC 2002 provides that the money/property must emanate from the commission of one or more of the predicate offence(s) for ML listed in the Act. In addition, the list of predicate offences for ML set out in the FLMLC 2002 should be extended to comprise the minimum list of offences as defined in the General Glossary of the FATF Recommendations, as otherwise the relevant FATF Recommendations are not completely fulfilled.

Secondly, the CBR 24/2000 establishes "reasonable grounds to suspect" as a basis for STRs, whilst the FLMLC 2002 requires actual knowledge. In other words, under the FLMLC 2002, the basis for submitting STRs is subjective, whilst the CBR 24/2000 imposes an objective standard. This conflict between the FLMLC 2002 and the AML regulations has caused confusion for banks. It has increased the number of STRs submitted to the AMLSCU, which is clearly evidenced by the huge difference between the number of STRs received by the AMLSCU and the number of STRs, which have been transmitted to the Public Prosecutions Office between June 2002 and May 2009. The discrepancy is because reporting entities are confused about the basis for submitting STRs and accordingly have adopted a defensive approach to ensure that they are safe and do not commit the failure to report offence contained in the FLMLC 2002.

Indeed, the FLMLC 2002 and the AML regulations have to be consistent and any ambiguity has to be avoided. The FLMLC 2002 and AML regulations should adopt an objective basis, namely reasonable grounds for knowledge or suspicion and a subjective basis, namely just actual knowledge. "Suspicion" should not be a ground to submit a STR since the term is too broad and gives rise to abuse.

Thirdly, the following sections should be amended/added in relation to AMLSCU's organisational set up:

1. The analytical function should be transferred from the STR Analysis and STR Database Management Section to a separate section specialised in analysing STRs and which should be called the Analytical Section. This is important since the analytical function constitutes the backbone of the AMLSCU.

2. The International Cooperation Section should make greater efforts to ensure that the relevant FATF Recommendations are fulfilled, especially in light of the 2012 revision of FATF Recommendations.
3. The Training and Development Section should be established within the AMLSCU and take responsibility for the following tasks:

   A. Provide training courses and arrange seminars for AMLSCU's staff, notably analysts who are responsible for analysing STRs,
   B. Provide training courses and arrange workshops and seminars for compliance officers, who work in banks and other financial institutions,
   C. Provide general and case specific feedback to the reporting entities.

4. A provision should be added to the FLMLC 2002 in order to establish a separate section called the "Asset Recovery Section" in the AMLSCU and to coordinate matters with the Ministry of Finance. The Ministry of Finance is best placed to cooperate with the AMLSCU when it comes to assets recovery issues, especially if laundered proceeds have to be returned to the government.

In addition, the AMLSCU should have sufficient human resources and experts in order to accommodate its responsibilities. It should provide semi-annual training courses and workshops to its staff, so that they are kept abreast of new forms of sophisticated ML transactions/activities. More importantly, strategic partnerships have to be formed with a number of LEAs, such as the police, the customs authority and public prosecution, so that the AMLSCU can utilise their experience.

Furthermore, it should be the responsibility of a specific committee, "the STRs Regime Committee," to provide valuable and comprehensive statistics about STRs on ML and to prepare and issue annual reports. This STRs Committee should be associated with the AMLSCU. However, the members of this committee should not just come from the AMLSCU, but also from strategic partners, namely LEAs and reporting entities. The annual reports should be made publically available via the AMLSCU's website with a view to increasing public awareness about ML.

Fourthly, in order to enhance the independence of the AMLSCU, it should be entirely detached from the Ministry of Finance with regard to its budget and human resources. Furthermore, the Head of the AMLSCU should be appointed by the Ministry of Finance, as long as the AMLSCU is located within this ministry. However, the AMLSCU should not be accountable to the Ministry of Finance, but instead should be accountable to another entity, which could also develop AMLSCU's policies. The AMLSCU could be accountable to the NAMLC with a view to ensuring that the AMLSCU is accountable to an independent body, which is specialised in AML affairs at the national level. The AMLSCU would have to provide its annual reports and the reports which contain results of strategic analysis to the NAMLC in order to assist the NAMLC in evaluating the overall policy of the AMLSCU, as well as future work. By adopting this proposal, it would be ensured that the NAMLC plays a greater AML role at the national level since one of its responsibilities is proposing AML regulations and controls.

Fifthly, the FLMLC 2002 should clarify the core functions of the AMLSCU to deal with STR. It should explicitly 1) require the AMLSCU to store all STRs, which it receives from the reporting entities, on its own database and 2) grant authority to the AMLSCU to require additional information/document(s) from the relevant reporting entities and LEAs, if such information/document(s) assists with analysing STRs. Moreover, the AMLSCU should be equipped with the power to authorise the freezing of suspicious transactions since it has knowledge about relevant STRs and is therefore best placed to exercise such a power. Indeed, granting such power is one of the advantages of the FIU law enforcement model.

Sixthly, the AMLSCU should improve its relationship and partnership with the reporting entities and the end users of the STRs, namely the LEAs. This should be achieved through the following:

1. The AMLSCU has to provide the reporting entities general and case specific feedback and guidelines. Otherwise, the quality of STRs will not improve if the AMLSCU cannot point out deficiencies of previous STRs. Equally, the AMLSCU should provide LEAs with questionnaires in order to receive feedback about the STRs regime,

so that their knowledge/experience about the operation of the STRs regime can be shared with the AMLSU, which also helps in providing feedback to the reporting entities.
2. An encrypted e-communication network has to be established by the AMLSCU with the Public Prosecution Office and the LEAs, such as the Ministry of Interior and local police departments in the cities, the Customs Authority and others. Such an encrypted e-communication network has a number of advantages, most notably facilitates the exchange of information between the AMLSCU and those entities, thereby also saving crucial time.
3. More importantly, the AMLSCU should utilise this secure e-link and store all results from the STRs analyses, which have been conducted by the AMLSCU, within this system. The LEAs should have secure access to this system to assist with the investigation of STRs when specific information is required.

Lastly, the FLMLC 2002 should criminalise the compliance officer or any employee in the banks and other reporting entities, if he proceeds with the transaction during the freezing period before the end of such period or without receiving permission. Currently, this is not outlawed.

It remains to mention that the sproposed UAE FIU hybrid model opens the door for future research in the area of the role of the AMLSCU in asset recovery while cooperating with the Ministry of Finance. Moreover, the proposal provides the consideration for the possibility of merging the NAMLC and the NCCT in one national committee and for the AMLSCU to be accountable to such committee. This, in turn, leads to further considerations of the possibility of applying the provided recommendations on the role of the UAE FIU in combating terrorism since the UAE FIU analyses STRs not only on ML, but also TF.

Bibliography

Books

Ali, S. A. (2003). *Money laundering control in the Caribbean*. London: Kluwer Law International.

Antoine, R.-M. (2002). *Confidentiality in offshore financial law* (1st ed.). Oxford/New York: Oxford University Press.

Blair, W., & Brent, R. (2008). Regulatory responsibilities. In W. Blair & R. Brent (Eds.), *Banks and financial crime: The international law of tainted money* (p. 241). Oxford/New York: Oxford University Press.

Booth, R., & others. (2011). *Money laundering law and regulation: A practical guide.* First Published, Oxford University Press.

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford: Oxford University Press.

Chambers English Dictionary, (Cambridge & Edinburgh 1988).

Clark, A., & Russell, M. (2003). Reporting regimes. In A. Clark & P. Burrell (Eds.), *A practitioner's guide to international money laundering law and regulation* (p. 115). Old Woking: City & Financial Publishing.

Commonwealth Secretariat. (2006). *Combating money laundering and terrorist financing: A model of best practice for the financial sector, the professions and other designated businesses* (2nd ed.). London: Commonwealth Secretariat.

W. Alhosani, *Anti-Money Laundering*,
DOI 10.1057/978-1-137-59455-6

Cranston, R. (2002). *Principles of banking law* (2nd ed.). Oxford: Oxford University Press.

Creswell, J. W. (2014). *Research design* (4th ed.). Thousand Oaks: SAGE Publications Ltd.

D'Souza, J. (2012). *Terrorist financing, money laundering, and tax evasion- examining the performance of financial intelligence unit*. Boca Raton: Taylor and Francis Group, LLC.

Damais, A. (2007). The financial action task force. In W. H. Muller, C. H. Kalin, & J. G. Goldsworth (Eds.), *Anti-money laundering: International law and practice* (p. 69). Chichester: Wiley.

Dannemann, G. (2008). Comparative law: Study of similarities and differences? In M. Reimann & R. Zimmermann (Eds.), *The Oxford handbook of comparative law* (p. 383). Oxford/New York : Oxford University Press.

Ellinger, E. P., Lomnicka, E., & Hare, C. V. M. (2011). *Ellinger's modern banking law* (5th ed.). Oxford: Oxford University Press.

Fisher, J. (2010a). UK Part IV: Confiscating the proceeds of crime. In M. Simpson, N. Smith, & A. Srivastava (Eds.), *International guide to money laundering law and practice* (3rd ed., p. 145). Haywards Heath: Bloomsbury Professional.

Fortson, R. (2008). Money laundering offences under POCA 2002. In W. Blair & R. Brent (Eds.), *Banks and financial crime: The international law of tainted money* (p. 155). Oxford/New York: Oxford University Press.

Ghattas, H. (2010). United Arab Emirates. In M. Simpson, N. Smith, & A. Srivastava (Eds.), *International guide to money laundering law and practice* (3rd ed., p. 1049). Haywards Heath: Bloomsbury Professional.

Gilmore, W. C. (2011). *Dirty money—The evaluation of international measures to counter money laundering and the financing of terrorism* (4th ed.). Strasbourg: Council of Europe.

Harrison, K., & Ryder, N. (2013). *The law relating to financial crime in the United Kingdom*. Farnham/Burlington: Ashgate Publishing Limited.

Hopton, D. (2009). *Money laundering, A concise guide for all business* (2nd ed.). Surrey: Gower Publishing Limited.

Hudson, A. (2013). *The law of finance* (2nd ed.). London: Sweet & Maxwell.

Hynes, P., Rudolf, N., & Furlong, R. (2009). *International money laundering and terrorist financing: A UK perspective* (1st ed.). London: Sweet & Maxwell/ Thomson Reuters.

International Monetary Fund. (2004). *Financial intelligence units.* 2004*: An overview*. International Monetary Fund Handbook. Available online at http://www.imf.org/external/pubs/ft/fiu/fiu.pdf

Jamall, A. (2003). Gulf Cooperation Council. In A. Clark & P. Burrell (Eds.), *A practitioner's guide to international money laundering law and regulation* (p. 665). Old Woking: City & Financial Publishing.

Knoblaunch, H., & Tuma, R. (2011). Videography: An interpretive approach to video-recorded macro-social interaction. In E. Margolis & L. Pauwels (Eds.), *The Sage handbook of visual research methods* (p. 414). London: SAGE Publications Ltd.

Kumar, R. (2011). *Research methodology* (3rd ed.). London: SAGE Publications Ltd.

Leong, A. (2007). *The disruption of international organised crime : An analysis of legal and non-legal strategies*. Aldershot: Ashgate Publishing Limited.

Lomio, J. P., Spang-Hanssen, H., Wilson, H., & Wilson, G. D. (2011). *Legal research methods in a modern world: A coursebook* (3rd ed.). Copenhagen: DJØF Publishing.

Lovett, G., & Barwick, C. (2007). United Arab Emirates. In W. H. Muller, C. H. Kalin, & J. G. Goldsworth (Eds.), *Anti-money laundering: International law and practice* (p. 643). Chichester: Wiley.

Muller, W. (2007). The Egmont group. In W. H. Muller, C. H. Kalin, & J. G. Goldsworth (Eds.), *Anti-money laundering: International law and practice* (p. 83). Chichester: Wiley.

Örücü, E. (2007). Developing comparative law. In E. Örücü & N. David (Eds.), *Comparative law: A handbook* (p. 43). Oxford/Portland: Hart.

Pang, A.-c. (2008). International legal sources III-FATF recommendations. In W. Blair & R. Brent (Eds.), *Banks and financial crime: The international law of tainted money* (p. 87). Oxford: Oxford University Press.

Peter, C. (1999). *Consumer protection in financial services* (International banking, finance & economic law). The Hague/Boston: Kluwer Law International.

Proctor, C. (2010). *The law and practice of international banking*. Oxford/New York: Oxford University Press.

Ryder, N. (2011). *Financial crime in the 1st century: Law and policy*. Northampton: Edward Elgar Publishing Limited.

Ryder, N. (2012). *Money laundering—An endless cycle?* First Published. Oxford: Routledge Cavendish.

Salter, M., & Mason, J. (2007). *Writing law dissertations*. First Published. Oxford: Pearson Education Limited.

Schott, P. A. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism* (Supplement on special recommendation IX 2nd ed.). Washington, DC: The World Bank.

Simpson, M. (2010). International initiatives. In M. Simpson, N. Smith, & A. Srivastava (Eds.), *International guide to money laundering law and practice* (3rd ed., p. 193). Haywards Heath: Bloomsbury Professional.

Simpson, M., & Smith, N. (2010). UK Part III: Practical implementation of regulations and rules. In M. Simpson, N. Smith, & A. Srivastava (Eds.), *International guide to money laundering law and practice* (3rd ed., p. 95). Haywards Heath: Bloomsbury Professional.

Srivastava, A. (2010). UK Part II: UK law and practice. In M. Simpson, N. Smith, & A. Srivastava (Eds.), *International guide to money laundering law and practice* (3rd ed., p. 27). Haywards Heath: Bloomsbury Professional.

Turner, J. E. (2011). *Money laundering prevention: Deterring, detecting and resolving financial fraud*. Hoboken: Wiley.

Ulph, J., & Tugendhath, M. (2006). *Commercial fraud. Civil liability, human rights and money laundering* (1st ed.). Oxford: Oxford University Press.

Webley, L. (2010). Qualitative approaches to empirical legal research. In P. Cane & H. M. Kritzer (Eds.), *The Oxford handbook of empirical legal research* (p. 26). Oxford/New York: Oxford University Press.

Wilson, G. (2007). Comparative legal scholarship. In M. McConville & W. H. Chui (Eds.), *Research methods for law* (p. 87). Edinburgh: Edinburgh University Press.

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Los Angeles: SAGE Publications.

Zweigert, K., & Kötz, H. (1998). *An introduction to comparative law*. New York: Oxford University Press.

Journal Articles

Akbari, P., Rostami, R., & Veismoradi, A. (2012, September). Study of factors influencing customer's use of electronic banking services by using Pikkarainens Model (Case Study: Refah Bank of Kermanshah, Iran). *International Research Journal of Applied and Basic Sciences, 3*(5), 950. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145494

Aldhouse, F. (2007, February). DPA section 55: Securing convictions. The Newsletter for Data Protection Professionals, *4*(2), 10. Available online at http://www.e-comlaw.com/data-protection-law-and-policy/article_template.asp?ID=351&Search=Yes&txtsearch=going

Alkaabi, A., & others. (2010). A comparative analysis of the extent of money laundering in Australia, UAE, UK and the USA [January 20, 2010] Finance and corporate governance conference 2010 paper 1. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539843

Alqudah, F. (1995). Banks' duty of confidentiality in the wake of computerised banking. *Journal of International Banking Law, 10*(2), 50.

Bell, E. (2009). Concealing and disguising the criminal property. *Journal of Money Laundering Control, 12*(3), 268.

Borlini, L. (2008). Issues of the international criminal regulation of money laundering in the context of economic globalization [November 1, 2008] paper no. 2008-34 Paolo Baffi Centre Research 1. Available online at http://ssrn.com/abstract=1296636

Bowling, B., & Ross, J. (2006, December). The Serious Organised Crime Agency—should we be afraid?. *Criminal Law Review,* 1019.

Brown, G., & Evans, T. (2008). The impact: The breadth and depth of the anti-money laundering provisions requiring reporting of suspicious activities. *Journal of International Banking Law and Regulation, 23*(5), 274.

Buchanan, B. (2004). Money laundering- a global obstacle. *Research in International Business and Finance, 18*(1), 115.

Campbell, A. (2000). The financial services authority and the prevention of money laundering. *Journal of Money Laundering Control, 4*(1), 7.

Chaikin, D. (2009). How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control, 12*(3), 238.

De Koker, L. (2006). Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of customer due diligence measures on financial exclusion. *Journal of Financial Crime, 13*(1), 26.

Diaz Andrade, A. (2009, March). Interpretive research aiming at theory building: Adopting and adapting the case study design. *The qualitative Report, 14*(1), 42. Available online at http://www.nova.edu/ssss/QR/QR14-1/diaz-andrade.pdf

Fisher, J. (2010b). The anti-money laundering disclosure regime and the collection of revenue in the United Kingdom. *British Tax Review, 3*, 235.

Gathii, J. T. (2010). The financial action task force and Global Administrative Law. paper no. 10-10 Journal of the Professional Lawyer, Forthcoming; Albany Law School Research 1. Available online at http://ssrn.com/abstract=1621877

Gentle, S. (2008). 'Proceeds of Crime Act 2002: update' (2008) 56 (May) Compliance Officer Bulletin 1.

George, B. C., & Lacey, K. A. (2003, January 1). Crackdown on money laundering: A comparative analysis of the feasibility and effectiveness of domestic and multilateral policy reforms. *Northwestern Journal of International Law & Business*, *23*(2), 1. Available online at http://ssrn.com/abstract=1431264

Gordon, R. K. (2010, May 4). Losing the war against dirty money: Rethinking global standards on preventing money laundering and terrorism financing, Paper no. 2010-20 Case Legal Studies Research 1. Available online at: http://ssrn.com/abstract=1600348

Harfield, C. (2006). SOCA: A paradigm shift in British policing. *British Journal of Criminology, 46*(4), 743.

Hay, R, (2002). Offshore financial centres: The supranational initiatives. *Private Client Business, 2*, 75.

James, H. F. (2008, April 25). Global markets and global vulnerabilities: Fighting transnational crime through financial intelligence. Financial crimes enforcement networks U.S. Department of the Treasury 1. Available online at http://www.fincen.gov/news_room/speech/html/20080425.html

Jensen, N., & Ann, P. -C. (2011). Implementation of the FATF 40 + 9 recommendations: A perspective from developing countries. *Journal of Money Laundering Control, 14*(2), 110.

Joan, W. (1990). Bank's confidentiality: A much reduced duty (1990) 106 (Apr) Law Quarterly Review 204.

Johnson, J. (2008). Little enthusiasm for enhanced CDD of the politically connected. *Journal of Money Laundering Control, 11*(4), 291.

Jun, T., & Ai, L. (2009). The international standards of criminal due diligence and Chinese practice. *Journal of Money Laundering Control, 12*(4), 406.

Kassean, H., Gungaphul, M., & Murughesan, D. (2012). Consumer buyer behaviour: The role of internet banking in Mauritius. European business research conference proceedings. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2131206

Khan, M. Z. (2011, April 20). An analysis of duty of confidentiality owed by banker to its customers. 1. Available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1815825

Latimer, P. (2004). Bank secrecy in Australia: Terrorism legislation as the new exception to the Tournier rule. *Journal of Money Laundering Control, 8*(1), 56.

Marshall, P. (2010). Does Shah v HSBC Private Bank Ltd make the anti-money laundering consent regime unworkable? *Journal of International Banking and Financial Law, 25*(5), 287.

McCluskey, D. (2009). Money laundering: The disappearing predicate. *Criminal Law Review, 10*, 719.

Mugarura, N. (2011). The institutional framework against money laundering and it s underlying predicate crimes. *Journal of Financial Regulation and Compliance, 19*(2), 174.

Murray, K. (2012). A suitable case for treatment: Money laundering and knowledge. *Journal of Money Laundering Control, 15*(2), 188.

Ping, H. E. (2008). The measures on combating money laundering and terrorist financing in the PRC: From the perspective of financial action task force. *Journal of Money Laundering Control, 11*(4), 320.

Preller, S. F. (2008). Comparing AML legislation of the UK, Switzerland and Germany. *Journal of Money Laundering Control, 11*(3), 234.

Radmore, E. (2013, May). Deferred prosecution agreements—For more enforcement action?. Financial Regulation International 1. Available online at http://www.dentons.com/insights/ s/2013/june/18/deferred-prosecution-agreements-for-more-enforcement-action

Realuyo, C. B. (2012, May). It's all about the money: Advancing anti-money laundering efforts in the U.S. and Mexico to Combat Transnational Organized Crime. Woodrow Wilson International Centre for Scholars, Mexico Institute. Available online at: http://www.wilsoncenter.org/sites/default/files/Realuyo_U.S.-Mexico_Money_Laundering_0.pdf

Ruce, P. J. (2011a, December 5). The Bank Secrecy Act: Considerations for continuing banking relationships after the filing of a suspicious activity report. *Quinnipiac Law Review, 30*(1), 43. Available online at http://ssrn.com/abstract=1968413

Ruce, P. J. (2011b, July/August). The Bank Secrecy Act: The Not-so-Safe Harbor Provision and the Whitney rule's double standard for SAR supporting documentation. Financial Fraud Law Report, *3*(7), 608. Available online at http://ssrn.com/abstract=1866455

Ryder, N. (2008). The Financial Services Authority and money laundering: A game of cat and mouse. *Cambridge Law Journal, 67*(3), 635.

Scott, K. A., & Stephenson, R. (2008). Enhanced customer due diligence for banks in the UK and the US. *Journal of International Banking and Financial Law, 23*(2), 89.

Shehu, A. Y. (2010). Promoting financial sector stability through an effective AML/CFT regime. *Journal of Money Laundering Control, 13*(2), 139.

Simonova, A. (2011). The risk-based approach to anti-money laundering: Problems and solutions. *Journal of Money Laundering Control, 14*(4), 346.

Stanton, K. (2010). Money laundering: A limited remedy for clients. *Professional Negligence, 26*(1), 56.

Stokes, R. (2007, August). The banker's duty of confidentiality, money laundering and the Human Rights Act. *Journal of Business Law*, 502.

Stokes, R. (2011). The Genesis of Banking confidentiality. *The Journal of Legal History, 32*(3), 279.

Stokes, R., & Arora, A. (2004, May). The duty to report under the money laundering legislation within the United Kingdom. *Journal of Business Law,* 332.
Stott, C., & Ullah, Z. (2008). Money Laundering Regulations 2007: Part 1. *Journal of International Banking Law and Regulation, 23*(3), 175.
Strauss, K. (2010, November). The situation of Financial Intelligence Units in Central and Eastern Europe and the Former Soviet Union. Working paper series no 09. Basel Institute on Governance. Available online at http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN044510.pdf
Tan, J. (2011). Can we still bank on secrecy? *Journal of International Banking and Finance Law, 26*(9), 564.
Terry, L. S. (2010). An introduction to the Financial Action Task Force and its 2008 Lawyer Guidance. *Journal of the Professional Lawyer, 3*. Available online at http://ssrn.com/abstract=1680555
Vibhute, K., & Aynalem, F. (2009). Legal Research Methods. Prepared under the sponsorship of the Justice and Legal System Research Institute. Available online at http://chilot.files.wordpress.com/2011/06/legal-research-methods.pdf
Wright, J. (2010). Introduction to amended guideline 12 (the Proceeds of Crime Act) and new guideline on the formalities for Drafting an Award. *Arbitration, 76*(2), 291.

Empirical Data

Interview with Mr. A, who works as a "Senior STR Analyst" in the Anti-Money Laundering and Suspicious Cases Unit.
Interview with Mr. L, who is the chief Dubai Public Prosecutor.
Interview with Mr. N, who works as an Officer in the Anti-Money Laundering and financial crime section at Dubai police.
Interview with Mr. Z and Mr. S, who work as a "Compliance Officer" in domestic banks in the UAE.
Semi-structured interviews conducted between March and May 2012.

Reports

Advisory notice on money laundering and terrorist financing controls in Overseas Jurisdictions issued by the HM Treasury. Available online at http://www.hm-treasury.gov.uk/d/advisory_notice_moneylaundering_nov2012.pdf

AMLSCU Annual Report—2009 as produced by the AMLSCU.
AMLSCU Annual Report—2010 as produced by the AMLSCU.
An introduction to the FATF and its work 2010, available on the FATF website at www.fatf-gafi.org
NCA Annual Plan 2013-14 as produced by the NCA in October 2013.
Camdessus, M. (1998). Money laundering: The importance of International Countermeasures as presented at the Plenary Meeting of the FATF on ML in Paris February 10, 1998. Available online at http://www.imf.org/external/np/speeches/1998/021098.htm
Egmont Group. (2004, September). Information Paper on Financial Intelligence Units and the Egmont Group. Available on the Egmont Group website at www.egmontgroup.org
FATF members and observers. Available online at http://www.fatf-gafi.org/pages/aboutus/membersandobservers
FATF membership policy, 29 February 2008. Available on the FATF website at www.fatf-gafi.org
FATF policy on observers, June 2008. Available on the FATF website at www.fatf-gafi.org
FATF Public statement, High-risk and non-cooperative jurisdictions, jurisdictions for which an FATF call for action applies published by the FATF on 18 October 2013. Available online at http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatf-public-statement-oct-2013.html
FATF Report. (2009, July). Money Laundering through the Football Sector. Available online at http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20through%20the%20Football%20Sector.pdf
FATF Report. (2010, October). Money laundering using new payment methods. Available online at http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf
FATF Report. (2010, July). Global Money Laundering and Terrorist Financing Threat Assessment. Available online at http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf
FATF revised mandate. (2008–2012). Available on the FATF website at www.fatf-gafi.org
Financial Action Task Force Mandate. (2012–2020). 20 April 2012. Available on the FATF website at www.fatf-gafi.org
Financial Conduct Authority. The Banking Conduct Regime. Available online at http://www.fca.org.uk/firms/being-regulated/banking/Conduct-regime
HM Government Report. (2010, October). A Strong Britain in an Age of Uncertainty: The National Security Strategy, Presented to Parliament by the

Prime Minister by Command of HM. Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

Home Office Report. (2011, June). The National Crime Agency- A plan for the creation of a national crime-fighting capability, Presented to Parliament by the Secretary of State for the Home Department by Command of HM. Available on the Home Office website at www.homeoffice.gov.uk

Kingdom of Saudi Arabia Mutual Evaluation Report. Anti-money laundering and combating the financing of terrorism as produced by the FATF on 25 June 2010.

Mandate for the Future of the FATF, September 2004—December 2012. Available on the FATF website at www.fatf-gafi.org

One Step Ahead—A 21st century strategy to defeat organised crime as produced by the Home Office in March 2004. Available online at www.soca.gov.uk/about-soca/library/doc…/67-one-step-ahead

SOCA annual Plan 2013/14 as produced by the SOCA on 28 March 2013.

FATF Public Statement, High-risk and non-cooperative jurisdictions published by the FATF on 19 October 2012. Available online at http://www.fatf-gafi.org/media/fatf/documents/FATF%20Public%20Statement%2019%20October%202012.pdf

QATAR Mutual Evaluation Report. Anti-money laundering and combating the financing of terrorism as produced by the FATF on 9 April 2008.

FATF Reference Document, Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems February 2013. Available on the FATF website at: www.fatf-gafi.org

FATF Reference Document, Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations October 2013. Available online at www.fatf-gafi.org/media/fatf/…/FATF-4th-Round-Procedures.pdf

FATF Reference Document, Methodology for Assessing Compliance with the FATF 40 Recommendations and FATF 9 Special Recommendations 27 February 2004 (Updated as of February 2009). Available on the FATF website at www.fatf-gafi.org

Sir Lander, S. Review of the suspicious activity reports regime as produced by the SOCA in March 2006. Available on the SOCA's website at www.soca.gov.uk

Suspicious Activity Reports Regime, Annual Report 2010 as produced by the SOCA.

Suspicious Activity Reports Regime, Annual Report 2011 as produced by the SOCA.

Suspicious Activity Reports Regime, Annual Report 2012 as produced by the SOCA.

Suspicious Activity Reports Regime, Annual Report 2013 as produced by the NCA.

The Egmont Group Annual Report. (2012–2013). Available online at www.egmontgroup.org/library/download/314

The Egmont Group Annual Report. (June 2009–July 2010). Available online at www.egmontgroup.org/library/download/99

The role of the Information Commissioner's Office. Available online at http://66.102.9.132/search?q=cache:QmVMbxrTq-kJ:www.ico.gov.uk/for_organisations/data_protection_guide/the_role_of_the_information_commissioners_office.aspx+right+to+request+an+assessment+by+the+ICo&cd=1&hl=en&ct=clnk&gl=uk

The United Arab Emirates Mutual Evaluation Report. Anti-money laundering and combating the financing of terrorism as produced by the FATF on 20 June 2008.

The United Kingdom Third Mutual Evaluation Report. Anti-money laundering and combating the financing of terrorism as produced by the FATF 29 June 2007.

UK FIU bulletin. Compliance and the Consent Regime as produced by the UK FIU in February 2011. Available on the SOCA's website at www.soca.gov.uk

UK FIU bulletin. Suspicious Activity Reports (SARs)—Top ten tips for the Accountancy Sector. Available on the SOCA's website at www.soca.gov.uk

Speeches and Conference Papers

Pereira, A. 'The role of AMLSCU in the recovery of proceeds emanating from money laundering, terrorist financing and related financial crimes' presented at the conference on (Recovery of proceeds of crime and asset sharing) in Dubai (Intercontinental Dubai Festival City) on 09th and 10th May 2012.

Newspaper Articles

Hamdan, S. (2009, June 23). Suspect funds on the rise. *The National*.

Johnston, P. (2013, October 7). The National Crime Agency: Does Britain need an FBI?. *The Telegraph*.

Miscellaneous Documents

Frequently Asked Questions (FAQs) as produced by the SOCA. Available on its website at www.soca.gov.uk

International Monetary Fund, *Financial system abuse, financial crime and money laundering—Background paper*, (International Monetary Fund 2001). Available online at http://www.imf.org/external/np/ml/2001/eng/021201.pdf

Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit. (undated). Available on the Egmont Group website at www.egmontgroup.org

Lending Standards Board, The Lending Code, Setting standards for banks, building societies and credit card providers (March 2012, revised 1st May 2012). Available online at http://www.lendingstandardsboard.org.uk/docs/lendingcode.pdf

Letter from Home Office (NCA Programme Team) in replay to one of my inquiries, received on 14 February 2012, Reference: T681/12.

Mourant. (2007, June). The duty of confidentiality: The rule and four exceptions. Available online at www.mourant.com

Proceeds of Crime Act 2002 Part 7—Money Laundering Offences (Updated 15/09/10). Available online at http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/

SOCA. FAQ and definitions. Available online on SOCA's website at www.soca.gov.uk

The Banking Code. (2008, March). Available online at http://www.bankingcode.org.uk/pdfdocs/PERSONAL_CODE_2008.PD

The Durant Case and its impact on the interpretation of the Data Protection Act 1998, Information Commissioner's Office 27/02/06. Available online at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf

The FATF Forty Recommendations. (2012, February). International Standards on Combating money laundering and the financing of terrorism & proliferation. Available online at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

UK FIU Guidance Note. Introduction to Suspicious Activity Reports (SARs) as produced by the NCA in October 2013. Available on the NCA's website at www.nationalcrimeagency.gov.uk

UK FIU Guidance Note. Reporting via SAR Online as produced by the NCA in October 2013. Available on the NCA's website at www.nationalcrimeagency.gov.uk
UK FIU Updates, New retention and deletion policy for Suspicious Activity Reports (SARs). Available on the SOCA's website at: www.soca.gov.uk

Websites

Abu Dhabi Judicial Department. www.adjd.gov.ae
Asia/Pacific Group on ML (APG). http://www.apgml.org
BBC. http://news.bbc.co.uk/1/hi/england/lancashire/6647473.stm
Caribbean Financial Action Task Force (CFATF). http://www.cfatf-gafic.org
Dubai Courts. www.dubaicourts.gov.ae
Dubai Financial Services Authority (DFSA). www.dfsa.ae
Dubai International Financial Centre (DIFC). www.difc.ae
Dubai Multi Commodities Centre (DMCC). www.dmcc.ae
Dubai Public Prosecution. www.dxbpp.gov.ae
Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). http://www.esaamlg.org
Egmont Group. www.egmontgroup.org
Eurasian Group (EAG). http://www.eurasiangroup.org
FATF. www.fatf-gafi.org
Financial Conduct Authority. www.fca.org.uk
Financial Services Authority (FSA). www.fsa.gov.uk
Her Majesty's Revenue and Customs (HMRC). www.hmrc.gov.uk
Home Office. www.homeoffice.gov.uk
Inter-Governmental Action Group against ML in West Africa (GIABA). www.giaba.org
Joint Money Laundering Steering Group (JMLSG). www.jmlsg.org.uk
Middle East and North Africa Financial Action Task Force (MENAFATF). www.menafatf.org
NCA. www.nationalcrimeagency.gov.uk
Office for Money Laundering Prevention (OMLP) in Slovenia. http://www.uppd.gov.si/en/about_the_office/
Prudential Regulation Authority. http://www.bankofengland.co.uk/PRA/Pages/default.aspx

RAK Courts Department. www.rak.ae
Securities and Commodities Authority (ESCA). www.sca.ae/english
SOCA. www.soca.gov.uk
The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). www.coe.int/moneyval
The Financial Action Task Force on ML in South America (GAFISUD). http://www.gafisud.info
The Group of International Finance Centre Supervisors (GIFCS), formally the Offshore Group of Banking Supervisors (OGBS). www.ogbs.net
UAE Central Bank. www.centralbank.ae/en/index.php
UAE Ministry of Finance. www.mof.gov.a
UAE Ministry of Justice. www.ejustice.gov.ae

Index

Note: Page numbers with "n" denote notes.

W. Alhosani, *Anti-Money Laundering,*
DOI 10.1057/978-1-137-59455-6

D

E