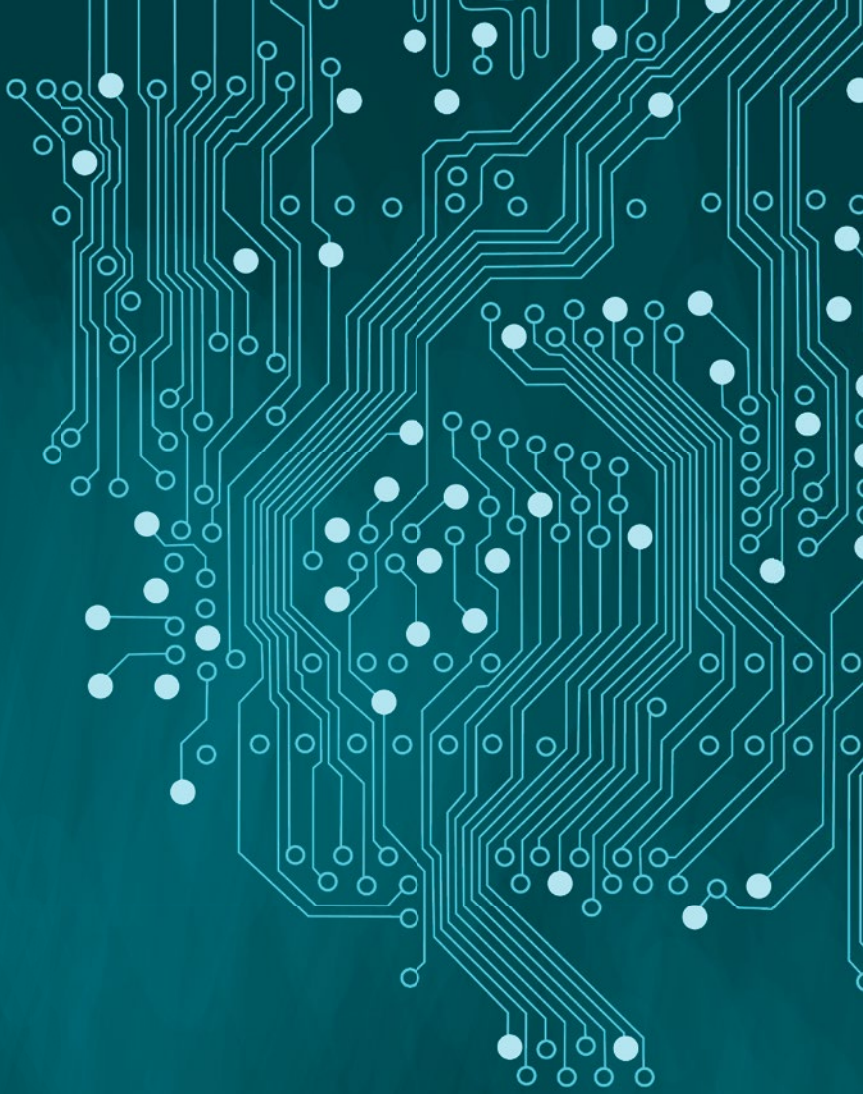
PALGRAVE ADVANCES IN THE ECONOMICS OF INNOVATION AND TECHNOLOGY



A History of Digital Currency in the United States

New Technology in an Unregulated Market

P. Carl Mullan

Palgrave Advances in the Economics of Innovation and Technology

Series Editor

Albert N. Link
Greensboro, North Carolina, USA

The focus of this series is on scholarly inquiry into the economic foundations of technologies and the market and social consequences of subsequent innovations. While much has been written about technology and innovation policy, as well as about the macroeconomic impacts of technology on economic growth and development, there remains a gap in our understanding of the processes through which R&D funding leads to successful (and unsuccessful) technologies, how technologies enter the market place, and factors associated with the market success (or lack of success) of new technologies. This series considers original research into these issues. The scope of such research includes in-depth case studies; cross-sectional and longitudinal empirical investigations using project, firm, industry, public agency, and national data; comparative studies across related technologies; diffusion studies of successful and unsuccessful innovations; and evaluation studies of the economic returns associated with public investments in the development of new technologies.

More information about this series at
http://www.springer.com/series/14716

P. Carl Mullan

A History of Digital Currency in the United States

New Technology in an Unregulated Market

palgrave
macmillan

P. Carl Mullan
Digital Currency Intelligence Authority Ltd.
White Stone, Virginia, USA

Palgrave Advances in the Economics of Innovation and Technology
ISBN 978-1-137-56869-4 ISBN 978-1-137-56870-0 (eBook)
DOI 10.1057/978-1-137-56870-0

Library of Congress Control Number: 2016957648

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Nature America Inc.
The registered company address is: 1 New York Plaza, New York, NY 10004, U.S.A.

Contents

List of Charts

CHAPTER 1

Introduction

For centuries, people of the world have used cash, such as coins and notes, as a medium of exchange. When modern economies adopted an electronic version of money, this government-issued digital value could only circulate through highly regulated banks and financial institutions. This electronic money also became a powerful government tool that provided daily control over a nation's money supply.

However, the new Internet delivered innovative methods of creating private digital versions of currency, along with many advanced methods for transferring this online value. The Internet's new decentralized features, protocols, and freedom altered the existing definition of electronic money and ushered in the concept of privately issued digital currency.

During the late 1990s, Internet entrepreneurs began to experiment building ingenious new versions of electronic money known as digital currency. Existing US financial regulations had only supervised and controlled the movement of electronic money through banks and regulated financial institutions. The new Internet digital currencies were moving locally and internationally well beyond the reach of US financial regulations and government supervision. In fact, from 1996 through 2006, some government agencies even had a difficult time identifying and defining these new financial technologies.

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_1

By 2016, there were thousands of Internet digital currency products representing money and other value, circulating alongside government-issued legal tender. In a few regions, the private digital currency has almost replaced the government's electronic version. Digital tokens have brand names, static and changing monetary values, and various features which directly compete with government-issued money and bank products.

The adoption of new financial regulations in the USA and the restrictive environment created by the new laws forced the closure of many innovative digital currency businesses. Of the nine businesses profiled in this book that operated between 1996 and 2006, only two are still operating in 2015. Seven of the digital currency systems were sidelined because of criminal activity or shut down due to US regulations. The notable exception to being "shut down" or regulated out of the business was e-gold. While the e-gold operators were convicted of multiple felonies related to the money transmitting operation and most of the company assets were forfeited, the business was never forced to close. The e-gold operation voluntarily closed down.

Only two of the nine companies, which had been early entries in the marketplace survived the changing rules and unregulated environment. These were GoldMoney and WebMoney Transfer. Both businesses are discussed in this book. Careful examination of digital currency history suggests why these companies were able to succeed while others had failed.

Beyond these nine businesses, dozens of other digital currency systems and products operated throughout that first decade. However, by late 2011, strict new financial regulations caused the closure of all digital currency operations in the USA. The only digital currency products left circulating through the USA were the newer decentralized cryptocurrencies that operated without a parent company or primary server. By 2012, foreign corporations engaged in US digital currency business and unwilling to comply with the strict new FinCEN regulations pulled out of the American market.

Many people and companies have been prosecuted by the federal government and state government for violating laws that related to Money Service Business and Money Transmitter Licensing. Seven of the nine companies profiled in this book, along with the business operators, were directly involved and connected to criminal prosecutions. Analysis of nine accepted digital currency systems that emerged in the decade between 1996 and 2006 includes the following topics.

1. The operators' motivations for developing the digital currency system
2. Features, currency design, and the development of exchange networks
3. Comparisons of early digital currency systems with conventional bank products
4. Technical structure that permitted the circumvention of existing US regulations
5. How US government agencies reacted to the new unregulated technology
6. US financial regulations created to combat the new unregulated digital currency systems
7. Government actions in the prosecution and asset seizure of the digital currency company assets
8. Why only two of the nine digital currency companies survived
9. The potential target market of users for each digital currency as defined by the operators early in their business
10. Identifying actual users along with motivations for using digital currency
11. What actions the two surviving companies voluntarily took that ensured the companies' survival
12. Why digital currency systems and products succeed in consumer markets and the primary reasons for failure

Digital currency offers many of the same functions of government-issued money. Digital currency is an efficient medium of exchange. Users can purchase goods and services using digital currency units. Digital currency is a store of value. Privately issued tokens have a value which can remain steady over time. Account owners can use online digital currency as a saving account for the long-term storage of value. Digital units backed by gold or denominated in a national currency can function as a unit of account. Digital currency units are modern, recognizable, and measurable economic units that are familiar in global economies.

When discussing private digital currency, it is important to recognize that the underlying topic is money. Most users identify privately issued digital currency as money. People around the world have preconceived notions of money and how it should function in their life. In modern societies, money is a very intimate topic. Spending habits, debt, credit cards, and banking are all money topics that are not openly discussed in public or

with strangers. Human patterns and values surrounding money are often learned as a child and remain with a person their entire life. Consequently, the introduction of a new kind of private money in a modern society will be met with resistance. This situation is particularly evident in America.

Who Uses Digital Currency and Why?

In the decade that followed 1996, over a dozen new digital currency systems were introduced to the world. Each system delivered new innovative technology along with exciting commercial features which were believed to be beneficial for the economy and the population. The first of these platforms was e-gold. The company's website described it as "Better Money[tm]." Compared to fiat paper currency, supporters claimed that e-gold was faster, cheaper, and safer than government-issued "bank" money.

The research presented in this book attempts to show the reasons an entrepreneur operator may have had for creating these digital currency businesses. The book also asks who used the digital currency and for what purpose. In understanding these questions, it may be possible to look ahead and plot a more successful strategy for the future introduction of new innovative digital currency products.

People with no access to banks or bank products will quickly adopt digital currency as a substitute for electronic government money and bank services. Whether the digital currency product is accessible from a cellphone, kiosk, or personal computer, it can immediately replace missing financial tools typically provided by a bank. In cases where a population with no bank access adopts a privately issued digital currency unit in place of bank services, users recognize those units of digital currency as money. In economies without bank access, a new digital currency should function well for both merchants and consumers. Historically in these environments, customers have used digital currency to purchase goods and pay for services including phone bills, utilities, food, transportation, local wages, and medicine. For a population without access to a bank or bank products, the use of a new digital currency does not replace existing bank products. In this kind of nonbank marketplace, as users adopt the new digital currency, they are not required to stop using an existing bank product such as a credit card. These users are entering the digital currency marketplace because they have no bank alternatives. Because they are not changing their existing financial habits, only adopting new methods of

payment, these populations should quickly and easily accept the new type of digital currency. In this economy, it is expected that both merchants and consumers will quickly accept the new digital currency product.

Two illustrations of newly adopted digital currency innovation are Kenya's MPESA and Russia's WebMoney Transfer. In Kenya, a lack of bank access caused the population to embrace cellphone digital payments. MPESA mobile payments provided services the banks could not offer. There was no competition for the private currency products offered through MPESA. Although a bank had not issued the digital units, the community quickly began to identify them as money. In Russia, a broad distrust of banks, which started in 1998, created a cash-based economy. While Russian banks were still in operation after 1998, a large part of the population did not trust or use the banks. This community was open to accepting a new digital currency product that would replace bank services. There was a genuine need for this financial product. WebMoney Transfer started offering private digital currency tools that replaced the bank's untrusted system. In both of these past cases, digital currency was successfully introduced and quickly adopted by a population of nonbank users. MPESA offered digital currency services to those with no bank access in a cash-based economy. WebMoney Transfer provided a substitute private digital currency to people untrusting of banks in another cash-based economy.

Existing populations which do not use banks because of factors such as cost, religion, distrust, or regulations are excellent markets for the introduction of digital currency products. Also, cash-based economies have been willing to adopt new innovative digital currency technology. Due to cultural restrictions, credit card use in the Middle East is small. Countries with large Islamic populations such as Egypt, Indonesia, and Malaysia should be ideal places to introduce nonbank digital currency products. In past years, these consumers have quickly recognized digital gold currency as a beneficial method of doing business online without the need for a credit card or bank.

Anywhere, participation in a market requires the adoption of an exclusive digital currency product, may also lead to a large new group of users. Markets, where access and participation requires a particular digital currency, can be illustrated by the activity taking place in Dark Markets on the hidden parts of the Internet. The anonymity of shopping for illegal drugs on a Dark Market website requires that the user pays using bitcoin or another cryptocurrency. Participation in this market requires bitcoin digital currency.

What Is Digital Currency?

Digital currencies are privately issued electronic units that circulate on the Internet. Banks do not accept private digital currency as a deposit and the Internet currencies are not legal tender. The units have brand names such as "Digital Grams," "Evos," "Gold Grams," "e-currency," and many others. Acceptance of this digital medium of exchange is 100 percent voluntary. The private companies and individuals that created the original digital currency products were also free to define the unit's commercial value. To build value into a digital unit, many operators permanently matched physical assets with the units. The industry described most digital currencies as being "backed by" an asset. Examples of these are digital currencies backed by gold, silver, dollars, and euros. In the case of bitcoin, some users describe it to be "backed by" computer processing power.

While each digital currency had a different brand name, all of these privately operated systems faced similar issues relating to the unregulated market environment. The decade from 1996 through 2006 allowed anyone, with or without previous banking experience, to introduce a new digital currency financial product to the global consumer marketplace. This book investigates and attempts to define characteristic features shared by all new digital currency products and further tries to identify common issues each business encountered.

Distinctive features of digital currency:

1. All transactions are final, irrevocable, and irreversible.
2. Digital currency units can be bought or sold through a third-party independent agent.
3. During a transaction, there is no requirement to return or exchange the digital units through the original issuer.
4. Digital currency is freely exchangeable for other digital currency units through a third-party independent agent.

There are nine digital currency businesses profiled in this book which circulated between 1996 and 2006.

1. e-gold
2. E-bullion
3. Liberty Dollar (eLibertyDollar)
4. Crowne Gold

5. Liberty Reserve
6. IntGold
7. OSGold
8. GoldMoney
9. WebMoney

New US Financial Regulations

Two US financial regulations changed the global digital currency marketplace and forced existing digital currency businesses to exit the US market.

1. On July 21, 2011, FinCEN published a Final Rule amending definitions and other regulations relating to money services businesses (the MSB Rule).[1]
2. On July 29, 2011, FinCEN issued a Final Rule on Definitions and Other Regulations Relating to Prepaid Access (the Prepaid Access Rule).[2]

Legal Cases

Key legal cases discussed in this book include:

Case 1:07-cr-00109-RMC

United States of America
v.
E-gold, Ltd.
Gold & Silver Reserve, Inc.
Douglas L. Jackson,
Barry K. Downey, and
Reid A. Jackson,
Defendants.
18 U.S.C. § 1956 (Conspiracy to Launder Monetary Instruments);
18 U.S.C. § 371 (Conspiracy);
18 U.S.C. § 1960 (Operation of Unlicensed Money Transmitting Business);
D.C. Code § 26-1002 (Money Transmitting Without a License)
18 U.S.C. § 2 (Aiding and Abetting and Causing an Act to be Done); and
18 U.S.C. § 982(a) (1) (Criminal Forfeiture).

Case 2:08-cr-00224-PSG

United States of America
v.
James Michael Fayed,
And Goldfinger Coin & Bullion, Inc.,
Defendants.
A violation of 18 U.S.C. § 1960

Case 3:08-cr-00085-N

United States of America
v.
Michael Comer
Operating an Unlicensed Money Transmitting Business
(A violation of 18 U.S.C. § 1960(a) and (b)(l)(B))

Case 5:09-cr-27-RLV

United States of America
v.
Bernard Von NotHaus,
Defendant.
18 U.S.C. § 371, conspiracy to violate 18 U.S.C. §§ 485 and 486, and substantive violations of 18 U.S.C. §§ 1341, 485, 486 and 2.

Case 1:13-cr-00368-DLC

United States of America
v.
Liberty Reserve S.A.,
(18 U.S.C. §§ 1956, 371, 1960 & 2)
Arthur Budovsky,

a/k/a "Arthur Belanchuk,"
a/k/a "Eric Paltz,"

Vladimir Kats,

a/k/a "Ragnar,"

Ahmed Yassine Abdelghani,

a/k/a "Alex,"

Allan Esteban Hidalgo Jimenez,

a/k/a "Allan Garcia,"

Azzeddine El Amine,
Mark Marmilev,

a/k/a "Marko,"
a/k/a "Mark Halls," and

Maxim Chukharev,
Defendants.

Case 1:08-cr-00717-JGK

United States of America
v.
David Copeland Reed,
Defendant.
Title 18 U.S.C. §§ 1956, 1343

Case 6:09-cv-01851-JA-KRS

United States of America
Plaintiff,
v.
47 10-ounce Gold Bars, 35 1-ounce Gold Coins, and 3,069 1-ounce Silver Coins, in rem,
Defendant.

Case 3:03-cv-00955-MA

United States of America
v.
47 10-Ounce Gold Bars et al
18 U.S.C. § 1960, 18 U.S.C. § 981(a)(I)(A).

The book also discusses several other criminal cases and civil actions as related to digital currency.

Building a Better Mousetrap

There is an old phrase, generally attributed to Ralph Waldo Emerson, which says "If you build a better mousetrap the world will beat a path to your door." The phrase is a metaphor for the power of innovation. If a person creates a better product, then the public should naturally want to purchase the new innovative item. Using this analogy, if government money is the old mousetrap, then digital currency was the better mousetrap, and consumers around the world should have been rushing out to use the innovative new digital type of money. In theory, consumers, merchants, and businesses all over the world should have all been adopting these new digital currency systems. However, the recent history of digital currency in America tells a different story. While consumers will rush to buy the newest cellphone technology, a majority of consumers will not race to use a new and improved version of private money. The markets of consumer activity where the "build-a-better-mousetrap" rule can be applied do not include money, payments, or personal finances.

Matters of personal finance are very private consumer issues. In America, financial payments and banking are almost considered "intimate" topics. While growing up, US shoppers become accustomed to certain methods of payment and everyday routines that surround personal financial activity. This reluctance of US consumers to change their personal spending habits is particularly relevant when discussing the introduction of new digital currency products.

In the late 1990s, entrepreneurs and innovators such as Douglas Jackson and James Turk recognized that government-issued money could use some improvement. These two gentleman and others were responsible for creating innovative private digital currency systems which emerged during the decade 1996–2006.

The design of digital currency allowed for widespread global use by any person with Internet access. Digital currency accounts have no setup

costs, no high monthly fees, and no lengthy identification requirements. Without identification requirements and costs, digital currency should be accessible and attractive for everyone. Online accounts could be instantly created and used by anyone from any nation on earth. It is the role of private digital currency to furnish everyday financial tools to unbanked persons. By design, digital currency systems are created for use outside of conventional financial institutions and cater to nonbank customers. Those persons unable to engage in a financial business through a traditional bank greatly benefited from the use of private Internet digital currency products.

However, from 1996 to 2006, Americans did not rush out and adopt the new and innovative digital currency products. While introducing this new commercial technology, the company operators had to navigate difficult waters of an unregulated US financial marketplace. Unforeseen US consumer reluctance to adopt digital currency became a dominant factor; stalling the growth and acceptance of digital currency in the USA. Beyond America's border, populations of nonbank users flocked to adopt this new version of electronic money.

A Lack of Early Digital Currency Regulation

When any new technology enters the consumer marketplace, it can take the government several years to adjust regulations that control the use of that new technology. This statement is especially so regarding new financial products. In 2015, the government is trying to catch up with the massive popularity of personal drones. As millions of new unregulated and unlicensed drones take to the skies, the Federal Aviation Administration (FAA), which is part of the US Department of Transportation, has been busy writing new laws and regulations that will catch up with this new technology. A very similar situation occurred in 1996 with new private digital currency systems and agents. When commercial digital currency emerged in 1996, this new financial product was not recognized or identified by existing US financial regulations. No existing US laws defined a digital currency system, a digital currency exchange agent, or a digital token backed by gold. No judge had ever rendered an opinion on the topic, and no individual had been prosecuted for breaking the law as it related to financial transactions and digital currency. Just like the new drone technology, digital currency that circulated online was a brand-new technology. Throughout that first decade, it was believed that a digital

unit transferred online was not considered money transmitting because it did not involve government-issued cash or currency. The government regulations did not yet recognize the movement of privately issued digital currency as transmitting legal tender. Operators of digital currency systems in the USA openly discussed the topic. No one at that time could definitively say that circulating a private digital currency units over the Internet was a financial activity that required government supervision or a license. No regulatory agency had yet defined the operation of a digital currency company as a money service business. Consequently, without any supervision or regulations, the digital currency business grew extremely fast. Freedom from US financial regulations afforded some great benefits to the users of digital currency systems.

While US banks and money service businesses were restricted by anti-money laundering (AML) programs, Internal Revenue Service (IRS) reporting requirements, and constant verification of customer identities, most of the early digital currency accounts did not have any of these demands. In those early years, exchange agents that swapped national currency for digital value were not yet considered financial institutions and also avoided all reporting and licensing requirements.

A digital currency account could be opened in a matter of moments and required only a verified email address. There were no restrictions on how much money or value could be deposited. There were no restrictions on how many transactions could take place each day, nor how much value could flow in and out of the account. Except for accounts at GoldMoney, a company that was created by executives from the banking industry, no other digital currency account required any identification documents. Consequently, there were also no jurisdiction or citizenship restrictions. Users in countries such as Iran and North Korea were free to use digital currency systems. The e-gold platform, and others, allowed free and easy access to sanctioned countries. Digital currency permitted a user to transact directly financial business with users in any other country, including the USA.

National currency that flowed into and out of these platforms moved through third-party independent exchange agents all over the world. From 1996 to 2006, there were also no requirements for these exchange agents to be licensed or requirements to follow established financial rules and regulations of the banking industry.

1. No source of funds disclosures or requests

2. No suspicious activity reports (SAR)
3. No currency transaction reports (CTR)
4. No reports of international transportation of currency or monetary instruments (CMIR)
5. No reporting of asset sales to authorities such as the IRS.

This green new industry was unregulated for approximately a decade. Because there were no restrictions on transaction size, a $10 trade carried the same requirements as a $20,000,000 anonymous transaction. Users opened digital currency accounts and anonymously sent and received funds. The only information captured by the digital currency system operator was the email and the user's IP address. There were no US financial regulations supervising or regulations any exchange agents during this time. Except for GoldMoney, no digital currency business recognized or complied with any existing US financial rules.

In 2008, Judge Rosemary Collyer's opinion in the e-gold case clearly identified both digital currency issuers and exchange agents as financial institutions that required proper US registration and licenses.

Before 2008, no US financial regulations defined the transfer or exchange of digital currency as value transmitted online. The 2008 judge's written opinion left no doubt that US digital currency issuers and agents require proper licensing as money service businesses. GoldMoney was the only company that required identification to operate a company account. GoldMoney was the exception, and voluntary restrictions along with customer identification are critical reasons the company is still in business in 2016.

During 1996 through 2006, why would any US consumer with access to banks and payment cards abandon those conventional tools and switch to a digital currency system? A digital gold currency payment system offered cheaper fees, faster settlement, and protection from inflation. However, very few people dropped their banks and adopted the digital gold currency. An average working American had no strong reason to dump the bank and adopt a new digital currency. The general public in America did not beat a path to these new financial products. From 1996 through 2006, these innovative new digital currency systems were largely ignored by average consumers and merchants.

A few of the highlighted and commonly discussed positive features of digital currency are:

1. All transactions are final. Digital currency transactions are non-repudiable, irrevocable, and irreversible.
2. Digital currency units can be bought or sold through a third-party independent agent. There is no requirement to return or exchange the digital units through the original issuer.
3. Digital currency is freely exchangeable for other digital currency units through a third-party independent agent.

Executing a digital financial transaction that no user could reverse offers a powerful advantage for criminals and con men. A person tricked into buying a product or making an investment that later turns out to be fraudulent has no recourse to obtain a refund or reverse the transaction. There is no possibility of the digital currency issuer freezing that account. The money sent in that transfer is lost.

The digital currency units from any transaction, either legal or illegal, are exchanged into national currency through independent agents located in any country on earth. Because financial regulations are lax or non-existent in many jurisdictions, anyone with digital currency, obtained either legally or illegally, can exchange it into national currency somewhere in the world without the worry of reporting the transactions or providing a source of funds.

For example, if a person has earned money illegally and received the funds through PayPal, there is an excellent chance that they will not be able to withdraw the illegal proceeds because the online PayPal units must move back through the issuer before exiting the system. That is not the case with digital currency products. The proceeds of crime can circulate through any of 1000 different independent agents in over 150 countries around the world without any scrutiny or verification from the issuer.

Illegal income requires its source to be hidden. Criminals can easily accomplish this task by quickly exchanging the value in one currency to another digital currency system. Anyone that may be investigating or tracking the illegal activity by following the money will hit a dead end when those units exchange for another currency that operates from yet another jurisdiction. By its design and original features, digital currency is advantageous for use in criminal activity.

In October 2001, the USA Patriot Act was signed into law by then-President George W. Bush. The full name of the Act is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. One focus of the Patriot

Act Regulations was to curtail possible money transfers taking place through Hawalas located in the USA.

Title III of the USA PATRIOT Act focused on improving America's defenses against money laundering and possible terror funding. Among the many new rules and regulations, Title III directly related to digital currency. Specific items focused on digital currency included the following:

1. New requirements for increased record keeping and reporting by financial institutions on all transactions involving "Jurisdictions outside the United States, Financial institutions outside the United States, and/or Classes of transactions involving jurisdictions outside of the United States that are considered by the Secretary to be a primary money laundering concern."[3]
2. Added to the definition of money transmitter, informal value transfer banking systems or networks of people facilitating the transfer of value outside of the financial institution's system. This provision attempts to establish regulatory oversight for informal "hawala" systems.
3. Made it a federal crime to operate a money transmitter business without an appropriate state license.
4. Required financial institutions to establish AML programs that include:
   (a) Development of internal policies,
   (b) Designation of a compliance officer,
   (c) Ongoing employee training programs, and
   (d) An independent audit function.[4]

Another important part of the Act, as it related to digital currency, is section 359. This section targets informal value transfer operations such as Hawalas.

> Sec. 359. Reporting of Suspicious Activities by Underground Banking Systems
>
> Section 359 of the USA PATRIOT Act expanded the definition of "financial institution" to include not only a licensed sender of money but any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside the conventional financial institution system. Any individual or group of people engaged in

> conducting, controlling, directing or owning an informal value transfer system in the United States is operating as a financial institution. Therefore, IVTS operators must comply with all Bank Secrecy Act (BSA) requirements, which include establishment of an anti-money laundering (AML) program, registration with the Financial Crimes Enforcement Network (FinCEN) as a money services business, and compliance with the record keeping and reporting requirements, which include filing suspicious activity reports (SARs)6. 3 See 31 U.S.C.5312 (a)(2)(R)[5]

These 2001 regulatory changes set the stage for the future prosecution and seizure of two well-known digital currency companies. E-bullion and Liberty Reserve. Between 1996 and 2003, about a dozen new digital currency companies were launched around the world. All of them serviced clients residing in the USA. Additionally, dozens of small independent exchange agents were operating across the USA from Oakland, California, to Tampa, Florida. Even in the midst of a flourishing 2003 digital currency marketplace, none of the businesses were licensed as money transmitters or registered as money service businesses.

Except for GoldMoney and WebMoney Transfer (A Russian Company), no other digital currency company offered any AML program or proper know your customer (KYC), and no company, neither agent nor issuers, was registered with FinCEN. In fact, it was not until 2005 before any US state or federal agencies recognized digital currency exchange agents operating in the USA as financial institutions that required the proper state money transmitter license and registration with FinCEN. In March 2003, the US Department of the Treasury Financial Crimes Enforcement Network released FinCEN Advisory, Issue 33, on the subject of Informal Value Transfer Systems (IVTS).

> This advisory provides financial institutions with information concerning Informal Value Transfer Systems (IVTS).
>
> The purpose of this advisory is to educate the financial community about IVTS by:
>
> 1) Explaining the operation of IVTS;
>
> 2) Describing how financial institutions may be used in the IVTS process; and
>
> 3) Identifying how the Bank Secrecy Act, as amended by the USA PATRIOT
>
> Act, regulates IVTS operators.[6]

Despite the fact that an IVTS operation, such as a Hawala, uses an almost identical routine in anonymously moving funds across the US border, FinCEN Advisory Issue 33 never once mentioned digital currency. Anyone can exploit a financial institution, or medium of exchange, such as digital currency, for criminal use or terrorist financing. Here is an illustration of that activity.

Chart 1.1 IVTS transaction vs digital currency transaction

Traditional IVTS	*General Digital Currency Transaction*
In a *basic* or *traditional IVTS* transaction (such as hawala), four participants are required: a sender of the funds, a recipient of the funds, and two IVTS operators in the respective countries of the originator and recipient. The following exercise demonstrates an example of a basic IVTS transfer where an individual (#1) in Country A wants to send money to an individual (#2) in Country B[7]	In a *basic* or *traditional digital currency* transaction (such as e-gold), four participants are required: a sender of the funds, a recipient of the funds, and one or two exchange agents in almost any country; however, they are often in the sender and receiver's locations. The following illustration is a simplified example of a digital currency transfer where an individual (#1) in Country A wants to send money to an individual (#2) in Country B
Step One: Individual #1 gives currency to an IVTS operator in Country A	Step One: Individual #1 gives national currency to an exchange agent in Country A
Step Two: The IVTS operator in Country A provides Individual #1 with a code or other identification mechanism	Step Two: The exchange agent in Country A provides Individual #1 with the digital currency
Step Three: The IVTS operator in Country A notifies his counterpart in Country B by phone, fax, or email of the transaction amount to pay Individual #2 and the code	Step Three: Individual #1 anonymously sends the digital currency over the Internet to his counterpart in Country B by cellphone or computer
Step Four: Individual #1 contacts the intended recipient, Individual #2, in Country B and provides the code to that person	Step Four: Individual #2 in Country B instantly receives the digital currency
Step Five: Individual #2 goes to the IVTS operator in Country B, gives the appropriate code and picks up the specified funds sent to him.[8]	Step Five: Individual #2 visits a local exchange agent and swaps his digital currency for cash or Individual #2 transfers the digital currency onto an ATM debit card and instantly withdraws the funds in cash

Notes

1. Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43,585 (July 21, 2011) (codified at 31 C.F.R. pt. 1010, 1021–1022).
2. Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45,403 (July 29, 2011) (codified at 31 C.F.R. pt. 1010, 1022).
3. 31 US Code § 5318A—Special Measures for Jurisdictions, Financial Institutions, International Transactions, or Types of Accounts of Primary Money Laundering Concern | US Law, (n.d), https://www.law.cornell.edu/uscode/text/31/5318A.
4. Department of Justice, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, (US Department of Justice, 2001), accessed May 17, 2015, https://www.justice.gov/archive/ll/highlights.htm.
5. US Department of the Treasury Financial Crimes Enforcement Network, FinCEN Advisory Issue 33, (Financial Crimes Enforcement Network, 2003), accessed March 26, 2016, https://www.fincen.gov/news_room/rp/advisory/pdf/advis33.pdf
6. US Department of the Treasury Financial Crimes Enforcement Network, FinCEN Advisory Issue 33, (Financial Crimes Enforcement Network, 2003).
7. "U.S. Money Laundering Threat Assessment," U.S. Department of the Treasury, accessed April 2, 2016, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf
8. Ibid.

CHAPTER 2

E-gold

E-gold was the world's first commercial digital gold online payment system. Gold was not the only digital metal the company offered through the digital platform. Customers also traded e-silver, e-platinum, and e-palladium. A parent company, named Gold and Silver Reserve, Inc. (G&SR), operated the e-gold business in Melbourne, Florida.

E-gold began offering services to the public in November 1996 through the website www.e-gold.com. Just over a decade later, a complicated federal criminal case surfaced against the company and its officers. By October 2008, e-gold had halted all transactions with the public and forfeited some of the company's bullion reserves and much of the money on deposit in company bank accounts. In 2008, the principal officers of the business pleaded guilty to multiple felony charges. While the penalties for these crimes included possible decades in prison, none of the convicted e-gold officers received prison sentences. From 2008 through 2015, the convicted e-gold operators attempted to work with the federal government and return tens of millions in seized customer funds.

E-gold was one of the first payment systems that permitted users to execute complicated global financial transactions outside of the regulated banking system. The birth of e-gold and the ensuing legal case were historical events in the world of online payments.

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_2

The overwhelming success of the e-gold system backed by precious metal also contributed to how the US government identified and categorized future online payment systems. Those regulations changed the way global digital currency companies engaged in business with US residents. The e-gold online platform was the world's first secure account-based monetary payment system that enabled the use of gold and other precious metal as currency. The co-founders of this system were Dr. Douglas Jackson and attorney Barry K. Downey.

Dr. Jackson was an Army veteran, a graduate of Pennsylvania State University College of Medicine and was board certified in Radiation Oncology. From 1986 through 1992, he served as a Major in the US Army Medical Corps, Chief of Radiation Oncology at the Brooke Army Medical Center, Fort Sam Houston, Texas. He was a founding partner of Florida Oncology, a group practice providing hospital-based oncology services.

He had no prior experience in the banking industry or the financial services business. A successful lawyer, his associate Barry Downey also had held no previous positions working in the banking or payments industries. Item 32 under Manner and Means in the first April 24, 2007, e-gold indictment, stated that the government also recognized this lack of banking experience.

> With few exceptions, the employees hired to operate the E-GOLD payment system had no experience in conducting financial transactions and no background in financial matters at all. Employees of the E-GOLD operation received no training regarding financial transactions or avoiding criminal transactions, nor were they provided any written materials on these matters.[1]

For decades, Dr. Jackson has been a libertarian and an admitted champion of the gold standard. Since e-gold's beginning, in the mid-1990s, he had also been critical of conventional banking systems, US fiat currency and many policies of the Federal Reserve Bank. Both he and Barry Downey are considered to be brilliant men.

The first e-gold public transactions were in November 1996, several years before the merger that formed PayPal, and at least, 11 years before the creation of bitcoin. From its opening day in November 1996 through the end of 1999, the e-gold.com payment system was operated by G&SR, a Delaware Corporation, formed January 24, 1996. AT&T ran the e-gold computer servers based in Orlando, Florida. The G&SR parent offices

were in Melbourne, Florida. During that three-year period, G&SR administered all payment settlement, along with currency exchanges and also served as Bailee for the precious metal bullion. That service included the currency exchange operations which changed the private digital currency to national money. These transactions, from 1996 to 2000, took place through the e-gold website. Douglas Jackson explains this further in a 2016 email.

> From 1996 - 1999, e-gold was a service of Gold & Silver Reserve, Inc. and it directly offered what we called InExchange and OutExchange. [see https://web.archive.org/web/19980627133859/http://www.e-gold.com/ Note that archive.org failed to capture the oldest stuff. The experience of these initial years informed a restructuring circa 2000 that implemented a number of refinements. The major thrust was to ring-fence the core functions of issuance and settlement to insulate them from the riskier business of currency exchange. The core e-gold functions were devolved onto e-gold Ltd., which had been formed specifically for that purpose. Concurrently, the e-gold Bullion Reserve Special Purpose Trust was brought into existence. It was in conjunction with these refinements that we conceived and fostered the emergence of a second global industry – third party provision of exchange services supporting exchange between privately issued brands of money and conventional currencies.[2]

Every e-gold account balance including gold, silver, platinum, and palladium represented by digital units circulating online was backed 100 percent, gram for gram, by physical precious metal held offline. The company maintained an inventory of these precious metals in secure vaults. E-gold was the most popular of the digital currency products.

When the payment platform went live in 1996, the precious metal coins and bullion were first stored in bank safe deposit boxes in Melbourne, Florida. The business also stored precious metal in the company offices. While G&SR operated from Florida, all of the bullion was eventually moved into professionally managed third-party custodial services in Canada, London, Zurich, Dubai, and other locations. During that time, the contracts for managing the bullion were often visible on the e-gold.com website.

With the creation of e-gold, Dr. Jackson and Mr. Downey were attempting to produce a type of "Better Money™," which is also a trademarked slogan owned by G&SR. During early development, Dr. Jackson had used his personal saving and paid out more than $1 million in startup costs.

He eventually sold his medical practice in favor of e-gold. He also took a very hands-on approach. Throughout the software's design and creation process, he was deeply involved with the creation of the platform and even wrote some of the original system code.

In 1996, Dr. Jackson and his associates had created a precise, convenient, and secure method of payment for global online financial transactions. This system was a centralized digital ledger and online payment platform that offered account holders the ability to make instant, secure transfers of value to any other account within that closed system. Users logged in to the centralized system and initiated transfers from their account while they were online. The primary function of e-gold was to render payments, in gold (silver, platinum, or palladium), from one customer to another.

In a 2016 email, Douglas Jackson further explains why he created the e-gold platform.

> I have always had an interest in history. Over time, this interest had evolved into a focus on the influence of economic factors on real world events. I discerned a recurring pattern of economic disruption giving rise to political upheaval and, all too often, war. By the mid-90s, it seemed evident to me that there was, in turn, a deeper layer of causality underlying economic disruption – a faulty monetary foundation. All historical and contemporary monetary regimes shared variations of the same embedded contradictions making them susceptible to a ratcheting process leading to eventual debasement. The crux was susceptibility to discretionary manipulation. It struck me that the only solution was a rules based system, bound by explicit contract and reinforced by systematic transparency measures that would enable immediate detection of deviations. This would require a private sector initiative since no sovereign is capable of being effectively bound by contract – especially when it comes to monetary obligations once they are no longer convenient.[3]

In his email correspondence, Douglas Jackson discussed that before creating e-gold, he had become aware of Vera C. Smith's 1936 publication entitled "The Rationale of Central Banking and the Free Banking Alternative."

Dr. Jackson detailed that Vera had concluded; "How to discover a banking system which will not be the cause of catastrophic disturbances, which is least likely itself to introduce oscillations and most likely to make

the correct adjustments to counteract changes from the side of the public, is the most acute unsettled economic problem of our day."

On several occasions, he indicated that severing that "Gordian knot" and distancing his new system from past monetary mistakes had become the goal and mission of his work. Mr. Jackson even said that he regarded this new mission, of creating an improved private financial solution, as his duty.

During the decade from 1996 through 2006, Douglas Jackson and James Turk had both explained how the Internet facilitated the creation of a global private digital currency solution. Before the commercial internet, no private individual or corporation with limited means could have established a boundless secure electronic network. James Turk commented in his early writings how prohibitive a task it would be for any single person or company to construct such a global financial system.

Douglas Jackson noted that "such as task required large-scale computational capacity, data storage and secure global means of communication," the costs of which were prohibitive for any party other than national governments. Furthermore, the global risks and costs associated with accepting credit cards were extremely high and horribly insecure. Before e-gold, there was no corresponding global payment mechanism operated by a private entity.

While government dominated monetary systems continued to underperform, Douglas Jackson stated his belief that there was a strong business case for an alternative global currency that could circulate beyond the risks and dangers posed by conventional banks. Mr. Jackson said that he believed the world should have, an efficient payment system designed from the ground up to serve the global market of "people who use money."

After conceiving of the e-gold solution, Douglas Jackson also stated that he felt it would not make any sense to solicit an existing conventional institution for the implementation of his new concept. He explained his reasoning for not approaching existing financial systems in collaboration or partnership; he said if any current bank "had the capacity to apprehend these possibilities," an existing financial institution would have already undertaken its creation.

In 2001, the e-gold website read, "The world wide web needs world wide money. Experts created e-Gold in response to this need."[4] A 2006 quote from an interview with Brian Grow for BusinessWeek Magazine provides further evidence of Dr. Jackson's motivation for building e-gold. Dr. Jackson reveals that he believed the e-gold system would, "advance

the material welfare of mankind." Later in the article, Dr. Jackson was also quoted as saying, "I thought there would be this flock of e-gold users, and I would be their messiah," and follows up by saying, "It just didn't happen."[5]

In 1996, no widely accepted commercial online payment system had ever existed before e-gold. The other well-known early innovator was the payment processor PayPal. That company, which was the outcome of a merger between Cofinity and X.com, was not formed until late 1999. The e-gold platform had already been processing digital payments backed by precious metal for nearly three years.

Co-founder Dr. Douglas Jackson had also designed an innovative platform that facilitated the anonymous transfer of value across international borders in real time. Years before PayPal, e-gold was already offering an efficient and secure global method of transmitting value and recording digital transactions over the Internet.

The e-gold system was not a Complementary currency. Complementary currency is best known as a medium of exchange that circulates alongside national currency and complements government money. Complementary currency is abundant. It moves to parts of the economy that are lacking government money and tends to fill the gaps created by scarce national currency. That model was not e-gold.

Experts identified e-gold as an alternative digital currency. Users recognized e-gold as an "alternative" to the US Dollar and a replacement for government-issued money. Dr. Jackson had set out to create an alternative to fiat currency. E-gold was seen by many as a privately issued currency that could directly compete with government-issued money from any country. His intent was to design a new precious metal backed online payment system that would outperform conventional bank payment operations; while providing users a convenient hedge against the inflation.

The e-gold platform was created for use by everyone in the world and at every level of society. Online access allowed those users who lived in abject poverty to send and receive funds as quickly and economically as a billionaire living on Fifth Avenue in New York City. By design, the creators of e-gold truly meant the platform to be "Better Money[tm]."

Many users viewed the e-gold system as having introduced healthy competition into the world of government-controlled fiat currency. It was a private online system offering very similar payment products as US banks. However, e-gold was cheaper, faster, performed better than bank wires, and permitted easy access for all persons in the world. After just a

few years in operation, it was evident from e-gold's commercial success that privately issued digital currency could very effectively compete with government-issued money.

The e-gold platform was already outperforming regular bank payments. By 1999, seven years before PayPal introduced a mobile platform, e-gold accounts could be operated using a web-enabled cellphone.

Why e-gold?

There are many reasons why new users were attracted to digital gold currency. Exchanging government money in and out of the e-gold system was not an easy task. After 2000, the issuer did not accept deposits. To add value to an e-gold account, a user had to seek out a reputable third-party independent agent that would accept government money and "in exchange" funds; adding value to the private e-gold online account. In e-gold early years, this task often took more than a day or two.

E-gold transactions were unlike regular bank payments. All e-gold digital currency transactions were final. There were no charge-backs. Neither the sender nor the receiver could rescind a completed payment. Even the system operator, e-gold Ltd., would not reverse a customer transaction. In the case of a legitimate payment error when sending funds to the wrong account number, the transaction was final. The funds remained in the wrong account, and there was no internal messaging system to contact whoever operated the account. If someone had been unlucky enough to spend a considerable e-gold amount to the wrong account, all an account holder could do was send an additional payment to that same account for a tiny amount such as 0.02 cents and include a note asking for the return of the gold.

Text from the e-gold website labeled the transactions as non-repudiable and the e-gold terms of use clearly spelled out the irrevocability of what was termed "Spends."[6]

The lack of charge-backs dramatically reduced the cost of e-gold's payment service. Merchants accepting e-gold benefited from the lower cost and the fact that customers could not reverse the transactions at some random future date. This feature also caused e-gold digital payments to look and feel more like a cash transaction than a bank payment.

The digital book entry ledger used by G&SR had been organized using a transaction model that allowed online payments as small as 0.0001 gr. This feature made e-gold payments highly divisible and created a very

practical micropayment system. Dr. Jackson later shared the fact that behind the consumer interface, precious metal payments were accurate to 15 digits.

After 2000, the legal issuer of the digital currency became a Nevis W.I. Corporation named e-gold Ltd. This entity was created to serve as a general contractor responsible for the duties outlined in the e-gold account user agreement. The separation of e-gold's US currency exchange business, which became OmniPay, from the operation of the e-gold payment system, was the action of a fiduciary agent attempting to protect the e-gold business and its customers. This move separated all e-gold client operations from potential payment default and other issues that are known to plague conventional bank transactions. The company's goal was separating the exchange agent services of G&SR with the e-gold payment system. G&SR was a US corporation while e-gold Ltd. was the Nevis non-US company.

In a 2016 email, Douglas Jackson describes this move.

> The Devolution Agreement that marked the separation of e-gold and OmniPay was effective 1/1/2000. It took months or years to implement all the elements but from the date of devolution, e-gold was no longer involved in exchange. That remained G&SR's business, dba OmniPay. I do not recall exactly when the OmniPay brand and site became publicly visible but here is an archive.org capture from 2000 https://web.archive.org/web/20001109193200/http://www.omnipay.net/[7]

OmniPay quickly became the largest e-gold exchange in the world. It served as the primary dealer exclusively working between the issuer, e-gold Ltd., and all other third-party independent exchange agents around the world. The headquarters of OmniPay was in Melbourne, Florida. OmniPay was the sole entity responsible for maintaining e-gold liquidity at all times. In a 2016 email, Douglas Jackson had these positive statements about OmniPay's verification of customer identification.

> However, OmniPay needed confirmation of ID. From 2000 to early 2003 it implemented three critical self-protective measures. 1) universal postal verification 2) it only accepted payment by bank wire 3) it set up safeguards to detect possible incoming third party payments. There was never a case where it turned out OmniPay had incorrect information regarding the identity of a customer.[8]

The company's activity included the exchange of national currency and digital units moving both in and out of circulation. After this 2000 separation, G&SR was able to focus more closely on their OmniPay exchange operations. In a 2016 email, Douglas Jackson revealed these thoughts on OmniPay and the exchange services.

> The first few years of e-gold were a learning experience (as have been all later years). A key insight was that the exchange aspects—accepting conventional money payments and also being exposed to exchange rate fluctuations—was risky. Our 2000 restructuring was to ring-fence off the core functions of a monetary authority—issuance and settlement of transfers—from the risky business of exchange. 2000 was also when we went to a Primary Dealer model, for the same reasons all major monetary authorities implement primary dealer models. [Turk, over time, went exactly the opposite direction, moving away from the concept of third party exchangers and reverting to being just another a gold dealer.] So as a result, e-gold was absolutely immune to risks stemming from non-performance on the part of any customer. It did not extend credit. It enforced a strict debit rule for Spends.[9]

The e-gold executives believed that "good fences made good neighbors," and this trust structure provided an additional legal separation of assets. It was called the e-gold Bullion Reserve Special Purpose Trust and domiciled in Bermuda. E-gold executives managed this entity for the purpose of collectively retaining legal title to all e-gold account holders' bullion. The purpose of the Trust was to insulate further client value from physical, legal, and political risks. The separation added yet another very effective layer of protection for the assets of e-gold customers.

One Hundred Percent Reserves at All Times

Unlike fractional-reserve banking, e-gold always held 100 percent of client funds in reserves. A million dollars of digital e-gold circulating online in customer accounts required a million dollars' worth of physical gold value to be held in allocated storage on behalf of the e-gold account owners. US banks only hold a tiny percentage of customer deposits while e-gold always held 100 percent of customer bullion. This feature obviously represented a level of security for many e-gold users that surpassed any representation of security they may have previously had for US banks.

Dr. Jackson was so concerned about the company's financial transparency that he built into the e-gold public website a daily audited disclosure

of the precious metal reserves backing customer accounts. On a page, entitled the "Examiner," daily live reports of precious metal reserves held on behalf of clients were listed. The page was a real-time audit utility containing the total quantity of e-metal versus the total physical precious metal reserves. This audit usually included the actual bar numbers. The Examiner was available online and accessible to the public throughout the life of e-gold. Much of the current e-gold research originates from this data previously recorded in the Examiner and now found in the Internet Archive.

Grams, Troy Ounces, and Kilos

Weight denominated all e-gold accounts. The online statement showed an account balance in grams and Troy ounces. Also built into the e-gold software platform was a corresponding account calculator that showed the weight of an account and its value denominated in popular world currency. The account screen automatically used the current price of gold in various popular national currencies multiplied by the weight of metal in the account. Payments to other account holders could be completed using a weight in metal, such as a gram, or an amount of national currency. An e-gold customer could spend $11.79 in e-gold or 1.7923 grams of gold.

By clearly defining e-gold's innovative features, Dr. Jackson was able to support further the company's argument that e-gold was not a bank, did not need to operate as an MSB and the company did not require any money transmitter licenses. E-gold offered a private digital payment system, backed by precious metal that enabled financial transactions outside the supervision of any government. The new e-gold platform allowed anyone in the world to send or receive value through the Internet without restrictions. E-gold customers could transfer as little as 10 cents a payment or millions of dollars' worth of digital value without restriction. No ID was required to open or operate an e-gold account. No bank account was needed, and no credit card or utility bill was needed for customer verification.

Most e-gold users opened multiple accounts and switched between accounts at their convenience. One person per account is a common restriction of all regulated US online payment businesses. One person equals one account. The rule is in place to combat money laundering and prevent the illegal use of a financial account. International financial transfers using e-gold were much cheaper, settled instantly and could occur

anytime. Digital gold currency opened up a new world of opportunity for anyone or any company involved in a cross-border trade or international financial settlements. The e-gold system removed any need for currency conversion during cross-border transactions.

This system also eliminated the burden caused by delays in cleared funds moving through a financial payment. By using a digital gold standard, instead of various foreign currency transfers, the receiver's funds were available instantly, and transactions could take place at any time across multiple time zones. All e-gold transfers cleared immediately. For merchants accepting e-gold, there were no "charge-backs." In using the e-gold system, merchants removed the fraud and expenses related to credit card transactions. In 2016, this feature, which prevents the reversal of a transaction, can also be found in cryptocurrency platforms such as bitcoin. Just as with the previous e-gold platform, no transaction can be blocked or reversed in the bitcoin system. Responsibility for sending the correct amount to the correct account rests solely with the account holder. In theory, if each payment is the responsibility of the sender, there should never be any reason for reversing a payment.

In a world saturated with credit card fraud, non-repudiable payments were a critical factor in e-gold's fast growth and worldwide popularity. E-gold growth occurred in markets that sold legal services and also many online markets that engaged in illegal activity. Furthermore, through the e-gold system, users had the capability to move funds across any international border and through any country on earth. International trade sanctions became obsolete, and online transfers easily circumvented currency controls. Since e-gold operated over the Internet, it was beyond the reach of conventional bank regulations and supervision. E-gold accounts required no Social Security number and no reporting to the Internal Revenue Service.

Another notable difference between credit card accounts and e-gold was the single type of e-gold account. Both merchants and individual users had the same kind of e-gold account. There was no difference between a "merchant" account and a "personal" account; there were no additional disclosures or verifications. The e-gold account was a one-size-fits-all. In popular online payment systems, a clear distinction exists between a personal user account and a business merchant account. Business merchant accounts require additional information, verification, and paperwork. This verification of clients was not the case with e-gold. Any user could label an

e-gold account for personal use or under the name of a company or business entity. The procedure for opening each account was identical.

History proves that new disruptive technology often exploits the gaps in existing financial regulations. From 1996 until mid-2006, the existing US financial regulations governing money service businesses and the state laws covering money transmitters were unclear and did not precisely define the regulatory status of new digital currency products such as e-gold. Bank Secrecy Act regulations enacted before 2001 did not clearly define the digital currency business. Neither the act of issuing digital currency nor the exchange of digital currency with federal money accurately fit into any existing US financial regulations.

Consequently, until 2006, a majority of digital gold operators openly made the claim that their businesses did not require any US licensing. Also, the operators of digital currency exchange companies in the USA claimed to be exempt from any licensing requirements. Operators based this claim on the fact that the US regulations did not define digital currency units as money or currency.

In the case of e-gold, the operators had tried to show clearly that the e-gold operation functioned vastly different from a bank. After 2000, the e-gold management never handled any customer funds or financial transactions. All incoming customer funds and outgoing monies were handled exclusively by third-party exchange agents. This separation guarded against financial risk. Additionally, no financial transaction information, such as check amounts or wire instructions were revealed to e-gold during any transaction.

The operation of an e-gold account generated no suspicious activity reports (SAR) or currency transaction reports (CTR). There was no anti-money laundering program in place at e-gold. The KYC or know your customer requirements of banks and money service businesses were not present at e-gold. Because of the technology, in the years before 2006, e-gold seemed to operate beyond all US financial regulations.

In Douglas Jackson's description of e-gold account activity, he detailed that the e-gold operation was merely maintaining a closed accounting system and transferring digital units from one account to another. He continually asserted that e-gold was not a bank, and it was not a financial company, and business operations never handled national currency customer funds.

Compared to all other online payments systems at that time, the e-gold digital precious metals platform was unique. The e-gold system had been

designed to be free from most financial risk. Within the system of 100 percent reserve metal value, there were no debts or contingent liabilities. All of the clients' gold was stored unencumbered in secure vaults. There was never any borrowing of metal, and no loans could be created using the metal as collateral.

The entire e-gold operation held no national currency, did not offer any currency exchange services to the public and had no bank accounts. From this profile, it is easy to understand how the e-gold operators, along with many users, had a belief that the company should not be considered a money transmitter.

By operating beyond US financial regulations, the e-gold business had no mechanisms in place that supervised accounts for suspicious activity; such as money flowing in and out on a daily basis. All regulated US financial services, including banks, brokerage firms, and even PayPal, have software that monitors account activity. If a PayPal account holder regularly withdraws digital funds into their bank account or prepaid card, that account is subject to being flagged and frozen, pending an inquiry by PayPal into the source of the activity. Flagging an account for possible money laundering activity occurs in PayPal with amounts as little as $500–$800 a month.

It is important to understand that when e-gold began operating, it was the first commercial online digital payment system in the world. As a new technology, digital gold had never before been used, defined, or regulated. No existing regulations covered the operation of a digital currency business. Historical legal terms which had been used to identify financial activity such as money, cash, and currency did not apply to the e-gold operation or its new Internet digital currency units backed by gold bullion.

Douglas Jackson and others directly involved in the e-gold platform, such as the employees of the company's primary dealer OmniPay, were known for having made statements regarding how e-gold was different from a bank. These viewpoints and disclaimers often highlighted differences between conventional bank operations and e-gold digital currency.

The e-gold user agreement and the OmniPay terms of service agreement both contained statements declaring that e-gold was not a bank and in no way operated a financial company responsible for holding deposits on behalf of customers. Under section 2 of the January 2001 e-gold user agreement, this statement can be found.

Conditions of Use
User acknowledges that (i) the e-gold service and Issuer are not a bank, (ii) e-gold accounts are not insured by any government agency, and (iii) the e-gold service and Issuer are not subject to banking regulations.[10]

In the OmniPay terms of service from February 2003, this statement was found, "User acknowledges that G&SR is not a bank, is not subject to banking regulations and does not hold any value on account for User."[11]

Text that first appeared on e-gold.com in 1998 and also found in both the FAQS and Terms of Service pages highlighted the company operator's determination to show that e-gold was not a bank. From the e-gold website in June 1998, here is an example of that argument.

> It is important to note the difference between a digital currency balance and a bank deposit balance. Deposits in a bank are regarded legally as loans to the bank. A bank is permitted to make investments (loans) using the money belonging to their depositors. Metal entrusted to G&SR is not a deposit at all: it is held as a bailment (like grain in a grain elevator). G&SR may not allow any encumbrance or lien to be placed on customer metal. G&SR is not borrowing it from you but rather safeguarding it for you for a fee. The banking system in general, operates on a fractional reserve basis. This is perfectly natural and legitimate for money in a savings account or time deposit. You, as an individual, may do what amounts to the same thing; borrow money from some people and use it to make loans to other people. In our view, however, "checkable deposit" is a contradiction in terms.[12]

In March 2016, Douglas Jackson directly responded to the idea that e-gold had been avoiding the label bank to gain a regulatory licensing advantage. Here is that exchange from his email.

> It is wearisome to see accusations that any element of e-gold's design ever stemmed from some desire to sidestep regulation. That simply never happened. That is starkly different from recognizing the multiple gross square peg round hole mismatches between what we were doing and the sorts of businesses contemplated by legislators and regulators. There was not then nor is there yet a regulatory rubric that properly fits with the model of a private sector monetary authority. There probably never will be. Lacking such, we have learned (at great cost) that it would have been expedient to seek regulation under any available auspices. One silver lining of the legal case was that the Plea Agreement laid out an explicit bespoke regimen deemed to be acceptable to the U.S. government. The stated intention btw was for e-gold to resume operation as a licensed registered and financial institution.

> My contrasting e-gold to a bank was part of my incessant efforts to explain to people what e-gold was. People are chock full of memes and preconceived notions that make it difficult for them to understand something new, even if it is very straightforward and coherent.[13]

Financial Risk

Physical metal backed all e-gold accounts; never a financial instrument or paper currency. Therefore, many users labeled e-gold as free from financial risk. Stock markets could tumble, and countries could default on their debts; however, gold will always be the physical commodity and always weigh the same. A gram of gold deposited in a vault will always contain the same gold when removed from the vault. This statement is true whether the term is 100 or even a 1000 years into the future. However, an absence of financial risk does not mean that the value of an e-gold account, as denominated in the national currency, will remain the same over time. The changing value of an e-gold account was an issue that confounded many new users. The national currency value of an e-gold account would fluctuate on a daily basis according to the price of gold. If an account holder's initial deposit had been $500, depending on the price movement of gold as denominated in US Dollars, a month or two later that account could be valued higher ($556.82) or lower ($489.11). In the early years of the digital gold empires, gold was relatively stable. However, approaching the 2008 recession and shortly after that gold increased in value more than 600 percent.

E-gold Versus Bank Payments

An e-gold "spend" was the movement of digital units from one account to another within the closed e-gold ledger. This process was very different from an average bank payment. Each new e-gold online transaction required owner approval for a spend at the time of the payment. This requirement established an important distinction between e-gold payment orders and regular bank payments. When compared to e-gold, credit card payments, bank wires, and personal checks, all used very different procedures for the transfer and clearing of funds.

Consumers adopted credit cards in the 1950s, and the card's design had not changed much since that time. Modern credit card payments are not fund transfers. At the moment of a card payment, either in a store

or online, the transaction taking place is an authorization to remove an amount of funds from the card account at some future date. Within the card's financial account, those funds are earmarked for transfer but remain in the account. It is not until a later settlement date that the merchant's financial company pulls the previously authorized funds from the account. This final step occurs automatically, and the cardholder is unaware of the settlement activity. In the case of credit card fraud, funds are pulled from the card owner's account without his knowledge or consent.

Sending or pushing funds from a customer's account into another account became known as an e-gold "spend." Text from the e-gold website explained this transaction.

> "Spend" means the act of transferring value between e-gold accounts in fulfillment of a payment order entered by User. Spends are accounted by weight and convey title to that precise fine weight of metal. Spends may not exceed Available Balance.[14]

Pushing the funds from a user's e-gold account is very different from someone other than the account owner pulling funds to settle a credit card transaction, days after the actual consumer's card purchase.

E-gold accounts did not permit any client to pull an amount of funds from another account such as a monthly reoccurring subscription payment. The "spend" was a direct action by the account owner recognized as a payment order. To execute an e-gold payment order, an account owner had to authorize the payment directly in real time by "pushing" the exact amount to the payee at the moment of the transaction. If the e-gold account owner was not online directly authorizing the payment, no digital gold value could ever leave the account. It was not possible for an e-gold user to permit a future payment or provide prior approval allowing someone other than the user to pull funds from the account. Clients "pushed" value out of the account and this was done by the account owner and authorized in real time.

As each account holder was always responsible for each spend, there was no apparent reason for any e-gold transaction to be reversed. Many users viewed this procedure as a vast improvement over slow and expensive conventional bank payments or credit cards.

Furthermore, during a credit card transaction, the account holder's personal information becomes part of the transfer. Often, at the time of a card payment, the account holder's personal information is improperly

handled leaving the identification data and personal information accessible to theft and exposed to possible fraud. The only information exchanged during an e-gold transaction was the account number. Credit cards have no purpose being used online in a digital environment. E-gold transactions solved these issues and other card transaction problems.

When compared to personal checks, the benefits of using e-gold were very clear. A consumer personal check is a withdrawal order. Once the receiver endorses that check, it becomes a draft. Again, as in the credit card settlement, the draft pulls funds from a bank account by someone other than the owner.

Additionally, it is possible for any merchant to receive a check payable from a customer's account only to find out at a later time, there are no funds in that account. Checks bounce in merchant bank accounts every day. E-gold account owners could only spend an amount up to the maximum balance in an account. The funds had first to be available before pushing the value into another account. An e-gold spend could never bounce.

The company was also publishing a statistics page that featured daily transaction data. The e-gold statistics page noted the current date and provided recent data based on the previous 24 hours of activity in the e-gold system. As of April 13, 2001, the data offered to visitors included:

The Total Number of Open Accounts e-gold System Activity in Past 24 Hours

New Accounts
Users Accessing Accounts
E-metal spends

The Velocity of Spends (Value Circulated by Spends over a Given Time)

Metal
Weight (oz.)
USD Equiv.

Balance Summary

Number of Funded Accounts
Average Funded Account Balance (oz.)
Metal in Circulation (oz.)

Balance Distribution of Funded Accounts (Stated for Gold, Silver, Platinum, and Palladium)
This balance distribution showed the exact number of accounts containing a balance of metal on that day. For example, on April 13, 2001, the following number of accounts held metal balances.

0–1 oz.	76,554
1–10 oz.	3369
10–100 oz.	512
100–1000 oz.	55
1000–10000 oz.	1
10000–100000 oz.	0

Historical Number of Accounts Created per Week[15]

This important transparency offered through the e-gold website has allowed visitors and customers to make critical observations about how account holders used e-gold. By researching the number of transactions made each day, the size of each payment and the amount of value in the account, it was possible to theorize accurately how customers used e-gold. Since e-gold users could send payment for as little as .0001 of a gram of gold, after 2001, the statistics page began to display thousands of tiny micropayments each day. Later research suggested a large percentage of these tiny spends had been mass "interest" payments conducted through online high-yield investment program (HYIP) Ponzi schemes.

The e-gold system also paid a tiny referral fee as an incentive to account holders for promoting the company through hyperlinks. While the payments were minuscule, some original account holders reported accumulating substantial amounts of gold over a period of years. This referral system did encourage legions of new accounts and new digital currency users.

Many of the early users of e-gold were fans of precious metal. The belief among this group of people was that holding value and savings in the digital precious metal, particularly gold bullion, could protect their savings from inflation and the risks inherent with fiat currencies. Some of these users were advocates of a single gold standard. Their arguments were similar to the many statements made by Douglas Jackson while describing e-gold as a superior currency.

The year 2000 ushered in an e-gold shopping cart and automation interfaces. E-gold digital currency was the first online payment system to capture a broad global base of both merchants and users. It was also the very first online payment system to offer an application programming interface (API). This detailed information on interacting with the e-gold website was available in early 2001.

E-Gold Shopping Cart Interface (SCI)—The e-gold SCI provides check-out capability to any e-gold account holder by allowing them to place a button on their Web page to accept e-gold payments.
E-Gold Automation Interface—These defined methods allow programmers to perform e-gold actions (spend, balance, history) via their own program.[16]

The interface enabled other online businesses to build applications on top of the e-gold platform and further expanded the company's e-commerce capabilities. The Gold Casino also launched in 2000. This popular website was full of real casino games and only accepted e-gold. The player's interface allowed direct funding of an account and immediate withdrawal to a player's e-gold account. This casino introduced e-gold to the world of online gambling.

Independent third-party exchange agents came online in dozens of countries around the world. These competing digital currency systems, such as WebMoney already had a small army of third-party agents. As the global market for digital currency expanded, many of them began to add e-gold to their in-house line-up of digital currency products. By 2001, WebMoney Transfer had already been in operation for about three years and was responsible for building an extensive global network of agents. The company also offered WebMoney prepaid cards.

This new liquidity provided through agent expansion fueled e-gold's growth. For consumers to widely adopt any digital currency, there needs to be a good fluid movement between federal money and digital currency. Increased points of exchange for digital currency and a wider variety of payment methods accepted at these points were the two primary factors that encouraged growth in the early digital currency market. Expanding liquidity is what occurred with e-gold during the years 2002–2006. With more exchange agents around the world and more ways to fund an e-gold account, consumers entered the e-gold market. This same activity can be

seen in 2015 as the payment methods and options for purchasing bitcoin expand around the world.

The feature that made e-gold payment non-repudiable also made it an attractive target for online hackers. If a thief was able to obtain the login credentials of an account holder, there was no stopping a crook from cleaning out the e-gold account. It was not possible to trace the stolen funds or verify the receiving account owner's identity. These factors made e-gold a popular target of criminal organizations and malware. Flaws in the Microsoft Windows operating systems and the Internet Explorer (IE) browser were used to uncover and record the e-gold credentials of unsuspecting e-gold users. The first-ever case of a phishing attack on a financial institution occurred with e-gold in mid-2001. Bad actors later adopted his type of attack for bank accounts.[17]

By late 2001, e-gold exchange activity was supporting more than a dozen large agents around the world that offered a convenient exchange of e-gold digital units for national currency. Payment options included wire transfer, Western Union, cash, money orders, eMoneyMail, and even personal checks. A few companies tried filling buy orders for e-gold by accepting credit card payments. However, this was an attractive scam for online carders. Since users could not reverse an e-gold transaction and banks often reversed credit card transactions, the selling agent was in for some big losses when the card transactions were deemed fraudulent and reversed. At that time, a market also developed for the exchange of other digital currency, such as WebMoney into e-gold.

The Ponzi Tsunami

Ponzi schemes are fraudulent high-yielding investment opportunities offered to unsuspecting investors. The core of the scam is taking funds from new investors and paying a high return to the old investors. By paying that high rate to early investors, those participants act as "shills" and gain the attention of more investors hoping to get rich. At some point in the scheme, the Ponzi operator stops paying investors and steals the funds. Ponzi schemes always collapse.

Before digital currency and e-gold, a Ponzi operator had to accept cash or cycle the funds through bank accounts. Historic e-gold data helps to illustrate how HYIP Ponzi schemes had a role in the dramatic growth of e-gold and other digital currencies. Some insiders speculate that HYIP Ponzi schemes were the only factor in the growth and early widespread

use of digital currency. Data obtained from the e-gold website provides some additional information on this topic.

Unfortunately, in 2016, HYIP Ponzi scams using digital currency are still widely found across the Internet. It is possible for anyone searching the Web to locate an active digital currency Ponzi scam quickly by simply Googling "HYIP bitcoin" or "HYIP Perfect Money."

E-gold's connection to fraudulent HYIP Ponzi schemes began just about three years into its operation. As detailed in court documents, between September 1999 and March 2000, parent company G&SR accepted $2,450,000 in funding from a Ponzi kingpin named John Wayne Zidar.

Zidar along with at least five other associates had been operating several private phony "investment" programs under the names Vista International, Oakleaf International, and Rosewood International. Zidar targeted "Christians" and illegally solicited money from consumers for bogus investments. He and others used the funds for their personal expenses and lavish lifestyles. These three investment schemes were said to be part of a "Private Asset Enhancement Program," which produced a very high return on investment with virtually no risk. Of course, there was no investment operation, only the Ponzi. Zidar, who was a former custodian at a steakhouse in Florida, also ran World Diversified International, which acted as an umbrella organization overseeing the services and cash flow of the other companies and "private investment" offerings. From late 1997 through May 2000, Zidar and his associates defrauded and stole approximately $74 million from more than 2500 individuals.[18]

These fraudulent investment schemes were nothing more than dressed-up Ponzi scams. Here is a description from the indictment of Zidar and five others.

> The essence of this scheme and artifice to defraud was to solicit investments from individuals and organizations by falsely promising investors that they could earn substantial profits on their investments in the "private economic arena" with virtually no risk. In truth and fact, the defendants were conducting a "Ponzi" scheme in which a portion of the invested funds from some investors was used to pay the promised returns and interest of these and other investors, thereby decreasing the amount of funds available for investments. Additional portions of the investors' funds were: (a) used to pay commissions to agents who solicited investors; (b) placed into highly speculative ventures which were either fraudulent or so risky that they resulted

> in a total loss of funds; and (c) misappropriated by the defendants for their personal use.[19]

Investors in these scams were instructed to send funds by mail, private or commercial interstate carrier, or wire transfer. The content and material on at least one of the Zidar websites recommended e-gold. However, there is no evidence that any of Zidar's Ponzi investment programs ever received investor funds through the e-gold platform.

However, between September 1999 and March 2000, $2,450,000 derived from Zidar's Ponzi scams was spent on the purchase of private stock in G&SR. The parent company of e-gold. Law enforcement agents later arrested Zidar and his associates. Initially indicted on more than 100 counts; in August 2002, he was convicted of more than two dozen counts including wire fraud, mail fraud, money laundering, and conspiracy to commit those crimes.[20]

Given the open opportunity to comment on what occurred with Zidar's investment, in a 2016 email, Douglas Jackson made these statements.

> In the course of our initial due diligence, we saw there was an SEC investigation. Zidar indicated to me when I made a site visit to his offices in Phoenix that it was routine and not uncommon with hedge funds. Later, in 2000, when the second tranche of investment, $2 million, was due, we learned of a grand jury investigation relating to alleged securities violations. We contacted the SEC and asked if we should refuse this second round. The SEC investigator advised that they would take no action against us if we proceeded to accept the money. During the same call, we had the impression that the case against Zidar may have had a political element in that the agent volunteered that Zidar advocated such things as homeschooling and mistrust in government. I was eventually called to testify for the defense in the Zidar case. The SEC never took any action against us and, in fact, we worked closely with the SEC in breaking up Ponzi schemes. In one subsequent case (Ebiz Ventures), the court-appointed receiver working for the SEC used the e-gold system for distributing seized money via Spends to Ponzi scheme investors.[21]

Zidar and the other defendants were found to be jointly and severally liable for a sum of money equal to $74,184,295.00 pursuant to Title 18, United States Code, sections 982 and 984. The indictment also listed a forfeiture to the USA of 450,000 shares in G&SR.

In July 2009, at age 66, John W. Zidar was sentenced in Seattle's US District Court to 30 years in prison and three years of supervised release for leading what prosecutors referred to as the largest Ponzi scheme ever prosecuted in the Western District of Washington. Investigators uncovered around $25 million of the victims' money and most of them received about 40 cents for each dollar they had invested. The fate of approximately 8 percent of the private stock in G&SR. purchased with Zidar's Ponzi money remains unknown.

By 2002, e-gold had over a million user accounts and the market for HYIP schemes was growing rapidly. In 2003 and 2004, discussion forums with names like Talkgold and Moneymakergroup were online promoting HYIP schemes. Each hyperlink promoting a scam included the owner's referral number, and the forum operators received payment for each victim that clicked through and invested.

During these years, as the Internet gained more users, new global markets of victims for each Ponzi scam emerged. A majority of the HYIPs accepted e-gold. There were tens of thousands of the HYIP Ponzi schemes between the years 2001 and 2008. The size and scope of these HYIPs are shocking.

While the history of the Ponzi scam includes banks, financial companies, mortgage firms, and even civic organizations, never before had it been so fast and straightforward to set up and operate a global financial scam. Digital currency allowed a Ponzi operator to hide in plain sight and to profit without identifying themselves.

These schemes did not solicit qualified and accredited investors. Fraudsters directed a majority of digital currency Ponzi schemes at people with very little money. The HYIPs would accept as little as one dollar, and most programs attracted a $1 and $5 investment. Here are some 2005 listing examples from the TalkGold HYIP promotional forum. These examples include possible minimum investments of $1, $5, and $10

- We pay 42 percent daily for three days directly to your e-gold account. Total 126 percent Minimum spend is $1.
- Egold Invest Inc. 30–40 percent Daily for Five Days. Minimum deposit is $1.
- InvClub.com Trade Precious Metals online with as little at $10, 3 Level 5 percent Referral bonuses
- Sun & Pine Group 4 Investment Plans to Choose From—$5 Minimum Investment

- Your Easy Street Unlimited income from a one-time payment of under $38.00[22]

A ridiculously high advertised rate of return on the HYIP scam was likely the reason so many unsuspecting people believed it was worth a risk. Here are a few more examples from the same 2005 TalkGold website.

- Gold Income Investment 105 percent in Seven Days
- Real-Life-Invest 95 percent on Each Deposit for Four Days
- Trading Experts 1 percent Daily Lifelong
- Elite HYIP Group 150 percent Daily for Two Days
- Alpine-HYIP 50 percent Daily for Six Days
- EWorldInvestment.com Variable Interest Rates up to 1460 percent
- FastHYIP.com 6–10 percent Daily for 30 Days and 7 percent Referral Paid Directly[23]

E-gold was not alone in providing digital currency services to the HYIP industry. However, e-gold was the first to introduce online payments to Internet Ponzi schemes. This activity paved the way for other operators such Liberty Reserve. HYIP programs will use whatever digital currency is popular at that time. When e-gold closed, Liberty Reserve became the HYIP digital currency of choice. In 2013, when Liberty Reserve was seized and shut down, Perfect Money digital currency took over the role as one of the primary mediums of exchange for HYIPs.

Ponzi Payments

On January 31, 2001, the US Securities Exchange Commission obtained temporary restraining orders and asset freezes against Donald A. English, E-Biz Ventures, and EE-Biz Ventures. Beginning in October 2000, Donald English has been operating an extensive fraudulent Ponzi scheme and using e-gold to accept funds and make payouts. Instructions for potential investors to funds the Ponzi clearly showed e-gold as the method of funding an E-Biz investment account.

1) You must be 18 years of age, have an Egold account and join E-Biz Ventures as a Member.

ABOUT SPENDING FUNDS TO E-BIZ VENTURES

> Go to the Website http://www.ee-bizventures.com and follow all the instructions for how to Spend to correct Egold accounts and what goes into the MEMO field of each Spend.[24]

The Securities and Exchange Commission charged that Donald English with creating and organizing an Internet Ponzi scheme identifying at least 22,000 investor accounts that lost, at least, $8.8 million.[25]

The January 2002 Wired.com magazine article entitled "In Gold We Trust" by Julian Dibbell further investigated the e-gold HYIP problem.

> But what troubles him [Douglas Jackson] most are the Ponzi schemes: Hundreds of online pyramid scams have made e-gold (because of its convenience and because it offers bilked users no way to cancel charges) their payment system of choice.[26]

The management of other popular companies in the digital currency industry, with insight into HYIP activity, stated that it was their belief a good percentage of e-gold's daily business came from HYIP Ponzi activity. After the e-biz scam collapsed, an associate of Donald English named Garry Stroud engaged in discussions with authorities and the receiver for the return of $9 million of the lost e-biz investor funds.

> The money [$9mil], he said [Donald English], would be provided by a benefactor named Garry Stroud, a resident of Canada who claimed to be the principal in a Swiss bank, Euro Credit and Exchange.[27]

However, Garry Stroud also turned out to be a complete scam artist. His intent was to secure the list of e-biz investor names for one of his Ponzi schemes. The $9 million check bounced and the investor funds were not returned. In June 2001, the U.S. Securities and Exchange Commission (SEC) filed suit against Garry Stroud in US District Court in Oklahoma City, Oklahoma. Since that time, several addition cases have been filed against Garry Stroud.

> The Commission's complaint charged Stroud with conducting an ongoing Internet investment scheme that fleeced over 2,200 investors worldwide of approximately $1 million since 1998. According to the Commission's complaint, Stroud, operating under several fictitious businesses, used Internet websites and email to hawk seven spurious investments, including so called "Morgenthau Gold Bond Certificates," foreign goldmining projects, and "primebank" trading programs, promising investors extraordinary returns

> with little or no risk. The complaint further alleged that these investments were, in every case, pure shams and that Stroud had not paid a single investor the promised returns. According to the complaint, Stroud targeted his fraudulent investment offerings mainly to investors who were recently defrauded in another investment scheme. That scheme, known as EBiz Ventures…[28]

Garry Stroud also used e-gold as a preferred method of accepting money from unsuspecting victims. In May 2001, $50,000 of funds received through e-gold was used to pay lawyers representing Donald English during his ebiz legal case. Angelic International was one of Garry Stroud's next investment schemes which also used e-gold.

> Records from E-Gold Ltd., the Internet payment service, reflect that he has raised approximately $300,000 from over 1,000 investors in the Angelic offering since April 2001. To invest in the Angelic International program, an investor deposits money via a credit-card transaction or wire transfer into accounts opened in their names at E-Gold.
>
> E-Gold then transfers E-Gold "currency" (in U.S. dollar denominated amounts) via the Internet, from the investor's account to one of three Angelic International accounts held at E-Gold.[29]

This Ponzi investment activity from late 2000 to early 2001 drew thousands of new users to the e-gold platform and generated fees for both e-gold and OmniPay.

The Elephant in the Room

At the beginning of e-gold's business, during the years 2001 and 2002, digital currency system operators, exchange agents, and customers across the industry were well aware of e-gold's widespread use as a method of payment in fraudulent online HYIP Ponzi scams. However, the activity was allowed to continue and flourish. Research has indicated that e-gold handled millions of payments on behalf of HYIP Ponzi schemes.

Mass payment or batch pay software that directly connected through e-gold permitted Ponzi operators to make thousands of tiny micro interest payments with a single keystroke. The e-gold interface matched with the ability to make a plethora of tiny payments at one time created a viable environment for the operation of online Ponzi scams. As an example, if a Ponzi HYIP had accepted 3000 "investors" all contributing one dollar, the operator may have had to pay out a 5 cent interest payment to those

3000 investors each day or two. The fees and costs to perform this task with an online payment company such as PayPal, even if the company allowed such activity, were prohibitive. However, these multiple payments were accomplished on the e-gold platform where the fees were low and the activity could be profitable.

Customers opened tens of thousands of e-gold accounts that never accumulated any real value. Users dubbed the reason for at least some of these low-value accounts as "dust spam." This activity was the opening an e-gold account and spamming the referral code out in millions of email addresses or through online posts. Tiny referral fees accumulated in the e-gold account without any other real activity. However, this activity could not account for the tens of thousands of tiny e-gold payments each week, which suggested interest payments on Ponzi investments.

In November 2004, the Australian Securities and Investments Commission (ASIC) gave notice to three local exchange agents operating without any financial licensing.

The ASIC release stated, "ASIC acts to shut down electronic currency trading websites." The agency called for each firm to obtain an Australian financial services license (AFSL) or cease activity. ASIC defined digital currency, such as e-gold, as noncash payment systems which do require that AFSL. Without any drama or seizures, the three companies quickly closed down or moved operations to another country. The closed digital currency operations were:

- www.goldex.net
- www.sydneygoldsales.com
- www.ozzigold.com

By 2005, the existing US financial regulations still did not define e-gold as a money transmitter business. However, on December 16, 2005, a Magistrate Judge in Orlando, Florida issued a search warrant allowing for the electronic investigation of Microsoft SQL Server databases which held a vast amount of the e-gold operation. The search turned up e-gold customer information, transaction records, and OmniPay's client database.

On the evening of December 19, 2005, F.B.I. and Secret Service agents raided the Melbourne offices of G&SR. At the same time, a team of federal agents also raided the nearby home of e-gold's co-founder Douglas Jackson. The US Department of Justice had named this action, "Operation Goldwire."

While agents seized boxes of financial information and several computers, no arrests were made. This move by law enforcement was the first of several major legal actions against e-gold.

The search warrants had allowed federal agents to copy approximately three terabytes of digital information from the e-gold servers operated by AT&T from Orlando, Florida. Along with 100 boxes of seized documentary evidence and a mirror image of e-gold's servers, Operation Goldwire had begun. Immediately after this seizure, all of the bank accounts operated by G&SR were frozen.

The lack of access to company funds temporarily crippled the exchange operation. As a direct result of this action, more than 200 customer checks sent by the company were returned for nonpayment. However, on January 13, 2006, during an emergency hearing in US District Court, the government failed to sustain some of the allegations made in the search warrant, and the court removed the government's freeze order on G&SR's bank accounts.

During the hearing, it was disclosed that G&SR had engaged in a dialog with agents of the US Treasury. Furthermore, G&SR had previously made a formal request during the spring of 2005 for the Internal Revenue Service, Small Business and Self-Employed (IRS SB/SE) Division to conduct a Bank Secrecy Act Compliance examination. This review could have determined a possible basis for regulating the company's activity. These facts and others showed that G&SR executives had been talking with government agents and regulatory agencies about the possible future regulation of e-gold's digital currency operation.

In a March 2016 email, Douglas Jackson commented on this situation.

> In 2005, we redirected a never ending IRS audit that had already been going on for 4 years. At our request, it became a formal BSA Compliance examination. Before 2005, I had never sought a determination because it was apparent to me that we did not meet any existing definition of a financial institution (again, see prior Middlebrook analysis). We had been in contact over the years with every Federal law enforcement agency, and no one ever uttered a peep to suggest they thought we were operating in violation of any laws. Most of my efforts had been to engage with and train law enforcement on how to best make use of our investigative resources – how to craft subpoenas as to make them most effective, how to fast track inquiries, how to provide feedback enabling more effective investigations on our part. These efforts were highly successful with the egregious exception of the SS [U.S. Secret Service]. It was evident for years that they were determined to not understand.[30]

Even with bank account issues and the government's seizures of business files and property, throughout this ordeal, G&SR had eventually met the business' financial obligations and remained fully operational. The e-gold system moved along without a slowdown or closure.

In January 2006, Douglas Jackson published an open letter on the e-gold website, highlighting the facts regarding the company's interaction with the government.

e-gold® welcomes US Government review of its status as a privately issued currency

> G&SR, for nearly a year, has been engaged with an agency of Treasury in a BSA (Bank Secrecy Act) compliance examination it had voluntarily initiated. G&SR had previously proposed to the Government that e-gold be classified for regulatory purposes as a currency, enabling G&SR to register as a currency exchange. In a Treasury report released January 11, 2006, however, the Department of Treasury reaffirmed their interpretation of the USC and CFR definitions of currency as excluding e-gold. The Treasury issued a report on January 11, 2006, confirming that E-gold accounts were excluded from the definition of "currency" under the United States Congress and Code of Federal Regulations definitions. The Treasury did not want E-gold to be acknowledged as a form of money, which made it impossible to obtain a money transmitter license.[31]

Iranian Accounts

In November 2006, e-gold closed all of the accounts operated by Iranians or at least all of those operated from Iranian IP addresses. At that time, a message was sent out to all of the Iranian e-gold account owners from the service department:

> Your account has been frozen in compliance with the laws which govern e-gold, Ltd. and its managers. e-gold, Ltd. has taken this step in strict compliance with the law. No further information is available at this time. When additional information is available it will be provided upon account login. Thank you.[32]

Many of the account owners, who had lost money through this action, complained about it on email lists and discussion forums. E-gold did not return the Iranian funds on deposit. There were rumors about why the accounts had been frozen and seized by e-gold; however, no further infor-

mation became available that year or the next. In July 2008, information surfaced regarding civil penalties and the Office of Foreign Assets Control (OFAC) regulations governing sanctions programs issued under the Trading with the Enemy Act, in 31 CRF part 501. C.

A July 11, 2008, document published by the OFAC of the US Department of the Treasury became available online. The paper listed enforcement information on two cases from June and August 2006. In both cases, US persons had been fined for alleged violation of the prohibitions in Iranian Transaction Regulations. Both individuals were engaged in buying e-gold digital gold currency from a popular exchange agent located in Kish Island, Iran.

The global nature of the Internet brings foreign companies and contacts into every American home. It is rare that a consumer would ever verify the identity or physical location of an online order with a well-known digital currency company. Furthermore, from the consumer's point of view, this type of investigation may not be regarded as the consumer's responsibility. Certainly, during a regulated bank transfer, the bank would immediately alert the account holder of attempted wire transactions or business with a sanctioned country. However, this was not the case with the unlicensed and unsupervised financial activity of e-gold and third-party independent agents. This lack of supervision had allowed any e-gold user to circumvent US Sanctions and engage in financial business with Iran. The following text is from the OFAC Enforcement Information July 11, 2008.

> One individual has agreed to a settlement totaling $840 for alleged violation of the prohibitions in the Iranian Transactions Regulations: OFAC alleged that in August 2006, the individual attempted to transfer funds to Me-Gold Kish, Co. in Iran in an apparent attempt to purchase electronic gold without an OFAC license. The individual did not voluntarily disclose this matter to OFAC.
>
> One individual has agreed to a settlement totaling $400 for alleged violation of the prohibitions in the Iranian Transactions Regulations: OFAC alleged that in June 2006, the individual attempted to purchase electronic gold from Me-Gold Kish Co. in Iran in apparent violation of §§ 560.201, 560.203 and 560.204 of the Iranian Transactions Regulations. The individual did not voluntarily disclose this matter to OFAC.[33]

Documents from the Director of the OFAC later showed that June 6, 2007, the OFAC had issued a Prepenalty Notice of $5,000,000 to G&SR. The reason for the penalty was stated as "exportation of financial

services in the form of 56,739 e-currency accounts through its website for persons located in Iran."

> In as much as no license or approval was issued by OFAC for these transactions, they violated the Iranian Transactions Regulations (the "ITR"), 31 C.F.R. Part 560, promulgated pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1706 ("IEEPA").
>
> OFAC has determined that GSR has violated the ITR and that a reduction from the proposed penalty amount, set forth in the Prepenalty Notice dated June 6, 2007, is warranted to account for the payments GSR is to make pursuant to other U.S. government enforcement action. Accordingly, a civil penalty in the amount of $2,950,000.00 is hereby imposed upon GSR pursuant to 31 C.F.R. § 560.705.[34]

Between September 2003 and December 2006, government investigators determined that persons located in Iran had opened more than 56,000 e-gold accounts. The e-gold operators had not voluntarily disclosed these violations to the OFAC and in 2008 G&SR was fined nearly $3 million.

Case 1:07-cr-00109-RMC

The 2007 US prosecution of e-gold Ltd. and its operators shaped the future of US financial regulations that focused on the movement of value online. The e-gold case had a dramatic impact on the present-day cryptocurrency industry and the potential licensing requirements of bitcoin products in the US market.

United States of America
v.
E-gold, Ltd.
Gold & Silver Reserve, Inc.
Douglas L. Jackson,
Barry K. Downey, and
Reid A. Jackson,
Defendants.
Violations:
18 U.S.C. § 1956 (Conspiracy to Launder Monetary Instruments);
18 U.S.C. § 371 (Conspiracy);
18 U.S.C. § 1960 (Operation of Unlicensed Money Transmitting Business);
D.C. Code § 26-1002 (Money Transmitting Without a License)

18 U.S.C. § 2 (Aiding and Abetting and Causing an Act to be Done); and 18 U.S.C. § 982(a)(1) (Criminal Forfeiture).

Prosecutors filed the original 28 pages in US Federal court on April 24, 2007. Details from the document showed that the grand jury had been sworn in almost a year earlier in May 2006. Count one of the e-gold indictment charged the defendants with transmitting monetary instruments or funds involving the proceeds of illegal activity. By knowing the e-gold transactions were designed to conceal the illegal source of funds, Count one alleged that the defendants had acted with the intent of promoting the illegal activity. Items 34 and 35 from the e-gold indictment stated:

> 34. Regularly, during the course of conducting the E-GOLD operation, the defendants and their employees recognized that certain accounts were being used for criminal purposes. On numerous occasions, the E-GOLD operation indicated in the account records contained in the "e-gold" computer database the type of criminal activity that the account-holder was engaged in, including, among other things, "child porn," "Scammer," and "CC fraud." The defendants nevertheless allowed transactions in these accounts to continue.
>
> 35. The E-GOLD operation regularly received complaints from customers that they had been the victim of a crime and also regularly received notification from customers of specific "e-gold" accounts that were involved in criminal activity. It was not the E-GOLD operation's practice to either close these accounts or, as is required by law for certain financial institutions, report the activity to law enforcement. In certain cases, the E-GOLD operation sent messages to customers who reported investment scams advising them to "educate" themselves about certain types of investment fraud.

Of the three dozen accounts seized through the government's indictment, a majority of them had been previously identified, through internal company procedures, as being involved in suspected illegal activity and were labeled by the employees and management of e-gold. The prosecutors had followed up on these labels and further identified the e-gold transactions from these accounts as alleged payments for child pornography, stolen credit card information, and wire fraud (Ponzi schemes). As odd as this situation appears, government investigators had not been out conducting separate investigations or uncovering any new child exploitation crimes that led them back to e-gold; investigators had merely read the labeled e-gold accounts and followed up on the lead.

The investigators that had been sorting through the e-gold database, secretly copied from the company's servers in Orlando, had uncovered the labeled accounts. The information provided by e-gold on the accounts had enabled investigators to work backward and uncovered the alleged crimes. Prosecutors used these same cases as the basis for the e-gold indictment.

Unlike a bank or any regulated money service business, that are both required to report suspicious financial activity, e-gold had made no mention of this activity or any other suspicious activity involving e-gold accounts to FinCEN regarding this or any other possible criminal activity. Had the company voluntarily reported suspicious activity through the appropriate channels by filing SAR with FinCEN, e-gold may have even retained some measure of protection from civil liability under Federal law (31 U.S.C. 5318(g)(3)).

As item 36 from the indictment also stated, in many cases, when e-gold employees' uncovered accounts tangled in possible illegal activities, e-gold merely required that customer to submit paperwork to the company indicating that the account owner had no direct affiliation with the e-gold business. Rather than closing the account, freezing the funds or even reporting the possible criminal activity, e-gold, attempted to distance itself from the customer's activity. These accounts were permitted to remain open, active, and any third-party agent could exchange the value of national currency. Item 37 explains this activity in great detail:

> 37. Knowing that "e-gold" was being used for criminal activity, including child exploitation, wire fraud (investment scams), and access device fraud (credit card and identity theft), the E-GOLD operation continued to allow accounts to be opened without verification of user identity, assigned only a single employee with no relevant experience to monitor hundreds of thousands of accounts for criminal activity, and encouraged users whose criminal activity had been discovered to transfer their criminal proceeds among other "e-gold" accounts.

One of the e-gold business activities that baffled most users along with the law enforcement community was the practice of placing a "value-limit" on an e-gold account. In the later years of the e-gold operation, if the e-gold operators recognized an account as possibly being involved in criminal activity, that account would receive a form of usage restriction identified by the term "value-limit." This restriction was the most severe action ever undertaken by e-gold against any alleged illegal activity not yet identified

by a court order or a formal request from law enforcement. If from within the e-gold company, alleged illegal activity was identified and labeled, that account could receive a value-limit restriction blocking the number of incoming transactions. This restriction limited only the amount of payments that could be received from other e-gold accounts.

The existing value already on deposit in these restricted accounts was not frozen or seized. The e-gold penalty assessed against recognized criminal activity was to block merely incoming transactions. As item 38 of the indictment details, value-limited accounts still maintained the ability of the account holder to spend the accumulated funds that were held in the account. As the indictment detailed: "Thus, even in circumstances in which the defendants knew that the account contained the proceeds of crime, the defendants allowed the funds to be exchanged out into national currency or transferred to another account."

If the e-gold company operators had identified illegal account activity, but no law enforcement agency had yet made a proper request for the seizure of an account, after being value-limited, any accumulated funds were transferred to a second or third e-gold account, and either exchanged into digital currency or sold for national money. In some instances, value-limited accounts that contained funds clearly identified as the proceeds of crime were simply transferred into another e-gold account operated by that same unknown user and the criminal activity continued unabated.[35]

By identifying e-gold accounts alleged by prosecutors to have been used in criminal activity, internally labeling those accounts by activity, and placing a value limit on them, the e-gold operators had simplified the government's investigation. A review of these value-limited accounts provided the government with ample evidence for a case against e-gold.

The indictment listed activity in 36 e-gold accounts that prosecutors alleged were used for the payment of child pornography, stolen credit card information, and wire (investment/Ponzi) fraud. The indictment stated the total value of e-gold funds transferred or caused to be transferred through the 36 accounts, from August 2000 to December 2005, was an approximately $145 million.

The additional three counts of the indictment alleged that e-gold was a money transmitter, had been operating without the proper licenses, and failed to comply with federal money transmitter regulations. Prosecutors had also argued that the e-gold operation had ignored federal anti-money laundering programs and had never filed even a single SAR.

The government served seizure warrants on G&SR ordering it to freeze, liquidate, and turn over the value represented by e-gold and OmniPay accounts along with many others linked to illegal activity. Surprisingly, the actual precious metal bullion had remained secure in the licensed and insured vaults. The government had requested that G&SR sell the metal and send a check.

E-gold Asset Seizures

At the same time of this indictment, government prosecutors filed 24 seizure warrants on 58 large e-gold accounts. The seized e-gold accounts were those of exchange agents and others that had been accepting deposits and moving money for criminal enterprises such as fraudulent investment Ponzi schemes and other illegal activity related to stolen credit cards. Lastly, several e-gold accounts belonging to an independent digital gold currency system which operated using e-gold as an asset were also seized. That system was known as 1mdc. The seized exchange agent accounts included:

- IceGold (European)
- The Bullion Exchange (USA)
- Gitgold (USA)
- Denver Gold Exchange (USA)
- uBuyWeRush (USA)
- AnyGoldNow (USA)
- Gold Pouch Express (USA)

The total amount of funds seized by the government was valued at just under $14 million ($13,960,857). G&SR sold the gold bars and the proceeds were delivered to the government. Some text from the affidavit shows the legal reasons for the seizures.

Affidavit in Support of Complaint for Forfeiture

(18 U.S.C. §§ 981, 1960, 1957)

3. This affidavit is being submitted in support of an application for a seizure warrant, based upon 18 U.S.C. § 981(a)(1)(A), for the property in the e-gold accounts listed below….

4. Based upon the evidence uncovered, there is probable cause to believe that the property contained in the above- identified e-gold accounts is involved in a violation of Title 18, United States Code, Section 1960, and

> is therefore subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).
>
> None of the digital currency exchangers (described below in this Affidavit) are registered with the federal government or licensed in the District of Columbia or the State in which they are physically present, as discussed more fully below.[36]

By seizing the e-gold value behind all 1mdc digital units, that system was abandoned by users and later closed. 1mdc had been successfully operated using e-gold digital units as backing for a simpler easy-to-use digital currency platform.

The following text is detailed case information on the seizures including the names on the e-gold account, the total amounts seized, and additional information on the parties. To reveal the size and scope of these operations fully, further details on the exchange agents may also include the total number of e-gold transactions along with the full amount of funds transmitted as listed in the Affidavit in Support of the Complaint for Forfeiture. These forfeitures were pursuant to the Racketing Influence and Corrupt Organizations Act (RICO). The anti-racketeering law is an example of a federal statute where violations of certain state laws are predicate offenses for federal penalties.

18 U.S.C. §§ 1961–1968 (RICO)

The modern RICO is a powerful federal law that was enacted by section 901(a) of the Organized Crime Control Act of 1970. RICO allows prosecution and civil penalties for racketeering activity. It focuses on certain acts (serious crimes) that are committed as part of an ongoing criminal enterprise. A RICO claim may also be used in a civil lawsuit and provides for an award three times that of the actual damages.

The following information did not appear in press reports, articles, or online discussions in the years surrounding the e-gold legal case (2007–2010). However, court documents disclosed that dozens of e-gold accounts were seized by the government and millions of dollars were forfeited under the RICO law. Each of these RICO cases resulted in the forfeiture of e-gold accounts as referenced from court documents.

Of the more than two dozen seized operations that were using e-gold, seven were popular exchange agents. The financial details on transactions through these early e-gold agents illustrates the enormous size and

fast growth of the early e-gold marketplace. Many early agents were tiny mom and pop operations, that had been overwhelmed by the hundreds of millions of dollars' worth of incoming e-gold exchange transactions. None of these agents were ever licensed or properly regulated as financial institutions. None of them ever obtained a money transmitter license and only one, the Denver Gold Exchange, eventually registered with FinCEN. These seven exchange agent seizures listed include:

- e-gold and OmniPay
- Gold Pouch Express
- GitGold
- The Bullion Exchange
- AnyGoldNow
- Denver Gold Exchange
- IceGold

§ 981—Civil Forfeiture

The 58 e-gold accounts seized were the result of civil action, in rem, brought to enforce the provisions of 18 U.S.C. § 981(a)(1)(A), which provides for the forfeiture of any property involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1960, or any property traceable to such property. This civil action, in rem, also seeks to enforce the provisions of 18 U.S.C. § 981(a)(1)(C), which provides for the forfeiture of any property which constitutes or is derived from proceeds traceable to a violation of any offense constituting "specified unlawful activity" or a conspiracy to commit such offense.[37]

1:07cv01337RMC

e-gold Ltd and OmniPay Accounts
E-gold Account Number: 544179 and 109243
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 01/06/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) was $1,481,976.38.[38]

1:07cv01341RMC

E-gold Exchange Agent Gold Pouch Express
E-gold Account Number: 118611
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 01/13/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) was $28,864.63.

Gold Pouch Express was operated by Roger and Mimi Savoie. This older couple ran the business from their residence which was a trailer located in an Arcadia, Florida, park for recreational vehicles. The exchange agent business utilized just one e-gold account number 118611. This account number also represents the ordered number of new e-gold accounts. The Gold Pouch Express was one of the first 120,000 e-gold accounts ever opened and processed transactions from February 2000 through March 2007. Court records indicate during this period, the account handled more than 26,000 e-gold transactions with a total weight of 59407.663122 grams or approximately $23 million.[39]

Amazingly, over seven years, this quiet older couple living in a central Florida trailer park, managed e-gold transactions valued at over $23,000,000.00 from their residence without any oversight, financial transaction reporting, regulatory supervision, or registration as a Money Service Business and Money Transmitter.

1:07cv01335RMC

E-gold Exchange Agent GitGold or Gitgold Worldwide, Inc.
E-gold Account Number: 310679
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 12/17/2008
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) was $6886.29.

Jane and David Anderson were the operators of a small Melbourne, Florida, mail service business called Stop N Mail. The business was located less than a 1.5-mile drive (five minutes away) from the Melbourne offices

of G&SR and e-gold Ltd. The Anderson's also owned and operated GitGold or Gitgold Worldwide, Inc. The Florida business functioned as an exchange agent for e-gold and other digital currencies including GoldMoney, e-bullion, INTGold, evocash, Netpay, and Ezcomoney. Court records indicated that the Andersons started GitGold in response to a solicitation from Douglas Jackson during e-gold's early development.

The e-gold account utilized by GitGold was number 310679, which also indicated the company's early entrance into the e-gold business. As e-gold halted its operation in 2008 with around 5 million accounts, a user in the first 300,000 was considered an early adopter. From the Stop N Mail location, the Anderson's accepted: Western Union, Money Orders, Cashier's Checks, International Bank Wires, Official Checks, and Teller Checks. Funds from these national currency methods of payment were then converted to digital currency. A fee was charged on the exchange transaction. The website listed David's AOL email address for fast contact.

GitGold's e-gold exchange operation began in May 2001. From 2001 through March 2007, the Anderson's e-gold account, number 310679, completed 31,064 transactions with a total weight of 62796.00473 grams. Court records indicated that this amount exceeded $24 million.[40]

Similar to Roger and Mimi Savoie of Gold Pouch Express, another local Florida e-gold exchange agent, Jane and David's GitGold money service business was never licensed or registered as a financial institution. The couple never received a Money Transmitter license in any US state nor registered with FinCEN. Apparently, the GitGold Bank account, through which a majority of the funds flowed, also was never identified as a Money Service Business account.

This trend is further illustrated in the additional exchange agent RICO seizures that were part of the 2007 e-gold case.

1:07cv01338RMC

E-gold Exchange Agent The Bullion Exchange
E-gold Account Numbers: 352900, 2325383, and 2449745
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 11/25/2008
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) was $67,476.71.

A husband and wife team named Don and Carole Neve operated The Bullion Exchange from Salt Lake City, Utah. The business accepted funds for transfer into the e-gold system by direct cash deposit or wire transfer into Wells Fargo Bank. The company also accepted cashier's checks and money orders.

The Neve's used three e-gold accounts, numbers: 352900, 2325383, and 2449745.

Court documents indicated that The Bullion Exchange operated account number 352900 from August 6, 2001 to October 2006. That account conducted 69,821 e-gold transactions with a total value of 370,331.7551 grams ($178,867,744.10).

Account number 2325383 in the name of "Bullion Exchange 2," was the account that participated in law enforcement's undercover exchange transaction. The Bullion Exchange began operating through that e-gold account number in August 2005. This was just days after the original July 2005 raid on the offices of G&SR and e-gold. From August 2005 through October 2006, the account conducted 6509 transactions with a total weight of 81,669.0983 grams ($38,840,867.00).

The third account used by the Neve's was number 2449725 which began operating in September 2005. From that time through October 2006, about one year, 9853 transactions occurred, with a total value of 22,142.99647 grams ($9,664,529.00).

As this analysis of the Neve's e-gold accounts shows, Don and Carole transacted at least, $227,000,000.00 through the three accounts over an approximately five-year period. A majority of those transactions occurred in the final months of the company's operation. This independent third-party digital currency agent also represents another small husband and wife operation.

As court records indicated, almost a quarter of a billion dollars flowed through these e-gold accounts. It is also worth noting that in addition to e-gold, this agent also exchanged a large amount of e-bullion digital currency. The total amount of financial transactions by The Bullion Exchange involving e-bullion was not available.[41]

1:07cv01342RMC

E-gold Exchange Agent and Debit Card Issuer: AnyGoldNow & GoldtoCard

E-gold Account Numbers: 183720, 148652, and 111318

Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 01/26/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) was $764,955.66.

As the low e-gold account number indicates (111,318), Patrick Verbeek of AnyGoldNow was an older established digital currency exchange operator. AnyGoldNow was an independent exchange agent for e-gold, INTGold, Pecunix, GoldMoney, e-Dinar, 1mdc, FSPay, NetPay, EMO, VirtualGold, and others, including Phoenix Silver. His business accepted bank wires, direct deposits, cash deposits, Western Union, and many other types of funding and digital currency exchange. Patrick also operated a debit card business that accepted deposits in digital currency. One of several debit cards issued by GoldtoCard worked through the Cirrus–Maestro network and could be obtained anonymously. The website advertisement stated, "No Name on the card. No need to send Identification documents. Just provide the ID information required."[42]

Another card offered through GoldtoCard was the Ingoldcard, which was issued through Michael Comer's organization and associated with INTGold. A third debit card from the GoldtoCard business was the "gCard" digital currency debit card. The gCard was one of the many ATM debit cards issued through a Canadian financial institution named North York Community Credit Union. For several years around 2005, this institution offered digital currency exchange agent resellers bulk prepaid card packages and master accounts. For a short time, the Canadian Credit Union furnished an integrated platform for loading the debit cards with e-gold. During those early years, many cards that could be loaded with digital currency were issued through North York including gCard,[43] BlueBanking,[44] GoldtoCard,[45] BestGoldCard,[46] and others.

Information obtained from the original 2007 e-gold case, showed that three e-gold accounts had operated by Patrick Verbeek. Those accounts labeled AnyGoldNow, Gold to Card, and GoldtoCard were numbers 183720, 148652, and 111318.

Number 183720 processed approximately 15,000 transactions including just over 6000 deposits into the account for a value exceeding $27,000,000.00. From December 31, 1999, through March 2007, e-gold account 111318 under the name Gold to Card conducted 10,630 e-gold transactions with a total value of 43,864.24359 grams ($21,153,789).

1:07cv01343RMC

E-gold Exchange Agent Denver Gold Exchange
E-gold Account Number: 3292324
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 01/26/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
US dollar value of the property recovered pursuant to the warrant(s) concerning the e-gold account(s) was $28,387.44

The e-gold account listed in court documents used by Denver Gold Exchange, in the undercover transaction with the United States Secret Service (USSS) was number 3292324. As it was a new company, this account had only been in use since June 2006. From that date until March 2007, about 14 months, the Denver Gold Exchange completed 2953 e-gold transactions with a total weight of 6286.879491 grams ($3,975,249.60). The USSS agent had determined that during the agency's investigation, the company was not registered with FinCEN. However, after direct contact with the USSS, on March 7, 2007, the business' owner Mr. David Metzel registered his company with FinCEN. Court documents also noted that even after the FinCEN registration, no reports with the Department of Treasury related to suspicious transactions or currency transactions were ever filed. The Denver Gold Exchange accepted direct cash deposits, bank wires, money orders, and Western Union.[47]

1:07-cv-01872-RMC

E-gold Exchange Agent IceGold, 25 percent Owned by Barry Downey & Douglas Jackson
E-gold Account Numbers 372 and 37273
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 10/17/2007 Date Terminated: 01/26/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) at issue here was $110,012.07.

IceGold was a very popular e-gold exchange agent. The business was operated from Estonia and exchange activity began in 2000. Startup funding for the business was partially received from e-gold co-founders Barry

Downey and Douglas Jackson. The two men reportedly held 25 percent of the ownership in return for some of the startup capital.

In court documents, the government prosecutors noted in a high number of e-gold exchange transactions in two of the IceGold operating accounts.

For the ten months from January 2006 through October 2006, account number 372 had a total of 20,071 transactions with a total weight of 192,810.66398 ($115,508,709).

Between September 2003 and March 2007, another IceGold operating account, number 37273, had 57,696 transactions with a total weight of 55,348.45387 grams ($31,815,473).[48]

1:07cv01336RMC

Accounts of the 1mdc Digital Currency System
E-gold Account Number: 808080, 808081, and 808082: 1mdc, 1mdc operations, 1mdc "BAIL IN" sweep account, or 1mdc assets.
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 03/18/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) at issue here was $380,636.60.[49]

1mdc was an independent ledger transaction platform. It operated "on top" of the e-gold system and 1mdc transactions were completely separate from the e-gold ledger. The 1mdc software package consisted of an independent closed digital ledger.

To add value into a 1mdc account, users deposited e-gold digital units into a specific e-gold account and automatically received 1mdc digital units of the same value deposited into the customers' 1mdc account. This deposit transaction was known as a "bail-in." This type of exchange transaction also operated in reverse. The action of deliberately moving 1mdc units back into e-gold was referred to as an "unbail." If a user unbailed a gram of 1mdc, they would then receive a gram of e-gold.

An advantageous user feature of 1mdc, which added an additional layer of privacy to the system data for all users was the method under which 1mdc was operated. All e-gold deposits were pooled into one account. That value of e-gold generated a single account record and history within the e-gold system. This collective sum of e-gold bailed-in rested on deposit

and did not move from the account until being unbailed. The permanent record of transactions for that deposited value was short. A review of the deposited amount only showed the lump sum of e-gold quietly resting within the e-gold vault. For all intents and purposes, a discoverable record of that value showed no movement or transactions. However, on deposit, the e-gold instantly became value available for transactions in 1mdc digital currency. Consequently, a 1mdc user could "bail-in" a million dollars' worth of e-gold and transactional records merely showed the funds on deposit in an e-gold account. Meanwhile, the value of that e-gold, as realized in 1mdc units, could be quietly moving through thousands of transactions outside the e-gold recorded ledger. No permanent transaction records were kept for 1mdc accounts. Exchanging e-gold for 1mdc was an instant and painless transaction that could protect the privacy of a user and leave no lasting financial records of transactions, payments, or ownership. The 1mdc operator did not accumulate any records of transactions, and no database history of the operation was available for future reference.

The 1mdc platform was considered innovative during its five years of existence. However, using bitcoin and other modern types of cryptocurrency, in 2016, this type of "off the books" digital currency platform is commonplace. Many modern day websites selling illegal items, such as drugs or stolen credit card information, will require both buyers and sellers to make deposits in bitcoin then receive credit for an "in-house" digital unit circulating outside of bitcoin. This type of digital currency product further anonymizes transactions by not creating a record on the bitcoin Blockchain.

While the 1mdc website provided no corporate registration or contact information, industry insiders knew John Paul May had created and operated the innovative system. Mr. May was very active in online discussions such as the e-gold list. Investigators eventually uncovered this obvious information and stated the software originated from an Anguilla, BWI domiciled company called Interesting Software, Ltd. and J.P May ran this innovative software company. Considering that 1mdc had not become hugely popular until the last few years before its closing, as indicated by legal documents, the volume of financial transactions handled by this small system was enormous.

> 1mdc utilizes three e-gold accounts for its operations: 808080 (in the name of 1mdc "BAIL IN" Sweep Account), 808081 (in the name of "1mdc operations"), and 808082 (in the name of "1mdc assets"). Analysis of activity occurring in e-gold account number 808081 from June 2001 through

> March 2007 yielded the following results: There were a total of 15,556 transactions totaling $51,256,764.15
>
> According to Omar Dhanani, an individual convicted of access device fraud in the Shadowcrew prosecution, in addition to e-gold, members of carding websites use the digital currency 1mdc to buy and sell stolen credit card numbers and other contraband particularly because 1mdc is completely anonymous, and advertises itself as being completely offshore. Also according to Mr. Dhanani, 1mdc is preferred over other digital currencies because 1mdc is out of reach of U.S. law enforcement.[50]

Hours after the government's seizure of the 1mdc accounts, in 2007, the platform's creator and operator, John Paul May, posted this ominous statement on the 1mdc website.

It is the opinion of your 1mdc team that:

1. The early era of Digital Gold Currency (DGC) privacy is over.
2. US citizens will simply never be able to use DGCs.
3. The only DGCs that operate from now on will:
   (a) Have no connection to the USA
   (b) Have no US users (exactly as Swiss banks have no US users)
   (c) Will have higher ID requirements than e-gold currently does.

You are welcome to email "team@1mdc.com" but, again, the realistic view is that the e-gold(R) will never be released. Note that of all e-gold confiscated by US court order, none has ever been released.[51]

After the 2011 MSB & Prepaid Access FinCEN regulations had gone into effect, J.P. May's predictions regarding the US and digital currency were fully realized.

This is an excellent point for a comparison between the early US digital currency marketplace and the modern US cryptocurrency market. In 2016, there are no small mom and pop Bitcoin exchange operations anywhere in the USA. Industry participants fully realize that businesses engaged in Bitcoin financial transactions must be properly licensed and operate within the recognized set of standards, including KYC and AML

financial regulations. National Bitcoin exchange companies such as Circle and Coinbase are fully registered, licensed, regulated, and supervised.

The US marketplace in 2016 affords no advantages for an unsupervised exchange operation such as Gold Pouch Express, which did business from a non-descript trailer located in a Florida RV park. There is little chance that a tiny Bitcoin agent, acting in a public capacity online, could ever again move $20 million of small individual deposits through any US bank account without receiving regulatory scrutiny and a mountain of SAR.

New Bank Secrecy Act regulations have changed how digital currency is recognized and regulated in the US marketplace. FinCEN's rules made the digital currency business much safer, particularly for consumers. The 2016 US Bitcoin exchange market is highly regulated and that new supervision prevents dangerous financial transactions from going unreported and acts to prevent many bad actors from engaging in US-based Bitcoin business. The new regulations instill confidence in the system and invite legitimate digital currency use.

In the early unregulated US marketplace, e-gold was able to host thousands of accounts that were openly engaged in illegal activity. E-gold never even required the customer's legal name. These next 20 e-gold account operations are also listed in the original 2007 case. These accounts were seized alongside the exchange agent accounts. Each of them was forfeited under the RICO Act laws through the government's civil action. These 20 accounts were not exchange agents, but alleged criminal enterprises using e-gold.

1:07cv01344RMC

HYIP Ponzi Investment Scheme/Fraud, Freeland Ops, Ambergold, New Millenium, Goldenbart, Freeland Credit 3, Freeland Credit 4, or Freeland Credit 2
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $312,567.62.[52]

1:07cv01346RMC

HYIP Ponzi Investment Scheme/Fraud, Legisi Holdings LLC.
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) concerning the e-gold account(s) at issue here was $1,769,264.19.[53]

1:07cv01349RMC

HYIP Ponzi Investment Scheme/Fraud, Foreign Fund, Foreign Fund Account, or Vasilis.
Cause: 18:1961 Racketeering (RICO) Act
Date Filed: 07/24/2007 Date Terminated: 03/31/2009
Nature of Suit: 690 Forfeit/Penalty: Other Defendant Property
The US dollar value of the property recovered pursuant to the warrant(s) was $440,068.11.[54]

1:07-cv-01322-RMC

HYIP Ponzi Investment Scheme/Fraud, Miguel Jimenez
Cause: 18:1961 Racketeering (RICO) Act
US dollar value of the property recovered pursuant to the warrant(s) was $945,491.22.[55]

1:07cv01323RMC

HYIP Ponzi Investment Scheme/Fraud, Syncinvest or Pierre Soalliet
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $137,219.65.[56]

1:07cv01325RMC

HYIP Ponzi Investment Scheme/Fraud, E-gold-invest.us
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $260,054.42.[57]

1:07cv01326RMC

HYIP Ponzi Investment Scheme/Fraud, VIP Invest Club, eg account, Eugene's Account, VIC, V.Smelov's account, Gromov`s account, Svetlov's account, Belov's acc, Happy, or Fast and Profitable.
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $43,218.23.[58]

1:07cv01324RMC

Vendor of stolen credit cards, financial accounts, and fraudulent passports, Maksik, Maksil's Job, or Maksik's account.
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $7007.41. "Maksik" is a known vendor of stolen credit card information, stolen financial accounts, and fraudulent Ukranian passports on the Shadowcrew, Mazafaka, and Carderplanet carding websites and accepts payment for this contraband in e-gold.[59]

1:07cv01327RMC

HYIP Ponzi Investment Scheme/Fraud, World Investment Group, Jrw, bill, huang ke, billy, tiger, china, dou yi feng, or HIK Group
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $3,038,718.66.[60]

1:07cv01328RMC

HYIP Ponzi Investment Scheme/Fraud, Quick HYIP or DOG
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $108,049.08.[61]

1:07cv01348RMC

Vendor of stolen credit cards, financial accounts, and fraudulent passports, Segvec or Harry Michaels
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $339,323.40
"Segvec" is a vendor of stolen financial information on the carding website Makafaka and accepts payment for his contraband in e-gold

1:07cv01329RMC

HYIP Ponzi Investment Scheme/Fraud, Nawaaz Meerun, or NM2, or NM3

Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $1,533,752.60.[62]

1:07cv01330RMC

HYIP Ponzi Investment Scheme/Fraud, Sime Securities or BConnected Technology Inc.
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $521,795.46.[63]

1:07cv01331RMC

HYIP Ponzi Investment Scheme/Fraud, E-Gold Daily Pro or EGDP
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $129,035.72.[64]
The US dollar value of the property recovered pursuant to the warrant(s) was $445,189.72.[65]

1:07cv01347RMC

HYIP Ponzi Investment Scheme/Fraud, Phoenix Surf or PwnAll egold
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $201,422.64.[66]

1:07cv01332RMC

HYIP Ponzi Investment Scheme/Fraud, FSI SRL Powerclub or F.S.I. Srl.
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $623,410.62.[67]

1:07cv01333RMC

HYIP Ponzi Investment Scheme/Fraud, Feeder Fund or werta's acc.
Cause: 18:1961 Racketeering (RICO) Act

The US dollar value of the property recovered pursuant to the warrant(s) was $405,464.66.[68]
1:07cv0in Support of Complaint for Forfeiture (18 U.S.C. §§ 981, 1957, 1960) filed in July 2007.
HYIP Ponzi Investment Scheme/Fraud, Southern Star P.I.B., SANTOS1, or DX-GOLD Currency Account
Cause: 18:1961 Racketeering (RICO) Act
The US dollar value of the property recovered pursuant to the warrant(s) was $275,797.99.[69]

1:07cv01345RMC

HYIP Ponzi Investment Scheme/Fraud, IFF "ULWES" or Sven Schalbe.
Cause: 18:1961 Racketeering (RICO) Act

Additional criminal charges relating to the e-gold case: E-gold Exchange Agent uBuyWeRush

In Long Beach, California, a gentleman named Cesar Carranza operated the exchange agent uBuyWeRush, Inc. which was located adjacent to uBuyWeRush's actual storefront location at 3327 E South Street, Long Beach, CA 90805.

Cesar was charged relating to his exchange operations and money laundering.

nyedce	1:2008-mj-00308	03/28/2008	All Defendants USA v. Carranza
cacdce	2:2008-mj-00926	04/15/2008	All Defendants USA v. Carranza

US Secret Service Special Agent Roy Dotson, from the Orlando Field Office, had further information and comments on e-gold's activity with Ponzi schemes. Here are a few of his statements along with detailed information from the Affidavit in Support of Complaint for Forfeiture (18 U.S.C. §§ 981, 1957, 1960) filed in July 2007.

> A search of the e-gold database revealed over 11,000 e-gold accounts that have been opened using the term "hyip" in either the account-owner's name or e-mail address, or where "hyip" appears in the "memo" field of the transaction record.
>
> Patterns of Investment Scams using e-gold
>
> 42. This investigation uncovered numerous promoters (or operators) of pyramid, HYIP, and other similar schemes, each of whom operated several

> different investment scams and laundered their proceeds through chains of interconnected e-gold accounts. Several patterns emerged with regard to the transaction activity within accounts operated by these promoters.
>
> First, the promoters would set up an e-gold account to which all investors would send deposits to the program. From this main account, the promoters would pay out three types of "returns": (1) payouts to a majority of investors in amounts much smaller than the investors' initial deposits in order that these investors would keep believing this was a worthwhile "investment"; (2) payouts to a select group of investors in amounts far exceeding their initial investment in order that these investors could continue to promote the scheme as actually paying out the "promised return"; and (3) transfers to e-gold accounts controlled by the same promoter in large amounts representing the profits of the scam (i.e., the stealing of investors' money).[70]

While the government ultimately obtained the value of precious metal contained in each seized account, it is critical to note that the government was not able to go to the vaults and confiscate any precious metal bullion. In a 2016 email, Douglas Jackson made this statement regarding the safekeeping of e-gold assets.

> "…the governance model of e-gold withstood the years' long shock and awe exertions of the IRS/SS/DOJ/US and they failed in one of their two primary purposes – to seize the gold reserves."[71]

The government's proposed reasons that e-gold management had created the innovative payments platform were made clear in the original indictment from April 2007.

> GOAL OF THE CONSPIRACY
>
> 30. It was the purpose of the conspiracy to engage in financial transactions with those known to be involved in criminal activity in order to build the market share and profitability of E-GOLD and enhance the personal wealth of DOUGLAS JACKSON, BARRY DOWNEY, and REID JACKSON.
>
> OBJECT OF THE CONSPIRACY
>
> 51. It was a goal of the conspiracy that defendants DOUGLAS JACKSON, BARRY DOWNEY, and REID JACKSON, and their co-conspirators, to provide money transmitting services to the public through the E-GOLD operation thereby establishing the E-GOLD operation as a viable private currency and enhancing their own personal wealth.[72]

OmniPay

In May 2007, OmniPay, the largest e-gold exchange agent in the world, suspended operations because the government had seized the company's bank accounts and frozen its e-gold assets. OmniPay had one remaining non-US bank account with SEB Bank in Estonia which had not been frozen or seized. However, citing a press release from the US Department of Justice, in late May, SEB Bank had also notified OmniPay that its account would be closed by May 25, 2007. This final bank account closure triggered several unsuccessful attempts by GS&R and OmniPay to circumvent restrictions imposed by the government's pending criminal case.

The first announcement from e-gold stated that G&SR would be leasing the OmniPay operation to another business entity known as OmniPay Africa. From that day forward, all money and e-gold to be exchanged through that company would move through an OmniPay Africa account, well outside of the USA. The announcement from e-gold contained the following text.

> OmniPay temporarily suspends exchange to transition to OmniPay Africa
>
> Effective immediately, G&SR will be leasing the OmniPay business to OmniPay Africa. All OmniPay exchanges will now involve e-gold transfers and money payments into/out of OmniPay Africa's e-gold and bank accounts, respectively. G&SR has contracted to serve as the Operator of OmniPay but will not be a party to actual exchanges. In terms of immediate impacts:
>
> - The OmniPay exchange service will suspend operation pending provisioning of a suitable bank account for OmniPay Africa. It is anticipated this service interruption will start May 24, 2007 with service resuming on or about June 18, 2007.
> - With resumption, all bank wires from customers must be directed to the new bank coordinates which will be posted on the omnipay.com website.

The original plan was for OmniPay Africa to organize as a licensee of G&SR, the US company that owns OmniPay. A substantial development effort was underway to support the additional requirements for over-the-counter exchange operations such as biometric validation. However, recent actions of the US government, originating from a long-standing

and misguided animus on the part of the US Secret Service, necessitate immediate action. We regret the temporary interruption of OmniPay services. Just as the US government's recent actions in seizing e-gold accounts of e-gold Ltd., G&SR, The Bullion Exchange, AnyGoldNow, IceGold, GitGold, The Denver Gold Exchange, GoldPouch Express, and 1MDC (and forcing G&SR to liquidate the seized assets!) have severely damaged not only these exchange businesses but also their innumerable customers, their forcing this complex transition to be performed on an emergency basis is simply shameful.

> We do not however regret the transfer of OmniPay responsibilities to OmniPay Africa. As will become abundantly clear in coming months, the OmniPay Africa team is highly qualified to guide OmniPay to a higher level, a genuinely global service that will foster a beneficial surge in e-gold's emergence while bringing significant advantages to emerging economies.[73]

This African plan never materialized. OmniPay Africa never opened, and e-gold did not secure any additional bank accounts. Neither did GS&R or OmniPay. The argument that e-gold did not verify account holders could be disqualified when focusing on any client funds that had been deposited into the e-gold system through OmniPay. The world's largest exchange agent, OmniPay, had an excellent record of customer identification and verification. Regarding OmniPay's strict customer compliance with KYC rules and other preventative measures, in a 2016 email, Douglas Jackson had these comments.

> OmniPay did verify identity of its customers. [The method was effective but may not have corresponded to either the "documentary" or "non-documentary" norms prescribed by FinCEN. We'll never know because no evidence was presented/examined in the course of the legal case.] Every exchange provider that accepts conventional money payments has no alternative but to verify identity because of the risk of payment reversal.
>
> [Financial institutions have always verified identity, not only to avoid loss but, in the case of conventional institutions, for many decades, in order to abuse the privacy of their customers by selling their information to third-party vendors who use it to barrage the customers with ceaseless unwanted advertising. By having governments write laws requiring verification, they can sidestep possible privacy concerns on the grounds that they are required to do it.][74]

The Judge's Opinion

In mid-2007, while the government's criminal case was progressing, the e-gold defendants filed a motion seeking to have most of the indictment dismissed. The argument presented by the e-gold defendants was identical to past statements offered by the e-gold management along with other digital currency operators and agents every year since 1996. The debate surrounded whether or not a digital unit of value circulating online was considered currency or money. For many years, Douglas Jackson had concluded that a digital unit backed by gold, denominated by weight that only circulated online was not money or currency. He had previously asked the US Treasury to declare e-gold a currency and had received a negative response. Experts from the digital currency industry all said the same thing. Digital gold currency was not cash; it was not a recognized currency, and it certainly was not money as defined by the US Government. If the e-gold business only handled digital units and never cash or currency, how could the company be considered a money transmitter?

District Judge Rosemary Collyer's Opinion, filed May 8, 2008, addressed all of these issues and defeated the defendant's motion. The opinion was 28 pages long. Selected portions of this document are shown below.

> They[Defendants] contend that Section 1960 does not apply to their operations because they never deal in cash or currency. Since they are not required to file reports with the IRS concerning cash transactions, they argue that they do not operate a "money transmitting business" and, therefore, cannot be an "unlicensed money transmitting business" within the scope of Section 1960.
>
> Title 18 of the United States Code ("U.S.C.") sets out federal law covering Crimes and Criminal Procedure. Title 31 of the U.S.C. sets out federal law covering Money and Finance, including the Internal Revenue Code. 18 U.S.C. § 1960 makes it a crime to operate an unlicensed money transmitting business. Section 1960 defines what it means to be unlicensed and what it means to engage in money transmitting. By those definitions, a business can clearly engage in money transmitting without limiting its transactions to cash or currency and would commit a crime if it did so without being licensed. The only definition in the United States Code for a "money transmitting business" per se is at 31 U.S.C. § 5330. Section 5330 defines a money transmitting business as one that, inter alia, is required to report certain cash or currency transactions to the Internal Revenue Service ("IRS").
>
> Before the Court is a motion to dismiss filed by the criminal defendants in this case. They have all been charged with operating an unlicensed money

transmitting business in violation of Section 1960. They contend that Section 1960 does not apply to their operations because they never deal in cash or currency. Since they are not required to file reports with the IRS concerning cash transactions, they argue that they do not operate a "money transmitting business" and, therefore, cannot be an "unlicensed money transmitting business" within the scope of Section 1960. They further argue that even if one could distinguish Section 1960 and Section 5330, Section 1960 is unconstitutionally vague as to the meaning of the term "money transmitting business," and therefore violates Defendants' rights under the Due Process Clause of the Constitution, or at least is ambiguous as to the meaning of that term, and the rule of lenity requires dismissal of most of the counts in the criminal indictment.

The Defendants have moved, pursuant to Federal Rule of Criminal Procedure 2(b)(3)(B), to dismiss Count Two of the Indictment for failure to state an offense under 18 U.S.C. § 371, and to dismiss Count Three for failure to state an offense under 18 U.S.C. § 1960. The Defendants also move to dismiss Count Four, based on the Court's discretion not to exercise jurisdiction over an alleged state offense, Money Transmission Without a License in violation of D.C. Code § 26-1002. Alternatively, the Defendants move to dismiss Counts Three and Four for failure to comply with Federal Rule of Criminal Procedure 7(c)(1).1 Whether the Defendants' business activities, described below, are criminal in nature has been orally contested since the Indictment was obtained. The Court is now advantaged by the written arguments presented by the parties, as well as a spirited oral argument, and finds that Counts Two and Three properly allege offenses of 18 U.S.C. §§ 371 and 1960. Since the Indictment remains intact, the Court will maintain the state-law count in Count Four. The motions to dismiss are based on a misreading of the statutory text and will be denied.

The United States obtained a Superseding Indictment in this case on the day before the motions hearing on the instant motions. Defendants conceded at that hearing that the Superseding Indictment robbed their Rule 7(c)(1) arguments of force and weight. They will not be addressed further here.[75]

The Superseding Indictment, filed April 3, 2008, showcased the large-scale nature of the e-gold business by detailing the number of employees and the amount of funds transferred ($145 million). From this argument, the court concluded that e-gold was a "money transmitter business." Furthermore, the court held that without ever handling government currency or coin, e-gold was still considered a money transmitter and subject to reporting requirements.

The District Court, Judge Rosemary Collyer, held that:

1. "money transmitting business" in governing criminal statute was not restricted to business that handled cash;
2. defendants operated "money transmitting business" within meaning of Money and Finance Code provision mandating registration of such businesses;
3. the criminal statute was not void for vagueness;
4. rule of lenity was not applicable; and
5. no novel statutory construction was involved in the instant prosecution.[76]

In the years before this judge's opinion, all digital currency businesses had maintained that the units exchanged between the closed ledgers were not "money" or "dollars" as defined by existing regulations. Furthermore, digital gold currency companies were not required to be licensed as money transmitters and were not considered financial institutions. However, after the Judge's opinion, the law was very clear. All digital currency businesses were required to be properly licensed and registered with FinCEN as money service businesses and money transmitters. The prosecution of e-gold was a landmark case in the history of digital currency.

Guilty Plea and Consent Order of Forfeiture

On July 21, 2008, all of the Defendants e-gold, Ltd. and G&SR pleaded guilty to violations of 18 U.S.C. §§ 1956(h) and 18 U.S.C. § 371 (Conspiracy to violate 18 U.S.C. § 1960).

In July 2008, the company and its three directors accepted a bargain with the prosecutors. E-Gold and its corporate affiliate G&SR each pleaded guilty to conspiracy to engage in money laundering and conspiracy to operate an unlicensed money transmitting business. The principal director of E-Gold and CEO of G&SR, Dr. Douglas Jackson, 51, of Melbourne, Florida, pleaded guilty to conspiracy to engage in money laundering and operating an unlicensed money-transmitting business. E-Gold's other two senior directors, Barry Downey, 48, of Baltimore and Reid Jackson, 45, of Melbourne each, pleaded guilty to felony violations of District of Columbia law relating to operating a money-transmitting business without a license.[77]

The company made an attempt to return legal e-gold funds back to the legal owners. Any e-gold account holder that could prove ownership of an account and the legal source of funds had the opportunity to request the return of their precious metal's value. E-gold labeled it the Value Access Plan.[78]

Approximately $92 million of bullion was now up for grabs by all legal owners. The period to submit a claim on e-gold funds lasted until December 31, 2013. The balance of unclaimed funds will be seized by the US Attorney's Office for the District of Columbia under the asset forfeiture law.

In November, G&SR CEO Douglas Jackson was sentenced to 300 hours of community service, a $200 fine, and three years of supervision, including six months of electronically monitored home detention. Jackson's six-month house arrest ended in June 2009. He had faced a maximum sentence of 20 years in prison and a $500,000 fine.

Reid Jackson, Douglas Jackson's brother, and E-Gold director Barry Downey were each sentenced to three years of probation and 300 hours of community service, and ordered to pay a $2500 fine and a $100 assessment. G&SR forfeited $1,750,000 of funds to the government.

The Federal Judge in the case stated that the court had determined that the founders of E-gold "had no intent to commit illegal activity." In a 2016 email, Douglas Jackson provided this additional information.

> In terms of providing payment services, e-gold was fully operational from November 1996 to April 2007. At that time Spend activity began a precipitous decline due to asset seizures affecting most major exchange services combined with a Post-Indictment Restraining Order that effectively barred redemption. e-gold suspended submission or execution of Spend Instructions in 2009 due to its inability to obtain state licensing as required under the Plea Agreement.
>
> The development team went on to develop a next generation system merging the proven monetary and transactional principles of e-gold with much more robust and scalable technology, innovative features and innumerable safeguards that meet not only applicable regulatory requirements but define a new standard for security and prevention of abuses. Even now as I address these questions we are also in the midst of a corporate restructuring designed to generate value for the long suffering shareholders of G&SR. It is definitely "too early to say" how the e-gold initiative plays out.
>
> Neither I or nor the other Directors of e-gold will be permitted to exercise any form of control over this next generation system. I nevertheless

> expect it to ultimately be perceived as my legacy and the fulfillment of what I set out to do with e-gold.[79]

The government did not close the e-gold business. As convicted felons, the original operators were unable to obtain or hold a financial license. They chose to voluntarily discontinue the operation. Before that decision, the company was preparing to reopen as a closely regulated US financial institution.

> Neither e-gold Ltd. nor G&SR Inc. were ever shut down by the government (that issue was explicitly addressed at sentencing). The gold reserves were never seized. Neither company ever failed to meet a financial obligation and G&SR has never missed a payroll. At great effort and expense, we were able to initiate an e-gold Value Access Plan that afforded former customers the ability to claim their value trapped in the system when Spends and exchange market activity were suspended. Successful claimants received 2-5 times the value they held in the system (in terms of USD) at the time of their last receipt of a Spend, due to continued appreciation of e-gold even after Spends were suspended.

Extracted from the e-gold Plea Agreement, the following directions illustrate a few of the additional stipulation required for the compliant operation of any future e-gold-type system.

> Registration as a Money Services Business: The Company agrees that it and Gold & Silver Reserve, Inc. are "financial institutions" as defined in 31 U.S.C. § 5312(a)(2) and are money services businesses under 31 C.F.R. § 103.l l(uu)(5). Further, the Company agrees that the e-gold operation (including both e-gold, Ltd. and Gold & Silver Reserve, Inc. doing business as OmniPay) is a money transmitting business within the meaning of 18U.S.C. § 1960, and, as such, may not operate without a money transmitting license in States that require licensing of businesses engaged in money transmitting and without registration with the Department of Treasury (FinCEN) pursuant to 31 U.S.C. § 5330 and 31 C.F.R.§ 103.41. Accordingly, the Company will not engage in operation of the e-gold digital currency system, or any other digital currency system, until it has registered with FinCEN. In addition, within thirty (30) days of entering this Plea Agreement, the Company will submit applications to obtain State licenses in States that require licensing of businesses engaged in money transmitting or submit a request for an advisory opinion from such a State that the Company is not required to be licensed.

The plea agreement addressed many other critical compliance issues. Because the e-gold operation had been registered in Nevis, outside of the USA, early in the e-gold business, there had been some confusion regarding acceptance of legal service, including subpoenas. In that new 1990s online era, a popular offshore concept had been to avoid locating any company offices on US soil. This loose rule was supposed to reduce the possibility of a company employee accepting service within the USA. It is unclear if the management of e-gold ever intended to use this tactic and avoid government requests for customer records; however, during that first decade of the digital currency business, many other financial operations, including e-bullion and Liberty Reserve, clearly engaged in this type avoidance. The operators of Liberty Reserve even boasted about their "offshore" jurisdiction of that business' corporate entities. An outcome of the e-gold case was the court's requirement for a legal US service address that might lead investigators.

> Service of Process: The Company agrees that it and Gold & Silver Reserve, Inc. will accept service of process at the business location in Melbourne, Florida or any other United States location from which they operate, including the location of any owner, or principal, regardless of whether that is the location of the principal place of business, incorporation, or registration.

The July 2011 FinCEN MSB regulations (Federal Register / Vol. 76, No. 140 / Thursday, July 21, 2011 / Rules and Regulations 43585) also clarified this issue.

> This Under the final rule, foreign-located MSBs will have the same reporting and recordkeeping and other requirements as MSBs with a physical presence in the United States, with respect to their activities in the United States.
>
> Foreign-located MSBs will also be required to designate a person who resides in the United States to function as an agent to accept service of legal process, including with respect to BSA compliance.[80]

Throughout the businesses' lifetime, neither G&SR nor e-gold Ltd. operated with a published anti-money laundering program. All Money Service Businesses in the USA require an AML program. However, since the e-gold platform was not recognized by its operators as a financial institution, no AML program had ever existed. The court was very clear that any continued operation of the e-gold platform required a legitimate audited AML program.

> Anti-Money Laundering Program: The Company agrees that it and Gold & Silver Reserve, Inc. are "financial institutions" as defined in 31 U.S.C. § 5312(a)(2) and are subject to the requirements to establish an anti-money laundering program in 31 U.S.C. § 5318(h) The Company agrees that it and Gold & Silver Reserve, Inc. will establish and maintain a Bank Secrecy Act compliance program, including an anti-money laundering program with internal controls, independent testing and other measures to detect and report potential money laundering, terrorist financing and other suspicious activity. Pursuant to 31 U.S.C. § 531S(h), this shall include, at a minimum, (A) the development of internal policies, procedures and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs. Further, the Company acknowledges that it and Gold & Silver Reserve, Inc., as currently operating, are a "high risk" operation with respect to money laundering and agrees that the anti-money laundering program to be established will be commensurate with those risks pursuant to 31 C.F.R. § 103.125.

As a critical part of this AML program, the e-gold business was required to engage an outside vendor to search proactively the Internet for instances where "e-gold" is being used for criminal purposes. By relating that activity to the company, the information was to provide even more data for an ever expanding AML program and prevent bad actors from accessing the platform.

One of the more unique items that appeared in the plea agreement was the following statement regarding policies and procedures that should be included in a website disclaimer and added to the e-gold account user agreement. The business was directed to establish policies that would prohibit e-gold from being used for illegal activity and publicize those procedures in the User Agreement and a website disclaimer within ten days of the signed plea agreement.

Apparently, over more than a decade of operation, the management of e-gold had never disclosed in a public statement on the website the idea, "that account holders were prohibited from using e-gold for anything illegal." This court request was a lively topic of commentary between industry participants. One exchange agent had even posted that this suggestion was analogous to telling famed Rolling Stones guitar player Keith Richards just to say "No" to drugs and alcohol. Additional requirements of the court in the plea agreement included customer identification, OFAC Compliance, SAR, and the supervision by the Internal Revenue's Bank Secrecy Act

Division. It is worth noting that the co-founders of e-gold voluntarily invited that last procedure well before being convicted of any crime.[81]

In a 2016 email, Douglas Jackson added these additional comments.

> I'll begin by addressing the legal framework and how the law was/is interpreted and applied. But first, some context may be useful. Please note however, my pointing out particular legal aspects—where the legal aspects were far from black and white or where laws were interpreted one way in our case and grossly differently in other situations—should not be taken to suggest I am unaware of the numerous errors I made in designing and implementing the first generation of e-gold.
>
> In fact, the whole e-gold story can be viewed from a lessons-learned perspective, an "if only I'd known and understood then what I know now" matter. But that is not how the world works for a pioneer.
>
> Twenty years of involvement in an activity does not necessarily equate to progress along a learning curve. But I have learned and continue to learn. My experiences have been complemented by and marinated in continuous study and reflection. Each lesson learned is woven into the fabric of the tapestry I am creating. In contrast to this, I will advance Success and survival will ultimately go to the enterprise built in accordance with a coherent model affording economic utility and immune to error, coercion or malfeasance.
>
> There was no lack of laws and regulations during that entire time [1996-2006], both before but especially after the 2001 PATRIOT Act modifications to the BSA. As it turned out, the most pertinent enactments involved MSBs in general and Money Transmitters in particular. I made the error of trying to interpret them based on their words, sentences and apparent logic of intent.
>
> To me, it was clear they had never contemplated the business model of e-gold Ltd. or of G&SR (dba OmniPay®).
>
> e-gold Ltd. and G&SR Inc. pleaded guilty to Operation of an Unlicensed Money Transmitting Business. The crux of this outcome was that the companies had provided services to customers residing in the District of Columbia without obtaining a license or a determination that license was not required.

Throughout the e-gold legal ordeal, which began in 2005, co-founder Douglas Jackson and many other industry participants openly objected to the government's actions. Across the Internet, there were suggestions that investigators were out to vilify digital gold at the request of the federal government. These types of suggestions led to ongoing conspiracy that those agencies responsible for the US dollar did not want direct monetary competition from precious metals.

In the modern 2016 online world, when one party wants to smear or degrade another party, the act of directly associating that party with child pornography, drugs, criminal activity, and terrorism is enough to destroy any US business. Certainly, there were many people in the digital currency industry who felt that type of smear campaign is what occurred with e-gold. As Douglas Jackson described in a 2016 email, he had also concluded that at least some government agents had tried to attach the label of "boogeyman" to the e-gold operation.

> Likewise, not until 2010 (notably not disclosed in the Brady letter) did we learn that the SS had in fact approached the state of Florida in 2005-6 soliciting a determination that e-gold and/or G&SR were operating as unlicensed Money Transmitting Businesses. Even more to the point, we were unaware that Florida determined that we weren't; >>>they concluded our business models did not fall within their statutory definitions (which were subsequently changed circa 2008). Only at the same time in 2010 did we learn that the SS had then (2005-6) proceeded to "shop" other jurisdictions to find one more amenable. Hence the involvement of DC, where at no time in prior history had the Money Transmitter label been applied to any entity lacking a physical presence in DC and that did not transact in paper cash.[82]

Even after the 2005 raid on the G&SR office, people still used e-gold. That year, this popular phrase began circulating in the digital currency community, "In Doug we Trust." For tens of thousands of e-gold users, these words were an absolute truth. Despite other digital currency products and options being available online during those years, e-gold users held firm, stood their ground, and continued using e-gold.

With the phrase, "In Doug we Trust," old e-gold users, had accurately formed the same conclusion shared by digital currency experts in 2016. They all believe that Douglas Jackson is a brilliant, honest, Internet pioneer.

Notes

1. Indictment at 1, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
2. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.
3. Ibid.

4. Internet Archive: Wayback Machine, e-gold.com accessed March 26, 2016, https://web.archive.org/web/20010201200700/www.e-gold.com/unsecure/qanda.html.
5. "Gold Rush—Bloomberg Business," Bloomberg.com, accessed March 26, 2016, http://www.bloomberg.com/news/articles/2006-01-08/gold-rush.
6. "Terms of Use," Internet Archive: Wayback Machine, e-gold.com, accessed March 26, 2016, https://web.archive.org/web/20040626023039/www.e-gold.com/unsecure/terms.htm.
7. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.
8. Ibid.
9. Ibid.
10. E-gold.com Douglas Jackson, "Terms of Use," Internet Archive: Wayback Machine, e-gold.com, accessed March 26, 2016, https://web.archive.org/web/20010210021039/e-gold.com/unsecure/terms.htm.
11. OmniPay, Douglas Jackson, "Terms of Service," Internet Archive: Wayback Machine, accessed March 26, 2016, https://web.archive.org/web/20030206080016/omnipay.com/terms.asp.
12. E-gold.com, Douglas Jackson, "E-gold Questions and Answers," Internet Archive: Wayback Machine, e-gold.com, accessed March 26, 2016, https://web.archive.org/web/20000621020050/www.e-gold.com/unsecure/Faq.htm.
13. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.
14. "E-gold Account User Agreement," Internet Archive: Wayback Machine, e-gold.com, accessed March 26, 2016, https://web.archive.org/web/20021217010505/www.e-gold.com/unsecure/e-g-agree.htm.
15. "E-gold Statistics," Internet Archive: Wayback Machine, e-gold.com, accessed March 26, 2016, https://web.archive.org/web/20010413124825/www.e-gold.com/stats.html.
16. "E-gold Programmer's Information," Internet Archive: Wayback Machine, e-gold.com, accessed March 26, 2016, https://web.archive.org/web/20011212171010/www.e-gold.com/unsecure/sci_home.html.

17. "Financial Cryptography: GP4.3—Growth and Fraud—Case #3—Phishing," Financial Cryptography, accessed April 3, 2016, http://financialcryptography.com/mt/archives/000609.html.
18. "FBI—Leader of $73 Million Ponzi Scheme Sentenced Again to 30 Years in Prison Second Judge Says 30 Year Term 'Rational and Reasonable,'" FBI, accessed March 26, 2016, https://www.fbi.gov/seattle/press-releases/2009/se071009b.htm.
19. "United States of America, Plantiff, No. CR01-108R v. John Wayne Zidar," Systemics, accessed November 18, 2015, http://www.systemics.com/legal/digigold/discovery/postings/society-server_indictmenta.html.
20. "Ponzi Scheme Mastermind is Convicted," Seattlepi.com, accessed March 26, 2016, http://www.seattlepi.com/news/article/Ponzi-scheme-mastermind-is-convicted-1093583.php.
21. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.
22. "TalkGold.com—E-Gold HYIP Forum HYIP Investments," Internet Archive: Wayback Machine, accessed March 26, 2016, https://web.archive.org/web/20050204031751/talkgold.com/.
23. Ibid.
24. "Hazlewood's Get-Rich-Quick Schemes," ZetaTalk, accessed March 26, 2016, http://www.zetatalk.com/index/hazelwo2.htm.
25. "Lr16886," SEC.gov | Home, accessed March 26, 2016, http://www.sec.gov/litigation/litreleases/lr16886.htm.
26. Julian Dibbell, "In Gold We Trust," wired.com, January 1, 2002
27. "U.S. Charges Internet Operation Was a Huge Scam—NYTimes.com," The New York Times—Breaking News, World News & Multimedia, accessed March 26, 2016, http://www.nytimes.com/2001/07/03/business/03PONZ.html?todaysheadlines=&pagewanted=2.
28. "Garry W. Stroud, Individually and D/b/a Diamond Global Holding Trust, Euro Credit and Exchange Bank Ltd., and Angelic International, Et Al.: Lit. Rel. No. 17988 / February 19, 2003," SEC.gov | Home, accessed March 26, 2016, https://www.sec.gov/litigation/litreleases/lr17988.htm.
29. "Hazlewood's Get-Rich-Quick Schemes," ZetaTalk, accessed August 6, 2015, http://www.zetatalk.com/index/hazelwo2.htm.

30. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.
31. "E-gold® Welcomes," Internet Archive: Wayback Machine, accessed March 26, 2016, web.archive.org/web/20060322134922/https://www.e-gold.com/letter2.html.
32. E-gold.com, "General Discussion of E-gold and Other Forms of Money, Especially Those Involving the Internet or Gold," E-gold discussion list, last modified November 28, 2007, http://comments.gmane.org/gmane.comp.finance.e-gold.user/6488.
33. Office of Foreign Asset Control, "Enforcement Information for July 11, 2008," OFAC, last modified July 11, 2008, https://www.treasury.gov/resource-center/sanctions/Documents/07312008.pdf.
34. "Enforcement Information for July 11, 2008," OFAC, last modified July 11, 2008, https://www.treasury.gov/resource-center/sanctions/Documents/07312008.pdf.
35. Indictment, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
36. Affidavit in Support of Complaint for Forfeiture, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
37. "18 U.S. Code § 981—Civil forfeiture | US Law | lii / Legal Information Institute," accessed March 16, 2015, https://www.law.cornell.edu/uscode/text/18/981.
38. "UNITED STATES OF AMERICA V. ALL PROPERTY IN/UNDERLYING E-GOLD ACCOUNT NUMBER: 544179 AND 109243 :: Justia Dockets & Filings," Justia Dockets & Filings, accessed November 8, 2015, https://dockets.justia.com/docket/district-of-columbia/dcdce/1:2007cv01337/126696.
39. "Other Cases, Dockets and Filings in the District of District of Columbia :: Justia Dockets & Filings," Justia Dockets & Filings—Cases 91-100 of 136, accessed March 26, 2015, https://dockets.justia.com/browse/state-district_of_columbia/noscat-7/nos-690?page=10.
40. Ibid.
41. Ibid.
42. "GoldCard Funding Page," Internet Archive: Wayback Machine, accessed January 27, 2016, http://web.archive.org/web/20050930212942/goldtocard.com/loadcard-en.html.

43. "GCard—Cash Card Debit Card Worldwide," Internet Archive: Wayback Machine, accessed September 21, 2015, https://web.archive.org/web/20050702013038/www.mygcard.com/.
44. "ATM Debit Card Maestro Cirrus Debit Card Without the Need for Credit Checks," Internet Archive: Wayback Machine, accessed September 20, 2015, https://web.archive.org/web/20060101030431/bluebanking.com/.
45. "GoldToCard Homepage—Gold to Card Goldcard," Internet Archive: Wayback Machine, accessed September 23, 2015, http://web.archive.org/web/20050930212942/goldtocard.com/.
46. "GoldToCard Homepage—Gold to Card Goldcard," Internet Archive: Wayback Machine, accessed September 23, 2015, http://web.archive.org/web/20050930212942/goldtocard.com/.
47. Ibid.
48. Ibid.
49. Ibid.
50. Affidavit in Support of Complaint for Forfeiture, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
51. "Get Paid Center: E-gold Hits the Wall! Government Seizes Major Agents' Accounts," Get Paid Center, accessed March 26, 2016, http://gptcenter.blogspot.com/2007/05/e-gold-hits-wall-government-seizes.html.
52. Ibid.
53. Ibid.
54. "Other Cases, Dockets and Filings in the District of District of Columbia :: Justia Dockets & Filings," Justia Dockets & Filings—Cases 91-100 of 136, accessed March 26, 2015, https://dockets.justia.com/browse/state-district_of_columbia/noscat-7/nos-690?page=10.
55. Ibid.
56. Ibid.
57. Ibid.
58. Ibid.
59. Ibid.
60. Ibid.
61. Ibid.
62. Ibid

63. Ibid.
64. Ibid.
65. Ibid.
66. Ibid.
67. Ibid.
68. Ibid.
69. Ibid.
70. Affidavit in Support of Complaint for Forfeiture, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
71. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016
72. Indictment, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
73. "OmniPay Temporarily Suspends Exchange to Transition to OmniPay Africa," www.alansmoneyblog.com, accessed March 26, 2016, http://alansmoney.blogspot.com/2007/05/omnipay-temporarily-suspends-exchange.html.
74. Douglas Jackson, Email question and answer interview, Melbourne, FL March 13, 2016
75. "07-109—USA V. E-GOLD, LTD. Et Al," U.S. Government Publishing Office, accessed March 26, 2016, https://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_07-cr-00109/content-detail.html.
76. "07-109—USA V. E-GOLD, LTD. Et Al," U.S. Government Publishing Office, accessed March 26, 2016, https://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_07-cr-00109/content-detail.html.
77. Plea Agreement of e-gold, Ltd., United States v. e-gold, Ltd., No. 07-109- 01 (D.D.C. July 21, 2008), 2008 WL 4234436.
78. "E-gold Blog: E-gold Value Access Plan—Claims Filing Deadline Extended a Third Time," E-gold Blog, accessed March 26, 2016, http://blog.e-gold.com/2013/12/e-gold-value-access-plan-claims-filing-deadline-extended-a-third-time.html.
79. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016
80. "Federal Register / Vol. 76, No. 140 / Thursday, July 21, 2011 / Rules and Regulations," U.S. Government Publishing Office,

accessed June 17, 2015, https://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.
81. Plea Agreement of e-gold, Ltd., United States v. e-gold, Ltd., No. 07-109- 01 (D.D.C. July 21, 2008), 2008 WL 4234436.
82. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.

CHAPTER 3

The Liberty Dollar and Bernard von NotHaus

The "Liberty Dollar" also known as "American Liberty Currency" (ALC) was a privately issued voluntary use currency product created through a nonprofit organization named the National Organization for the Repeal of the Federal Reserve and Internal Revenue Codes (NORFED). Early users had also referred to versions of the currency as "American Patriot Currency."

Mr. Bernard von NotHaus formed NORFED in 1998. He started this organization with clearly stated goals and lawful intentions. His mission was to create a legal alternative to US fiat currency that represented an amount of precious metal value. Compared to national currency, the Liberty Dollar was not issued through the creation of debt; it was sound money with real value. Bernard created this commercial product to compete directly with Federal Reserve Notes (FRN) issued by the government of the USA. His organization compared the Liberty Dollar with the US dollar and presented reasons for consumers and merchants to use the "silver backed" Liberty Dollar instead of the debt-issued FRNs that had no precious metal backing. The task of creating a physical currency that acted as an alternative to national money was an enormous undertaking. The history of the Liberty Dollar and Bernard von NotHaus is an authentic David versus Goliath real-life tale.

In the late 1990s, Bernard was known as a monetary architect. His ideas inspired tens of thousands of honest Americans. By educating others about the perils of fiat currency and the enormous national debt that

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_3

looms over America, Bernard has inspired a small but broad segment of the American population. Additionally, his pioneering work in private currency forged a passageway leading many other entrepreneurs to the concept of sound money. The Liberty Dollar's creator set out with the best of intentions, made some mistakes as pioneers will do, and finally encountered a hailstorm from US Courts and prosecutors. Much can be learned by carefully reviewing the details of Bernard's currency and its relationship to a consumer marketplace. The digital version of the Liberty Dollar called the eLibertyDollar is of particular interest.

Throughout his career, Bernard used a comparison of the FedEx private delivery service as private competition for the US Postal Service to be similar to the Liberty Dollar private currency that competed against government money. Here is an example of that statement from the Liberty Dollar website in 2006.

> Works Just Like US Dollars
>
> Just as FedEx brought competition to the post office and it became incredibly successful, the Liberty Dollar emulates the same model by bringing competition to our country's monetary system.[1]

That year, in 2006, NORFED became Liberty Dollar Services, Inc. Bernard, who had been the president of NORFED, became the executive director of Liberty Dollar Services, Inc. Bernard stated that he recognized a change in the marketplace and described it in these terms, "…the market and the people in the LD [Liberty Dollar] movement changed. It grew up."[2] The business enterprises responsible for both NORFED and Liberty Dollar Services, Inc. were both nonprofit companies incorporated in the USA. NORFED made a genuine plea for Americans to own interest-free money that was redeemable in something of value (silver). At NORFED, Bernard von NotHaus gained the title of Monetary Architect.

The ALC paper currency was a warehouse receipt for silver on deposit. The vault service issued the warehouse receipts. The company holding the precious metal was Sunshine Minting, Inc. NORFED also offered the silver "tokens" or "rounds" (not coins) along with the paper currency starting in October 1998. The organization issued an electronic version of the currency in early 2003. All three units of exchange, the precious metal tokens, the paper warehouse receipts and the electronic digital payment system were known as ALC. The digital version of the currency was called the "eLibertyDollar." It was a digital representation of the ware-

house receipt. At the time of its introduction, there were approximately 30,000 ALC users.

Customers could now email or transfer online the digital currency version of a warehouse receipt. The units moved between online accounts within the closed ledger system. This new Internet activity caught the attention of an existing digital currency community that had not previously heard of the Liberty Dollar and usage quickly spread beyond the USA. The digital units were said to be exchangeable on a one-for-one basis into other forms of the Liberty Dollar currency. However, there was no significant network of exchange agents, as was available for all other digital gold currency systems. If a client had $5000 worth of digital Liberty Dollars, there were no consistent exchange agent operations that would swap that digital value into national currency. While the ALC warehouse receipts were "backed by silver," the value of the precious metal, in dollars, did not equal the face value of the currency. Consequently, exchange agents were reluctant to accept any exchange of national value into the digital Liberty Dollars, except at a severe discount.

The company's marketing efforts billed the Liberty Dollar as "America's second most popular currency." The advertising stated that the currency could be marketed and exchanged, in the community, generating a profit for its users.

In November 2007, at the time of the government's seizure of Liberty Dollar assets, there were an approximate $8 million worth of precious metals seized and Bernard later stated that approximately $6 million of that was silver held in the vault that backed the circulating digital currency. Users of the Liberty Dollar had faith in the digital currency version of the currency and had considered it a safe.

To obtain electronic Liberty Dollars, anyone could purchase them directly from the corporate office in Evansville, Indiana and pay using a credit card, wire transfer, money order, or check. Consumers purchasing the digital units had to pay an equal face value in US dollars for electronic Liberty Dollars (1-to-1 exchange). Those participating in the multilevel marketing as Liberty Associates or Regional Currency Offices (RCOs) receive the digital units at a discount. All of these Liberty Dollar products either contained metal (silver, gold, and copper) or were backed by precious metal warehouse receipts.

The founder of ALC and one of the parties ultimately prosecuted by the government was Bernard von NotHaus. Bernard is a man with a keen understanding of history's monetary systems.

NORFED's corporate office, which was also known as the "Fulfillment Office," was located in Evansville, Indiana. All company business flowed through this location including all contracts for the creation and printing of the currency, the minting of the precious metal tokens, and the issuance of the digital currency. Users purchasing currency or redeeming currency back into national money, transacted business through this Evansville office. However, the RCOs that dotted the USA and were operated independently of the company also provided limited exchange services for all type of ALC.

Asheville, North Carolina was another busy location for the exchange and promotion of Liberty Dollars and NORFED. Mr. Willian Kevin Innes operated the Asheville RCO. He was also one of the three members that made up the NORFED Executive Committee responsible for the activities of the nonprofit business.

A young lady named Sarah Bledsoe was the NORFED fulfillment office manager in Evansville, Indiana. Another young lady named Rachelle Moseley also worked in the Evansville, Indiana corporate office of NORFED. According to court documents, she had also been employed as the Regional Currency Office Manager and Chief Operations Officer. Bernard, Kevin, Sarah, and Rachelle were the four persons named in the Government's criminal case which ended the Liberty Dollar.

NORFED

The mission of NORFED was to restore an honest monetary system for all Americans. Here is how the NORFED website communicated that idea to potential new members.

> When Congress unlawfully gave private interests the control of federal money, the sovereign States were left without any lawful money to use. By default, the people had to begin using Federal Reserve Bank Notes in lieu of gold or silver-backed currency. Originally the people's money was issued without interest and left little room for inflation. Today, however, Federal fiat money is loaned into circulation with interest and creates inflation. Federal Reserve Notes (FRN's) do not belong to the people and are not redeemable.[3]

A majority of Americans do not realize how money is issued or created. Very few Americans realize that in the last 90 years, the purchasing

power of one dollar has lost 96 percent of its value. Bernard's websites, speeches, and documents were always quick to point out the damage that monetary inflation has done to the economy and the lives of Americans. One of Bernard's statements was to ask readers this question, "Do you remember when you could buy a candy bar and soda for $1?" That purchase is not possible in 2015 because inflation has shrunk the purchasing power of the almighty dollar. Another great example of inflation is found in the Seventh Amendment to the US Constitution, which states the following:

> In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.[4]

In the 1700s, the founders of the USA wrote into the Constitution a requirement that no lawsuit could proceed unless the value of the suit exceeds $20. At that time, $20 was a great deal of money! Inflation has corrupted every corner of the American economy and society. No one communicated this information more effectively than Bernard von NotHaus. ALC offered users an alternative to FRNs.

American Liberty Currency Circa 2000

NORFED issued paper ALC in three denominations of warehouse receipts $1.00, $5.00, and $10.00. For convenience, this alternative currency was denominated in US dollars. The $10.00 Certificate is backed by one Troy ounce of pure .999 fine silver. The term "convenience" is used here to reflect that goods and services in America are priced in dollar amounts.

In 2000, a Troy ounce of silver started the year priced at approximately $5.25 per oz. At that time, precious metal prices were stable and the value of silver, as quoted in US dollars, slowly trended downward the entire year. It ended in December at approximately $4.70 per oz. At no time during the year did the market price of silver rise above $5.50 per oz. Consequently, a $10 face value ALC warehouse receipt, convertible into 1 ounce of silver, had a cash liquidation value of about half its US dollar face value. Other values of ALC were proportionally backed by smaller amounts of silver. The $5 certificates were backed by a half-ounce and the $1 by a tenth ounce of silver.

While the NORFED organization was able to purchase silver in bulk at spot prices, then mint or store that metal issuing ALC warehouse receipts, there was always an obvious lower exchange value on the amount of silver as compared to the $10 face value of the currency.

Many users were not concerned about this obvious value difference because their intent in using the currency was to make a statement about government-issued money. More than any other feature or benefit, using the Liberty Dollar opened up a discussion and dialog between American's about how the government created money. Spending $20 in ALC on a sandwich, drink, and chips for lunch was not the act of a domestic terrorist or attempt to undermine the trillion-dollar global US economy. Using the Liberty Dollar in everyday commerce was a consumer choice and one person's voluntary statement of their desire for a stronger America. An everyday consumer, accepting the currency and respending it at another local merchant was an excellent way to show support for NORFED and the Liberty Dollar.

Both the Liberty Associate and RCOs were able to buy the currency at a discount to face value, and trade out of it through merchants or sell the currency at a higher value to the public. This structure generated a multi-level profit scheme and benefited NORFED by continually placing more currency into circulation. As a nonprofit company, NORFED was able to self-fund the day-to-day activity of the organization and did not rely on outside grants or loans to advance the cause of sound money.

As a consumer receiving cash change from a merchant, which was a popular method of putting the currency into circulation, the consumer would receive face value on the currency. As a merchant accepting the Liberty Dollars, and a Liberty Associate or RCO, the business could obtain the currency at a lower price and distribute it (exchange it) to consumers at face value. The NORFED website explained that in the exchange of federal money for ALC, a modest margin of profit was generated for the organization. The profit arose between the final sale price of the finished product, minus the value of the raw silver, plus manufacturing and operating costs. NORFED was to use those funds for research and political action in the furtherance of repealing the Federal Reserve and IRS.

NORFED also issued a $500.00 gold certificate backed by 1 ounce .9999 fine gold and the Gold Liberty precious metal token also contained 1 ounce .9999 fine gold. Just like the paper warehouse receipt (Gold Certificate), the face value of the gold token was $500. The trading range for gold, as priced in dollars, during 2000 was between approximately

$263 and $312. Again, to purchase one of these products, at face value during the year 2000, was locking in profit for anyone trading on the various levels between the manufacturer (NORFED) and the retailer.

There are two points in the Liberty Dollar discussion which need closer examination. Point one states that there is nothing wrong with an organization manufacturing a commercial product and selling it for a profit. Point two states that any entity responsible for the creation and issuance of "money" or "currency," perhaps, should not be making a profit at that task.

Companies representing e-gold, E-bullion, and other digital gold currencies sold the units by weight priced at the daily spot market cost. A user would buy a gram of gold valued at the spot price. A Liberty Dollar user would pay a price based on the face value of the token or currency. That face value did not fluctuate or correspond to a changing price of precious metal. The face value was an arbitrary amount given to the currency above the market price for the purpose of generating an organizational profit. In later years, as the price of silver and gold moved up, so did the arbitrary face value of all Liberty Dollar products. As the price of silver moved from approximately $3 to around $48, the original $10 base moved up to $20 face value, then to a $50 base. One ounce equaled a $50 face value.

Bernard von NotHaus

Today in his seventies, much of Bernard's adult life has been devoted to the cause of free market money as outlined by Friedrich August von Hayek in his book the Denationalization of Money.

Bernard Von NotHaus and another associate are recorded as having formed The Hawaiian Mint in late 1974. In January 1986, that original company filed for bankruptcy and was reorganized as the Royal Hawaiian Mint.[5] To further clarify the use of this name, in 1969, the "Royal Hawaiian Mint" name had also previously been used as the name for a corporate division of Royal Hawaiian Coins, Inc. of Honolulu, Hawaii.

Bernard tried very hard to focus his efforts on educating the public about the history of money in America and the issuance of Federal Reserve Bank Notes or "FRNs" as American money. His ALC exemplified the principles of a free market, value-backed, private currency. His target market of users was also clearly defined.

Once again in the modern world of private currency, Bernard had invented what he believed was a better mousetrap. ALC was a paper cur-

rency at least partially backed by precious metal. Being a "better" currency, Bernard and many others believed the world would beat a path to his door.

The Liberty Dollar website held an important page of links to outside sources that seemed in one way or another to support the idea of freedom, patriots, sound money, and liberty. Many of these are still in operation in 2016.

In 2001, Bernard Von NotHaus and Steve Forester, a former e-gold employee, had created another private currency issuer known as 3PGold which offered a digital currency product backed by gold. In 2002, 3PGold was eventually sold to a group of operators lead by Terry Neal and including Sean Trainor. Not long after that acquisition, 3PGold became Crowne Gold. There is another chapter in this book detailing Crowne Gold.

Recognized Issues

Issue 1

The Liberty Dollar, in any form, a certificate, metal, or digital, would have to contend with Gresham's Law, which stated that bad money drives out good money. In simple terms, if consumers had a choice of two legal tender currencies, one made of precious metal, with a $10 face value and one made of worthless paper with a $10 face value, people will spend the paper and hoard the intrinsic value of silver and gold. If the pure silver $10 Liberty Dollar was used in shopping alongside the paper $10 Federal Reserve Note, a majority of people would hold on to the silver and spend the paper. This hoarding causes the cheap paper money to circulate more widely, and eventually the precious metal currency would disappear from circulation. The concept is credited to Sir Thomas Gresham, and known as "Gresham's Law." However, Gresham's Law presupposes that both currencies are legal tender. As in the case of the privately issued Liberty Dollar versus the government-issued legal tender FRN, the situation does precisely match. However, the end effect is very similar.

Issue 2

Because of the "base" structure of the ALC, the face value will always be higher than the spot price of the underlying commodity. During most of the annual trading of precious metals, the face value is near twice the spot

price of the metal. Consequently, consumers would ask, "Why Would I Want to Pay Twice the Price for Silver?" Both the NORFED and the Liberty Services, Inc. website had a detailed explanation overcoming this sales objection. Through the years, as the price of precious metals rose, NORFED provided more and more excellent reasons supporting the use of silver-backed commodity money. This information caused thousands of American to rethink the concept of "money" and how big government takes advantage of the public's ignorance of inflation and monetary policy. The underlying argument was always that precious metals fluctuate in value, and the denomination of units in precious metal are not convenient for daily commerce. However, ALC has overcome this issue using the base currency levels or face values that change with the market movement of silver. ALC currency made it possible to carry 100 ounces of silver in a wallet. The value of silver issued as a warehouse receipt allowed ALC to become a valuable tool for daily commerce. However, as the face value was always stepped higher, there was always this discrepancy between liquidation value and face value.

Issue 3

While the website and materials stated that ALC could be exchanged back into national money at any NORFED Redemption Center, the Main Fulfillment Center in Evansville, Indiana or some RCOs, the availability of exchange was very limited. In comparison with any other digital gold currency, which could handle the exchange of millions in gold each week, continuous successful exchange of Liberty Dollars was a failure. Those consumers and merchant who ended up with the currency either had to find a place that would accept the currency at face value or hold on to it as a novelty investment. Fortunately, for those holding and hoarding the silver currency, precious metal prices skyrocketed in value. Silver moved from about $5 per ounce in 1999 to more than $46 an ounce in 2010. Bernard was 100 percent correct in his prediction that Liberty Dollars did not lose their purchasing power as did fiat currency.

100 Percent Gold and Silver

In later years, after the name changed to Liberty Dollar Services, Inc., the Liberty Dollar was defined as a private voluntary barter currency (PVBC). The paper ALC was more than just a medium of exchange. As one law-

yer stated, the ALC certificate is an expression of a US citizen's First Amendment right to petition for the redress of grievances.

In 2004, with the rising price of silver, the currency also moved up from a $10 silver base to the new $20 silver base and face value. However, in 2009, the internal pricing for the units changed to a new bullion pricing not based on a percentage of the face value. It was labeled private voluntary barter currency, and the business minted the letters PVBC on each metal token.

The $20 face value of the "Silver Liberty" token was based on the spot metal price plus a small premium which covered the administration and minting costs. This level of pricing also made a higher profit for those intermediaries known as Liberty Associates and RCOs that were marketing the currency.

Digital Liberty Dollars

The organization that first issued the eLibertyDollar was NORFED and the online currency was defined as a "Digital Warehouse Receipt." Similar to other digital currency systems at that time, only a simple name and email was required to open and immediately operate an account. There were no KYC requirements for new accounts under $10,000. At any time, if an account rose above $10,000, the account holder had 30 days to submit identification.

A Digital Warehouse Receipt was similar to a paper warehouse receipt. It was a contract between the warehouse and another party that acted as the bearer of the digital certificate. The paper warehouse receipt and the digital warehouse receipt had the same seven qualifying elements that made it a legal, binding agreement.

1. Term of receipt
2. Date of issue
3. Description of item warehoused
4. All additional charges or conditions
5. Expiration of receipt
6. Address of warehouse
7. Signature of the warehouse official.

Warehouse Receipts that had been issued by Sunshine Minting, Inc. to NORFED in paper form were later distributed as electronic Liberty Dollars also known as digital warehouse receipts. Just like digital gold, a

digital warehouse receipt was divisible into fractions of a unit. The digital units could be broken down into thousands, and parts of the total receipt were circulated online as fractional payments. An account holder could send .09 in eLibertyDollars to another user. The bearer could also execute this fractional amount on demand, so long as the whole never exceeds the quantity of silver in the warehouse.

Here is the critical difference between all other digital precious metal systems at the time and the electronic Liberty Dollars. Silver backed this digital currency at a $10 base, which meant that for every $10 in digital currency in a user's account, there was one Troy ounce of silver on deposit. Consequently, if the account showed $10 and silver was trading at $4.30 an ounce, a conversion of that digital warehouse receipt into actual silver would create a loss of more than $5.00 on that exchange. $10 in digital Liberty Dollars on that day converted into a value of $4.30 in silver. The "minting" of that digital unit at a price higher than the spot price of silver, produced a profit for NORFED, the manufacturer and any party within the marketing platform ending with general consumers. As a Liberty Associate or RCO, participating in the multilevel marketing of this product, both parties were able to purchase digital Liberty Dollars at a price less than the $10 digital face value. The marketing of eLibertyDollars was almost identical to the price levels and marketing of the physical silver or the ALC.

As with any other digital precious metal currency, strict measures were taken to ensure that the company held the resources represented by the digital currency. These assets were kept in the secure and insured vaults at Sunshine Minting, Inc. The company generated daily transaction reports and a monthly audit that verified all the precious metal was backing the digital units at all times. The Liberty Dollar organization even published the reports on the company's website.

However, this system was in no way equal to other existing precious metal digital currency systems. In e-gold, GoldMoney, e-bullion, and all other digital gold currencies, $10 exchanged produced $10 in value withdraw to the account holder. A digital ounce of gold exchanged for national currency resulted in a value equal to the spot price of an ounce of gold. This always occurred because there was no profit margin built into the face value or in this case the spot price. The quoted spot price was the face value.

For some existing Liberty Dollar users, and many newer ones, the announcement of an electronic version of the silver-backed private currency

was very exciting. Designers had created the eLibertyDollar software with an available application programming interface (API) that allowed business websites to integrate the digital currency into their online operations.

With the addition of this new eLibertyDollar electronic version of Bernard's silver-backed currency, he was clearly attempting to advance the use of Liberty Dollars in both business and consumer transactions. This attempt included a person-to-person online payments, email payments, person-to-business, consumer payments, online shopping, and the exchange of eLibertyDollars for physical consumer merchandise.

In a marketplace with existing precious metals-backed digital currencies such as e-gold, e-bullion, Pecunix, WebMoney, and GoldMoney, an important question faced the electronic Liberty Dollar, and many users and exchange agents asked, "Could the eLibertyDollar compete with other precious metal backed digital currency products?"

There is no better example of how online commerce using the eLibertyDollar functioned than the Gold-Stores (www.gold-stores.net) website business. The Gold-Stores operated online from mid-2003 until the first quarter of 2009. The business changed hands once in 2004. The Gold-Stores was a full Amazon affiliate online store. The operator had modified the software changing the methods of online payment that were accepted by the store. At the time of check out, shoppers were presented with various digital currency options instead of conventional bank methods of payment. The Gold-Stores did not accept credit cards, bank payments, or PayPal. However, the store did accept e-gold, e-bullion, WebMoney, 1mdc, Pecunix, and Evocash. In mid-2003, the owner of the operation was first introduced to the eLibertyDollar.

At that time, the eLibertyDollar was seen as "another digital currency backed by precious metal." Since the eLibertyDollar website offered an API, the business added the new digital currency as an automatic payment method for Gold-Stores shoppers. After this addition, anyone could visit the Gold-Stores, place any Amazon merchandise in the online cart, and automatically check out using the eLibertyDollar.

In 2003, digital currency was still a brand-new consumer online payment tool. The Gold-Stores offered users the ability to spend a variety of popular digital currencies across many categories of consumer goods. Online orders were being placed each day using e-gold, e-bullion, WebMoney, and 1mdc.

Behind the scene, the store operator was accepting digital currencies, then using a credit card to place orders through Amazon. At the end of

each week, all of the digital currency accounts were emptied and sold through exchange agents for national money deposits. After the owner had exchanged the digital currency, national currency was transferred to the bank account for the credit card account and the balance returned to zero. The Web business not only facilitated the everyday use of digital currency for consumers but the business also generated a small profit.

The Gold-Stores functioned very well accepting: e-gold, e-bullion, WebMoney, 1mdc, Pecunix, and Evocash in large part because at that time, in 2003, the exchange market for these digital currency products was very liquid. There were hundreds of agents around the world that would buy the digital currency and pay out national currency by wire, usually within 24 hours. E-gold, E-bullion, 1mdc, and Pecunix were all 100 percent backed by gold. Consequently, if the total amount of e-gold orders during a week was $10,000, the total digital currency was sold for approximately $10,000, minus the agent's fee. The Gold-Stores bank account then received the funds by wire transfer. WebMoney and Evocash were digital units denominated in US dollars, and there was never any question that an agent would accept those digital currencies for the exact face amount. If $8395.50 in WebMoney were exchanged, the Gold-Stores would receive a wire for that amount minus the exchange agent's commission.

Exchanging these digital currencies into national currency, through a third-party agent, caused a one- or two-day delay in posting the funds to the bank account. However, as the Gold-Stores operator's credit card only required a payment every 30 days, this minor delay was of no consequence.

eLibertyDollar Consumer Transactions

After the Gold-Stores had begun accepting electronic Liberty Dollars, the online shop was promoted across the Liberty Dollar community. Dozens of orders for Amazon merchandise were received, and thousands of digital Liberty Dollars flowed into the new Gold-Stores eLibertyDollar account.

The store accepted all digital currencies at face value. If $100 in e-gold was received, $100 of merchandise was exchanged. The store also accepted eLibertyDollars at face value. A $100 Amazon order would require the customer pay out 100 eLibertyDollars. The eLibertyDollar operation functioned exactly like the other digital currencies. Electronic Liberty Dollars that accumulated during the week were then to be exchanged back to national currency each weekend.

During the first week of accepting eLibertyDollar, thousands of dollars in merchandise was sold and shipped and all of the new eLibertyDollar digital units accumulated in the Gold-Stores account.

A week later, after processing around $8000 in eLibertyDollar transactions, the store operator began liquidating all of the prior week's digital currency income and exchanging it into national currency. One of the Gold-Stores' first calls was to the Liberty Dollar operation in Evansville, for the purpose of selling the $8000 worth of eLibertyDollar in exchange for a wire transfer.

Much to the operator's surprise, the Liberty Dollar employee informed them that their office would not buy back the eLibertyDollar currency at its face value. The staff suggested calling a RCO. Additional attempts to exchange the digital currency for dollars through the RCO were also unsuccessful. The RCO stated that they would only buy small quantities of the eLibertyDollar and not at face value.

Because agents in the organization could purchase both the Liberty Dollar and the eLibertyDollar at a discount to face value, there was no one willing to buy back the eLibertyDollar at its digital face value. There was no liquid exchange from the eLibertyDollar into national currency at face value. At least, not more than a few hundred dollars a month. The store owner could not liquidate the $8000 in eLibertyDollars which had accumulated during the previous week.

No agent or party would buy the digital units at a price anywhere near $8000. The cost of the physical merchandise purchased on a credit card could not be covered by a highly discounted sale of eLibertyDollar. The terms of service listed on the website from August 14, 2003, defined the value and backing of a digital eLibertyDollar.

> 10. Valuation of Silver Backing
>
> Each ALD with a Face Value of $1.00 (one Liberty Dollar) is backed by one-tenth Troy ounce of .999 fine silver, and any fraction of a dollar is likewise backed by an appropriate prorated amount of silver. Just as the valuation of the Liberty Dollar is identified on the paper warehouse receipts, the valuation of the ALD is identified on the website as "$10 SILVER BASE." When the market price of silver rises or falls so as it is no longer possible for NORFED to provide an $1.00 (one Liberty Dollar) in ALD that is backed by one-tenth Troy ounce of .999 fine silver, NORFED may at its sole discretion, raise or lower the valuation of ALD so that the currency is still 100% backed by physical silver in the warehouse.[6]

On August 14, 2003, the price of silver in US Dollars was $5.00 per Troy ounce. One-tenth Troy ounce of fine silver would have a value on that day of 0.50 cents. Unlike all other digital currencies in operation at that time, the digital Liberty Dollar face value, as represented in the online account, did not represent its free exchange value. $10 of eLibertyDollar did not translate into $10 of national money, and there was no large volume daily exchange because the circulation of digital units was very low.

The eLibertyDollar was functioning more like a Complementary currency than it was acting like a digital precious metals account. Complementary currency always sells at a discount to federal money. However, all other digital currency products in circulation had digital values equal to the liquidation price, which was the converted value of precious metal using the price at the time of exchange. The electronic Liberty Dollar had few exchange agents, casual acceptance by the issuer, and no national currency liquidity.

This digital medium of exchange was not an online payment product that business and consumers could have ever widely adopted as a medium of exchange for daily shopping. Merchants that sell online need to replenish their cash flow as quickly as possible and cannot afford to lose money on those currency exchanges. If the market for digital currency is convenient and liquid, online merchants will accept any method of payment. When users can quickly and cheaply convert the digital units into dollars, euro, or yen that digital currency has a good chance of being accepted. Unfortunately, because of the multiple sales levels and profit built into the creation of the eLibertyDollar digital units, as it had worked in the physical currency, the electronic Liberty Dollars were not practical for daily commerce. Once again, there was no financial regulations that outlined the exchange procedures of this digital currency.

A great example of this fluid exchange, in 2015, are the large bitcoin exchange agents such as Coinbase. These licensed and regulated US financial agents provide daily liquidity for bitcoin merchants. Instead of accumulating digital currency for a week and liquidating it through a third-party agent as the Gold-Stores had operated, Coinbase converts bitcoin to USD every business day and deposits it into the merchant's bank account. If bitcoin were not liquid and, users had to sell the coins at a 40 percent or 50 percent discount to the market price, no merchant selling tangible goods could ever afford to accept bitcoin as payment for goods.

Federal Bureau of Investigation Raid and Seizure

In a November 2007 letter from Bernard von NotHaus openly published on the Internet, he stated that Federal Bureau of Investigation (FBI) and US Secret Service agents had raided the Liberty Dollar office in Evansville, Indiana. During the raid, government agents seized all of the gold, silver, and platinum the business was storing at the office along with nearly 2 tons of newly minted "Ron Paul Dollars." Agents seized all of the company files, computers, and office records. Additionally, the government froze the company bank accounts. At Sunshine Minting in Idaho, agents had seized all of the precious metals, including the silver that was backing both paper and digital warehouse receipts. The agents even took the dies that were used to mint the Liberty Dollar Tokens.

Here are the details from that government seizure:

Pursuant to 18 U.S.C. § 982(a)(2)(A) and 18 U.S.C. § 982(a)(3)(E); and 18 U.S.C. § 981(a)(l)(C), 28 U.S.C. § 2461, 18 U.S.C. § 1956(c)(7), and 18 U.S.C. § 1961(1), because it is property which constitutes or is derived from proceeds and gross receipts traceable to the offense of mail fraud, a violation of 18 U.S.C. § 1341:
3039.375 Pounds of Copper Coins,
5930.32 Troy Ounces of Silver Coins,
63.24 Troy Ounces of Gold Coins, 3 Platinum Coins,
168,599 Silver Troy Ounce Coins, 147 Gold Troy Ounce Coins,
17 Gold .05 Troy Ounce Coins,
710 Silver .5 Troy Ounce Coins,
11 Silver Bars and Silver scrap totaling 10,720.60 Troy Ounces,
1000.5 Troy Ounces of Silver Coins,
Dies, Molds, and Casts Seized at Sunshine Minting, Inc. November 14, 2007,
16,000.05 Troy Ounces of Raw Silver,
100 Ounces of Copper Coins,
$254,424.09 in US Currency

In classic Bernard style, his commentary on the events included some fun sarcasm. He once stated that he hoped any future arrest did not interfere with his existing commitments! Bernard showed up to a speaking event dressed in striped "prison" attire and even once with a phony ball and chain. Describing the FBI in a live TV interview on a top affiliate

station, he coined the phrase "G-boys" and referred to his primary FBI handler as "Agent Andy." Because at the time, Ron Paul was considering a presidential run, confiscation by the government of the 2 tons worth of copper, Ron Paul Dollars also created some national headlines.

Many complementary currency users were mixed in with the throngs of Liberty Dollar users across America. Although there were collectors and Liberty Dollar users in other countries around the world, local currency fans had promoted the use of Liberty Dollars, in areas or regions, as a local trade currency.

In many instances, Liberty Dollars were compared to a complementary currency such as Ithaca Hours. This observation was incorrect. Complementary currency takes many forms and shapes; however, all of them are designed to be plentiful and circulate alongside national currency. A Complementary currency "complements" national currency; it does not try to replace it. Bernard had created the Liberty Dollar as a replacement for national currency. Backed by the precious metal, Bernard proposed that the Liberty Dollar was a better design than debt-issued government money.

There are two widely accepted categories of complementary currency. There are social purpose currencies and commercial purpose currency. The social purpose currency functions to match unused resources with unused or underused assets. Here is a great example based on the mutual credit system that is known as a Local Exchange Trading System or LETS. In a town with high unemployment, there are 500 out-of-work men on one side of the city. On the other side of the city, many unfinished jobs could be completed by the 500 unemployed workers. The problem is no one in the city has the money to hire and pay the workers because national money is hard to obtain; it is scarce. The solution to this unemployment problem may be to use a LETS mutual credit system and create a local unit of currency that is plentiful and freely circulates in the community. The benefits of this currency are derived from the units remaining in circulation and often changing hands through many transactions around the town. This currency can never be loaned out; its identified value never changes and does not pay interest. It is plentiful. Users can derive no benefits from hoarding or saving the complementary currency. Users spend LETS units into existence. The system administration does not loan the units into circulation. The LETS system functions on the commitment of its users to maintain both a "give and take" in equal proportions. An organization measures success in a complementary currency by any increase

in circulation within the small area of usage. If the town had out-of-work residents and jobs to be done but no money, mutual credits could be created to pay those workers and complete the unfinished jobs. Attempting to grow the usage area of a LETS will cause the units to decrease in circulation, and this is one reason that complementary currency does not achieve a wide geographic usage. It only works on a local basis. In a new LETS community, users are encouraged to go out and spend the currency into circulation.

It's very clear that ALC could not be considered a complementary currency. The ALC in all of its forms was commodity money. Liberty Dollars functioned as a scarce alternative to national currency. Backed by silver, the Liberty Dollar was designed to be "better" than national currency and was marketed to replace US dollars. Being backed by a commodity, the currency was hoarded and considered scarce money. Users recognized that any increase in the value of silver would be a benefit and often choose saving Liberty Dollars instead of continued circulation. One of the benefits of Liberty Currency was its ability to preserve purchasing power. The private currency's value did not deteriorate as quickly as fiat currency. The commodity backing the currency worked to preserve purchasing power. Complementary currency does not replace any other currency; it is not scarce, and it flows into places that national currency does not circulate.

Another popular form of complementary currency is the commercial purpose currency. Commercial purpose currency has real money value. It is designed only to circulate within a small area or region, and by design it directs shoppers away from large national stores and into locally owned shops and merchants. A commercial purpose currency, such as the Berkshares, which circulates in the Berkshire region of Massachusetts, is obtained by exchanging dollars into local currency through a network of locally owned banks. Users deposit 95 cents into a participating bank and one Berkshare, with a one-dollar face value, is exchanged for that national currency. There is no profit in this transaction. The Berkshares nonprofit organization that operates this commercial purpose currency is privately funded from outside grants and loans. The operation runs on donations and does not profit from operating the currency or the currency exchange. Only local merchants and stores within a defined area accept the Berkshares. Because the currency cannot be deposited in a large international commercial bank or leave the area bound for out-of-state manufacturers and overseas suppliers, the currency must stay and circulate within

the locally accepted area. The Berkshares continue to circulate in the local area, where it can be converted back into national currency through the local banks. Use of this commercial purpose currency bolsters the local economy. Experts estimate that one Berkshare circulates through five transactions with locally owned merchants before being converted back into national currency. Because it holds no value outside of its circulation area, the money stays in the local market. This multiplier is the main benefit of a commercial purpose local currency.

The Liberty Dollar did not offer the full benefits of a complementary currency because:

1. It was scarce commodity money prone to being hoarded.
2. The currency designer's intent was to replace national currency and not complement it.
3. It achieved a global circulation. It easily left the community that the currency originated in and held its value outside of the state and country.
4. The generation of profits from the exchange of each unit for national currency prevented it from achieving any long-term sustainable use.

For these primary reasons and others, ALC was not considered a complementary currency.

In parts of Michigan and Arkansas, areas developed where many local merchants would accept the silver tokens for consumer goods. Consequently, when the Liberty Dollar ran into legal trouble, many Complementary currency users in the USA began to question their local currency products. However, attorney and executive director of the Sustainable Economies Law Center (SELC), Janelle Orsi, was able to clarify some of the differences between Bernard's Liberty Dollars and most local or complementary currencies circulating in US towns. Regarding the Liberty Dollar, this text is available from CommunityCurrenciesLaw.Org, an SELC e-resource library.

> In 2011, a man named Bernard von NotHaus was convicted of several federal charges in connection with a coin currency he created, called the Liberty Dollar. The prosecution of this case sent a wave of worry through local currency projects around the country. However, there was some important difference between von NotHaus' coins and other local currencies. The Liberty Dollar coins had a "$" symbol, used the words "dollar," "USA,"

> "Liberty," "Trust in God" (instead of In God We Trust) and looked in design like coins of the national U.S. currency.[7]

While the nonprofit NORFED organization was exchanging a digital currency for national money, without a money transmitting license, as other digital currency exchange agents were doing, law enforcement did not focus any effort on this issue. Court documents from the Liberty Dollar case exposed that the organization had been under investigation by August 2005 at least until July 2007.

Bernard von NotHaus, Sarah Bledsoe, and Rachelle Moseley from the Evansville, Indiana, home office were all listed in the criminal indictment along with Mr. William Kevin Innes from the Asheville, North Carolina, RCO. FBI executed a seizure warrant for the Evansville, Indiana, office of the Liberty Dollar organization, following the multiyear investigation. Prosecutors filed superseding federal indictment on November 17, 2010. All these charges related to the silver pieces. The government did not challenge the legality of paper warehouse receipts.

The Liberty Dollar Case

United States of America
v.
Bernard Von NotHaus
William Kevin Innes
Sarah Jane Bledsoe
Rachelle L. Moseley
Violations:
18 U.S.C § 371
18 U.S.C § 485
18 U.S.C § 486
18 U.S.C § 2

In the 13-page, November 17, 2010, federal indictment (Docket No. 5:09 CR-27), the government harshly defined the company's activities and the Liberty Dollar PVBC. Here are select portions of that document.

1. It was a part and an object of the conspiracy that the defendants, and others both known and unknown to the grand jury, (a) did falsely make, forge, and counterfeit any coin, to wit, the Liberty Dollar

coins as identified in the Introduction, in resemblance and similitude of coins of a denomination higher than 5 cents, coined or stamped at any mint or assay office of the USA or in actual use and circulation as money within the USA and (b) did pass, utter, publish, sell, and possess any false, forged, or counterfeit coin, to wit, the Liberty Dollar coins as identified in the Introduction, knowing the same to be false, forged, or counterfeit, with intent to defraud any body politic or corporate, or any person, all in violation of Title 18, US Code, Section 485.

2. It was a part and an object of the conspiracy that the defendants, and others both known and unknown to the grand jury did make, utter, and pass, and attempt to make, utter, and pass, a coin of silver intended for use as current money, in resemblance of genuine coins of the USA, or of original design, to wit, the Liberty Dollar coins as identified in the Introduction, all in violation of Title 18, US Code, Section 486.[8]

After a lengthy undercover investigation and prosecution, spanning a number of years, in March 2011, Bernard von NotHaus was convicted in Statesville, North Carolina, of conspiracy and counterfeiting. US prosecutors concluded that "the use of NORFED's 'Liberty Dollar' medallions" was a crime and violated 18 U.S.C. § 486. This Liberty Dollar case was the first time in US history where the federal government had successfully prosecuted a US person for directly competing with the Federal Reserve Bank.

Immediately after that conviction, the district's US Attorney, Anne M. Tompkins, issued a statement that Bernard Von NotHaus had engaged in a "unique form of domestic terrorism."[9] For the entire digital currency industry along with Bernard's friends and associates, this public statement was laughable!

2015 Sentencing

Federal prosecutors had asked for a sentence of up to 17 years in prison for Bernard. However, US District Judge Richard L. Voorhees of the Western District of North Carolina sentenced him to six months of home detention and three years of probation.

Most of Bernard's time during the operation of NORFED and Liberty Dollar Services, Inc. was spent traversing the country speaking at events

and meeting with groups. He focused his attention at the grass roots level encouraging the use of silver-backed ALC. Bernard von NotHaus was the most vocal of all private currency operators during this time.

Unlike other instances of private digital currency, neither the warehouse receipts nor the eLibertyDollars had any issues with fraudulent activity, criminals, or misuse. Bernard knew who his audience was and the groups of people that may become interested at the grass roots level. In 1998, the price of a Troy ounce of silver was around $5.50 most of the year. From 1998 on up until the end of 2003, the price of silver was reasonably stable around $5.00 per ounce. Those users who purchased the precious metal tokens during this time owned a stable investment. During the next six years, from 2003 to 2009, the price of silver rose from $6.00 to around $18.00 an ounce. In 2010, silver's price moved from $18 to $30, and the following year the price peaked above $46. In a perfect world, those following Bernard's encouragement and saving a stack of silver Liberty Dollars captured an investment increase of over 800 percent. The emergence of the Liberty Dollar occurred in the years preceding a slowdown of the American economy to its lowest point since the depression. Silver was the ultimate investment of this time.

Here is the essential difference between Bernard and rest of the country. Over the past 60 years, many intelligent people have written about the problems of inflation, Federal Reserve Banks, and fiat paper currency. However, it was Bernard von NotHaus who decided to take action and educate others by creating his own private value-backed ALC. His intent to educate the public on the government's debt-issued fiat currency eventually reached countless Americans. He did not just talk or write about these monetary problems, he created a silver-backed currency and opened that world up to all people.

It is the belief of many in the legal establishment and others who have followed Bernard's work over the decades that the federal court system should vacate his conviction, or the executive branch should immediately pardon him.

Notes

1. "American Liberty Dollar," Internet Archive: Wayback Machine, accessed March 26, 2016, http://web.archive.org/web/20061004012445/www.libertydollar.org/index.php.
2. Bernard von NotHaus, Private email, September 22, 2015

3. "NORFED—Frequently Asked Questions," Internet Archive: Wayback Machine, accessed March 26, 2016, https://web.archive.org/web/20000818064637/www.norfed.org/norfaq.htm.
4. "7th Amendment U.S. Constitution—Civil Trials," U.S. Government Publishing Office, accessed June 8, 2015, https://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-8.pdf.
5. Royalhawaiianmint.com, "About Royal Hawaiian Mint," Royal Hawaiian Mint, accessed November 15, 2015, www.royalhawaiianmint.com/about-rhm.
6. Elibertydollar.com, "Agreement of Terms of Service," Internet Archive: Wayback Machine, accessed July 24, 2015, https://web.archive.org/web/20030814160356/www.elibertydollar.com/terms_service.html.
7. "CommunityCurrenciesLaw.org | Laws Related to the Issuance and Form of Currencies," CommunityCurrenciesLaw.org, accessed March26,2016,http://www.communitycurrencieslaw.org/currency-laws/.
8. "USA V. Von NotHaus Et Al :: North Carolina Western District Court :: Criminal Case No. 5:09-cr-00027, Judge Richard Voorhees Presiding," PlainSite :: The Law in Plain Sight, accessed June 15, 2015,http://www.plainsite.org/dockets/ml9yompp/north-carolina-western-district-court/usa-v-von-nothaus-et-al/.
9. GATA, "Case 5:09-cr-00027-RLV-DCK Document 270 Filed 11/10/14," Gold Anti-Trust Action Committee, accessed January 13, 2015, http://www.gata.org/files/VonNotHausOrder-Nov-10-2014.pdf.

CHAPTER 4

E-Bullion and Mr. James Fayed

In February 2008, a federal grand jury returned a single-count indictment against James Michael Fayed and Goldfinger Coin and Bullion, Inc. (GCB) the operator of e-bullion. The alleged crime was Operating an Unlicensed Money Transmitting Business (18 U.S.C. § 1960).

1. Mr. Fayed has allegedly been conducting business without an appropriate money transmitting license in a state where committing that crime is punishable as a felony under California State law.
2. GCB had also failed to comply with the federal money transmitting business registration requirements under section 5330 of title 31, US Code, or any of the regulations prescribed under that section.
3. The financial activity of both operations, GCB and e-bullion, had involved the transportation or transmission of funds that were known to the defendant as having been derived from a criminal offense or were intended to be used for the promotion or support of unlawful activity.

In the years before the government unsealed this 2008 e-bullion indictment, numerous digital currency issuers and exchange agents had previously been charged with violating state law for operating a money transmitter business without a state license. However, Mr. Fayed and GCB were charged under the federal statute. Almost two years earlier, July 27, 2006, Arthur Budovsky and Vladimir Kats, the operators of Goldage.

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_4

com, one of the industry's oldest and most well-known digital currency exchange agents, were indicted by the State of New York. The charge was operating an unlicensed money transmission business in violation of New York State's Banking Law §650(2)(b)(1). After pleading guilty, each man received probation and their companies forfeited more than $2 million in seized funds.

In July 2007, the e-gold legal case led to at least half a dozen indictments and seizures of independent digital currency exchange agents for operating without the proper state money transmitter license. In these cases, each exchange business was charged with violating the money transmitter laws in both their home state and the District of Columbia, which was the location of the investigating US Secret Service Agent. Those cases included:

AnyGoldNow and Gold to Card, California
Cal. Fin. Code §1800.3
District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., D.C. Stat. § 26-1002. Violation of the money transmitter statute
The Bullion Exchange, Salt Lake City, Utah
Section 7-1-501 of the Code of Utah, Financial Institutions Act
District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., D.C. Stat. § 26-1002. Violation of the money transmitter statute
Denver Gold Exchange, Colorado
CO ST § 12–52–104, Colorado Transmitters of Money
District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., D.C. Stat. § 26-1002. Violation of the money transmitter statute
GitGold Worldwide Inc.
Florida Money Transmitter's Code, Florida Stat. §§ 560.101-560.408
District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., D.C. Stat. § 26-1002. Violation of the money transmitter statute
Gold Pouch Express
Florida Money Transmitter's Code, Florida Stat. §§ 560.101-560.408
District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., D.C. Stat. § 26-1002. Violation of the money transmitter statute
uBuyWeRush
Cal. Fin. Code §1800.3.
District of Columbia Money Transmitters Act, D.C. Stat. §§ 26-1001 et seq., D.C. Stat. § 26-1002. Violation of the money transmitter statute

Before the September 11, 2001 terrorist attacks on America, US laws governing money transmitters were enforced by state governments. Before the USA PATRIOT Act, violations of operating as an unlicensed money transmitter in California and Florida would have been prosecuted by the state and not the federal government.

However, in late 2001, the USA PATRIOT Act legislation amended existing federal regulations to include new federal penalties for failing to obtain a required state license. The Act included amendments targeting the supervision and licensing requirements of Hawala money transfer operations. These types of exchanges are categorized as IVTS. These new rules also further restricted the working environment for all US digital currency companies.

The US Government viewed Hawalanders as potentially dangerous agents for transferring money that could fund global terrorism. Without open recognition of this fact, a digital currency transaction, which silently moves value over international borders, has the same function of a Hawala money transaction. During a Hawala transfer, cash is deposited with an agent in one country, and the value is quickly "transferred" to an agent located in another country. Hawala payments that permit money to move around the world, unsupervised by conventional banks and financial institutions, are almost identical to digital currency transactions. Without any government record of the money moving in and out of a country, those transactions go unreported. Suspicious activity, which would get flagged by a bank, silently occurs through both Hawalas and digital currency, leaving behind no proper financial records.

Without raising flags or triggering any reporting requirements, a Hawalander in Pakistan could accept $25,000 worth of Pakistani rupee, call a Hawalander in Brooklyn, New York, and moments later direct that agent to pay out $25,000 in cash to a local New York person. While the physical cash in a Hawala transaction never moves from the transactions original country, the value silently travels through countries and over international borders.

This quiet financial activity of a Hawala can be replicated using a digital currency transaction. New Internet digital currency systems introduced in the 1990s offered similar advantages as a Hawala. Neither digital currency nor Hawala required identification of the sender or receiver. Digital currency users were not required to provide a declared source of funds on either end of the transfer, and there were no transaction records of the activity which could link a legal person to the money.

Among the many legal changes that emerged from the USA PATRIOT Act, certain amendments had established better the federal government's authority to prosecute of anyone illegally operating a money transmitter business. The new laws directly affected all digital currency companies domiciled in the USA and also foreign digital currency companies engaged in business with US customers. The USA PATRIOT Act expanded federal anti-money laundering registrations along with other Bank Secrecy Act reporting requirements, such as suspicious activity reports (SAR). Companies including e-gold, IntGold, e-bullion, and Liberty Reserve were all subject to the registration and licensing requirements under section 5330 of title 31, US Code.

The USA PATRIOT Act also amended 18 U.S.C. § 1960 by changing the mens rea term; clarifying the requirements for § 1960 prosecutions. By replacing *intentionally* with the lower *knowingly* element, the failure to register as a money transmitter became a general intent crime punishable as a felony.[1]

After the new USA PATRIOT Act laws had gone into effect, it was disclosed on page 139 of the 9/11 Commission Report that those responsible for the 9/11 terror attacks had not used Hawalas or IVTS. The report stated:

> **No hawalas, self-funding, or state support**
>
> The extensive investigation into the financing of the 9/11 plot has revealed no evidence to suggest that the hijackers used hawala or any other informal value transfer mechanism to send money to the United States. Moreover, KSM and the other surviving plot participants have either not mentioned hawalas or explicitly denied they were used. Wire transfers, physical importation of funds, and access of foreign bank accounts were sufficient to support the hijackers; there seems to be no reason al Qaeda would have used hawalas as well. Although al Qaeda frequently used hawalas to transfer funds from the Gulf area to Pakistan and Afghanistan, we have not seen any evidence that al Qaeda employed them in moving money to or from the United States.[2]

Despite the 9/11 Commission Report findings that no Hawala (IVTS) had been used for the terror attacks, the USA PATRIOT Act's new legislation had moved the money transmitter violation into the federal courts and provided new tools for prosecuting digital currency businesses. It was these new federal regulations, amended through the USA PATRIOT Act legislation, which were used to originally charge and arrest James M. Fayed

in July 2008. This case halted e-bullion's digital currency operation and triggered yet another massive asset seizure. All e-bullion corporate entities, including GCB and Goldfinger Bullion Reserve Corporation, were shut down by agents of the federal government on August 1, 2008.[3]

It is worth noting that the new 2001-amended federal money transmitter regulations have never been used to prosecute a Hawala money transfer. However, the federal government has used the regulations created by the legislation in criminal cases against the following digital currency businesses: e-gold, IntGold, e-bullion, and Liberty Reserve SA.

E-Bullion Advantages

James M. Fayed was the co-founder, president, and CEO of E-Bullion Inc. and GCB. These two companies comprised the popular digital currency system operated through the domain www.e-bullion.com. The online payment system was open to the public from July 2001 to July 2008. E-bullion was very similar to e-gold and all other unregulated digital gold currency operations that existed during the years 1996–2006.

James Michael Fayed

James grew up near Bethesda, Maryland, in the Metro Washington, D.C. area. He served in the US Navy for a few years and is reported to have worked for businesses that had contracted with the US Department of Defense in the 1980s. When he married Pamela Goudie in 1998, she had been working in the gold casting and jewelry business for about four years. The same year, the couple converted her precious metals business into a vast mail-order coin and bullion enterprise. The operation became one of the largest coin and bullion dealers in the State of California.

Development of the e-bullion digital currency concept and system reportedly began in 1998 and lasted for approximately three years. James and Pamela Fayed had no previous employment experience in the banking industry. Neither had ever operated a money transmitter business in California or any other state. GCB had been a sole proprietorship until James was advised by legal counsel to incorporate the business. On November 28, 2000, GCB was incorporated in the State of Delaware (File Number: 3320441). Goldfinger Bullion Reserve Corporation was also incorporated in Delaware about a month later on December 8, 2000 (File Number: 3326734)

The e-bullion.com website and transactions platform was launched on July 4, 2001, alongside the existing Goldfinger precious metals business. The e-bullion corporate entity was a registered Panamanian International Business Company formed in 2000. It was reported to be wholly owned by Goldfinger Bullion Reserve Corp. and controlled by James M. Fayed. Before the formation of these new digital currency companies, the GCB precious metals business had grown into a successful and profitable enterprise. E-bullion digital currency was an additional product for the existing business.

In 2014, James stated that he structured these corporate vehicles for development into an initial public offering of stock. James stated that his legal counsel had advised him this would have been the optimal structure for an Initial Public Offering (IPO). In a 2014 letter, he said:

> E-bullion account funding requests were in the $1-million to $1.5 million (per day) and climbing. That equates into annual sales of $300(+) million-per-year and well in line with my plans to begin to formalize the process to take the company 'public' within one year or so. I had Attorneys start on the process (filings/paperwork/Etc.) to prepare to launch e-bullion on the exchanges with a target of summer-2009, as early as 2007 this was put in place.[4]

Unlike other digital gold companies, which operated during those early years, such as GoldMoney, Mr. Fayed never felt the need to have third-party audits of Goldfinger Bullion Reserve Corporation, e-bullion, or GCB. He stated that until the business had grown substantially larger, he did not see the need for transparent audited financials.[5] Consequently, there are no lasting records available that might have detailed the company's precious metal ownership or the balances and statistics of customer value that had moved through the digital currency system.

E-Bullion History

James stated, at the time of e-bullion's closure in July 2008, the businesses held approximately $60 million in precious metal and bank deposits. He commented in his postal mail:

> There was $20 million alone in physical metal located in California, kept close at hand always to ensure that any possible 'rush' on account liquida-

> tions would be fulfilled promptly) this hypothetic rush never even came close to occurring at any time during our operations, but we felt it our duty to be prepared in case. Long story short, I think that if our customer base did not have full confidence in e-bullion and the Goldfinger entities that we wouldn't have lasted more than a few months.[6]

Goldfinger Bullion Reserve Corp. and the other related companies operated from an administrative office in Camarillo, California. James and other parties managed the digital e-bullion system along with GCB from this California office. An office address in Panama and a legal presence were maintained to satisfy local regulations. In the 2002 PlanetGold interview, James reported that the business was exploring an expansion into Panama, which would have moved the daily administration of the company out of California. However, this transition did not happen.

From the time his digital currency launched, James had stated his well-defined vision for the future of e-bullion. He had forecast that many of his existing GCB precious metal customers would be adopting e-bullion digital gold. In 2014, letters from James restated this original vision for e-bullion and added his thoughts on the use of e-bullion as a superior payment system and alternative to national money. Six years after his arrest, he said:

> I did think that an existing marketplace of clients was available and in fact, I thought that it was a logical step of evolution to have precious-metal 'E-currency' as another product which we could offer our customers. Many of the clients who bought physical bullion should've been clients of e-bullion too. That was our primary motivation behind launching e-bullion – it was simply the Internet (Digital) version of the product we already offered through 'Goldfinger' and even though we never could see it replace physical ownership I certainly believed that it was a very good method to augment physical specie holding and an excellent way to easily and quickly monetize precious metals as well as a superior payment system which offered non-reputable payments (no funny money), much in the same manner that U.S.A. currency had used to function before it was debased & degraded when the dollar was removed from the Gold Standard – and coins were no longer required to be Silver.

Mr. Fayed stated his belief that after being inflated each year over many past decades the US dollar would eventually collapse. Like many others, within the digital currency industry, he believed that digital money backed

by precious metals could then rise to meet the world's financial needs. In his letters, he further detailed the situation.

> This tragic movement away from precious metals as U.S. currency has led to financial chaos, and Inflation/Deflation cycle and ensures that the U.S.D. is well on the way to being completely worthless and will soon be replaced as the "world's reserve currency." I do not doubt and have been saying this for 20 years now. In fact, if people were not compelled by federal law to forced acceptance of the U.S.D. for debt settlement I think many would "opt-out" of the dollar. Basically – I envisioned that e-bullion as (e-currency) could do everything the dollar could do and do it better, that was the 'gist' behind another "trademark" of ours, one that sums it all up in a banner: "Real money in real time™" I think that says it all. Signed, James Fayed

A prediction that fiat currencies, particularly the US dollar, would eventually become worthless is a very common theme among all digital gold currency operators. In 2004, GoldMoney's James Turk and author John Rubino co-wrote a book entitled The Coming Collapse of the Dollar and How to Profit from It (ISBN-10: 0385512236). In 2008, with the economy heading into recession, an updated version of the book was published. However, the word "Coming" had been removed from the title (The Collapse of the Dollar and How to Profit from It [ISBN-10: 0385512244]).

A bold concept that emerged alongside the new commercial Internet, during the 1990s, was the idea to use the decentralized technology and create a private digital currency that could circulate with public users; unaffected by the actions of the governments and central banks. James Turk, Douglas Jackson, and James Fayed, all believed that private digital gold currency systems could survive long after a central bank default or monetary collapse.[7]

James also had stated previously that a majority of former GCB and e-bullion customers were buying and selling precious metals for the following purposes:

1. Trading
2. Long term investment—buying and storing
3. Industry uses such as jewelry
4. Dollar hedge

By understanding this existing GCB customer profile, it is reasonable to conclude that those precious metal clients, who added an e-bullion digital gold account, would be using digital gold for trading, long-term investment, and perhaps even integrating digital gold into the client's jewelry business. James had a clear idea of "who" he believed would be using e-bullion's new digital gold currency and "why." He also considered e-bullion to be unique, as compared with other digital gold currency companies. He explained this benefit in one of his 2015 letters.

> That the 'Goldfinger' Companies were well established already in the Precious Metals Business. "Goldfinger" had an established reputation (stainless) in the industry and worldwide resources available. For example – 'Goldfinger Coin & Bullion' was well into the physical sales and delivery long before we developed e-bullion, and, also, Goldfinger-coin had its list of clients who bought and sold physical metals with us on a daily basis. "Goldfinger Bullion Reserve" was already providing the services needed to manage physical specie (Gold-Silver-Platinum) storage, holding and receipt/shipment at its facilities and leased (Treasury-Grade) facilities before e-bullion was developed. Therefore, it was only a logical extension of our business model to "peg" e-bullion's reserve specie management to G.F.B.R., and for G.F.C.B. (Goldfinger Bullion Reserve Corp. & Goldfinger Coin & Bullion Inc.) to handle all the conversion of fiat to specie orders exclusively. G.F.C.B. processed all requests to convert e-bullion to U.S.D./Swiss Francs/Euro's and vice-versa. On the Goldfinger side of the fence, our experience and channels in the bullion markets allowed Goldfinger to fulfill orders very quickly. If someone wants to bail in/buy 100-kilo bars, for example, we can fill that order on the same day.[8]

James was obviously very focused on the precious metals side of his businesses. Throughout 18 months of recent interviews for the creation of this book, he made few references to any US financial regulations, reporting requirements or government registration. He and his now deceased wife had both been very skilled at buying, selling, and trading precious metals. The couple had built an extraordinary precious metal sales company. At that stage in the company's growth, the idea of adding a digital gold currency to augment the precious metal business was an exciting addition. However, the digital currency began as a secondary inspiration. In a February 2015 letter from Mr. Fayed, he offered his thoughts on possible future e-bullion clientele.

> It's the symbiosis of like-minded individuals. I like to think of the traditional buyers as the "old-school" & the "e-currency" advocates as the "new-wave" (in those days). But in the end, both the traditional buyers (who prefer to take delivery of physical metals) and the "e-currency" advocates shared the same ideology, just different methods of putting it into effect. I think there would have been a huge crossover of both schools of thought (physical & electronic) had the business been allowed to grow roots. The traditional buyers would've slowly embraced "e-currency" and the digital side would've also diversified and embraced physical ownership. It would have evolved into a "sea-change" of thought and exploded in growth, and e-bullion/Goldfinger would've been there- completely ready & able to serve both worlds![9]

Competition

Unlike Douglas Jackson of e-gold, James Fayed harbored no master plan to aid the world by introducing a gold-backed version of electronic money. James did not set out to build a better mousetrap. His concept was to offer a high-quality digital gold service for those existing clients and also further expand his empire capitalizing on the growing precious metals market niche.

WebMoney Transfer is a Russian company that has built a successful global online payment network by creating specific digital currency products that purposely meet the needs of nonbank users. Unlike WebMoney Transfer, e-bullion's digital currency services did not meet an immediate or critical need of nonbank users. E-bullion did not focus new products or marketing efforts on any specific region of the world that was desperate for nonbank payment services. WebMoney Transfer's financial products cater to the needs of distinct customer groups through the features and design of WebMoney digital currency products. As WebMoney products were released, nonbank customers flocked to access the new nonbank financial tools previously unavailable in their region of the world. Similar to e-gold, the e-bullion digital currency system did not focus any marketing efforts on nonbank customers. Both e-gold and e-bullion were in one-size-fits-all digital currency category.

The research undertaken for this book has attempted to determine each company operator's reasons and motivation for creating a new digital currency product. The book makes a comparison between customers an operator had projected would be using the digital currency at the start

of the company and who the majority of actual users were in later years. Here are some of those important questions and the answers received from James in 2015.

(Question) After launching the e-bullion business, what caused the digital payments side of your business to grow?

(Answer)

1. Users switching over from other digital currencies, like dropping e-gold for the cheaper e-bullion
2. Existing gold customers, adding e-bullion digital gold to their portfolio
3. New users looking to engage a nonbank online payment system
4. New users with recent interest in gold as a hedge against the dollar
5. Users that wanted the debit card, because cards were hard or impossible to obtain in their home country
6. PayPal was not available in their country, and they wanted to do business online, they turned to e-bullion because merchants were happy to accept it.

(Question) What were the driving forces that built up the 1.2 million accounts?

(Answer) Exceptional customer service, superior website security, ease of use (Acct. Fund/liquidate), debit card, corporate reputation.[10]

It's well known that HYIP Ponzi schemes contributed greatly to the growth of digital currency companies from 2000 through 2010. From online digital currency directories operating during those early years and direct information provided by popular exchange agents, it also known that e-bullion did not have a large merchant following. Compared to e-gold, which was the industry standard at that time, the e-bullion marketplace of goods and services available to consumer was drastically smaller. E-bullion merchants and the consumer marketplace for products paid for with e-bullion would not have been enough activity to propel the size growth that emerged from e-bullion digital currency.

(Question) Where did the million or more new customers originate? Unbanked? Word-of-mouth? What was driving them to e/b [e-bullion]?

(Answer) Primarily word-of-mouth, repeat users, biz model. Frankly the youth of the Internet and the infancy of the digital currency industry stifled growth. If it [e-bullion] were launched five years later, growth would've been huge. It is the symbiosis of like-minded individuals. I like to think of the traditional buyers as the "old-school" and the "e-currency" advocates as the "new-wave" (in those days). But in the end, both the traditional buyers (whom prefer to take delivery of physical metals) and the "e-currency" advocates shared the same ideology—Just different methods of putting it into effect—I think there would have been a huge crossover of both schools of thought = (physical and electronic) had the business been allowed to grow roots. The traditional buyers would've slowly embraced "e-currency" and the Digital side would've also diversified and embraced physical ownership—It would have evolved into a "sea-change" of thought and exploded in growth and e-bullion/Goldfinger would've been there—completely ready and able to serve both worlds!
Signed, James Fayed[11]

HYIP Ponzi schemes widely used E-bullion digital currency. During the period starting in 2001 and ending in 2008, HYIP scams accounted for massive growth across the entire digital currency industry. Despite these facts, in his letters, Mr. Fayed made no mention of being involved with HYIPs or investment schemes. Although every other online digital currency, except GoldMoney and WebMoney Transfer, had experienced a substantial influx of new customers from the flourishing HYIP industry, Mr. Fayed never once mentioned any investment scheme having an e-bullion account. When asked about the driving forces that contributed to the growth of over a million new e-bullion accounts, Mr. Fayed answered that it was e-bullion's exceptional customer service, superior website security, ease of use, debit card, and corporate reputation that had fueled the company's growth and success.

Innovation

When questioned about the innovative products and features exclusive to e-bullion from 2001 through 2008, Mr. Fayed stated.

> As far as innovations go, I believe we [e-bullion] were first in offering the following:

> A) "No-fee" account funding. It was free to fund your e-bullion account, and the only fee was upon liquidation to a fiat-currency.
>
> B) Removed the monthly "storage-fee" charge, and instead moved to a minuscule monthly service fee (which was the same for all accounts, no matter the size of the balance.)
>
> C) Offering a debit card (which could be used worldwide at A.T.M.s or P.O.S.) that was directly linked to an account, with 'Batch' funding twice a day so you could see the card fund in as little as a few hours and never later than 24hrs.
>
> D) Processing of liquidation orders to three different fiat currencies (U.S. Dollar/Swiss Franc/Euro's) as well as the option for conversion to physical metal.
>
> E) First, to offer "encrypted" (Two-factor) Authentication protection for accounts via the ('crypto-card').
>
> F) 1st in fully encrypting the account database, actually we 'doubled' that protection in that any and all "Administration" user's had to have a crypto-card to access the database.
>
> All those locations also had 24x7 [Recorded] C.C.T.V. Cameras (color/Hi-res) covering them at all times.[12]

James further stated in 2002, "I think being the first to offer CRYPTO Card protection is one of our crowning achievements."[13] Certainly, the CRYPTO Card protection and the ATM debit card linked to e-bullion accounts were two notable factors in the success of e-bullion. No other popular digital gold currency offered these products during the early first decade of the industry. In October 2004, the company even introduced a dollar-backed digital unit of e-currency. The first reserve summary page on the website that featured a balance of e-currency appeared in October showing $625,477.00 in USD funds.

E-Bullion's Competition

In a 2014 letter, Mr. Fayed recalled e-bullion's position in the industry and talked about the digital gold currency competition.

> As far as competition – the usual's; 'E-gold' for certain as they were the 1st to market and 'philosophically' wise probably the closest to (us) regarding the idea of using precious metals as money (again), and realizing the impact the Internet could have to facilitate this. Of course 'James Turk' had (his) patents, (and as far as we understood from a copious review of his claims by our attorney's) they didn't apply to the system we built and

> offered (e-bullion). We didn't "infringe" on Mr. Turk's work, but I think he felt that all of the issuers (at that time) were somewhat cheating him as he felt he thought of the idea 1st, and he felt we all owned him "Royalties." However, we agreed to disagree and our legal counsel's opinions was our basis for what we felt was a valid and strong position and as far as I know we were never legally-challenged or publically accused of violating "anyone's" Intellectual property rights (or) patents (or) any other protected property, including Mr. Turk or "GoldMoney."[14]

As of July 2002, around one year of commercial operation, e-bullion held 15,599 oz. of gold in the company vaults. In an online interview, James stated, "Presently we have over 19,500 accounts, and more than half of the accounts are funded and actively used."[15]

The information below includes a quick asset comparison between the one-year-old e-bullion company and the six-year-old e-gold operation.

Computer Operation, Servers, and Security

Regarding the protection of client funds, account security, and network resilience, in 2015, Mr. Fayed conveyed that it was always paramount that his data and his client's information be secure. Here are his statements.

> We had no servers or networks in the U.S.A. other than the corporate network at the California offices (which were firewall and I.D.S. protected as well). All the "Business"-end Goldfinger/e-bullion servers were overseas/offshore on wholly-owned equipment (not leased or rented gear) and plugged directly into the "Internet" Pipe for the corresponding geographic area.
>
> We had banks of servers located in Switzerland (Geneva & Zurich), back-up's and redundant servers in Canada and Asia, and plans to even – further expand the "footprint" of our Network in the future.
>
> The Network design was superb indeed, and for the 7(+) year we were (live) online we never suffered a single outage (other than planned routine maintenance and software upgrades) – No downtime from either a hacking attempt or attack, nor from a D.D.O.S., or downed I.S.P., Etc… Redundancy was "live" and should (one) server-pod go dark; the others would instantly & automatically pick up the demand and load with zero disruption to the Network, or the client. In fact, an account holder wouldn't ever notice the (switch-over) should it occur. Also, for the corporate to connect to the server's access was restricted by use of "Static-IPs" via the

Chart 4.1 2002 Asset comparison of E-gold.com and E-bullion.com

Quick asset comparison mid-2002 between e-gold.com and e-bullion.com

August 4, 2002—e-gold.com

e-metal balance sheet for e-gold.com in Troy oz.

Gold	57,975	×	$308per/oz.	$17,856,300
Silver	143,796	×	$4.63	$665,775
Platinum	600.00	×	$525	$315,000
Palladium	499.22	×	$320	$159,680
August 4, 2002	**Total e-metal assets in USD**			**$18,996,755**[a]

June 3, 2002—e-gold.com

Currently, there are 460,192 e-gold accounts

Bal. Summary Gold (only)

# of Funded Accounts	Average Funded Acct Bal. in grams
150,322	12.86 g = *$127 ($9.90 per gm)*

June 3, 2002[d]

By August 2002, e-gold.com had been in operation for approximately five years and eight months.

June/July 2002—e-bullion.com

(Approximate balance in Troy oz.)

Gold	15,599	×	$320per/oz.	$4,991,680
Silver	21,800	×	$4.85per/oz.	$105,730
June/July 2002	**Total e-metal assets in**			**$5,097,410**

The information for these numbers came from a 2002 interview of James Fayed. The approximate balances he stated were backed up by the public balances shown on the E-bullion Reserve Summary on dates during the months of June and August 2002.[b] Planetgold.com online interview with James M. Fayed, published Monday, July 29, 2002[c]

June/July 2002—e-bullion.com

There were approximately 19,500 e-bullion accounts

Bal. Summary Gold (only)

# of Funded Accounts	Average Funded Acct Bal. in USD
Approx. 8,250+	Approx. $600

June/July 2002

The information for these numbers came from a 2002 interview of James Fayed. The approximate balances he stated were backed up by the public balances shown on the E-bullion Reserve Summary on dates during the months of June and August 2002[e]

By July 2002, e-bullion.com had only been in business for one year.

[a]"E-gold Examiner," Internet Archive: Wayback Machine, accessed February 26, 2015, https://web.archive.org/web/20020810223425/www.e-gold.com/examiner.html.

[b][e]"E-Bullion," Internet Archive: Wayback Machine, accessed September 12, 2015, https://web.archive.org/web/20020604190154/www.e-bullion.com/reserve.php.

[c]"Planetgold," Internet Archive: Wayback Machine, accessed February 11, 2015, https://web.archive.org/web/20030216110351/planetgold.com/interview.asp?SPID=71133546.

[d]"E-gold Statistics," Internet Archive: Wayback Machine, accessed April 2, 2016, https://web.archive.org/web/20020611044932/www.e-gold.com/stats.html.

> corporate V.P.N. (encrypted) and log-in to the overseas networks was by (two-factor) "Crypto-card" authentication only.[16]

The federal charge related to money transmitting against James Fayed and his company was eventually dropped and never pursued by the State of California. The money transmitting case disappeared; however, the assets were still in possession of the government. Unfortunately, for Mr. Fayed, as the smaller charges were dropped, a more severe case was filed that kept him continuously incarcerated.

> As for seizures – the Goldfinger/e-bullion network was never seized by federal authorities. However, the government did (Illegally) seize the corporate offices and all assets by an (Invalid, overbroad & faulty) warrant issued by a federal magistrate. The U.S. Attorney office (U.S.A.O.) colluded with L.A.P.D. (Los Angeles) to illegally arrest me and wrongfully detain me (Violating the Bail Reform act-denying me Bail on a simple "Statute" charge of running a business without a license) for months in federal custody, preventing my access to property & assets as well as preventing my participation in mounting a proper defense as well. In mid-2011 upon advice from legal counsel, we did release the servers to the U.S.A.O., roughly 3 1/2 years after my illegal arrest and illegal detention by the U.S.A.O. & the L.A.P.D. As I mentioned, this release was upon the recommendation of legal counsel (and we protested by pre-trial motion – "denied") almost four years after my incarceration in 2008.[17] Actually – I didn't find this piece of info (out) until years later but, while we were pursuing our cases in federal court there came a point approximately in 2011 (Three years after my arrest) where we were ordered by a federal judge to ("turn over the servers or suffer a default judgement against you") – I had been refusing to turn the servers over to the prosecutors until that point (where it was in our best interest) and upon legal advice we released the servers in Switzerland to the federal prosecutors (who gave them to the F.B.I. for investigation). Anyway – I understand that our system was well enough secured that it took the best the fed's had, roughly 14-mos (one year and two months of 24 hours a day attacking) before they broke the encryption and accessed the servers. That is an incredible amount of 'Brute-force' (entire F.B.I. tech resources) on our "little-old-e-bullion" network before it finally gave-up-Tough.[18]

It is worth noting that in the e-gold case, the business' servers were operated by AT&T from Orlando, Florida. A court order early in the e-gold investigation had allowed US agents to access the server easily and create a mirror image of all data, including all customer account records of those

persons not accused of a crime. The encrypted privacy and foreign jurisdiction of the e-bullion servers appeared to create serious challenges for US investigators. Mr. Fayed detailed this situation in his letters.

> Now, Switzerland flatly refused requests by the U.S.A.O. for the servers without proof of illegal activity on my part or my company's part. Which of course did not exist since we were not engaged in illegal activity. Thus, the U.S.A.O. was stymied in their requests since Switzerland would not be "Bullied" into their pressure tactics and the Swiss required (proof) of criminal activity (By trial verdict or plea) before release. As far as I know the fed's had no knowledge of any other of servers (Backups & Redundant overseas) therefore, their pursuit was of Switzerland exclusively. Upon the release waiver of (2011), I understand that U.S.A.O. had to pay the Swiss firm's several hundred thousand dollars for all the fees in maintaining the equipment after my arrest, and also, it is my understanding as well that the F.B.I. Computer Science Division took roughly 14 months (one year and two months) to crack the protection we had on the servers and access the encrypted data.

Finally, Mr. Fayed concluded this discussion reiterating that no criminal charges were ever pursued relating to e-bullion's activity.

> All in all, to date no charge against me or my companies regarding illegal or criminal conduct, has been proven or survived legal challenges, and this is simply because no criminal activity existed, period.[19]

While Mr. Fayed presents fascinating information, the details may not paint a clear picture of e-bullion's actual day-to-day operation. Like other digital currency owners, when the platform opened to the public, Mr. Fayed made an informed prediction about the uses that future clients might have for the innovative and unregulated digital gold payment system. However, both he and his co-partner wife lacked any experience working in regulated financial services. Neither James nor his wife Pamela had any previous experience running a money transmitter business nor had either person administered a financial company that required knowledge of anti-money laundering regulations. However, Mr. Fayed had engaged well-suited full-time legal representation that had advised his business.

As with other digital currency during that early decade, James Fayed's innovative digital gold technology allowed the e-bullion business to circumvent existing Bank Secrecy Act (BSA) regulations on KYC and

AML. This advanced and unregulated technology gave the e-bullion operation a large advantage over licensed regulated banks and other conventional financial products. An e-bullion account offered extraordinary opportunity and benefits beyond conventional bank services.

Just as e-gold had been doing since 1996, e-bullion operated beyond the reach of old state and federal regulations. From 2001 through 2006, almost the entire life of e-bullion, there were no federal or state regulations that identified a digital gold currency issuer as a money service business or money transmitter.

In his 2015 letters, Mr. Fayed clearly states his position regarding e-bullion and regulations governing money transmitter businesses in California. "…at the time of our 'Shutdown'/Seizure we were in no violation of federal or state law as it was written at that time."[20]

As observed in the GoldMoney operation, if the e-bullion business had followed some common sense regulations such as those of a conventional bank or regulated money service business, perhaps e-bullion would have survived the changing regulatory environment. During the early years of digital currency, company operators were not compelled to adopt existing bank reporting or financial regulations. It is evident that the digital currency companies which voluntarily and wisely implemented existing regulations for financial institutions not only survived the changing US laws but also continued to thrive in 2015. Those digital currency companies operated by persons who believed their financial business was exempt from government regulations were prosecuted and closed.

An e-bullion employee reported that in 2002, both e-bullion and GCB had applied to the State of California for a money transmitter license. The unconfirmed response from the state office was that the company did not fall under the definition of a "money transmitter" and did not require a license.[21] No further evidence is available to confirm this event.

Exchange Agents

A critical moment in all digital currency transactions is the point of exchange with national currency. This swap usually occurs through a third-party independent exchange agent. This third-party exchange point does not exist for online payment processors such as PayPal; the exchange of digital units through a third-party agent is against PayPal's terms. According to PayPal's terms, all national currency exchanges (withdrawals) take place through PayPal, not outside agents.

A digital currency exchange, either into national currency or another electronic currency product is not required to move through the original issuer. This mutual exclusive activity is one of the revolutionary features presented by new digital currency systems. In this instance, digital currency acts more like cash than an online payment processor.

Digital units moving through an online payment processor are more like chips circulating through a Vegas casino. By comparison, Internet digital currency is more like cash and can be exchanged or traded anywhere.

Players in the casino, exchange national currency for house chips which represent value. Visitors then use the chips for gambling. At any time in a casino's operation, the number of circulating chips can easily be determined because users must always redeem the chips through the casino; that was the original issuer. This kind of system is essentially a closed ledger. When one person loses $1000, the house gains $1000. If a player wins $10,000, they redeem that value or "cash out" through the house bank inside the casino. Players exchange the casino chips for national currency (cash). The casino keeps a very careful record of who wins and who loses. The house can always easily identify the day's winners and losers along with how much money is in play at just about any time. When the token issuer is the only point in the circulation for the redemption of tokens back into national currency, this situation allows for an extraordinary amount of control over casino players and their activity.

PayPal operates in a similar fashion, when a PayPal account holder spends $1000, another account holder receives that $1000. This system is also a closed ledger. Just like the casino operation, the issuer, in this case PayPal, redeems the outstanding tokens for national currency. In fact, similar to using casino chips, the only way to exchange digital PayPal tokens is to return the units to the original issuer. Exchanging one casino's chips outside the casino is forbidden. Likewise, the exchange of PayPal digital units through a third-party financial agent is also not permitted.

In both of these cases, the issuer maintains exceptional knowledge of who is using their tokens and for what purpose. Proper KYC and (AML programs require this kind of single issuer financial structure. For payment processors, like PayPal, offering one path for the redemption of digital units into national currency is the preferred method and the required method of doing business in the USA. Financial regulations in the USA function well for money service businesses and payment processors that utilize this structure.

However, from 1996 through 2006, new digital currency operations, such as e-bullion, offered the exchange of digital units for national currency without requiring the account holder to interact directly with the original issuer. Just as with e-gold, many third-party e-bullion exchange agents became independent buyers of e-bullion digital currency. This situation created a liquid marketplace for e-bullion transactions. Anyone with digital e-bullion could exchange those units through an independent third-party agent and receive national currency or another digital currency product. Contact with the original issuer was not required for account holders to "cash out." While the e-bullion operation always knew how much digital gold the business had issued and circulating, there was no method to identify who was accumulating digital currency and who was selling it. Given that no ID was required to open or use an account, there was no certain method of identifying which users had received funds or where the funds originated.

Third-party transactions were a day-to-day activity of e-bullion for the life of the company. However, these facts are in contention with the details provided by Mr. Fayed in his 2015 letters.

Background

The Bullion Exchange (TBE), Salt Lake City, Utah, was operated from 2001 to 2007 by Carole and Don Neve using a local Wells Fargo Bank account. The business only handled e-gold and e-bullion digital gold products. One primary service of TBE was the exchange of e-gold for e-bullion. This exchange service offered fast manual transactions between the digital currencies; it was not an automated process. The frequently asked questions (FAQ) section found on the TBE website, in 2005, explained the transactions as "simple, easy and fast…all you need to know is your E-Bullion and E-gold account numbers, and we do the rest for you!" When asked if TBE was affiliated with e-gold, E-bullion, or GoldMoney, the company's answer found in that same FAQ section was an emphatic, "No."[22]

Unrelated to e-bullion, in July 2007, TBE's bank accounts and e-gold accounts were seized by the government during the e-gold prosecution.

While there are no records available that can show how much value moved through the TBE e-bullion accounts, the e-gold legal documents showed that Don and Carole moved, at least, $227,000,000.00 through TBE's e-gold accounts during an approximately five-year period.

This quarter of a billion dollars' worth of e-gold proved that the company had a large, visible, well-known digital currency exchange operation. Much of the TBE business was the conversion of e-gold into e-bullion. Consequently, it is conceivable that while executing this large amount of business in e-bullion digital currency, that TBE had openly and directly engaged GCB in a five-year-long multimillion-dollar e-bullion relationship. It is also believable that the operators of e-bullion would have been well aware of the five-year-long relationship and the frequent multimillion-dollar transactions taking place between e-bullion and TBE.

Based on the structure of e-gold's independent exchange agent network that operated through e-gold's primary agent, OmniPay, it is easy to assume that companies such as TBE might be considered to be third-party exchange agents. The fact that for years, many of these companies openly advertised and operated, buying and selling e-bullion, through GCB might lead a person to believe that the company's activity was well known, accepted, and permitted.

However, in his 2015 letters, Mr. Fayed explains a different situation regarding all third-party independent companies. This text is Mr. Fayed's detailed explanation of the e-bullion exchange process. Additionally, this information from Mr. Fayed's point of view seems to advance further the justification that e-bullion's business was not a money service business nor a money transmitter and did not require registration or licensing.

> Mr. Mullan – I think you may have forgotten much as to "How" e-bullion functioned versus other DGC's, yes? I am perplexed that you think the 'Neves' and "TBE" were e-bullion exchange agents. Again – official (or sanctioned) agents for e-bullion did not exist except for Goldfinger Coin. GFCB was the only Exchange-Agent for e-bullion (making it free to fund your account and a modest fee to liquidate your account to fiat). The only way to officially fund or liquidate your account was through GFCB. The entire system was programmed as such (one-way 'in' & one-way 'out') this maximizes fraud protection and account security – now, what some private party chooses to do is not our business but they are subject to the same exit as all others, so if they run afoul of the T.O.S./U.A. [terms of service/user agreements for e-bullion] or law-enforcement that's at their risk or peril (Just like fiat currency) Note: free account funding pretty much negates any need for Private Exchange Agents, yes?
>
> As I mentioned previously, Goldfinger/E-bullion were not "e-gold" in any shape, way or form. Our business model was significantly different from other 'DGCs', on the surface a casual observer could conclude some simi-

> larities, but that casual surface look was all. Our system did not promote or sanction "Exchange-Agents," or a "free-for-all" come as you are attitude (like e-gold & others). In fact, it was my contention and belief that this 'Wild-West' attitude toward allowing anyone to act as exchange agents was dangerous, encouraged fraud and would likely be the downfall of the fledgling industry.
>
> Also, by stopping this "free-for-all" policy toward AEP's [exchange agents] and restricting exchange-services to Goldfinger only we closed the thousand(s) of exits available to criminal at other (DGC's) and forced all e-bullion "exits" through one door. Which, of course, is more easily watched and policed for illicit activity than having to monitor hundreds/thousands of exits. I believe this made us more successful at our business than others![23]

Mr. Fayed presented that the company had no "approved or sanctioned" third-party exchange agents other than GCB. It was his belief that this structure was one of the primary reasons why GCB was not required to operate as a licensed money transmitter in the State of California or any other state that held e-bullion clients. Mr. Fayed addressed similar questions his response from a 2015 letter.

> Long before the M/T rules and regs were being "skewed" & slowly applied toward "e-currency™," I had teams of legal counsel(s) plowing through the books (Goldfinger/e-bullion retained top-notch legal counsel and spent hundreds of thousands of dollars on corporate legal counsel annually) and the legal "loophole" found in the regulations was – a money transmitter was defined as; an "Entity transferring money for a fee" (the laws have likely been updated and changed since my arrest, I am not sure?). So-thus long before (years) the M/T laws were applied to our business model, we changed the structure of our business model to allow for (free) account funding & (free) transfers between account holders, therefore, neither company was in violation of federal law as we were not transferring money for a fee. As far as liquidations to fiat that wasn't a violation either as it was digital-metal fully backed by physical specie being sold back to Goldfinger Coin (no fee in the transfer to Goldfinger by the account holder (no violation by the account holder) and a simple flat fee to convert their holdings to U.S.D./Swiss franc/Euros. No different from when a client would bring in Quantity-100 Gold coins to sell and convert to fiat currency at a small premium. As far as I know, no one else had this business model. It was a trade secret that we employed to ensure we were in compliance with federal laws and regulations.[24]

Why Accept E-Bullion?

Why was anyone willing to accept privately issued e-bullion digital gold currency in exchange for dollars? The answer is very simple; e-bullion digital units were reported to be 100 percent backed by gold bullion. The value of one digital ounce of e-bullion was the same as 1 ounce of physical gold bullion. Gold is a liquid asset, and anyone can exchange gold, for cash in any country around the world.

This version of a freely circulating digital currency exchange opportunity moves to an even higher level with bitcoin. Cryptocurrency has no original issuer. Various third-party individuals and organizations mine all the units. No unit can be redeemed through an issuer because there is no issuer and users must sell the units to a third-party exchange agent. Consequently, bitcoin units do not receive value from a redemption price, as with PayPal, or the price of an underlying commodity as e-bullion. Third-party buyers and sellers always determine the price of bitcoin. Additionally, no identification or verification is needed to set up and operate a bitcoin wallet. All exchange transactions around the world are taking place through tens of thousands of unregulated and unsupervised independent third-party agents. When compared to PayPal, it is easy to understand how cryptocurrency is shaking up the financial world and also how the existing regulatory model does not work for bitcoin.

E-bullion and e-gold were very similar to GoldMoney. However, GoldMoney was a system created by a former banker and operated by executives with decades of banking experience. GoldMoney was not required to follow existing US financial regulations until late 2011 when the company changed its structure. During a decade of GoldMoney operation from 2001 through 2011, the business was not required to operate as a licensed US financial institution. However, the former bankers in charge of the business voluntarily instituted a strict customer acceptance program (KYC) and also followed an appropriate AML program. Other digital currency companies, such as e-bullion, appeared to be working hard at developing reasons why the bank regulations did not apply to the company's digital currency business. Both e-gold and e-bullion were prosecuted and these business ended. The GoldMoney business has never had any US legal issues. In 2016, the company is still in operation.

Fraud Prevention

The E-Bullion CRYPTO Card made it virtually impossible for a hacker to gain access to an online account. In his letters, he stated:

> No matter how secure we make the E-Bullion network – The weakest link in the E-Bullion system is the account holder being sloppy or careless with a password for an account. The Crypto Card removes that weakest link in the chain and we encourage all users to upgrade today. After one year of operation, we do not know of any cases of fraud or password theft against E-Bullion account holders. There were a couple of cases of things like auction fraud that spilled over into E-Bullion via E-Gold and Evocash and others, but we were able to negate this issue very quickly. As long as some customers use passwords to access their accounts, it is statistically bound to happen that someone will give away their password or have it stolen by a Trojan, but at least with E-Bullion, the customer has the OPTION of CRYPTO Card protection. If they choose not to use it and someone steals their password, it is a risk they choose to take.[25]

The statements about Crypto Card access were very true. E-bullion was ahead of its time for implementing the two-party identification in 2001. In 2016, this type of security is widely used.

HYIP Ponzi Scams and E-Bullion

On July 15, 2010, the US Financial Industry Regulatory Authority (FINRA) issued a news release entitled, "FINRA Warns Investors of Social Media-Linked Ponzi Schemes, High-Yield Investment Programs." It stated:

> The Financial Industry Regulatory Authority (FINRA) warned investors today about Internet-based Ponzi schemes called high-yield investment programs (HYIPs), which purport to offer returns of 20, 30, 100 percent or more per day. HYIPs are unregistered investments sold by unlicensed individuals using sophisticated-looking websites.[26]

Associated with the FINRA news release of the same date was an investor alert entitled, "HYIPs—High Yield Investment Programs Are Hazardous to Your Investment Portfolio." Even in 2010, this message further highlighted the global unregulated nature of digital currency systems.

> Offer e-gold and other online payment systems that provide the means by which participants fund their accounts, get "return" on their "investment" and, presumably, enrich the scammer. Investors should be aware that not all digital currency sites are subject to federal regulation. And some have been tied in recent years to criminal activity, including money laundering, identity theft and other scams.[27]

Regarding HYIP Ponzi activity using e-bullion, Mr. Fayed stated in a 2015 letter, "We neither condoned nor endorsed nor engaged in 'HYIP' activity, but we were not law-enforcement either."[28] This statement is identical to comments made by every other digital currency operator and exchange agent across the industry. Despite the fact that tiny micro payments made through multiple HYIP accounts were technically very easy to identify, track, and prevent, digital currency operators refused to prevent these very profitable, industry building, scams. The exception was GoldMoney and WebMoney Transfer; neither company permitted such activity. Another popular statement heard across the digital currency industry was, "We can't tell account holders what to do with their money, if someone wants to invest, it's not up to us to try and prevent them." If Satoshi Nakamoto had an actual voice in the cryptocurrency industry of 2016, it would likely be repeating a similar statement.

> FBI and IRS investigators determined that about $35 million per month funneled through Goldfinger and e-Bullion at the company's height, and very little of it came from trading precious metals.[29]

Criminal activity plagued every unregulated digital currency company, such as e-bullion that operated without common sense customer verification. About the asset size of e-bullion's digital currency operation, the amount of money generated by Ponzi scams that flowed through e-bullion and GCB was substantial.

During the company's seven-year existence, thousands of HYIP Ponzi schemes used e-bullion accounts as conduits for the illegal proceeds derived from criminal activity. Hundreds more schemes used the bank accounts of GCB to send and receive third-party "investor" funds which were quickly converted into e-bullion digital currency and siphoned back out of the platform by HYIP Ponzi scam operators. Court documents and statements from law enforcement clearly show that victims of HYIP Ponzi scams were sending funds directly to GCB, purchasing e-bullion for the

single reason of funding a Ponzi investment scheme. The customers were not interested in investing in gold, owning precious metal or the advantages of new digital currency technology. This type of customer usage of a digital currency business is the same situation that occurred with Crowne Gold, IntGold, and others. The company bank accounts acted as third-party deposit and withdrawal operations on behalf of these massive illegal Ponzi scams. This illegal activity only occurred through digital currency companies that did not follow established KYC and AML procedures. The exploitation of digital currency systems from 1996 through 2006 was a direct result of the unregulated environment.

Just as had been used with e-gold, IntGold, and many others, "Batch Payment" automated software had been at e-bullion to pay multiple accounts a micro amount of "interest" for those participating in these HYIP schemes.

HYIP forums such as ASA Monitor, MoneyMakerGroup, Talk Gold, and MyCashForums promoted these Ponzi schemes. Referral links paid a commission to the operator of the forum each time a victim following the forum's link funded a Ponzi account. Investigators have linked E-bullion to thousands of HYIP Ponzi schemes. Here is a short list showing a few of the more notable scams that used e-bullion to accept funds from victims and later helped move the illegal proceeds around the world.

AdSurfDaily ($110 Million)

CR-10-320 filed Nov. 23, 2010, case related to 08-CV-2205, 08-CV-1345
A Ponzi scheme disguised as an online advertising company, from around September 2006 to August 2008; this scam collected about $110 million from investors. Much of the funding moved through e-bullion. In September 2011, the US Department of Justice and US Secret Service returned $55 million to around 8400 people by swindled AdSurfDaily.

Legisi ($72 Million)

Case 4:08-cv-11887-PVG-VMM Filed 05/05/2008
Gregory N. McKnight and Legisi Holdings, LLC.

Operators targeted the Legisi scheme at Christians. From December 2005 through November 2007, the scam raised approximately $72.6 million from between 3000 and 4000 members of the public residing in all 50 states and several foreign countries. According to the court-appointed receiver Robert

D. Gordon, more than 85 percent of the $72.6 million directed at the Legisi HYIP Ponzi flowed through the e-Bullion payment processor.

FEDI HYIP Ponzi Scheme (2003) Multimillion

Flat Electronic Data Interchange (aka FEDI)
FEDI was pitched as a "scriptural-based public trust" funded by wealthy Arab families located in the Middle East. Funds moved through e-bullion and GCB bank accounts. Prosecutors linked the FEDI scheme with Abdul Tawala Ibn Ali Alishtari, also known as Michael Mixon. Ali Alishtari pleaded guilty in 2009 to financing terrorism and fleecing investors in the FEDI scheme. From June 2006 to December 2006, Alishtari was involved transferring $152,000 on behalf of an individual claiming to be a wealthy Pakistani, seeking to support terrorist training camps. Alishtari moved these funds with the understanding that the money was intended to be used to purchase such items as night vision goggles, medical supplies, and other equipment for use at terrorist training camps. (The $152,000 in terror funding did not move through e-bullion or GCB.)

Gold Quest International ($28 Million)

Case 2:08-cv-00566-LDG-LRL Filed 05/06/2008
From May 2006 through July 2008, Gold-Quest, a Panamanian Corporation and its owners, David Green aka "Lord David Greene," John Jenkins, and Michael McGee raised more than $27.9 million from over 2100 investors in the USA and Canada through direct solicitations and an Internet website. Gold-Quest maintained a single e-bullion account through which the operators received and pooled investor funds. Victims were instructed to transfer funds to Gold-Quest's e-bullion account. Victims had previously been able to send fund to a domestic bank account; however, after the Securities and Exchange Commission subpoenaed the bank account records, Gold-Quest eliminated that option for e-bullion digital currency.

Pathway to Prosperity ($70 Million)

Profitable Sunrise (Estimated in the Tens of Millions of Dollars)
Hundreds of millions of dollars moved through e-bullion received from victims of these scams and others. In later pretrial court documents dated August 5, 2008, government prosecutors provided critical details on the size and type alleged illegal activity. The documents showed that during a short period beginning in 2005, tens of millions of dollars received by GCB and had been transacted through the e-bullion platform for the funding and support of fraudulent HYIP Ponzi schemes. The following text is from the Government's Memorandum of Points and Authorities in Support of Application to Criminal Duty Judge for Review of Magistrate Judge's Bail Order, dated August 5.

> The Pretrial Services report and additional evidence to be introduced at this hearing shows that during a roughly eight-month period in 2005 and 2006, bank accounts in the name of GCB, over which defendant was a signatory (along with his deceased, estranged wife), received and transferred out over $20,000,000 in proceeds from Ponzi scheme victims. The victims did not intend to use defendant's business to purchase gold or precious metals, as defendant's website represents as the service offered by defendant's company. Neither defendant nor the entities he admittedly controls were licensed to transfer such funds. Accordingly, defendant was charged with operating an unlicensed money transmitting business.[30]

Liquidity in the E-Bullion Marketplace

Another not-so-obvious issue for e-bullion grew from the liquidity provided by the e-bullion debit card. By quickly and safely redeeming customer funds, a digital currency issuer, acting as the responsible financial party, creates market liquidity for its financial products and builds user confidence.

PayPal is a good case in point. In 2016, with more than 179 million account holders, there is little doubt that customers will continue to exchange PayPal digital units to national currency. If a user's online PayPal account shows a balance of $100.00, there is no doubt in that user's mind that he or she can easily convert the digital balance into national currency.

Customers add and remove funds from the PayPal system each day. The money leaves a PayPal account through bank transfer, check, or credit to a PayPal prepaid MasterCard. Unlike PayPal, the job of building consumer

confidence in a privately issued digital currency is a difficult task. Active participation by the digital currency issuer or an exchange agent business directly linked to that operator can provide helpful assurances for new users. Both e-gold and e-bullion offered this type of liquidity confidence.

The active participation of third-party exchange agents OmniPay and GCB vastly contributed the financial health both commercial platforms along with a wider global acceptance of the digital units. As illustrated by the PayPal system, when an account holder recognizes that they can quickly liquidate digital units into national money through the original issuer or by a corporate entity operated by the parent company, those users are likely to have a much higher level of confidence when using that digital currency.

E-bullion was very similar to e-gold and most other digital currency products circulating in those early years. Shared traits between e-gold and e-bullion included:

1. All transactions were final
2. Backed by gold bullion
3. Small fees
4. Instant cleared funds
5. No ID or verification required to open and operate an account
6. Multiple accounts for one person
7. Instant set up and operation (no cost)
8. Third-party exchange of the digital units

As the first mover, e-gold had critical advantages and an established global base of customers which allowed the digital currency to dominate the marketplace for almost a decade. E-gold had quickly developed into the de facto method of payment across the entire digital currency industry. Partially because of OmniPay's involvement, consumers trusted e-gold and were comfortable that they could complete an exchange from digital to national currency without any issues. Even after federal agents raided the company offices in 2005, dozens of exchange agents still accepted e-gold and millions of customers were still using the platform. E-gold and OmniPay had created the liquidity and confidence needed to retained existing customers and also attract new ones.

All digital currencies which emerged between 1996 and 2006 were exchangeable into e-gold. Merchants that required a nonbank method of payment adopted e-gold, WebMoney, or both. Just as bitcoin is in 2015

considered the center of a cryptocurrency universe, e-gold had held the same title for almost a decade. This open market digital currency exchange that occurred between e-gold and many other digital currencies was a vital component of growth for the entire digital currency industry.

Around 2005, during the peak years of e-gold's popularity, there were approximately 120–150 very active third-party independent exchange agents around the world. Along with OmniPay's deep pockets and a large inventory of cash and digital metal, the trading activity of these 120–150 e-gold agents supported a genuine liquid marketplace for e-gold's digital currency.

Any new online merchant that wanted to attract new customers through the addition of new payment methods could open a business to many other forms of payment simply by adding e-gold.

With a broad market of third-party exchange agents converting other digital currency products back and forth into e-gold, online merchants did not have to bother with adding new shopping cart tools for each brand of digital currency. By accepting e-gold, the merchant could receive sales from across the digital currency industry. Instead of opening a WebMoney account, an online merchant could direct WebMoney clients to swap funds into e-gold for use in their online store.

Around-the-clock liquidity is perhaps the most important requirement for the successful operation of a retail consumer digital currency product. All digital gold currency, in those unregulated early years, was easily exchanged into e-gold and shared the benefits of e-gold's successful liquid exchange market.

This e-gold to e-bullion relationship greatly benefited e-bullion and helped to build the e-bullion customer base. Eventually, most popular e-gold exchange agents also began accepting e-bullion. Many online exchange agents had automated website software which offered customers an instant exchange between various digital currencies. The automated exchange allowed e-gold users to spend $500 in e-gold and moments later receive $500 in e-bullion, minus a small fee. Both e-gold and E-bullion measured units in gold grams that same type of automatic exchange might have been measured by spending 9.5 grams of e-gold and instantly receive 9.45 grams of e-bullion (.05gr fee). This automated exchange also helped to advance commerce within the industry and is still popular in 2016. New instant exchange websites such as ShapeShift (https://shapeshift.io/) will instantly and automatically exchange between cryptocurrency digital units just as dozens of exchange agents did with e-gold more than a

decade ago. In 2016, examples of centralized platforms that automatically exchange digital currency are found on BestChange (http://www.best-change.com). BestChange is a specialized online e-currency exchange service that monitors the exchange rates of popular agents in near real time. If a user wants to exchange one currency for another, visiting BestChange will provide the current agents accepting those transactions and the fees of each agent. APIs from each website provide almost real-time accurate information. This Web business provides dozens of exchange options for digital currency including bitcoin, debit cards, and national currency. Similar exchange rates comparisons, without the APIs, were developed on the original Gold Pages Digital Currency Directory in 2004.

Hundreds of independent exchange agents around the world facilitated the instant exchange for dozens of digital currency products during that first decade. E-gold had grown into a highly accepted nonbank method of online payment; it was not necessary for new digital currency companies to recreate that success through another brand. As long as exchange agents would swap between e-gold and any new currency, the newer brand could achieve popularity much faster. Because third-party agents easily exchanged e-gold and e-bullion through, the growth and success of e-bullion did not depend on acquiring new retail, commercial customers, or merchants. Additionally, through the e-bullion debit card, those accounts were directly linked to ATM cash withdrawals. Anyone desiring instant cash liquidity simply converted whatever brand digital currency they owned into e-bullion. Users could then quickly access that value through just about any ATM in the world. Money quickly flowed from across the digital currency industry into e-bullion and out of ATMs.

James Fayed had created the only digital gold currency, which offered users an in-house ATM debit card linked to a digital currency account. The card dispensed cash withdrawals from a digital currency account through millions of ATMs around the world. For customers wishing to avoid the hassles and fees of third-party exchange agents, these ATM cards offered a liquid advantage. As an example, users no longer had to sell e-bullion to a third-party agent in another country and wait to receive an expensive Western Union cash transfer. E-bullion card holders could instantly withdraw large amounts of cash from ATMs.

The e-bullion operators manually executed bulk loading of funds onto debit cards at least once a day. For e-bullion users, cards were easily obtained, inexpensive, and had few limits. The text on the e-bullion

website described the cards as "anonymous & numbered" with "no preset spending limits."[31]

E-bullion ATM debit cards had forged a lucrative channel of cash flowing out of digital currency. Because e-bullion was exchangeable with other digital currencies, users were able to swap other brands of digital currency into e-bullion and then access funds through an ATM. As an example, if an HYIP Ponzi operator had received $50,000 of e-gold that value could be instantly exchanged into e-bullion and quickly removed from an ATM. This quick exchange of one digital currency into e-bullion also helped to obscure the funds' source. As digital value transferred from one currency into another, such as e-bullion, any activity related to tracing those funds ended.

Digital currency criminal organizations employ "cashers." A casher's job is to convert digital currency proceeds from the organization's criminal activity into physical cash. It is also during this process that the digital funds' source can be disguised, as users convert the digital units to cash. ATM cards were a preferred method of so-called "cashers" in executing these transactions.

This type of ATM debit card, which converts digital funds into cash, is still very popular in 2016. It was James Fayed and e-bullion that created this successful digital currency combination in 2001. The ability to exchange any brand of digital currency into e-bullion and then move the funds into ATM cash was a definite user advantage.

However, from a US regulatory point of view, transactions that occurred through a US digital currency auto-exchange did not generate the financial reporting or supervision required by US financial regulations. In 2016, this type of convenience is not available for US customers. Even WebMoney Transfer does not permit this automated exchange of WebMoney Transfer digital currency. In 2006, after the closure of Goldage, most digital currency exchange agents discontinued the automated version of this service or greatly increased user verification and compliance.

Between 2001 and 2005, there were more than a dozen popular digital currencies circulating online.

The fees generated from this type of e-gold and e-bullion exchange was a billion-dollar-a-year business. The extraordinary benefits of e-gold's shared liquidity were positive factors in the e-bullion business.

A similar market exists between bitcoin and other cryptocurrencies. Bitcoin is widely accepted across the industry and experts identified it as the most popular cryptocurrency by a large margin. Trading exchanges

will accept bitcoin deposits, there are bitcoin debit cards, and almost all agents will accept bitcoin. The convenient third-party exchange between digital currency brands and products delivers this additional liquidity across an entire industry. With more than 1000 cryptocurrencies circling the globe in 2016, the exchange route between national currency and cryptocurrency value almost often runs through bitcoin.

CR No. 08-00224 US District Court for the Central District of California

February 2008 Grand Jury

United States of America, Plaintiff, v. James Michael Fayed, and Goldfinger Coin & Bullion, Inc., Defendants.

18 U.S.C. § 1960: Operating an Unlicensed Money Transmitting Business

On February 26, 2008, James Fayed and GCB (E-bullion) were charged in a two-page, one-count sealed federal indictment for allegedly operating a money transmitter business without the appropriate state license or federal registration. The government made this indictment public on August 1, 2008, the same day of Mr. Fayed's arrest.

In a July 2015 letter, Mr. Fayed recounted, in his words, the events that took place on the day of his arrest for Operating an Unlicensed Money Transmitting Business. Minutes after sunrise on August 1, 2008, James was at his ranch home, situated on 286-acres in rural Venture County, Moorpark, California. In the early light, a combined force of more than 120 FBI Agents and LA Police Department personnel "stormed" the ranch and the buildings on the property. The invasion force included two fully armored Special Weapons And Tactics (SWAT) teams (one federal and one Los Angeles Police Department [LAPD]), armored "Bear-Cat" style SWAT vehicles, one FBI Helicopter and one LAPD helicopter support team, one Department of Homeland Security federal surveillance blimp (for monitoring and surveillance support), a team of US Marshals, multiple camouflaged snipers concealed at various locations around the property, assorted Police Captains and Lieutenants, Assistant US Attorney's, Police detectives and uniformed federal agents, and other local officers carrying side arms and automatic weapons. James also had two Schutzhund-trained Reisenschnauzers as pets which were quickly tasered by officers, netted and zip-tied. Finally, James writes that, along with the federal law enforcement response, a medevac helipad and Level 2 Trauma Center had been placed on standby at nearby Los Robles

Hospital and Medical Center in Thousand Oaks, California.[32] While these details came directly from Mr. Fayed; this information could not be independently verified.

On September 15, 2008, just 45 days after his arrest, the federal charges relating to an unlicensed money transmitter business, the only charge against James M. Fayed, was dropped and the federal case against him terminated. The money transmitter charges remained pending against GCB until May 2009. On May 4, 2009, the government also dismissed those charges.

On August 18, just over two weeks after Mr. Fayed's arrest, his attorneys filed an Ex Parte Joint Defense Application for Order Releasing $300,000 of Seized Funds to Preserve Exculpatory Evidence of Internet Servers and Network System. The defense was going to use the funds for paying the $100,000-a-month ongoing maintenance costs of the Swiss Internet servers and extensive computer network system operated by e-bullion.com. Maintaining the servers would have preserved any exculpatory evidence contained within the e-bullion records.

The application was supported by several points listed in the 19-page document. Among them was a Memorandum of Points and Authorities. An introduction section of the Memorandum located on pages three, four, and five contained the following disclosures regarding the e-bullion business.

> On February 26, 2008, Mr. Fayed and Goldfinger were named in a one-count sealed indictment for allegedly operating a money transmitting business without obtaining the appropriate state license or federal registration. Defendants Mr. Fayed and Goldfinger, however, have not broken any laws and operated a lawful business enterprise, and will prove at trial that they violated no laws. In fact, Goldfinger and Mr. Fayed may not even have been the actual targets of the longstanding FBI and IRS investigation. On February 26, 2008, the prosecutor, Assistant United States Attorney Mark Aveis, told the United States District Court magistrate in a sworn statement: Goldfinger Coin & Bullion, Inc., and its related Internet site, e- Bullion, are highly visible, international going concerns. The indictment represents one of several steps in a long-term investigation by the FBI and IRS regarding fraud, money laundering, and terrorist financing, and both agencies believe that defendant Fayed and his company can provide valuable assistance to law enforcement authorities, both historically, in terms of tracing the flow of criminal proceeds, and more importantly, proactively, in terms of continuing to operate his business for real-time monitoring of the flow of criminal proceeds.

For an attorney, or even someone not licensed to practice law, this statement to the court, by Mr. Fayed's lawyer, appears to be an across-the-board offer to cooperate with the government. Not only did this cooperation extend to past investigations, it also appears that Mr. Fayed's legal representative is suggesting e-bullion could operate as a so called "honey pot" and provide ongoing real-time information on possible crimes committed through the e-bullion system.

If e-bullion and Mr. Fayed had, "… not broken any laws and operated a lawful business enterprise, and will prove at trial that they violated no laws," suggesting this offer of cooperation through an open declaration to the court, this may have been signaling a change in legal strategy!

The attorney's statement continues.

> Accordingly, the government believes it is in the best interests of the government and defendants to avoid disclosure of this indictment and related papers so as to give the government the opportunity to approach defendants toward cooperating in further investigation.
>
> Similarly, disclosure of this indictment would most certainly cause disruption, if not a complete shut-down, of the relevant Internet sites and would, accordingly, likely destroy any possibility of a proactive, ongoing investigation of very "important targets."
>
> In fact, Mr. Fayed, Goldfinger, and e-Bullion.com have a history of cooperating with federal, state and local authorities. In the past thirty- six months, Mr. Fayed and Goldfinger have cooperated with inquiries from the U. S. SEC, United States Attorneys' Offices in Connecticut, Nevada, and Washington state, the Federal Bureau of Investigation, the U. S. Commodity Futures Trading Commission, Federal Trade Commission, as well as state and local law enforcement agencies. (See partial list attached as Exhibit 1) Defendants have complied with lawful subpoenas and seizure orders from federal, state and local agencies, including seizures by the U.S. Marshals Service in excess of $1.8 Million.
>
> As Mr. Aveis acknowledged six months ago, defendants were involved in highly visible going concerns and providing valuable assistance to law enforcement authorities.

The following chart, from the same court documents, references a very long list of contact information for subpoenas received from law enforcement and regulatory agencies directed to GCB, Goldfinger Bullion Reserve Corp. and E-Bullion Co.

Chart 4.2 Contact information of law enforcement and regulatory agencies received by Goldfinger Coin & Bullion, Inc., Goldfinger Bullion Reserve Corp. and E-Bullion Co.

Memorandum of points and authorities

Contact Information for Subpoenas Received from Law Enforcement and Regulatory Agencies Directed to GCB, Inc., Goldfinger Bullion Reserve Corp. and E-Bullion Co.

Ansu N. Banerjee, Staff Attorney U.S. Securities and Exchange Commission Division of Enforcement Washington, D.C. 20549-0708	Mr. Scott McGeachy Internal Revenue Service Portland, OR 97204	Jill D. Helbling, Esq. Pennsylvania Securities Commission Pittsburgh, PA 15222-1210
Lawrence Lincoln US Attorney's Office Seattle, WA 98101-1271	Mr. David D. Smyth Securities and Exchange Commission Division of Enforcement Washington D.C. 20549-5631	Special Agent Karen Jurden Federal Bureau of Investigation New York, NY 10278
Ms. Amy Blaser Internal Revenue Service Medford, OR 97504	Ms. Maura Kelly Special Agent Federal Bureau of Investigation Ventura, California 93006 Mr. Paul R. Shipley Internal Revenue Service Bellevue, WA 98004-5526:	Gregory Freemon, Esq. Securities and Exchange Commission Division of Enforcement Washington, D.C. 20549
Ms. Cindy Jameson Mr. G. Kenny Walker Internal Revenue Service Denver, CO 80208	Mr. Philip Rix US Commodity Futures Trading Commission New York, NY 10005	Ms. Patricia E. Foley Securities and Exchange Commission Denver, CO 80202
Carolann Gemski Securities and Exchange Commission Division of Enforcement Chicago, IL 60604	Mr. Stephen Caivano, IRS/CI Houston, Texas 77074	Detective Dwight Taylor Urbandale Police Department Urbandale, IA 50322
Special Agent Kurt Siuzdak Federal Bureau of Investigation New York, New York 10278	Detective Chris Weaver State College Police Department State College, PA 16801	Mr. James G. O'Keefe Securities and Exchange Commission Chicago, IL 60604

Memorandum of points and authorities

Scott D. Pomfret, Staff Attorney Securities and Exchange Commission Boston District Office Boston, MA 02110	Marissa J. Reich, Esq. Federal Trade Commission, Midwest Region Chicago, Illinois 60603	Detective Dwight Taylor Urbandale Police Department Urbandale, IA 50322
Mr. Jonathan Biran Assistant US Attorney US Attorney's Office New Haven, CT 06510	Ms. Jane M. Domboski FBI New Haven, CT 06511	Mr. Gary Garcia Colorado Attorney General's Office Denver, CO 80203
Ms. Terrie Murray Assistant US Attorney Las Vegas, NV 89101	Ms. Melody Berkheiser US Attorney's Office Portland, OR 97204-2902	Paula Henderson Revenue Agent Internal Revenue Service Medford, OR 97504

Case 2:08-cr-00224-PSG Document 18-2 Filed 08/18/2008 (4 Pages)

In a July 2015 letter, Mr. Fayed reinforced the fact that no state or federal charges, in regard to the alleged money transmitting violation, were ever fully prosecuted against himself or his company.

> The fact that all federal charges against my companies (Business related) and myself personally were dismissed with the federal government eventually settling (out of court) with myself & defense attorney's should attest to that fact! The states(s) never filed business related charges at all, and the I.R.S. dropped all charges along with the federal dismissal/settlement![33]

Murder of Pamela Fayed

Court records indicate as early as October 2007, agencies of the federal government had been actively investigating James Fayed, GCB, and e-bullion. During that same period in October 2007, James filed for divorce from his wife, Pamela. This separation created an opportunity for federal investigators to acquire private books and records on the couple's businesses without alerting James Fayed of an ongoing criminal investigation.

Six months later, in April 2008, the Judge appointed a receiver to audit and secure all of the business' precious metal holdings and company assets. This action would have allowed Pamela's accountants to value the entire marital estate as required in the divorce. Without informing James

about an investigation, government investigators immediately subpoenaed Pamela's accountants to produce all of the files on GCB and e-bullion obtained for the audit.

Information from court documents indicates that in June 2008, unaware of the sealed indictment, James Fayed hired Jose Luis Moya, one of his local ranch employees to kill his wife, Pamela. After at several missed attempts to murder Pamela, on July 28, 2008, a young criminal gang member, hired by Moya, killed Pamela. The assault took place in a parking garage minutes after meeting with Mr. Fayed and attorneys. James Fayed's credit card was used to rent the vehicle Jose Luis Moya drove bringing Pamela's killer to the parking garage. A security camera recorded the vehicle's license plates immediately after her murder.

James Fayed was eventually tried for murder by the State of California, found guilty and sentenced to death. Since his arrest on August 1, 2008, on federal charges, Mr. Fayed had remained incarcerated. He was held in federal custody until the State of California charged him with murder. Since that time, he has been an inmate in California State Penitentiary. Over the course of 18 months, from 2014 to 2016, James provided firsthand information for this book through interviews conducted using US mail.

Remission

On November 18, 2015, the US Attorney's Office Central District of California issued a press release saying that the USA had returned approximately $11.7 million in e-bullion fraud proceeds to more than 1000 victims who had funds on deposit with e-bullion when the business closed in 2008. The recovered funds included previously seized bank accounts and $5.4 million worth of gold, silver, and platinum.[34]

Victims of an earlier HYIP Ponzi scam had also received a distribution of $1.8 million in December 2014. Those seized funds had originated from more than 300 victims who paid money through e-bullion into a Ponzi scheme known as Kum Ventures. This scam accepted funds through both e-gold and e-bullion.

Statements from the Department of Justice detailed how the e-bullion operation had allowed HYIP fraudsters and scammers to accept funds from victims, move the money anonymously through e-bullion accounts, and wire transfer the proceeds from GCB into the third-party overseas accounts. Government lawyers alleged that James Fayed not only allowed

the illegal scams to operate while collecting substantial fees in the process, he also further profited by keeping any funds left behind when the fraudsters fled and abandoned the e-bullion Ponzi accounts. FBI and IRS Criminal Investigations uncovered these details.

It was not until Mr. Fayed had released the encrypted computer servers from Switzerland that the government was able to obtain the past client account information. Once in possession of this information, the claims administration company retained by the Department of Justice was able to distribute the forfeited funds to past legitimate e-bullion account holders. The e-bullion users resided in several countries, including the USA, Australia, and Canada. The authority to grant remission originates with the Department of Justice, under the Code of Federal Regulations, Chapter 28, Part 9.[35]

The Remission Administrator mailed checks to previous e-bullion account holders in mid-November 2015. The amount of funds disbursed to e-bullion victims did not cover the total cost of the group's claims. Of the total amount requested, less than one quarter was distributed to victims. Therefore, each client only received 22.72 percent of the recognized loss amount.[36]

It is also worth noting that the Remission Administrator works in conjunction with the US Treasury Offset Program; a program administered by yet another government agency, the Bureau of the Fiscal Service's Debt Management Services. Several of the e-bullion Remission Petitioners, who were eligible for remission payments, had been identified as individuals with past government debts that qualified for collection through the Treasury Offset Program. This program is a centralized offset program that collects delinquent debts owed to federal agencies and states (including past-due child support), in accordance with 26 U.S.C. § 6402(d) (collection of debts owed to federal agencies), 31 U.S.C. § 3720A (Reduction of tax refund by amount of the debts), and other applicable laws.[37]

To satisfy previous government obligations, checks were reduced even further for those e-bullion users with past delinquent debts. The US Attorney's Office, the FBI and IRS Criminal Investigation, along with the cooperation of Australian Federal Police also secured the forfeiture of approximately $12 million in precious metals held by James Fayed and his companies in Perth, Australia. Efforts to repatriate the Australian proceeds for distribution to the e-bullion victims are ongoing.

Notes

1. Andrew Schouten, "Unlicensed Money Transmitting Businesses and Mens Rea under the USA PATRIOT Act," McGeorge School of Law, University of the Pacific, accessed July 12, 2015, http://www.mcgeorge.edu/Documents/Publications/07_Schouten_MasterMLR39.pdf.
2. "Terrorist Financing Staff Monograph, Appendix A: The Financing of the 9/11 Plot," UNT Libraries: CyberCemetery Home, accessed March 26, 2016, http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_App.pdf.
3. James Fayed, Private mail December 1, 2014.
4. Ibid.
5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. James Fayed, Private mail February 7, 2015.
10. Ibid
11. James Fayed, Private mail December 1, 2014.
12. James Fayed, Private mail December 8, 2014.
13. Planetgold.com, "Planetgold E-bullion Interview," Internet Archive: Wayback Machine, accessed October 12, 2014, https://web.archive.org/web/20030216110351/planetgold.com/interview.asp?SPID=71133546.
14. James Fayed, Private mail December 8, 2014.
15. Planetgold.com, "Planetgold E-bullion Interview," Internet Archive: Wayback Machine, accessed October 12, 2014, https://web.archive.org/web/20030216110351/planetgold.com/interview.asp?SPID=71133546.
16. James Fayed, Private mail February 7, 2015.
17. Ibid.
18. James Fayed, Private mail December 8, 2014.
19. James Fayed, Private mail February 7, 2015.
20. James Fayed, Private mail July 2015.
21. Ken Griffith, Former VP of e-bullion, email July 2013.
22. "The Bullion Exchange Gold Exchange Provider. Precious Metals, E-Gold and E-Bullion," Internet Archive: Wayback Machine, accessed November 13, 2015, https://web.archive.org/web/20051124062407/www.thebullionexchange.com/faq.shtml.

23. James Fayed, Private mail July 2015.
24. James Fayed, Private mail July 2015.
25. "PlanetGold E-bullion Interview," Internet Archive: Wayback Machine, accessed March 26, 2016, https://web.archive.org/web/20030216110351/planetgold.com/interview.asp?SPID=71133546.
26. "FINRA Warns Investors of Social Media-Linked Ponzi Schemes, High-Yield Investment Programs," FINRA.org, accessed January 12,2016,https://www.finra.org/newsroom/2010/finra-warns-investors-social-media-linked-ponzi-schemes-high-yield-investment-programs.
27. "HYIPs—High Yield Investment Programs Are Hazardous to Your Investment Portfolio," FINRA.org, accessed March 26, 2016,http://www.finra.org/investors/alerts/hyips%E2%80%94high-yield-investment-programs-are-hazardous-your-investment-portfolio.
28. James Fayed, Private mail 2015.
29. "FBI—Fool's Gold," FBI, accessed March 27, 2016, https://www.fbi.gov/news/stories/2016/january/fools-gold/fools-gold.
30. US District Court for the Central District of California, United States of America, Plaintiff, v. James Fayed, et al., Defendant. No. CR08-224, Government's Memorandum of Points and Authorities in Support of Application to Criminal Duty Judge for Review of Magistrate Judge's Bail Order, (United States of America, Plaintiff, v. James Fayed, et al., Defendant. No. CR08-224, 2008).
31. E-bullion.com, "E-Bullion," Internet Archive: Wayback Machine, accessed October 29, 2015, https://web.archive.org/web/20020126214534/www.e-bullion.com/debit.php.
32. James Fayed, Private mail July 2015.
33. James Fayed, Private mail July 2015.
34. "United States of America Et Al V. $1,802,651.56 in Funds Seized From E-Bullion et al :: California Central District Court :: Federal Civil Lawsuit No. 2:09-cv-01731, Judge Philip S. Gutierrez Presiding," PlainSite :: The Law in Plain Sight, accessed March 26, 2016, http://www.plainsite.org/dockets/i060c1du/california-central-district-court/united-states-of-america-et-al-v-180265156-in-funds-seized-from-ebullion-et-al/.
35. "28 CFR Part 9 – Regulations Governing the Remission or Mitigation of Administrative, Civil, and Criminal Forfeitures | US

Law," LII / Legal Information Institute, accessed November 28, 2015, https://www.law.cornell.edu/cfr/text/28/part-9.
36. "FBI—United States Returns Nearly $12 Million to Victims of Illegal Money-Transmitting Business Called E-Bullion," FBI, accessed May 8, 2015, https://www.fbi.gov/losangeles/press-releases/2015/united-states-returns-nearly-12-million-to-victims-of-illegal-money-transmitting-business-called-e-bullion.
37. "Treasury Offset Program," Bureau of the Fiscal Service, accessed March 26, 2016, https://fiscal.treasury.gov/fsservices/gov/debtColl/dms/top/debt_top.htm.

CHAPTER 5

Crowne Gold

In July 2008 news began to spread that defendants in the e-gold criminal case had entered an agreement with government prosecutors and had pleaded guilty to multiple felonies relating the e-gold digital currency business. About a week later, in July 2008, Crowne Gold announced the company was voluntarily closing.

In December 2000, a man named Stephen H. Foerster had been caught in a wave of corporate layoffs and left his position as Technical Director at e-gold and G&SR/OmniPay. Steve also had a part in creating the e-gold-tech discussion list which is still online at https://www.mail-archive.com/e-gold-tech@talk.e-gold.com/. This mailing list has become an important source of facts and history for digital currency enthusiasts. It contains comments from many of the original creators and operators of digital currency systems.

A month later in early 2001, Mr. Foerster used his knowledge and technical skill to co-found a new online digital gold payments business called 3PGold. The operation's slogan was "Gold around the world, around the clock." The other 3PGold co-founder was Mr. Bernard von NotHaus, who was well-known in the industry and referred to as a "Monetary Architect." This book also includes a chapter on the Liberty Dollar and Bernard von NotHaus. 3PGold (3PGold.com) was Crowne Gold's predecessor. It was the company that provided Sean Trainor and entrance into the digital gold business.

During late 2001, the 3PGold website displayed a company registration from the Commonwealth of Dominica, West Indies. The website also

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_5

described the online payment business as enabling clients to buy, store, and sell gold at anytime from anywhere in the world.

By examining the services offered through the organization's website, 3PGold.com appeared to be largely of an offshore asset protection and financial services firm that may have been catering to US clients. During the first quarter of 2002, co-founders Steve and Bernard sold the entire 3PGold operation to a group of US associates that included companies and individuals. The buyers group was led by Mr. Terry Leroy Neal and included Mr. Sean Trainor. These two men were the drive behind the acquisition of 3PGold. On March 4, 2002, 3PGold was taken over by this new group and the operation renamed Crowne Gold (CrowneGold.com).

In April 2002, during the business's first month of transactions Sean Trainor gave an online interview to Vladimir Kats for Planetgold.com. In the interview, Mr. Trainor explained that his involvement in digital gold currency began after a meeting with a man named Bernard von NotHaus. At the time of the acquisition, neither Mr. Neal nor Mr. Trainor was acknowledged as a corporate officer or shareholder of the new business.

Terry Neal

By 2002, Mr. Terry L. Neal had written several books on financial topics and was considered to be an advocate for offshore corporate and financial services. His books included the following titles:

- 1996: Barter and the Future of Money: The Currency Crisis[1]
- 1998: The Offshore Advantage: Privacy, Asset Protection, Tax Shelters, Offshore Banking & Investing[2]
- 2001: The Offshore Solution: Privacy, Asset Protection, Tax Shelters, Offshore Banking and Investing[3]
- 2002: The Nevada Advantage: When, Why and How to Incorporate: Regardless of Where You Live and Work[4]

In 1999, Mr. Neal and one of his US companies, Itex Corporation, were involved in a civil action with the Securities and Exchange Commission:

> Litigation Release No. 16305 / September 28, 1999
>
> S.E.C. V. Itex Corporation, Terry L. Neal, Michael T. Baer, Graham H. Norris, Cynthia Pfaltzgraff and Joseph M. Morris, Civ. No. 99-1361 (HA) (D. Ore. September 27, 1999)

> S.E.C. Filed Fraud Case Against Itex Corporation
>
> On September 27, 1999, the Securities and Exchange Commission filed a civil fraud action in the United States District court for the District of Oregon against Itex Corporation ("Itex"), Terry L. Neal, Michael T. Baer, Graham H. Norris, Cynthia Pfaltzgraff and Joseph M. Morris (Civil Action 99-1361-HA). The Complaint alleges that Terry Neal, Itex's founder and control person orchestrated and implemented a broad-ranging fraudulent scheme by making materially false and misleading disclosures about the company's business and by failing to disclose numerous suspect and in many cases sham barter deals between Itex and various mysterious offshore entities related to and/or controlled by Neal. The complaint also alleges that Neal, a control person of Itex, orchestrated these transactions and made profits of approximately $6.3 million from sales of Itex stock through a variety of primarily offshore accounts he controlled.[5]

In September 2000, the SEC settled their Itex case with Terry Neal and five other defendants. He was barred from serving as an officer or director of any public company and ordered to pay back $2,300,000 in ill-gotten gains plus interest, along with an additional $200,000 as a civil penalty.[6]

Just over two years later, in December 2002, Terry L. Neal was arrested on federal tax charges after a criminal complaint was filed against him in the US District court for the District of Oregon, in Portland.[7]

The federal agent who filed the affidavit for the search warrant was a Special Agent employed by the Internal Revenue Service (IRS), Criminal Investigation. The 17-page document listed the criminal statutes involved in his investigation:

a. Attempt to Evade or Defeat Tax
   Title 26, United States Code, Section 7201
b. Failure to File Return
   Title 26, United States Code, Section 7203
c. Filing Materially False Tax Returns
   Title 26, United States Code, Section 7206(1)
d. Conspiracy to Commit Offense or to Defraud the United States
   Title 18, United States Code, Section 371[8]

In August 2006, a US Senate permanent subcommittee on investigations issued a final report on tax haven abuses and offshore financial activity. Their report included detailed information on the illegal activity of Mr. Terry Neal:

> United States Senate, Permanent Subcommittee on Investigations
> Committee on Homeland Security and Governmental Affairs
> Norm Coleman, Chairman
> Carl Levin, Ranking Minority Member
> Tax Haven Abuses: The Enablers, The Tools and Secrecy
> Minority & Majority Staff Report
> The Subcommittee began this investigation into offshore abuses over one year ago. Over that time period, the Subcommittee has consulted with numerous experts in the areas of tax, securities, trust, anti-money laundering, and international law. The Subcommittee issued 74 subpoenas and conducted more than 80 interviews with a range of parties related to the issues and case histories examined in this Report. This Report examines the offshore industry behind these statistics, including the role of offshore service providers, the interactions between offshore and U.S. professionals who help to establish and manage offshore entities, and the range of sophisticated schemes being used today to enable U.S. citizens to hide and secretly utilize offshore assets.[9]

Testimony before The Subcommittee included specifics on offshore promoter Mr. Terry Neal. While living in the USA, Mr. Neal had recruited clients through the Internet and helped them create offshore structures. Here is part of that text:

> Greaves-Neal: Diverting U.S. Business Income Offshore. This case history examines a U.S. businessman who, with the guidance of a prominent offshore promoter, moved between $400,000 and $500,000 in untaxed business income offshore. Kurt Greaves, a Michigan businessman, told the Subcommittee that he first contacted Terry Neal, an offshore promoter based in Oregon, after seeing an advertisement for offshore services in an in-flight magazine. Under Mr. Neal's guidance, Mr. Greaves used a variety of sham transactions to transfer untaxed business income offshore without giving up the ability to use and manage those funds. Mr. Greaves told the Subcommittee that all of the offshore service providers who managed his offshore corporations readily complied with his requests on how to handle his assets, even though he did not technically own any shares in the offshore corporations. He said that the offshore service providers even fabricated documents to support fictitious tax deductions, including a phony mortgage and insurance policy. Like Mr. Holliday, Mr. Greaves established shell corporations in Nevada as an additional layer of separation between him and his offshore assets, and arranged for fictitious bills and loans to move funds

between his Nevada and offshore entities. In 2004, both Mr. Greaves and Mr. Neal pleaded guilty to charges related to federal tax evasion.[10]

Although it was a 13-count indictment, Mr. Neal ultimately only pleaded guilty to one charge of conspiracy to defraud the USA by impeding the IRS (18 U.S.C. §371). He received a sentenced of five years in prison followed by three years' probation and a $50,000 fine.[11]

In late December 2002, Special Agent Scott McGeachy of the IRS, Criminal Investigation, filed an affidavit for search warrant. Law enforcement agents were requesting to search the Portland, Oregon, office of Laughlin International and in Carson City, Nevada, the office of Privatech Group, LLC. A US Magistrate Judge agreed and granted the search warrant. Agents seized the following amount of precious metal from the Portland office of Laughlin International:

- 47 10-ounce gold bars,
- 35 1-ounce gold coins, and
- 3069 1-ounce silver coins

Special Agent Craige Walker of the IRS provided sworn statements that a transaction or attempted transaction in violation of 18 U.S.C. § 1960 involved the seized precious metal. The agents made the claim that under the provisions of 18 U.S.C. § 981(a)(1) the precious metal should be forfeited, because it was traceable to illegal activity.

Many bold statements were made in Special Agent Walker's sworn statement including that as part of a scheme to defraud the IRS, Mr. Neal and others formed Crowne Gold and operated a money "transferring system."

On April 24, 2003, a federal grand jury indicted Terry Neal, Lee Morgan, Aaron Young, and James Fontana for conspiring to impair and impede the IRS. Agents alleged that the men created and facilitated a scheme to move US citizens' untaxed funds offshore and bring the money back into the USA without paying taxes on those funds.

Crowne Gold did not register as a money transmitter with the State of Nevada, Oregon, or Florida. Crowne Gold was also not registered as a money service business with the Financial Crimes Enforcement Network (FinCEN) or any other agency required by federal law. Based on Special Agent Craige Walker's affidavit, prosecutors had alleged that Crowne Gold was an unlicensed money transmitting business in violation of Title 18, United States Code, Section 1960. Furthermore, the gold and silver

seized December 27, 2002, was property involved in violations of this statute and was, therefore, subject to forfeiture under Title 18, United States Code, Section 981(a)(1)(A).

As the government was in no hurry to give back any precious metal, the case dragged on into mid-November 2004. At that time, the attorneys for Sean Trainor and Crowne Gold began to oppose the seizure vigorously. Lawyers filed a motion to strike and also objected to Special Agent Craige Walker's sworn statements, requesting that the government prove Crowne Gold was, in fact, a Money Transmitter business that required licensing. Along those same lines, if Crowne Gold was not shown to be guilty of any offense, then the precious metal could not be tied to a crime and should be returned to its rightful owner. Crowne's attorney claimed that most of the declaration by Agent Walker was hearsay, speculation, and otherwise inadmissible conclusory statements which are unsupported by any evidence. Lawyers asked the court to strike all of the exhibits because they were not authenticated, and accordingly, the court had no means of determining their authenticity or reliability.

One of the most interesting statements from Agent Walker was the inclusion of text from the Crowne Gold website that stated, "Crowne Gold clients may digitally transfer any part of their holdings instantly to anyone, anywhere in the world via secure, fully encrypted, Internet payment system."

However, the court recognized references on the Crowne Gold website that "gold holdings" were not money. According to one of the legal exhibits, which included a screen shot of the Crowne Gold website, clients could only transfer a "gold holdings." Gold holdings are not money or currency.

Sean Trainor's lawyers fought the characterization that Crowne Gold was a money transmitter. Mr. Trainor described the Crowne Gold business as "an Internet gold and silver broker." The website stated that Crowne Gold "facilitates the ability of its individual clients to buy, sell, store, and exchange gold and silver."

Mr. Trainor asserted that the business was a gold and silver broker that allowed clients to transfer gold holdings which are backed by physical gold. Crowne Gold and Trainer were not named defendants or otherwise even mentioned in the Neal indictment. Furthermore, in 2002, Crowne Gold had entered into an agreement for Laughlin International to provide a secure Portland facility for storing gold and silver. Laughlin International was merely holding the seized precious metal in the office safe before

being shipped to account holders of Crowne Gold. There had been no criminal activity which involved the precious metal.

For a summary judgment in the case, the USA had to establish that it was more probably true than not true that Crowne Gold was operating an illegal money transmitting business. Plus, there had to exist a substantial connection between the seized gold and silver and the criminal offense.

In late January 2005, the court denied the government's motion for summary judgment against Crowne Gold and Mr. Trainor. By mid-September 2005, the lawyers for Mr. Trainor were noticeably aggravated by the government's delay. This anger was evident in the September 16 Pre-Status Conference Statement of Crowne Gold and Sean Trainor.

> Much like Humpty Dumpty in Alice in Wonderland, the government attempts here to say to this court, "Words mean whatever I say they mean." For this court has identified in the statute, 31 U.S.C. §5330, the references repeatedly to "money," not to gold. (Ditto for Oregon law.) For the government's sake, the obvious point should be made: gold is not money and money is not gold. Gold is a commodity. Gold is not money any more than pork bellies or corn are money.
>
> All of this, of course, will prove that Crowne Gold is not a money transmitter, but a broker which receives payments by wire transfer and pays to its customer's monies by wire transfer, and is not engaged in the business of making payments to third parties by debit card or otherwise.
>
> [I]f the Government's theory of forfeiture is that the property … was involved in the commission of a criminal offense, the Government shall establish that there was a substantial connection between the property and the offense. 18 U.S.C. § 983(c)(3).

Less than a week later, the court had filed settlement agreements and returned a partial amount of precious metal to Crowne Gold and Sean Trainor. Through his attorney's Mr. Trainor received 16 10-ounce gold bars, 15 1-ounce gold coins, and 3069 1-ounce silver coins. Mr. Terry Neal even received nine one-ounce gold coins provided by the court.

A March 23, 2006, television news report from KATU in Portland, Oregon, that aired just after Mr. Terry Neal's sentencing stated that Crowne Gold had been "part of the scheme" that had allowed Mr. Neal's clients to purchase gold over the Internet. However, no charges relating to Terry Neal's activities were ever filed against Crowne Gold or any of the company's other executives. After his arrest and during his legal battle with the US government, Mr. Neal was able to author and publish at least

four additional books. However, none of the books were related to offshore services or taxes.

Crowne Gold

Crowne Gold, Inc. was a Nevada Corporation formed in 2002. From statements made by Mr. Trainor at the outset of the new Crowne Gold business, both he and the organization appeared to have had very honest and legal intentions. Early in Crowne Gold's new business operation, Mr. Trainor showed he had a long-term vision for the new business. He also stated he was hopeful about the future of digital gold currency. In a 2002 online interview with Planetgold, Mr. Trainor offered his prediction about future Crowne Gold users. He discussed "who" he believed would be using the products and services of Crowne Gold. He said the target market consisted of English-speaking persons and Internet sales companies.[12]

No one in Crowne Gold's management had any experience in the payments industry or the online payment business. Mr. Trainor served as a Director of Crowne Gold beginning in March 2002. As of June 29, 2003, the Crowne-gold.com website listed Sean Trainor as president and director of Crowne Gold.[13]

No officer or director of Crowne Gold had ever held a position with a bank. As illustrated by Mr. Trainor's comment, the company's target market of future users seemed unclear. Similar to the vision of other online digital gold currency owners and operators of that time, the Crowne team would be attempting to market the payment product and bullion services to a broad range of potential new users.

With several other digital gold companies already flourishing in the marketplace, Crowne Gold showed no immediate plans for competing with these businesses. Additionally, the Crowne Gold operators had not targeted any particular jurisdictions.

Some of the early digital currency companies had focused marketing on customers in areas of the world where credit cards were unpopular. As an example of this regional activity, jurisdictions where credit cards were hard to obtain, such as the Middle East, had both offered an abundance of potential new digital currency customers. Digital currency products, in general, are designed for ease of use, instant access and low cost. Participants in the e-gold operation had widely viewed the payment system as a financial product that could be adopted by anyone, wealthy

or poor without the need for a pre-existing bank account or credit card. Crowne Gold did not present these features or actively target any of these underserved areas and nonbank populations.

Marketing by Crowne Gold advertised its digital gold system as an ideal method to buy and hold physical gold for profit through appreciation or as a safe hedge against inflation. The company manufactured pure gold one-ounce medallions and convenient ten-ounce bars that could be readily ordered online by Crowne Gold clients. These same bullion products were also available for purchase from hundreds of other online sellers around the world.

The one distinction marketed by Crowne Gold was the high level of purity offered in the company's products. While outside manufactured gold bullion products usually had a purity of 0.995 percent fine gold, Crowne Gold's medallions and bars all had a purity of 0.9999 percent fine gold.

There was a significant difference in cost of buying gold from a well-known precious metals dealer and physical gold delivered from Crowne Gold. Crowne Gold's fees were exceptionally high.

$7 Million Hack

In August 2002, barely five months into Crowne Gold's new operation, the Crowne Gold server was hacked, and the intruder attempted to steal around $7 million of digital gold. The stolen digital units moved around the Crowne server within the company's ledger, and the theft caused some embarrassment for the enterprise. However, no money or gold was ever lost.

The attack was unsuccessful, and in a letter from the company representative, Sean Trainor, he explained that a group effort by members of the digital gold community had helped track down the problems and the funds. The hacker was able to transfer digital units within the closed system. However, no units were ever exchanged into cash, and ultimately, the theft was a failure. The crook had not earned even one dollar of profit from the illegal entry. Other than a brief server shutdown, the Crown Gold system was not damaged.

After the hacking event, the management of Crowne Gold made substantial upgrades to a better platform. Sean Trainor had been very open and accessible to the community regarding the events. The entire issue did not seem to have any long-term adverse effects on Crowne Gold.

Crowne Gold's new online digital gold platform was a turnkey package known as Corniche banking, which was commercial online banking system software from Megasol Technologies. Any person or company can purchase this online banking application software. The platform is suitable for private, offshore banks and other payment services. In 2016, Megasol Technologies software is used by several offshore services companies and private banking businesses.

Finanzas Forex/Evolution Marketing Group (EMG)

Evolution marketing group (EMG) was a high-yielding "Investment" program also categorized as an HYIP that was marketed online around the world. The scheme primarily targeted people in Central and South America, particularly Colombia. However, victims have turned up in dozens of countries around the globe. Popular HYIP websites such as ASA Monitor and the TalkGold forums also promoted this program.

EMG advertised investments in Forex trading promising an exceptionally high return. EMG operated by paying a referral commission for each new account created existing account holder's link. Similar to all other digital currency online HYIP schemes, this referral fee played a significant role in the program's growth.

EMG was a massive program, and the operators were extremely corrupt. Experts described EMG as complex money-laundering networks linked to a heavily promoted online HYIP. Court documents showed that EMG funds had even involved money from the international narcotics trade. Funds flowed through at least 59 bank accounts worldwide, and the scam allegedly took in more than $300 million of investor funds.

Case No. 3:08-cv-01045

Crowne Gold, Inc. v. Evolution Market Group, Inc. et al
In September 2008, Crowne Gold filed documents with an Oregon court in a civil matter.
United States District court District of Oregon
Crowne Gold, Inc., a Nevada corporation,
Plaintiff,

V
Evolution Market Group, Inc., a Panama corporation;
Columbo Asset Management, Inc., a Panama corporation;
Zentrum Bix, Inc., a Panama corporation;
Oceania, S.A., a Panama corporation;
German Cardona; and
Lina Maria Mantilla Grande,
Defendants.

This legal action by Crowne Gold was a Complaint for Declaratory Relief. It is a type of preventive measure that results in a legal determination by the court resolving some legal uncertainty for litigants. The "relief" is typically a legally binding preventive adjudication by which the parties involved in an actual or possible future legal matter have a court ruling on the dispute. The documents named Evolution Market Group, Inc., which was an existing Crowne Gold customer residing outside of the USA. The information filed outlined the Crowne Gold client fee schedule as appearing in the terms of agreement for clients of Crowne Gold.

The preemptive action by Crowne Gold's law firm described the higher than standard fees being charged by Crowne Gold for the manufacture and delivery of precious metal bullion products. Additionally, the filing had favorably positioned the company in advance of any potential legal action from the group of foreign customers which included Evolution Market Group, Inc. Documents indicated that the case had been filed by Crowne Gold, to clarify the company's fee schedule for delivery of physical gold and establish the jurisdiction of any legal action as the State of Oregon. Crowne Gold has included in its terms of service, a fee on all funds that were converted into physical gold and delivered to any client. The fee was 20 percent of the total amount. Noting that EMG investors had deposited more than $130 million with Crowne Gold, EMG now stood to pay a fee of more than $20 million for delivery of the precious metal. Ironically, court documents indicated that the operators of EMG considered the 20 percent fee was being "stolen" from the organization's account.

Shortly after lawyers for Crowne Gold filed the case in Portland, Oregon, there was a flurry of activity between the litigants which culminated in a quick settlement agreement. The Oregon court held jurisdiction under 28 USC § 1332 (Diversity of Citizenship) and 28 USC § 2201 (Declaratory Judgment). Venue in the District of Oregon, Portland Division, is proper

under 28 USC § 1391 and Local Rule 3.4. The parties entered into an Account Settlement Agreement July 29, 2008.

Both sides agreed to the closure of EMG's account with Crowne Gold and a distribution plan on the existing balances, plus any additional future deposits that Crowne Gold may receive on EMG's behalf. Crowne Gold would convert the funds that had been received to gold bullion and certain funds received on July 26, 2008, or after this date would be wire transferred to a company only identified as Pegasus Capital.

The agreement specified that EMG would provide Crowne Gold with an appropriate location, for the physical delivery of approximately $122.5 million in gold bullion. This figure was the balance of funds available after Crowne Gold had deducted a 20 percent fee for delivery of the physical gold. The $122.5 million in gold bullion represented the investor funds Crowne had received from Ponzi victims on behalf of EMG, after Crowne had deducted its fee for acting as EMG's financial agent.

The Crowne Gold account balance converted into approximately $122.5 million worth of 294 gold bars (262 gold bars from the Delaware Depository Service Company and 32 gold bars from Inwood Security Vaults) was later seized by federal agents before it could leave the USA.

As detailed in the affidavit, EMG investor funds subsequently converted into gold bars by Crowne Gold represented the proceeds of wire fraud violations. Federal agents captured the bullion under seizure warrants issued by this court on February 9 and 11, 2009. The court had probable cause to believe that the bars constituted proceeds traceable to wire fraud offenses, in violation of 18 U.S.C. § 1343.[14]

In October 2013, the District court for the Middle District of Florida entered orders of forfeiture for over $138 million in seized gold bullion. Proceeds from the sale of bullion were to be distributed through agents of the US Department of Justice to any eligible victims of the EMG fraud through remission.[15]

Crowne Gold had retained its 20 percent delivery fee, and those funds had also been converted into gold bullion and prepared for distribution to Crowne Gold's operators.

Affidavit of Brian DiPerna

Court records show that information uncovered during a federal investigation of Crowne Gold indicated that November 19, 2008, and December 3, 2008, Sean Trainor had two shipments of gold and silver, from Crowne

Gold, delivered by Brinks to a Tampa warehouse. On February 4, 2009, seizure warrants were issued by a US Magistrate Judge for the Middle District of Florida, Tampa Division, seeking these millions of precious metal bullion sitting in the Tampa warehouse (Case No. 09-MJ-1051-T-EAJ).

Special Agent (SA) Brian DiPerna with the Department of Homeland Security, Immigration and Customs Enforcement (ICE) filed an affidavit with the court on October 30, 2009, detailing the alleged reasons for the seizure. Once again, the digital gold currency company was alleged to be a money transmitter.

The document stated that the Crowne Gold investigation had been conducted jointly by the US Secret Service (USSS), the Internal Revenue Service (IRS), and ICE and the St. Cloud (FL) IRS-USSS Financial Task Force (task force). Information on the very first page concluded that Crowne Gold's business was almost identical to that of e-gold citing United States v. e-Gold, Ltd., 550 F. Supp. 2d 82 (D.D.C. 2008). Furthermore, the government was alleging that Crowne Gold accounts had allowed customers to avoid the Bank Secrecy Act reporting requirements contained in Title 31, United States Code, Chapter 53.

> There is an obvious lure for individuals to use this system simply because those individuals wishing to retain their anonymity and escape the scrutiny of financial institutions gladly accepted the higher rates to do business with Crowne Gold as a simple cost of doing business.[16]

The affidavit alleged that Crowne Gold was a money transmitting business involved in criminal activity. That alleged activity had been in violation of Florida's money transmitter laws.

> The Florida Money Transmitter's Code, Fla. Stat. §§ 560.101 and 560.408, prohibits a person from engaging in the business of a money transmitter without registering with the Office of Financial Regulation. Fla. Stat. § 560.125(1). Crowne Gold did not register with the Office of Financial Regulation when it operated its business. Violation of the money transmitter statute is a felony. Specifically, the penalties for violating this statute are as follows: by wire, facsimile, electronic transfer, courier, or otherwise. Fla. Stat. § 560.103(10). As mentioned above, Crowne Gold created and maintained a transaction database which allowed clients to openly and freely conduct financial transactions with any other Crowne Gold account holder. Moreover, Crowne Gold would "cash out" client funds and then send the funds to clients, or designated third parties, by check or bank wire. Thus,

> Crowne Gold was operating as a money transmitting business by acting as a transferor of funds for Crowne Gold's investors/clients from around the world. However, Crowne Gold failed to register with the Office of Financial Regulation as required by Florida law. Thus, Crowne Gold operated in violation of 18 U.S.C. § 1960(b)(l)(A) because it operated without an appropriate money transmitting license in Florida, and such failure is punishable as a felony under Florida law.[17]

Additionally, as had previously occurred in past digital currency prosecution cases, it was alleged that Crowne had violated the federal requirements for registration 1960(b)(1)(8) and additional requirements for the regulated operation of a financial institution.

Additionally, as had previously occurred in past digital currency prosecution cases, it was alleged that Crowne had violated the federal requirements for registration 1960(b)(1)(8) and additional requirements for the regulated operation of a financial institution.

> With regard to the registration requirements established in Section 1960 (b)(1)(8), a money transmitting business is required to register by filing the appropriate information with the Financial Crimes Enforcement Network (FinCEN), an agency within the Department of Treasury. 31 U.S.C. § 5330(a); 31 C.F.R. § 103.4l(a)(l) and (b). Crowne Gold never registered with FinCEN. Consequently, Crowne Gold also operated in violation of 18 U.S.C. § I 960(b)(l)(8) because it failed to register with FinCEN, in violation of 31 U.S.C. § 5330.
>
> 20. As a result of not being registered, neither FinCEN nor the Florida Department of Financial Regulation was able to ensure Crowne Gold had established proper anti-money laundering programs or that Crowne Gold was in compliance with such programs, which are required of money transmitting businesses if they are properly registered. Specifically, 31 U.S.C. § 531S(h), requires that all financial institutions shall establish an anti-money laundering program, to minimally include:
>
> (A) The development of internal policies, procedures, and controls;
> (B) The designation of a compliance officer;
> (C) an ongoing employee training program; and
> (D) an independent audit function to test programs.
>
> The term "financial institution" includes both "a currency exchange" and a "person who engages as a business in the transmission of funds." 31 U.S.C. § 5312(a)(2)(J) and (R).[18]

There was also the allegation of failure to file any reports of suspicious transactions (Suspicious Activity Reports or "SARs").

The affidavit stated that, through a "merchant relationship," Crowne Gold had opened bank accounts in the USA and been accepting deposits on behalf of Evolution Market Group (EMG). EMG was an organization under investigation by federal law enforcement AML task force in Orlando, Florida, for operating an international Ponzi/Pyramid scheme in violation of 18 U.S.C. § 1343. EMG did business as Finanzas Forex (FFX) and had been the largest client of Crowne Gold.

EMG had claimed that the company was investing in forex markets. However, EMG had misrepresented the business and made no such investments. The funds deposited to Crowne Gold were also not used to purchase precious metal. EMG was another case of a Ponzi scheme using a digital gold currency system as a method of accepting funds and quietly moving that money into the pockets of the fraudsters, in this case, that was EMG. The Crowne Gold terms of service also included a phrase stating that all wire transfers to the company were final, and no refunds would be possible. The affidavit alleged that the firm was clearly a money transmitter.

> Exhibit C, pp. 4–5. Crowne Gold claimed that it is not a bank and did not offer money services, and yet, in its own words, described itself as a money transmission business.[19]

The government's investigation had clearly outlined Crowne Gold's Relationship with this Ponzi scheme. From 2007 through March 2009, a Panamanian corporation had been operating several websites soliciting individuals to invest in high-yielding financial products. The investments would return between 77 percent and 300 percent. EMG stated that the high returns came from trading in the forex market. This kind of enticement was the same sales pitch that digital currency HYIP scams had been using for many years.

Additionally, the investigation revealed that Crowne Gold kicked back a percentage of each deposit directly to the operator of the scam, EMG President Mr. German Cardona. EMG victims had not deposited money into Crowne's bank accounts for the purpose of purchasing precious metal and that Crowne Gold had not used the funds to buy any gold. In fact, Sean Trainor later advised investigating agents that EMG had specifically established a relationship with Crowne Gold to receive wire transfers from

its customers. Instead of purchasing gold, Crowne wired funds directly to EMG's bank account, EMG promoters' bank accounts, investment companies, and third parties as directed by EMG operators. It was an obvious scam, and Crowne Gold had collected over $120 million from EMG investors through Crowne Gold's bank accounts.

It was not until seven months into the business relationship with EMG that Crowne Gold had even purchased a large amount of gold on behalf of EMG clients. The date of that purchase had been the end of July 2008, just as Crowne Gold was closing down its business. Records indicate Crowne purchased $120,992,245.76 in gold for EMG. In this document, the government had made several critical points in the attempt to identified Crowne Gold as a financial institution:

- The funds received by Crowne Gold on behalf of EMG customers were not used to purchase any gold and thus Crowne Gold was not following its Terms of Service or advertised business model.
- Crowne's business with EMG contradicted earlier verified statements from Sean Trainor that Crowne Gold was merely in the business of brokering precious metals.
- The records clearly showed that Crowne Gold had utilized its merchant relationship with EMG to operate as an unlicensed money transmitter.
- As Crowne Gold's largest and most profitable client, the merchant relationship with EMG was not collateral, but an integral part of the operation. The numerous Crowne Gold's US bank accounts that had accepted funds for EMG showed large volumes of deposits followed by correspondingly large amounts of outgoing transfers during the same period.

Forfeiture

Records disclosed the first week December 2008, indicated that on November 19, 2008 and December 3, 2008, Sean Trainor had two shipments of gold and silver delivered by Brinks to a Tampa warehouse from Crowne Gold. On February 4, 2009, seizure warrants were issued by a US Magistrate Judge for the Middle District of Florida, Tampa Division, for Sean's precious metal (Case No. 09-MJ-1051-T-EAJ). Trainor later admitted that the seized precious metal represented his profits from Crowne Gold.

As detailed in this affidavit, there was probable cause to believe that the seized Tampa precious metal constituted proceeds of violations of 18 U.S.C. § 1960, operating an unlicensed money transmitting business. The precious metal assets were, therefore, subject to forfeiture by the USA, under 18 U.S.C. § 98l(a)(l)(A) (property involved in a violation of 18 U.S.C. § *1960*). The court's authority to order forfeiture of property for violations of 18 U.S.C. § 1960 is found in 18 U.S.C. § 98 l(a)(l)(A). Section 981(a)(l)(A) provides for the civil forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of Section 1960, or any property traceable to such property. 18 U.S.C. § 981(a)(l)(A).

On February 5, 2009, during an interview with government agents, Mr. Trainor Stated that Crowne Gold was not a money transmitter and did not conduct financial transactions.

Notes

1. Terry L. Neal and Gary K. Eisler, *Barter and the Future of Money: The Currency Crisis* (New York, NY: MasterMedia, 1996).
2. Terry Neal, *The Offshore Advantage: Privacy, Asset Protection, Tax Shelters, Offshore Banking & Investing* (Portland, OR: MasterMedia Pub. Corp, 1998).
3. Terry Neal, *The Offshore Solution: Privacy, Asset Protection, Tax Shelters, Offshore Banking and Investing* (Reno, NV: MasterMedia Pub. Corp, 2001).
4. Terry Neal, *The Nevada Advantage: When, Why & How to Incorporate; Regardless of Where You Live and Work* (Reno, NV: MasterMedia Pub, 2002).
5. "Litigation Release No. 16305 / September 28, 1999," SEC.gov | Home, accessed March 26, 2016, https://www.sec.gov/litigation/litreleases/lr16305.htm.
6. "Litigation Release No. 16708 / September 18, 2000," SEC.gov | Home, accessed March 27, 2016, http://www.sec.gov/litigation/litreleases/lr16708.htm.
7. Plainsite.org, "USA v. Neal, et al :: Oregon District Court :: Criminal Case No. 3:03-cr-00035-HA," accessed October 6, 2015, http://www.plainsite.org/dockets/4xd3d574/oregon-district-court/usa-v-neal-et-al/.

8. Plainsite.org, "USA v. Neal, et al :: Oregon District Court :: Criminal Case No. 3:03-cr-00035-HA," accessed October 6, 2015, http://www.plainsite.org/dockets/4xd3d574/oregon-district-court/usa-v-neal-et-al/.
9. "- TAX HAVEN ABUSES: THE ENABLERS, THE TOOLS AND SECRECY—VOL. 1 of 4," U.S. Government Publishing Office, accessed October 11, 2015, https://www.gpo.gov/fdsys/pkg/CHRG-109shrg29760/html/CHRG-109shrg29760.htm.
10. "- TAX HAVEN ABUSES: THE ENABLERS, THE TOOLS AND SECRECY—VOL. 1 of 4," U.S. Government Publishing Office, accessed October 11, 2015, https://www.gpo.gov/fdsys/pkg/CHRG-109shrg29760/html/CHRG-109shrg29760.htm.
11. United States v. Neal, Criminal No. CR 03-35-HA (D. Oregon 2003), Criminal Docket.
12. "PlanetGold Interview with Sean Trainor of Crowne Gold," Internet Archive: Wayback Machine, accessed January 11, 2014, https://web.archive.org/web/20020816165353/planetgold.com/interview.asp?SPID=12652563.
13. "Crowne Gold Corporate Data," Internet Archive: Wayback Machine, accessed March 27, 2016, https://web.archive.org/web/20030629143530/www.crowne-gold.com/corpdata.asp.
14. "United States of America V. Sixty-Four 68.5 Lbs. (Approx.) Silver Bars Et Al," United States Courts Archive®, accessed August 21, 2015, https://www.unitedstatescourts.org/federal/flmd/233477/.
15. "Emg | USAO-MDFL | Department of Justice," U.S. Department of Justice, accessed February 14, 2015, http://www.justice.gov/usao-mdfl/emg.
16. "United States of America V. Sixty-Four 68.5 Lbs. (Approx.) Silver Bars Et Al," United States Courts Archive®, accessed August 21, 2015, https://www.unitedstatescourts.org/federal/flmd/233477/.
17. Ibid.
18. Ibid.
19. Ibid.

CHAPTER 6

Liberty Reserve

On May 20, 2013, government prosecutors filed a sealed criminal indictment in New York against Liberty Reserve S.A., a Costa Rican business, and its operators.

United States of America
Liberty Reserve S.A., Arthur Budovsky,
a/k/a "Arthur Belanchuk," a/k/a "Eric Paltz,"
Vladimir Kats,
a/k/a "Ragnar,"
Ahmed Yassine Abdelghani,
a/k/a "Alex,"
Allan Esteban Hidalgo Jimenez,
a/k/a "Allan Garcia,"
Azzeddine El Amine,
Mark Marmilev,
a/k/a "Marko,"
a/k/a "Mark Halls," and
Maxim Chukharev,
Defendants.
Indictment
13 Cr. (18 u. s. c. §§ 1956, 371, 1960 & 2)

Unlike the decade of unregulated digital currency growth from 1996 to 2006, by 2013, US government lawyers and prosecutors had become experts at identifying and prosecuting illegal activity in digital currency

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_6

businesses. This new US prosecutorial experience was very apparent during the Liberty Reserve S.A. case.

On June 6, 2013, the US Government published a notice of finding in *The Federal Register*, indicating that the digital currency company, Liberty Reserve S.A., which had been operating outside the USA, was now a Financial Institution of Primary Money Laundering Concern. (Title 31, Subtitle IV, Chapter 53, Subchapter II § 5318A)[1]

The finding was issued under the authority provided by 31 U.S.C. 5318A. This action, which restricted access to the US financial system, was undertaken to guard the nation against international money-laundering and financial crimes. Public notice, in The Federal Register, also alerted the global financial community to the possible risks and consequences of doing any additional financial business with Liberty Reserve S.A. The notification had virtually halted any further Liberty Reserve S.A. financial activity through foreign banks.

Text from the document stated that the US Department of Justice was engaged in a criminal action against Liberty Reserve S.A. and related individuals. The details included legal matters that government prosecutors would eventually use against Liberty Reserve S.A. It offered a detailed account of the business' financial operation and showed the extent to which Liberty Reserve S.A. had been used to facilitate and promote money laundering.[2]

The May 2013 indictment stated:

> Through the defendants' efforts, Liberty Reserve has emerged as one of the principal means by which cyber-criminals around the world distribute, store, and launder the proceeds of their illegal activity. Indeed, Liberty Reserve has become a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. Because virtually all of Liberty Reserve's business derived from suspected criminal activity, the scope of the defendants' unlawful conduct is staggering.[3]

The text from the indictment tell a story about how carefully the government investigators had labeled, documented, and reported the ongoing illegal activity of Liberty Reserve S.A.:

- Liberty Reserve's system is structured so as to facilitate money laundering and other criminal activity while making any legitimate use economically unreasonable.

- Liberty Reserve seeks out jurisdictions with weak regulatory environments.
- Liberty Reserve is designed to facilitate money laundering and illicit finance.
- Liberty Reserve is regularly used to store, transfer, and launder illicit proceeds.
- Liberty Reserve is not designed for legitimate use.[4]

While Liberty Reserve S.A. "Costa Rica" digital currency is one of the most highly publicized cases involving the US prosecution of a digital currency company, Liberty Reserve digital currency was never an industry leader or important element in the more than a decade of early digital currency development.

Over the ten years spanning 2004–2014, the now imprisoned Liberty Reserve operators had copied and mimicked every other previous digital currency system in the world. Any success or popularity attributed to Liberty Reserve occurred by accident.

With new regulations approaching and the closure of other digital currency businesses, such as e-gold, Liberty Reserve had managed to be the "last man standing." Liberty Reserve's operation took the place of failed and shuttered past digital currencies and filled the void left by recent US prosecutions. In articles and discussions that referenced the government's attempt to eradicate all traces of digital currency in the USA, many bloggers had been using the term "whack-a-mole." This phrase referenced the fact that as one digital currency closed, another popped up to take its place.

Because Liberty Reserve S.A. was functioning after the downfall of e-gold, Liberty Reserve S.A. "Costa Rica" quickly became the most obvious e-gold replacement. In the Internet game of "whack-a-mole," when e-gold got hit, up popped Liberty Reserve S.A. Details contained in the indictment further confirmed this activity.

> LIBERTY RESERVE thereupon grew exponentially, filling the void left by E-Gold and becoming the predominant digital form of money laundering used by cyber-criminals worldwide.[5]

After the closure of Liberty Reserve S.A., the massive group of users still seeking the advantages of an unregulated market migrated over to Perfect Money. In 2016, this digital currency system, now on servers in Iceland,

along with bitcoin cryptocurrency has become the newest successors to the whack-a-mole legacy.

In 2008, Liberty Reserve was not the only option for digital currency users; this system was just a convenient replacement for anyone who required the use of anonymous digital funds.

In any successful digital currency marketplace, liquidity is one of the primary factors that contributes to a broad consumer use. More than 200 liquid third-party Liberty Reserve exchange agents were operating in countries around the world.

The popularity of Liberty Reserve digital currency also produced dozens of "No Id" debit cards that furnished instant access to the cash value of Liberty Reserve's digital units. Hundreds of active exchange agents also connected users with more than a hundred conventional banks around the world. If you needed to buy Liberty Reserve or exchange it for cash, there are many convenient options available.

Throughout the history of Liberty Reserve digital currency, which crossed multiple jurisdictions and included various corporate entities, the operators never succeeded in making any positive advances with their technology. After 15 years of researching Liberty Reserve and the persons who created the digital currency, it can be said that those operating the business were simply in business to make profits; anyway, they could. The fastest path to the unregulated world of online digital currency is catering to the bad actors and criminal users which benefit the most from using anonymous digital currency. That was the targeted group of users sought by Liberty Reserve business.

Background on Liberty Reserve

Any discussion about the rise and fall of Liberty Reserve S.A. requires some additional background information on the previous versions of the company. Many times, throughout its online history, the business grew into new business structures. Like a hermit crab, when a new corporate shell appeared to be a better fit, Liberty Reserve adopted the new corporate entity. Each new structure helped to create a cloudy chain of ownership as the operators moved through various companies and jurisdictions.

In March 2001, one of the oldest independent digital currency exchange agents in the USA, operating from New York State under the name "Goldage Inc.," was raided by agents of the US Secret Service. That business owner had been a man named Parker Bradley, and he, along with

Goldage, was being investigated for credit card fraud. This well-known digital currency exchange business had been accepting credit cards for the online sale of digital currency, such as e-gold. Goldage would receive credit card payments from online retail customers, which were refundable and reversible. After charging the card of the client, Goldage would pay out an amount of digital currency. As digital currency transactions are almost always final and nonrefundable, the scam can be very lucrative if the exchange agent does not catch the card fraud. As it turned out, many of the credit card transactions which occurred through Goldage had been from stolen cards.

A year later in April 2002, Vladimir Kats and Arthur Budovsky purchased Goldage.net from Mr. Bradley. This transaction was labeled "the sale and rebirth of Goldage," within the small digital currency industry. The company had previously been well known as a successful digital currency exchange agent.

Just a month later, in May 2002, a written interview was published on a website named PlanetGold.com. This online portal offered digital currency promotional news and even some precious metals information. Vladimir Kats and Arthur Budovsky operated it. It included a market makers' directory, banner ads, a shopping guide, and links to ancillary digital currency services that would accept digital currency payments.

The title of that May 2002 article was "Interview with Liberty Reserve, Interview with Arthur Budovsky of Liberty Reserve, conducted by Ragnar Danneskjöld, editor, Planetgold.com."[6]

Ragnar Danneskjöld is a fictional pirate character from Ayn Rand's novel *Atlas Shrugged* and a regular alias of Vladimir Kats.

Ragnar, from the Planetgold.com website, was, in fact, Vladimir Kats using the name of Ayn Rand's pirate character as an alias. The two parties in this interview were, Vladimir, talking to his partner, Arthur, promoting a new digital currency they both owned, on a website they both operated behind the scenes. This practice of using phony names, aliases, front companies, and websites would surface many times throughout the Liberty Reserve operation, and the alias names would follow the pair until their arrest. As an example, here is a portion of the 2013 federal indictment from the Southern District of New York listed their names as:

Arthur Bodovsky, a/k/a "Arthur Belanchuk," a/k/a "Eric Paltz,"
Vladimir Kats, a/k/a "Ragnar"[7]

During this 2002 PlanetGold.com interview, Arthur provided these details to Vlad regarding their new digital currency Liberty Reserve. The business launched in May 2002.

> Arthur: Liberty Reserve was originally an escrow service for our private clients engaged mostly in the international import and export business. We have been operating for about three years [since 1999], and only recently decided to expand Liberty Reserve into a digital currency.
>
> In effect, it was our clients who asked us to provide digital currency type services (similar to e-gold). For example, we would see more and more clients simply accumulating money in their escrow accounts and then calling us with instructions to send money to one place or another or to simply debit and credit their accounts between various third party accounts. We were transformed into a stored value type system without even realizing it.[8]

From the first days of Liberty Reserve's operation in 2002, both Arthur and Vlad recognized their service was created to accept incoming funds, store value, and transmit money on behalf of third-party clients. On numerous occasions, both men openly acknowledged Liberty Reserve as a money transmitter, yet never sought a proper license.

During the interview, Vlad, asked his partner, Arthur, the following question identifying that the original Liberty Reserve had originally been formed as an offshore Nevis Corporation. At the time, this small Caribbean nation was also the home for some corporate entities of the e-gold business.

> planetgold [Vlad]: Do you have any legal concerns about this type of business, such as government regulation or invasion of privacy?
>
> Arthur: Since we're based in the Caribbean (Nevis to be exact), we have not to date, nor do we anticipate any sort of problems of that type. We do respect our clients' privacy and only a subpoena served in Nevis would prompt us to consider providing anyone's personal information to a third party. However, since we're not a bank, we don't collect much in the way of personal information anyway. Because we're based in Nevis, you have to be a murderer, kidnapper, or drug kingpin for us to be forced to divulge any sensitive information.[9]

In late 2002, Crowne Gold, which was one of the newer digital gold currencies, was redomiciled from Nevis to Nevada. The reasoning behind this corporate move was a topic of discussion throughout the digital currency industry.

In 2004, the Liberty Reserve website had changed and now stated, "Liberty cash is an electronic currency that will be issued by Liberty Reserve, a Nevada corporation, which will be backed at all times by the Liberty Reserve Trust."[10]

However, at that point, the LibertyReserve.com website displayed a Brooklyn mailbox service in New York as the company's business address.

2106 Bath Avenue, Suite #101
Brooklyn, NY 11214 USA[11]

In February 2005, the Liberty Reserve Account User Agreement was still representing the company's jurisdiction as Nevis.

> 8. Jurisdiction This Account Agreement will be governed by the laws of Nevis as such laws are applied to agreements entered into and to be performed entirely within Nevis by Nevis residents.[12]

In January 2007, an updated website showed Liberty Reserve to be operating from Panama.

> Liberty Reserve is incorporated under the laws of Panama, with offices worldwide, including New York, Germany, and France.[13]

In July 2007, another interview was published between the operator of a digital currency HYIP blog and the Liberty Reserve "marketing manager," Mr. Joul Lee. It was disclosed later in documents that the name Joel Lee was another alias used by Arthur Budovsky. During that interview, Arthur pitched his new Costa Rican company, Liberty Reserve S.A. He stated:

> Customer privacy, security and absolute confidentiality are top priorities for the management and staff at Liberty Reserve. Incorporated in Costa Rica this organization is also a long time member of the Global Digital Currencies Association.[14]

The Global Digital Currencies Association or GDCA was yet another business used primarily by both Vladimir and Arthur. Some good activity occurred through the GDCA, but it was mainly window dressing. This organization was created to give the public an appearance of legitimacy for digital currency businesses and the self-regulated digital currency industry.

The GDCA was essentially a hoax that lasted almost a decade. In 2015, an Internet search of older exchange agent websites still in operation can often yield visible GDCA logos and memberships.

The original GDCA operated from about 2004 to 2008. After 2008, this online organization continued until about 2013. There was never any legitimate email contact, individual names, corporate documents or legal association information, city licenses, or phone number offered to back up the website's claim of legitimacy. From 2002 until 2005, the only address that appeared on the GDCA website was Vladimir's mailbox in Brooklyn:

2106 Bath Avenue, Suite #101
Brooklyn, NY 11214 USA[15]

By October 2007, the Liberty Reserve website presented what would be its final and most famous version of the business. Liberty Reserve S.A. was domiciled in Costa Rica. That same month, another interview emerged with someone named Eric Paltz. The interview stated that he was "…in charge of business planning and development [at LibertyReserve]."[16] The name Eric Paltz turned out to be yet another alias of Arthur Budovsky. The 2013 Liberty Reserve S.A. indictment disclosed this fact.

2006 Goldage Indictment

In the spring of 2006, no existing US financial rules or regulations were defining digital currency or the activity of a digital currency exchange agent. That unregulated and unsupervised market had existed for a decade. However, on July 27, 2006, the Manhattan district attorney's office announced the indictment of two people on charges of operating an illegal money transmittal business.

Here are excerpts from the district attorney's press release:

Goldage.net Indicted
NYC District Attorney New York County, News Release, July 27, 2006
Manhattan District Attorney Robert M. Morgenthau announced today the indictment of two people on charges of operating an illegal money transmittal business. Eight subsidiary businesses operated by the defendants have also been indicted. The indictment charges that the defendants operated an illegal money transmittal business that received and transmitted $4 million between January 1, 2006 and June 30, 2006. The

investigation leading to today's indictment determined that GOLDAGE (www.goldage.net) was set up by BUDOVSKY and KATS in 2002, and at least $30 million was illegally transmitted to accounts worldwide since the start of the defendants' illegal activities. BUDOVSKY and KATS allowed individuals to open accounts at GOLDAGE with limited documentation of identity. The investigation is continuing into the identity of the defendants' customers and the source of customers' funds.

In addition, the district attorney's Office has begun an asset forfeiture action against the defendants in the amount of $2 million.

The indictment charges the defendants with violating the State Banking Law, which makes it a class "E" felony to engage in the business of transmitting money without a license.[17]

The phrase "asset forfeiture" also became an important term to recognize in this case, as more than $2,000,000 was seized from the defendant's businesses by the State of New York and forfeited. Many industry insiders that were not familiar with the term "asset forfeiture" would soon understand that phrase to be an important factor in future prosecutions and digital currency seizures.

The 13-count indictment presented in New York accused the defendants of committing the crime of operating an unlicensed money transmission business in violation of State Banking Law §650(2)(b)(1) The charge had allowed the Supreme Court of New York to approve an order freezing GoldAge financial assets. On September 5, 2006, the court issued this order regarding ($2,091,847.08) of assets.

The action was based on the following attested allegations:

1) defendants are not licensed by the New York State Department of Banking to engage in the business of money transmission and are operating as unlicensed money transmitters (Rosenzweig Supp. Aff. at 11 2);

2) during the period January 2, 2006 to June 30, 2006, Budovsky and Kats utilized the Goldage related entities in a single, systemic business scheme, to illegally receive and transmit $2,091,847.08 via cash deposits, postal orders, wire transfers and checks "into a store value currency known as "E-Gold", in an attempt to hide the source of the money." (Herbert Aff. in Support of TRO at 122, see *also* Rosenzweig Supp. Aff. at 725);

3) bank records revealed that the defendants made thousands of systematic deposits of cash, wire transfers, money orders and personal checks

> received from various individuals and entities (defendants characterize as its retail customers) into Goldage related entities' accounts;
>
> 4) utilizing a "layering" technique, defendants transferred these funds out of these accounts into other accounts;
>
> 5) plaintiff corroborated this illegal money transmission scheme via an undercover operation conducted between March 2, 2006 and June 29, 2006 (Rosenzweig Supp. Aff. at 135); and
>
> 6) Defendants' bank records show a pattern of regular deposits and subsequent withdrawals evidencing an illegal money transfer business (Rosenszweig Supp. Aff. at 7138).[18]

Very few people in the USA had any previous experience with digital currency products or the methods of regulating them. Several digital currency operators asked government agencies for clarification on the Bank Secrecy Act, the operation of a Money Service Business along with the money transmitting regulation. No one in the digital currency industry received accurate or useful guidance, from any source.

After the GoldAge arrests, except Arthur and Vlad, it was business as usual for the entire industry. As more information on the GoldAge case circulated, a few digital-currencies-related companies decided to attempt some random changes such as adding a page of KYC text or some AML language on their exchange agent websites. One popular online business posted lots of arbitrary AML rules including the 40 FATF recommendations from many years earlier. Another agent discussed splitting his US exchange operation into several different corporate entities. One company would only accept national currency for the sale of digital gold and gold coins. While another company would only buy the digital currency and pay out funds. Based on the GoldAge indictment that business operator believed his strategy legally circumvented any need for a money transmitter license. After the arrests, ownership of the following digital currency businesses, and others, was directly linked to Arthur and Vlad.

Cambist.net—http://cambist.net
Asiana Gold—http://asianagold.com
FastGold—http://www.fastgold.net
Cambist.com—http://cambist.net
Flash Funding—http://www.flashfunding.net/
Goldage—http://www.goldage.net
GDCA—http://www.gdcaonline.org

Gold Stores—http://www.goldstores.com
Liberty Impact—http://www.libertyimpact.com
Liberty Reserve—http://libertyreserve.com

This 2006 New York case sent shock waves through the digital currency industry. Never before had there been any indication that US exchange agents would be the target of a state or federal prosecution. Only months later, as many US exchange agents were rethinking corporate structures and financial activity, Arthur Budovsky was busy establishing Liberty Reserve S.A. in sunny Costa Rica.

In 2007, both men pleaded guilty to the New York State charges of operating an illegal money transmittal business, and each received a sentence of five years of probation. There was no jail time for either party. They forfeited more than $2 million in frozen funds to the government.

In July 2007, another person calling himself, Mr. Joul Lee, gave a Liberty Reserve S.A. interview to a popular digital currency blog. In the interview, Mr. Lee detailed the new business features of Liberty Reserve S.A. including some benefits of operating from Central America instead of Brooklyn.

> Liberty Reserve customer funds are protected by an offshore Trust, and at all times accounts are 100% backed by U.S. dollars for LR-USD accounts and gold bullion for LR-gold accounts and Euros for LR-Euro accounts. Customer privacy, security and absolute confidentiality are top priorities for the management and staff at Liberty Reserve. Incorporated in Costa Rica this organization is also a long time member of the Global Digital Currencies Association.
>
> Liberty Reserve is a one-stop, all inclusive, merchant facility where any online business, no matter in which country situated, can accept payments from anyone in the world. Liberty Reserve has exchange providers that accept deposits in Europe, Asia, United States, Australia, Central and Latin America, etc., and the number of agents is growing. LR also does not compete with exchangers by running its own exchange, unlike other digital currencies. This way, 100% of all volume passes via independent exchange providers who have no fear that LR will steal their clients. All this, plus our low rates and superior privacy and friendly jurisdiction is why Liberty Reserve is growing so fast already. It basically sells itself by word of mouth. Within a month, LR will add LR-Gold and LR-Euro.[19]

Even with the new freedom of operating from Latin America, in 2007, the Liberty Reserve Terms of Service Agreement still included familiar

terminology which stated that Liberty Reserve S.A. was not subject to any banking laws.

> 2. Conditions of Use
>
> User acknowledges that (i) Liberty Reserve is not a bank (ii) Liberty Reserve accounts are not insured by any government agency and (iii) Liberty Reserve is not subject to banking regulations.[20]

By late 2007, Liberty Reserve had replaced e-gold as the preferred method of payment for accepting funds on HYIP Ponzi websites. The company's operators were well aware of Liberty Reserve being popular with HYIP schemes. Over the next two years, the Liberty Reserve S.A. global online operation experienced massive growth. Barely three years into the Latin American operation, Costa Rican authorities became aware of the Liberty Reserve digital currency business. In 2009, Costa Rica's Financial Institution Superintendency notified Liberty Reserve S.A. that it needed to apply for a license to operate as a money transmitting business in Costa Rica.[21]

By the end of 2009, Liberty Reserve had applied for the Costa Rican license and been denied. The 2013 US federal indictment of the company stated:

> …but SUGEF refused to grant the application based on concerns that LIBERTY RESERVE did not have even basic anti-money laundering controls in place such as "know your customer" procedures, and otherwise lacked any effective means of tracking suspicious activity within its system.[22]

In a move to try and outwit SUGEF, the Liberty Reserve operators designed a phony online portal that appeared to provide access to supervision over the business and transactional information to Costa Rican authorities. However, it was soon revealed that a majority of the data displayed was fake and manipulated. Phony information was presented to the authorities with the intent of convincing them the company's operation was properly regulated. The operators had concealed the real information that could implicate the company. According to state prosecutor José Pablo González, Liberty Reserve was denied a business license in Costa Rica due to a lack of transparency regarding "how" the company was funded.

In 2011, Arthur renounced his American citizenship.[23] He told US immigration authorities that he was severing ties with the USA because of

concern the "software" his "company" was developing "might open him up to liability in the U.S."[24]

In legal documents, the Costa Rican Prosecutor's Office later stated that both government and law enforcement officials, including the Judicial Investigation Police, had begun a criminal investigation of Liberty Reserve S.A. March 7, 2011. The reason provided for this action was multiple suspicious financial activities previously filed by Costa Rican banks, Banco Nacional and Bancrédito.[25]

At least twice, once during 2011 and once during 2012, Costa Rican officials seized funds from local bank accounts that belonged to Liberty Reserve.[26] In November 2011, the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a notice to its network financial institutions detailing the risks of providing financial services to Liberty Reserve S.A.

The notice stated that: "information obtained by the United States Department of the Treasury indicates LIBERTY RESERVE is …currently being used by criminals to conduct anonymous transactions to move money globally."[27] Several weeks later, the application for a money transmitting license in Costa Rica was withdrawn after Arthur had obtained a copy of the FinCEN notice from a third party. He also falsely informed SUGEF that a foreign entity had purchased the Liberty Reserve business, and his organization would no longer operate the company from Costa Rica. Without the approval of SUGEF, Arthur Budovsky and his associates encountered difficulty in conducting banking business through both Costa Rica and Panama.

While Liberty Reserve purported to close the local office in Costa Rica, they remained in business using scaled down services and a series of shell corporations controlled by Arthur Budovsky. At that time, Arthur, Allan, and Azzeddine El Amine began to transfer the bulk of Liberty Reserve funds held in Costa Rican banks to shell company accounts in Cyprus and Russia. However, because of a request by US law enforcement authorities, at that time the Costa Rican government was able to seize around $19.5 million in Costa Rican bank accounts. In direct reference to this seized $19.5 million from local banks, the May 2013 federal indictment further stated:

> Following that seizure, Budovsky, Hidalgo, and El Amine sought to evade further seizure action by moving Liberty Reserve funds into more than two dozen shell-company accounts held in locations around the world, including Cyprus, Hong Kong, China, Morocco, Australia, and Spain.[28]

The Liberty Reserve S.A. Indictment and Case

United States of America
v.
Liberty Reserve S.A. Arthur Bodovsky,
a/k/a "Arthur Belanchuk," a/k/a "Eric Paltz,"
Vladimir Kats,
a/k/a "Ragnar,"
Ahmed Yassine Abdelghani,
a/k/a "Alex,"
Allan Esteban Hidalgo Jimenez,
a/k/a "Allan Garcia,"
Azzeddine El Amine,
Mark Markilev,
a/k/a "Marko,"
a/k/a "Mark Halls," and
Maxim Chukharev,
Defendants.

In May 2013, after seven years of operating from Costa Rica, the US Department of Justice closed Liberty Reserve S.A. US prosecutors have stated that the Liberty Reserve S.A. case is the largest money-laundering case ever prosecuted in American history and allege that the online system handled $6 billion worth of criminal proceeds.

On May 24, the Liberty Reserve website along with about 50 other sites related to the digital currency business became unavailable. The home page of every former Liberty Reserve website displayed a government warning and seizure notice from the US Global Illicit Financial Team. The five seized domains that had been directly operated by Liberty Reserve were:

Libertyreserve.com;
Exchangezone.com;
Swiftexchanger.com;
Moneycentralmarket.com;
Asianagold.com; and
Eurogoldcash.com.

Pursuant to Title 18, US Code, Section 98l(a)(1)(A), the following domains that had been operated by third-party independent exchange

agents dealing in Liberty Reserve digital currency were also seized and forfeited.

Wm-center.com;
E-naira.com;
Ecardone.com;
Ebuygold.com;
Getemoney.com;
Epaymonster.com;
Instantgoldng.com;
Jtgold.com;
Goldnairaexchange.com;
Superchange.ru;
Webmoney.co.nz;
M-gold.com;
Goldmediator.com;
Absolutexchange.eu;
Mewahgold.com;
Centregold.ca;
Electrumx.com;
Tukarduid.com;
Entelnova.com;
Tacoauthorized.com;
Intexchange.com;
Ukrnetmoney.com;
Wmirk.com;
Nigeriagoldexchanger.com;
Edealspot.com;
Duyduychanger.com;
Magnetic-exchange.com;
Moneyexchange.vn;
Abc-ex.net;
Mi-billetera.com;
Nicceixchange.com;
Exhere.com;
Alertexchanger.com;
Velaexchange.com;
Goldexpay.com.[29]

US Prosecutors were alleging that Liberty Reserve S.A., at the time of closure, had more than one million users worldwide and that around 200,000 of those users resided in the USA.

The indictment noted that at no time had the Liberty Reserve operation registered with the US Department of the Treasury as a money transmitting business, as required by US financial regulations.

Identified as a domestic financial institution which is engaged in business with US customers, Liberty Reserve had been subject to the § 5313 reporting requirements and was also required to register with the Department of the Treasury.

Prosecutors in New York froze and seized 45 bank accounts from countries around the world. Here is a partial list of bank accounts from the forfeiture allegation.

As a result of committing one or more of the offenses alleged in Counts One and Three of this Indictment, the defendants shall forfeit to the USA, pursuant to Title 18, US Code, Section 982(a)(1), all property, real and personal, involved in the offenses and all property traceable to such property, including but not limited to:

A sum of money of at least $6 billion in US currency.

All funds on deposit in the following accounts:

Banco Credito Agricola de Cartago (Costa Rica)
Grupo Mutual Alajuela (Costa Rica)
Banco Lafise (Costa Rica)
Banco BAC San Jose (Costa Rica)
Hellenic Bank (Cyprus)
National Bank of Greece (Cyprus)
Cyprus Development Bank P.C. (Cyprus)
EuroBank EFG (Cyprus)
Sovetsky Bank Zao (Russia)
Bank of Communications (Hong Kong)
Shenzhen Bank (China)
Attijariwafa Bank (Morocco)
Banque Marocaine de Commerce Exterieur (Morocco) Account No.
Barclay's Bank (Spain)
Rietumu Bank (Latvia)
SunTrust Bank

- Up to $36,919,884 on deposit in the following accounts:

Westpac Bank (Australia) Account No. 034702289721, held in Technocash Ltd.;
Westpac Bank (Australia) Account No. 034705205706, held in Technocash Ltd.;
Westpac Bank (Australia) Account No. 034702807875, held in Technocash Ltd.[30]

Unsealed by prosecutors May 28, 2013, Arthur Budovsky was just one of the seven individuals charged in the federal indictment. Law enforcement actions took place across 17 different countries. Liberty Reserve S.A. was investigated by:

- The US Secret Service,
- Internal Revenue Service-Criminal Investigation,
- US Immigration and Customs Enforcement's Homeland Security Investigations, with assistance from the Secret Service's New York Electronic Crimes Task Force,
- The Judicial Investigation Organization in Costa Rica,
- The National High Tech Crime Unit in the Netherlands,
- The Financial and Economic Crime Unit of the Spanish National Police,
- The Cyber Crime Unit at the Swedish National Bureau of Investigation, and
- The Swiss Federal Prosecutor's Office also provided assistance.

The case was prosecuted jointly by:

- The Criminal Division's Asset Forfeiture and Money Laundering Section (AFMLS),
- The US Attorney's Office's Complex Frauds Unit and Asset Forfeiture Unit in the Southern District of New York, and
- The Criminal Division's Office of International Affairs and Computer Crime and Intellectual Property Section.[31]

The indictment alleged that during the past seven years, Liberty Reserve had moved $6 billion in online funds around the globe. The indictment

alleged that a majority of the funds had been the proceeds of criminal activity. The indictment charged Budovsky and his associates with three felony counts:

1. Conspiracy to commit money laundering in violation of 18 U.S.C § 1956(h);
2. Conspiracy to operate an unlicensed money transmission business in violation of 18 U.S.C. § 371; and
3. The operation of an unlicensed money transmission business in violation of 18 U.S.C. § 1960.[32]

Not surprisingly, these charges against Liberty Reserve S.A. were some of the same charges that were used to end the e-gold digital currency operation, just five years earlier.

18 U.S.C.—1956 (Conspiracy to Launder Monetary Instruments);
18 U.S.C.—371 (Conspiracy);
18 U.S.C.—1960 (Operation of Unlicensed Money Transmitting Business);
18 U.S.C.—982(a)(1) (Criminal Forfeiture).[33]

In addition to the e-bullion case, Liberty Reserve S.A. was another digital currency company prosecuted using some of the new rules and regulations from the USA Patriot Act, including Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern.

Arthur Budovsky and another Liberty Reserve officer Azzeddine El Amine had been arrested at Madrid's Barajas International Airport, by Spanish Police, during a connecting flight to Costa Rica. Both men had been held by Spanish authorities pending extradition to the USA. Eager to fight extradition to the USA, after a period in Spanish custody, authorities in Spain dropped all charges and released Arthur into the waiting arms of US agents. He was put on a plane to the USA. After the release, Arthur's lawyer claimed the extradition was a breach of Spanish and international law.[34]

Local police had also raided three homes in Costa Rica and seized half a dozen corporations used in the Liberty Reserve business, classified by authorities as "shell corporations." Other men charged in the indictment had been arrested in New York and Costa Rica at the same time. Arthur's

longtime friend and business associate was arrested in Brooklyn. Vladimir Kats's name also appeared on the federal indictment. Two of the men listed in the indictment, who resided in Costa Rica, could not be located and remained at large. The charges against Liberty Reserve S.A. and the seven individuals were made using provisions of the USA Patriot Act.

> The United States Attorney in Manhattan, Preet Bharara, stated that the unlicensed Liberty Reserve had processed an estimated 55 million separate financial transactions. He further contended that some of the transactions were directly linked to crimes including credit card fraud, identity theft, investment fraud, computer hacking, child pornography and narcotics trafficking.[35]
>
> One specific allegation of the prosecutors is that the site played a role in laundering the $45 million stolen from the Bank of Muscat and the National Bank of Ras Al Khaimah in May 2013.[36]

In addition to the felony charges related to Liberty Reserve S.A., prosecutors also stated that in 2002 Vladimir Kats entered into a phony New York State marriage to help a woman fraudulently obtain US citizenship. He was also found guilty of downloading child pornography from the Internet.

The operation's business model also reflected a level of secrecy surrounding the identities of users. Paying a 1 percent fee, users of Liberty Reserve could conduct transactions with other users. But for an additional "privacy fee" of 75 cents, the user's account number could be hidden, "effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system," the indictment stated. The company also relocated its network servers—as many as seven—from Costa Rica to the Netherlands, Switzerland, and other countries, a source said. Tuesday, an announcement finally appeared on LibertyReserve.com: "This domain name has been seized by the United States Global Illicit Financial Team." There were seven men charged in the Liberty Reserve S.A. case. The primary defendants are listed here:

- Arthur Bodovsky, a/k/a "Arthur Belanchuk," a/k/a "Eric Paltz," was charged under several statutes with creating and operating an unlicensed money transmitting business designed to facilitate illegal financial transactions and launder criminal proceeds. He was the principal founder of the Liberty Reserve operation. The May 2013 indictment alleged that Arthur had designed the Liberty Reserve operation to help criminals conduct illegal transactions and launder

the proceeds of their crimes. Furthermore, by offering anonymous and untraceable financial activity, Liberty Reserve had deliberately attracted and maintained a customer base of criminals. In 2016, Arthur is still awaiting trial in New York.

- Vladimir Kats, a/k/a "Ragnar," was the co-founder of Liberty Reserve-directed company operations until 2009. He returned to the USA in 2009. He also ran multiple exchange agents that serviced Liberty Reserve digital currency. Vlad was charged with multiple felonies. His case included the following:

Count: 1 Citation: 18:1956-4999.F Offense Level: 4
18:1956-4999.F Money Laundering—Fraud, Other (Conspiracy)
Count: 2 Citation: 18:371.F Offense Level: 4
18:371.F (Conspiracy to Operate an Unlicensed Money Transmitting Business)
Count: 3 Citation: 18:1960.F Offense Level: 4
18:1960.F Monetary Laundering (Operating an Unlicensed Money Transmitting Business)
Count: 1s Citation: 18:1956-4999.F Offense Level: 4
18:1956-4999.F Money Laundering—Fraud, Other (Conspiracy)
Count: 2s Citation: 18:371.F Offense Level: 4
Conspiracy to Operate Unlicensed Money Transmitting Business
Count: 3s Citation: 18:1960.F Offense Level: 4
18:1960.F Monetary Laundering (Operation of Unlicensed Money Transmitting Business)
Count: 1ss Citation: 18:1956-4999.F Offense Level: 4
18:1956-4999.F Money Laundering Conspiracy
Count: 2ss Citation: 18:371.F Offense Level: 4
18:371. F Conspiracy to Operate Unlicensed Money Transmitting Business
Count: 3ss Citation: 18:1960.F Offense Level: 4
18:1960.F Operation of Unlicensed Money Transmitting Business
Count: 4ss Citation: 18:2252A.F Offense Level: 4
18:2252A. F Receipt of Child Pornography
Count: 5ss Citation: 8:1325.F Offense Level: 4
8:1325.F Marriage Fraud

On October 31, 2013, Vladimir Kats pleaded guilty to one count of conspiring to commit money laundering, which carries a maximum sen-

tence of 20 years in prison; one count of conspiring to operate an unlicensed money transmitting business, which carries a maximum sentence of five years in prison; one count of operating an unlicensed money transmitting business, which carries a maximum sentence of five years in prison; one count of receiving child pornography, which carries a maximum sentence of 40 years in prison and a mandatory minimum sentence of 15 years in prison; and one count of marriage fraud, which carries a maximum sentence of five years in prison. Vladimir will likely testify against Arthur, and Vladimir's sentencing has been postponed.[37]

In separate court documents filed in January 2016, it was made public that Vladimir Kats had pleaded guilty under a cooperation agreement with the government. He has agreed to help the government's prosecution and expected to testify against his former partner Author Budovsky. As noted in this letter to the judge from the lead prosecutor, Vladimir's cooperation as a government witness is ongoing.

January 13, 2016
Hon. Denise L. Cote
United States District Judge
Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
Re: *United States v. Vladimir Kats*, S6 13 Cr. 368 (DLC)
Dear Judge Cote:

On October 31, 2013, defendant Vladimir Kats pleaded guilty to the above-referenced information pursuant to a cooperation agreement. Pursuant to an order of the Court requiring the Government to provide an update on Kats' status, the Government writes to report that Kats' cooperation remains ongoing. As the Court is aware, the lead defendant in the case, Arthur Budovsky, is pending trial scheduled for February 2016. Kats is expected to testify as a Government witness against him. Kats' cooperation is therefore not expected to be completed until the case against Budovsky has been resolved. In light of the foregoing, the Government respectfully requests that no sentencing date be scheduled for Kats at this time. The Government will plan to ask the Court to set a sentencing date for Kats following the conclusion of Budovsky's trial.

Respectfully,
PREET BHARARA
United States Attorney[38]

- Mark Marmilev, a/k/a "Marko," a/k/a "Mark Halls," was a citizen of Russia and resident of Costa Rica; Maxim Chukharev was also a close associate of Arthur Budovsky and responsible for designing and maintaining Liberty Reserve's technological infrastructure. He was arrested in San Jose, Costa Rica, in May 2013. On Sept. 11, 2014, the former chief technology officer of Liberty Reserve pleaded guilty in a Manhattan federal court to one count of conspiring to operate an unlicensed money transmitting business that failed to comply with federal registration requirements while being aware that the transmission of funds was derived from criminal activity. The felony conviction carried a maximum sentence of five years in prison. On Dec. 12, 2014, Mark Marmilev, was sentenced to five years in prison.
- Since 2010, Azzeddine El Amine operated an exchange agent that serviced Liberty Reserve digital currency. On Aug. 14, 2014, Azzeddine El Amine pleaded guilty in a Manhattan federal court to one count of conspiring to commit money laundering, which carries a maximum sentence of 20 years in prison; one count of conspiring to operate an unlicensed money transmitting business, which carries a maximum sentence of five years in prison; and one count of operating an unlicensed money transmitting business, which carries a maximum sentence of five years in prison. In January 2016, he is awaiting sentencing.

On June 23, 2015, from his jail cell, defendant Arthur Budovsky and his attorneys filed with the US District Court in New York requesting to dismiss the government's May 2013 indictment. Not surprisingly, many of the arguments offered by the Budovsky legal team were identical to the arguments made by previous digital currency operators and exchange agents during the years 1996 through 2006.

In the request for dismissal, Budovsky was again trying to reason that Liberty Reserve did not require licensing because digital currency or virtual currency was not money. The document included the following statements made by Budovsky's attorneys.

- …the transmission of a virtual currency falls outside the scope of § 1960 in Count Three because virtual currencies are not "funds."
- …virtual currencies are not "monetary instruments" and thus transactions in virtual currencies are not "financial transactions."

- …argues that because LR[digital currency unit] does not qualify as a "monetary instrument,"
- Budovsky argues that Congress could not have intended for virtual currencies to be "funds" under § 1956 because virtual currencies did not exist when the money laundering statute was enacted.[39]

The court's response even referenced the 2008 e-gold case.

> United States V. E-Gold, Ltd., 550 F.Supp.2d 82, 94-97 (D.D.C. 2008) (holding that virtual currency services are subject to FinCEN regulations under §§ 5330 and 5313).[40]

On September 23, 2015, District Judge Denise Cote denied Arthur Budovsky's motion to dismiss. In January 2016, this case continues to be prosecuted.

Notes

1. "31 US Code § 5318A—Special Measures for Jurisdictions, Financial Institutions, International Transactions, or Types of Accounts of Primary Money Laundering Concern | US Law," LII / Legal Information Institute, accessed March 27, 2016, https://www.law.cornell.edu/uscode/text/31/5318A.
2. "Federal Register | Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern," Federal Register, accessed March 27, 2016, https://www.federalregister.gov/articles/2013/06/06/2013-12944/notice-of-finding-that-liberty-reserve-sa-is-a-financial-institution-of-primary-money-laundering.
3. "United States of America v. Liberty Reserve S.A," U.S. Department of Justice, accessed May 8, 201, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted_0.pdf.
4. Ibid.
5. Ibid.
6. "PlanetGold Interview with Liberty Reserve," Internet Archive: Wayback Machine, accessed January 31, 2015, http://web.archive.org/web/20030416025128/planetgold.com/interview.asp?SPID=08248138.

7. "United States of America v. Liberty Reserve S.A," U.S. Department of Justice, accessed May 8, 201, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted_0.pdf.
8. "PlanetGold Interview with Liberty Reserve," Internet Archive: Wayback Machine, accessed January 31, 2015, http://web.archive.org/web/20030416025128/planetgold.com/interview.asp?SPID=08248138.
9. Ibid.
10. "Liberty Reserve," Internet Archive: Wayback Machine, accessed March27,2016,https://web.archive.org/web/20040401112631/libertyreserve.com/About/About.asp.
11. "Liberty Reserve—DGC Wiki," Home—DGC Wiki, accessed March 27, 2016, http://dgc.wikifoundry.com/page/Liberty+Reserve.
12. Ibid.
13. Ibid.
14. Ibid.
15. Ibid.
16. "Protect Gold—High Yield Investment Money Making Programs Monitor: Interview with Eric Paltz, Founder of LibertyReserve," Protect Gold—High Yield Investment Money Making Programs Monitor, accessed March 27, 2016, http://protectgold.blogspot.com/2007/10/interview-with-eric-paltz-founder-of.html.
17. "Goldage and Cambist, Shutdown!" Cannabis.com—The World's Cannabis Site, accessed March 27, 2016, http://boards.cannabis.com/threads/goldage-and-cambist-shutdown.78233/.
18. "Non-final Disposition," Supreme Court of the State of New York, New York County, last modified September 13, 2006, http://decisions.courts.state.ny.us/fcas/FCAS_docs/2006SEP/300402970200615CIV.PDF.
19. "Liberty Reserve—Interview with Mr. Joul Lee Pt.1," Internet Archive: Wayback Machine, accessed March 27, 2016, https://web.archive.org/web/20071012233507/www.digitalmoney-world.com/liberty-reserve-interview-with-mr-joul-lee-pt1/.
20. "Liberty Reserve Terms of Service," Internet Archive: Wayback Machine, accessed April 25, 2015, https://web.archive.org/web/20071010112847/www.libertyreserve.com/en/terms_of_service/.

21. "Costa Rican President Chinchilla Denies Link to Liberty Reserve Attorney—The Tico Times," The Tico Times, accessed March 27, 2016, http://www.ticotimes.net/2013/05/30/costa-rican-president-chinchilla-denies-link-to-liberty-reserve-attorney.
22. "United States of America v. Liberty Reserve S.A," U.S. Department of Justice, accessed May 8, 201, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted_0.pdf.
23. "Liberty Reserve: A Cyberweb of Intrigue -The Tico Times," The Tico Times, accessed October 20, 2015, http://www.ticotimes.net/2013/05/27/liberty-reserve-a-cyberweb-of-intrigue.
24. "Liberty Reserve Founder Extradited from Spain | OPA | Department of Justice," U.S. Department of Justice, accessed February11,2015,http://www.justice.gov/opa/pr/liberty-reserve-founder-extradited-spain.
25. "Costa Rican President Chinchilla Denies Link to Liberty Reserve Attorney—The Tico Times," The Tico Times, accessed March 27, 2016, http://www.ticotimes.net/2013/05/30/costa-rican-president-chinchilla-denies-link-to-liberty-reserve-attorney.
26. Ibid.
27. "United States of America v. Liberty Reserve S.A," U.S. Department of Justice, accessed May 8, 201, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted_0.pdf.
28. Ibid.
29. "Verified Complaint," U.S. Department of Justice, last modified May 28, 2013, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve,%20et%20al.%20Related%20Exchanger%20Website%20Domain%20Names%20Redacted%20Filed%20Complaint%2013CV3565%20final%20with%20exhibits.pdf.
30. "Full Text of "Liberty Reserve Indictment"," Internet Archive: Digital Library of Free Books, Movies, Music & Wayback Machine, accessed April 9, 2015, https://archive.org/stream/704540-liberty-reserve-indictment/704540-liberty-reserve-indictment_djvu.txt.
31. "Liberty Reserve Founder Extradited from Spain | OPA | Department of Justice," U.S. Department of Justice, accessed

February 11, 2015, http://www.justice.gov/opa/pr/liberty-reserve-founder-extradited-spain.
32. Ibid.
33. Indictment, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241.
34. "Liberty Reserve Founder Budovsky Extradited to U.S. From Spain," WSJ, accessed March 27, 2016, http://www.wsj.com/articles/liberty-reserve-founder-budovsky-extradited-to-u-s-from-spain-1412974424.
35. "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme | USAO-SDNY | Department of Justice," U.S. Department of Justice, accessed August 21, 2015, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.
36. "In Hours, Thieves Took $45 Million in A.T.M. Scheme—The New York Times," The New York Times—Breaking News, World News & Multimedia, accessed March 27, 2016, http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=0.
37. "Full Text of "Liberty Reserve Indictment" ", Internet Archive: Digital Library of Free Books, Movies, Music & Wayback Machine, accessed April 9, 2015, https://archive.org/stream/704540-liberty-reserve-indictment/704540-liberty-reserve-indictment_djvu.txt.
38. "USA V. Kats Et Al Docket Item 250," United States Courts Archive®, accessed January 21, 2016, https://www.unitedstates-courts.org/federal/nysd/412082/250-0.html.
39. "U.S. V. Budovsky by Denise Cote, District Judge | Leagle.com," Leagle.com | A Leading Provider of Copies of Primary Caselaw from All Federal Courts and All State Higher Courts, accessed January 12, 2015, http://www.leagle.com/decision/In%20FDCO%2020150924C30/U.S.%20v.%20Budovsky.
40. Ibid.

CHAPTER 7

IntGold

Another digital currency that operated from 2003 until 2005 was IntGold. The platform offered prepaid debit cards linked to IntGold digital currency accounts. After the IntGold website had opened in February 2003, its index page advertised that all IntGold accounts were 100 percent backed by gold. However, after just a few months, the artwork and text that had detailed the 100 percent gold backing suddenly disappeared from the website. From that day forward, there was no further mention of any IntGold precious metal.

Because many exchange agents accepted IntGold, the company's debit cards gained popularity with digital currency users. Any digital currency platform that offered convenient access to cash through an ATM debit card was popular with digital currency users. Any digital currency system, with the linked ATM card, did not need widespread use or merchant acceptance of its underlying digital currency brand. Users exchanged substantial amounts of other digital currencies into IntGold accounts and accessed ATM cash with the IntGold card. The deposits and transactions generated by this out-exchange activity could have quickly built a profitable and growing IntGold digital currency operation. If merchants across the Internet were not yet accepting IntGold, it would not have slowed the growth of IntGold debit card accounts.

Depositing funds into IntGold through the exchange with other brand currencies became a natural outlet for value moving from digital to national currency. Through a third-party exchange agent, just about any

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_7

other modern digital currency could have been swapped for IntGold and its value then moved on to a prepaid card.

Internet Gold Inc., known as IntGold, was incorporated in the State of Texas and launched in February 2003. Greenville, Texas, was the company's headquarters. Serving as CEO, Mr. Michael C. Comer established and operated the business.

Michael Comer also worked the website responsible for INGoldCards. Internet Gold Inc. was the sole owner of the INGoldCard ATM debit card system. The software platform linked each stored value ATM debit card to an IntGold digital currency account. The cards provided customer access to the value stored in online digital IntGold accounts. The INGold debit card platform operated from the domain www.ingoldcard.com. This card program also accepted deposits from IntGold other brands of digital currencies such as e-gold.

IntGold functioned as an exchange point and deposit location for a variety of digital currency and national money methods of payment. There were about a dozen possible exchange agents that accepted and facilitated the transfer of IntGold into national currency and other digital currencies. The 2005 list of independent third-party exchange agents for IntGold includes the 11 agents shown here:

1. Gold Now http://www.goldnow.st
2. Gold-Trader http://goldtrader.com
3. GoldEx http://www.goldex.net
4. Pay By Gold http://www.paybygold.com
5. AnyGoldNow http://www.anygoldnow.com
6. Goldage http://www.goldage.net
7. Fast Gold http://www.fastgold.net
8. Instant Gold http://www.instantgold.net
9. X-Changers http://www.x-changers.com
10. London Gold Exchange http://www.londongoldexchange.com
11. Gold-Cash Exchange http://www.gold-cash.biz[1]

Through these IntGold website listings, exchange agents benefited from the added advertising and promotion. IntGold had a significant difference from both e-gold and e-bullion. While e-gold had used OmniPay as the operation's primary exchange agent and e-bullion had used Goldfinger Coin & Bullion for deposit and withdrawal activity, IntGold had acted

as the main exchange facility. Customer deposits and withdrawals moved directly from the company bank account.

All incoming deposits by cashier's check or money order were made payable to IntGold and received at the enterprise address: IntGold, 3931 Joe Ramsey Blvd Ste. # C, Greenville, Texas 75401. According to legal documents, all of these incoming funds were deposited into just the one company bank account at Bank of America.

Through INGold, Michael Comer had offered multiple types of debit card products and various card programs. The most popular INGoldCard, linked to a digital currency account, was issued on the MasterCard network. Account holders could use this debit card for ATM cash withdrawals, retail point of sale transactions, and online purchases.

The INGoldCard network also served as a debit card marketing program. Bulk card packages were available for digital currency businesses. Mr. Comer gave volume discounts, permitted mass payments over the network (Batch Pay), and paid commission referral fees. The company distributed cards through an INGoldCard Internet Business Package or corporate card program. Agent income, generated through commissions and fees, was advertised as "monthly residual income." This program was available for any agent able and willing to operate an independent stored value debit card program. At least one large digital currency exchange agent issued INGoldCard ATM debit cards. Patrick Verbeeck of AnyGoldNow issued cards through GoldtoCard LLC.

The business of operating an exchange agent required not only liquid cash assets but also active and consistent sources of cheap digital currency. Making a profit at buying and selling digital gold currency required cheap sources of digital gold which could be marked up and sold at a profit. For any significant exchange agent, there was no better consistent source of cheap, below market priced, digital gold than the incoming deposits of ATM debit card holders. As the operator of an ATM debit card program, the exchange agent received weekly digital currency deposits from card holders. This incoming digital currency was then marked up and sold to other exchange agent buyers. Active digital currency cards also generated healthy card loading and transaction fees.

A bulk card business package consisted of an operator's primary funding account and multiple sub-accounts. Each sub-account was a stored value customer card. Once a day the program operator would submit a bulk payment spreadsheet which moved funds from the one primary account into hundreds or thousands of client sub-accounts.

Retail customer deposits to these cards were made using a variety of digital currencies such as e-gold, e-bullion, EvoCash, GoldMoney, IntGold, and NetPay. These card programs also offered a generous sign-up referral fee to participating IntGold account holders and INGoldCard users. The individual or business entity operating an INGoldCard bulk card or corporate card program was not required to disclose the owner's corporate or personal identity. The card did not contain operator's name, nor did it appear in the encrypted data on the card's magnetic stripe. Additionally, the operator's name was not discoverable from the transaction lists or online statements. According to the company's website, the business package provided a high degree of privacy for the program operator and the card holders because of "nondisclosure regulations."[2] Despite being contrary to US laws designed for greater supervision and reporting of US prepaid card activity, INGoldCard's method of privately operating a debit card program was widely advertised.

The IntGold 2005 user agreement also contained some familiar statements declaring that the business was not a bank. Agreements and documents used by all other digital currency companies such as e-gold, e-bullion, and GoldMoney contained similar language.

User agreement (2005)

Definition of IntGold service

Under International Banking legislation, IntGold is not a bank or to be used as a bank, but an Internet Online payment system. The account holder agrees that IntGold is the following:

IntGold is not a bank or banking service

IntGold is not subject to banking regulations[3]

The company had not registered with FinCEN and held no money transmitter license in any US State.

In 2005, dozens of complaints from IntGold users began appearing on discussion forums and blogs related to digital currency. These websites had warnings about using IntGold including closed accounts, frozen funds, and an inability to withdraw money. Two of the many popular complaint sites were www.intgoldsucks.com and www.intgoldsux.com. IntGold was found to be accepting funds on behalf of multiple investment scams including Your Money Machine Success System—YMMSS (Kim Inman)—and IT4US, International Trading.

In late 2005, several Internet fraud lists had posted warnings about IntGold, and a majority of third-party exchange agents no longer accepted any IntGold transactions. During November and early December, depos-

its to INGoldCards and withdrawals from IntGold were not completed, and checks mailed to customers from IntGold had been bouncing.

On Saturday, December 17, 2005, reporter Brad Kellar, from the *Herald-Banner* in Greenville, Texas, published an article that detailed a federal raid on the IntGold offices. The article stated that on Friday, December 16, federal authorities, including agents from the FBI and US Secret Service, had served a search warrant on the IntGold offices. The article also quoted a local police chief as stating this had been an active investigation for more than a year. At that time in December 2005, no one was arrested.

Years later, in March 2008, operator Michael Comer pleaded guilty to two counts in Case 3:08-cr-00085-N. The following Information came from documents filed in federal court on March 28, 2008. The documents indicated that there had not been a grand jury.

COUNT ONE

Operating an Unlicensed Money Transmitting Business (A violation of 18 U.S.C. § 1960(a) and (b)(l)(B))

From on or about February 12, 2003, until on or about December 16, 2005, in the Northern District of Texas and elsewhere, the defendant, Michael Comer, did unlawfully and knowingly conduct, control, manage, supervise, direct, and own all or a part of an unlicensed money transmission business that affected interstate or foreign commerce, to wit: defendant Comer did knowingly conduct, control, manage direct and own all or a part of Internet Gold, Inc., which transferred funds on behalf of the public by means including but not limited to wire transfers within the United States, and which failed to comply with the money transmitting registration requirements under Title 31 United States Code, Section 5330, and regulations prescribed thereunder. All in violation of 18 U.S.C. § 1960(a) and (b)(l)(B).

COUNT TWO

Forfeiture Allegation [18 U.S.C. § 982(a)(l)]

As detailed in the legal documents, Mr. Comer had previously been cooperative with the government during his investigation. His name also surfaces on government documents in other unrelated court cases. Facing significant monetary and legal challenges, Michael Comer agreed to a Waiver of Indictment. Also filed March 28, 2008, the Waiver of Indictment was consent for his case to be prosecuted by Information and not presented to a grand jury. Included was a signed plea agreement between the gov-

ernment and Michael Comer conceding his guilt and forfeiting the listed assets. The document stated:

> 2. Waiver of rights and plea of guilty: Comer waives these rights and pleads guilty to the offense alleged in Count One of the Information, charging a violation of 18 U.S.C. § 1960, Conducting an Unlicensed Money Transmitting Business.

Court documents also indicated that Michael Comer would aid the government in investigating and prosecuting others involved in the activity of IntGold and any legal issues surrounding this case.

> Defendant's cooperation: Comer shall cooperate with the government by giving truthful and complete information and/or testimony concerning his participation in the offense of conviction and his knowledge of the criminal activities of others.

The guilty plea included recommended sentencing.

> 4. Sentencing Following a Rule ll(c)(l)(C) Plea: Pursuant to Federal Rule of Criminal Rule 1l(e)(l)(C), the government and the defendant agree that the imposition of a sentence of a term of imprisonment of eighteen months, to be followed by a term of supervised release of three years, the first six months of which would be on home confinement, and restitution would be the appropriate disposition of this case…

Michael Comer forfeited a long list of personal assets in the court agreement. As reported in documents, the total value cash assets were approximate $1,442,000. The list included other property such as a car and two houses. When IntGold was shut down by the government, there were approximately 300,000 accounts. Because the company had been openly experiencing problems leading up to the time of its closure, only around 25,000 accounts were still active with balances. On December 16, 2005, the total cash balance of those accounts equaled more than $3,000,000. **From the factual resume

In April 2008, a nearby Dallas-based prepaid card company, also involved in the digital currency industry, named Virtual Money Inc. (VMI) was seized by agents of the federal government. Third-party exchange agents had also been loading the VMI prepaid cards using digital currency. Federal prosecutors charged the VMI owners and company with

Laundering of Monetary Instruments and Conspiracy to Launder Money. Court documents showed that funds moving through the company had been the proceeds of drug trafficking. Approximately $7 million had been loaded onto the VMI stored value cards in the USA and withdrawn in cash from ATMs in Medellin, Colombia (3:08-cr-00097-MRK-1 USA v. Hodgins et al.).

A year later in 2009, court documents indicated that Michael Comer was sentenced to 18 months in prison, a $100 court assessment, three years of supervised release, restitution, and the previous forfeiture of assets.

From 2000 through 2008, dozens of prepaid debit cards, stored value cards, and virtual card products crowded the digital currency industry. No card program that was loaded using digital currency operated for more than a short time except the e-bullion card.

In 2011, FinCEN created strict new US regulations governing the sale and use of digital currency, stored value products, and prepaid cards. The combined use of digital currency and prepaid cards, along with the cross-border movement of funds through stored value networks for more than a decade, had been a focus of these new regulations.

July 2011

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

31 CFR Parts 1010 and 1022

RIN 1506-AB07

Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Final rule.

SUMMARY: FinCEN is issuing this final rule to amend the Bank Secrecy Act (BSA) regulations applicable to Money Services Businesses (MSB) with regard to stored value. More specifically, this final rule amends the regulations by: renaming stored value as prepaid access and defining that term; deleting the terms issuer and redeemer of stored value; imposing suspicious activity reporting, customer information and transaction information recordkeeping requirements on both providers and sellers of prepaid access, and, additionally, a registration requirement on providers only; and exempting certain categories of prepaid access products and services posing lower risks of money laundering and terrorist financing from certain requirements. These changes address regulatory gaps that have resulted from the proliferation of prepaid innovations over the last twelve years and their increasing use as an accepted payment method.[4]

Notes

1. "INT Gold—User Agreement," Internet Archive: Wayback Machine, accessed March 27, 2016, http://web.archive.org/web/20050113180212/intgold.com/m/agreement.cgi/10000
2. "INTERNET GOLD—Prepaid Cash Cards," Internet Archive: Wayback Machine, accessed March 27, 2016, http://web.archive.org/web/20030621160057/www.ingoldcard.com/docs/about-us.htm
3. "INT Gold—User Agreement," Internet Archive: Wayback Machine, accessed March 27, 2016, http://web.archive.org/web/20050113180212/intgold.com/m/agreement.cgi/10000
4. "Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access," FinCEN.gov, accessed January 10, 2016, https://www.fincen.gov/statutes_regs/frn/pdf/Prepaid:Final_7-22-201.pdf

CHAPTER 8

OSGold

The trick to operating a successful Ponzi scheme is to have collaborators who will provide the scam credibility. With outside credibility, that Ponzi functions under the pretense that it is somehow a legitimate paying opportunity. This authority and credibility should then attract additional new investments.

Online Ponzi schemes do not grow because of the operator's individual promotional skills. Spreading the false message of HYIP profit, through a digital currency Ponzi schemes require many helpers. HYIP schemes grow because the greedy, ignorant, and desperate initial program investors quickly tell others of their successful investment.

As occurred in the OSOpps Ponzi, a program's shills are compensated with a referral fee each time a new victim signs up. Anyone acting as a shill can create a website for the active promotion of HYIP scams. These websites and forums earn a substantial income through HYIP referrals.

Many uninformed public visitors are led to believe these investment programs are authentic.

However, in the history of the Internet, there has never been a legal or legitimate HYIP program powered by digital currency. Recidivist scam operators will always use digital currency for a Ponzi scam because the payment company cannot reverse the transaction and those operating the accounts can easily conceal their legal identity. One Ponzi scheme that illustrates the size and scope of digital currency use in online HYIP scams is the case of 12DailyPro.com.

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_8

StormPay Example

In 2002, a man named John R. McConnel, Jr. living in Clarksville, Tennessee, created an online payment processor called StormPay. StormPay received direct bank payments from customer bank accounts and credit cards. In exchange for these national currency deposits, users would receive StormPay digital credits into an online account.

While StormPay was a licensed online payment processor similar to PayPal, the StormPay digital units were being exchanged through third-party agents for other digital currencies. Digital units were being "cashed out" without going back through the original issuer. This was a bank payment processor being used as a digital currency.

As users created profit through online pyramid and MLM scams using StormPay, those units could then be exchanged into another digital currency, such as e-gold, and quickly sold by any third-party exchange agent.

In 2005 and early 2006, StormPay had been processing payments for an online "paid autosurf program," named 12DailyPro, which in reality was a massive Ponzi scheme. During the ten-month period ending in February 2006, 12DailyPro had raised more than $500 million from approximately 175,000 investors around the world through investments in sizes ranging from $6 to $6000.[1] This scheme promised a return of 44 percent in just 12 days. It was one of the largest online Ponzi schemes in the history of the Internet, and in addition to StormPay, the scheme had used several other digital currencies. More than 300,000 investors were ultimately involved with 12DailyPro.com. During the program's operation, the 12DailyPro website was ranked as the 352nd most heavily trafficked website in the world.[2]

Eventually, in February 2006, the Securities and Exchange Commission put a stop to the scam. However, during the prior six weeks, StormPay had processed tens of millions of dollars in credit card and bank deposits for 12DailyPro members. As a result of the SEC action, StormPay froze approximately $50 million of customer Ponzi deposits processed through the StormPay platform. Additionally, many of those StormPay customers had also reversed their charges through the card companies and were in the process of filing complaints against StormPay. The Better Business Bureau released these statements in February 2006:

> "The Better Business Bureau of Middle Tennessee alerts the public to the business practices of StormPay.com of Clarksville, Tennessee. During the

> first six weeks of 2006, StormPay.com has generated more complaints to BBB than any other Middle Tennessee or Southern Kentucky business. In the past seven days, BBB has received 18,926 inquiries from consumers around the world checking on the reliability of StormPay.com. On February 16, 2006, BBB discontinued processing complaints with the company due to the company's failure to respond to complaint volume."[3]

The SEC complaint had alleged that the 12DailyPro sale membership units constituted the fraudulent unregistered sale of securities under the federal securities laws. It is illegal in America to sell unregistered investments through any means of solicitation including over the Internet.

On March 1, 2006, the SEC obtained permanent injunctions and other relief against 12DailyPro in an alleged Internet-based fraud and Ponzi scheme. This program is a classic example of why HYIP scheme operators use digital currency for the method of accepting payments in online scams and not bank cards or consumer protected bank products. Any HYIP Ponzi that uses only digital currency products has no worries about the reversal of payments. In 2006, during the 12DailyPro Ponzi scheme, there were no consumer protection regulations for non-bank privately issued digital currency products. In 2016, there are not yet any US consumer protection rules in place for privately issued, non-reversible digital currency payments such as bitcoin.

A Time of Acceptance

From 1996 until late 2006, the consequences of a digital currency industry unrestricted by all existing financial regulations had allowed any person in the world to register a domain and operate an international digital currency business. New Internet technology had provided the freedom to engage in financial business outside of highly regulated banks.

This new Internet freedom allowed a person residing in one jurisdiction to circumvent easily any local financial regulations and virtually do business from any other country in the world. Financial regulations in one jurisdiction could be overcome using foreign corporate registrations, proxies, and false or misleading information. Anyone in Russia, China, or even North Carolina could create an online digital currency empire registered through a foreign corporation.

The period 2001–2004 was a prosperous and spirited time for new digital currency systems and payment products. A rapidly expanding online

consumer marketplace was slowly gaining deeper penetration into distant new population centers. Millions of new Internet users came online during those years. Additionally, because of limited access to conventional banks in places around the world, many these new users had no previous experience with financial services, banks, or payment products.

Many of these new users were attracted to emerging digital currency products.

Brand-new non-bank Internet users quickly understood the benefits of digital currency. This group of users was eager to adopt digital currency as a bank replacement and method of payment. Non-bank digital currency financially connected millions of people and businesses that previously lacked access to any personal banking and financial tools. Because of the bullish momentum created by new digital currency users, from 2001 through 2005 the unregulated digital currency marketplace also became ground zero for online HYIP Ponzi scams.

The legitimate advantages created by unregulated digital currency were only surpassed by the opportunities afforded to those bad actors willing to exploit the new technology. Online criminals, willing to take full advantage of digital currency features, were one of the first largest groups of users attracted to these new financial tools.

An illegal online business can effortlessly access global customers and operate from any jurisdiction. Over the Internet, an unlicensed financial entity can quietly access foreign markets and solicit investments and new customers without worrying about government supervision or the influences of regulatory agencies. Research shows that often there is a pattern involved with a majority of these operations. Many of these unscrupulous individuals, who are engaged in online scams, will have the same modus operandi. They will form a paper company or entity over the Internet, through a jurisdiction recognized by a lack of government supervision. The operators will locate the scam's website and data servers in yet in another distant external data center. Additionally, the scheme's bank accounts should be remotely opened in a third foreign jurisdiction. Lastly, the physical location of the operators should be in another distant, separate, and secure jurisdiction. It is advantageous for criminals and bad actors to spread their operations across multiple foreign jurisdictions. This arrangement makes any future investigation into the scam harder for law enforcement. The sheer effort required to interact with two or three foreign governments during a financial investigation is enough to impede the efforts of most local law enforcement agencies. David Reed and his

associates similarly structured Off-Shore Gold (OSGold) for this type of fraudulent operation.

On February 24, 2009, the public information office of the US Attorney for the Southern District of New York issued a statement detailing the February 2009 arrest of David Copeland Reed, in South Carolina, on charges stemming from the online digital gold currency known as OSGold identified a "gold unit" Ponzi scheme. The release stated that OSGold had an estimated 66,000 customers. From those accounts, David Reed and his associates stole approximately $12.8 million.

OSGold was an unregulated, unlicensed, and unsupervised scam. Benefiting from a high degree of anonymity provided by digital currency, several of the early operations were complete frauds designed. The online activity of these associated companies perpetuated the financial scam. In the case of OSGold, the entire operation was a fraud, designed to steal customer's money.

After the business had collapsed, OSGold became one of the most egregious matters from the early years of digital currency. In 2016, research into OSGold offers some valuable insight into the new digital currency marketplace.

Off-Shore Gold and OSOpps

In March 2001, while living in North Carolina, a young man named David Copeland Reed and his associates began setting up a new online digital gold currency operation called Off-Shore Gold (OSGold). Those running the operation presented it to the public as being very similar to the e-gold system. The company's website and marketing advertised the digital units as 100 percent backed by gold bullion. Text from the company's website stated:

> OSGold is a product of One Groupe International, Inc. of Panama providing services you need and the protection you deserve safeguarding your financial assets offshore. Your OSGold dollar is 100% backed by gold.
>
> An OSGold Account is an online monetary system which allows you to convert money to gold, store it online and spend at your convenience.[4]

One Groupe International, Inc. was a Panamanian IBC, a paper company, purchased through an Internet website by David Reed and his associates. This company and millions of other paper corporate entities get created

each year in foreign jurisdictions and sold online. A Panamanian local agent supplied nominees for company officers and directors, paid the registration fees, and completed the company formation. Local marketing then sells the paper companies through an "offshore" portal or website. The company status and registration provide an air of legitimacy to any scam and conceal the operator's identity. From his residence in North Carolina, David Reed began hiding his legal identity and overnight his business One Groupe International, Inc., a registered Panamanian IBC corporation emerged.

All online scams require new customers. One of the easiest ways of generating new clients is paying referral commissions. As new users open digital currency accounts, a referral link is created which can generate profit simply by referring others. E-gold defined new accounts created through referrals as progeny accounts. The original user receives a commission for each new account created through their referral link. It was common practice in the digital currency business for users to post their referral link on discussion forums, email lists, HYIP groups, investment boards, and any other online locations where active new members could be found. OSGold offered a generous referral fee to all account holders. When the online payment system opened, many new users in the Internet community viewed it as an opportunity to get in early on the ground floor of an emerging new digital currency system.

> OSGold is an online monetary system which allows you to convert money to gold, store it online, and spend at your convenience.[5]

However, the OSGold system was neither offshore nor back by any gold. A clue to the fictitious nature of the OSGold system was the lack of any operational transparency available through the company and its website. While other digital gold companies openly displayed total audited amounts of precious metal held on behalf of customers along with audited financial statements, OSGold offered no such information. While e-gold offered extensive details on system balances, daily activity, and even daily transaction information, OSGold offered no information at all.

Exchange Service

Operating from an entirely separate domain, independent from OSGold, David Reed and several of his associates also formed an exchange agent business called Ecommerce Exchange, Inc. The website company oper-

ated similarly to other digital currency exchange agents. However, this company catered almost exclusively to OSGold users. Online customers could transfer national currency funds into an Ecommerce Exchange financial account, and the agent would exchange that value for OSGold digital currency units.

A deposit of national currency funds into an OSGold account, through Reed's Ecommerce Exchange, was possible using a variety of payment methods including Western Union, bank wires, checks, or money orders. The Ecommerce Exchange showed a North Carolina business address located in the same area as David Reed's residence at that time. The Ecommerce Exchange website showed the following "company" address: Ecommerce Exchange Inc., 7199 Beach Dr. SW #3, Ocean Isle Beach, NC 28469.

During that period, e-gold was the recognized most popular digital gold currency, and David Reed had incorporated e-gold directly in the OSGold online client account software. An OSGold account holder had the option to deposit e-gold through the website's OSGold member dashboard. There was no fee for this exchange. Participating customers could easily spend e-gold and receive OSGold on deposit in a client account.

Just a few months after OSGold's launch, Reid Jackson, brother of Douglas Jackson, co-founder of e-gold, posted a message online that eventually found its way to the very public e-gold digital currency discussion list stating, "We do not wish to be associated, even indirectly, with osgold.com; therefore, we have removed all links from the e-gold website to websites that link or make reference to osgold.com."[6]

Despite this message and many other warnings from leading industry experts, telling users to stay away from this company, the new OSGold digital currency business quickly gained both users and deposits.

Digital currency has shown that significant growth and expansion into consumer markets always requires liquidity between national currency and digital units. Any lack of liquidity or inability to exchange federal money for digital units can be a significant impediment to any digital currency product. A lack of liquidity is one of the primary reasons why consumers reject new digital currency products. OSGold did not have this problem. During its existence, the OSGold scheme operated by The One Groupe had opened between 60,000 and 100,000 accounts. Civil lawsuits later estimated that the total amount of funds deposited through both operations, OSGold and OsOpps, was over $250,000,000.

A segment of victims in this OSGold scheme that did not receive any attention in any civil action was a group of existing investors that had recently lost money through an HYIP scam named Cash Over Time. Nearing the end of its Ponzi investment cycle, sometime in early 2001, the operators of that scheme announced that all existing members would receive future payouts from the new OSGold platform. At the beginning of 2001, Cash Over Time investors were facing a total loss. However, each member mysteriously received information that brand-new digital currency account through OSGold would be automatically opened for them and all projected payments from Cash Over Time would then be deposited into the OSGold account. This group of people was the first clients of the OSGold system. It is still unclear if OSGold had originally been created to bail out this existing HYIP Ponzi.

Connected to OSGold and soon promoted through its website was an HYIP Ponzi scheme called OSOpps. This scheme only accepted OSGold funding for deposit. Those wanting to participate in the high-yield investment had to convert funds into OSGold and invest using the digital currency. In May 2001, those associated with OSGold, including David Reed, began promoting this new HYIP investment to all OSGold account holders. The scheme was named OSOpps and the program operated from a separate website, http://www.osopps.com.

According to the program's website, investing digital currency in the OSOpps program would guarantee a 30 percent compounded return over three months or a 45 percent rate of return if the principal remained invested for a minimum of 12 months. Text on the website boldly proclaimed that all investor's principal was fully guaranteed, and this assurance made reference to the OSGold platform as a partner in this arrangement. An added convenience allowed the movement of digital funds between OSOpps and the OSGold platform through the client account web interface.

David Copeland Reed and his associates represented that trading in foreign exchange markets had produced the extraordinarily high returns yielded by the OSOpps investment program. It was a very common for online Ponzi scams to allege huge profits from FOREX trading. However, this claim was a total fraud. OSOpps was a traditional Ponzi scam. Those in charge of OSOpps had never even attempted any investments or trading.

This HYIP Ponzi scam was almost identical to all other HYIP schemes across the Internet, except OSOpps appeared to be a partnership with the digital gold currency platform OSGold. Perhaps the direct OSGold connection had provided a small boost to the HYIP investment's repu-

tation. The OsOPPS website identified this beneficial digital currency link for users, "Finally we have it!! OsOPPS by OsGOLD! The SAFE & GUARANTEED OSGold Investments! Finally the ONE we've all waited for – REAL investments." The OSOpps' online HYIP scheme was created with the same intent of every other Ponzi scheme since in the 1920s. Unsuspecting new "investors" paid digital currency into the OSOpps program expecting a very high return. Once the funds arrived into the OSOpps digital currency (OSGold) accounts, it was immediately used to pay out extraordinary high returns to the older investors. Throughout the life of this scam, David Reed and his associates were withdrawing millions of dollars for their personal use. OSOpps had no other method of generating revenue other than the incoming funds from new investors. At maturity, the OSOpps' guaranteed scheme was promising to pay 30 percent and 45 percent monthly rates of return. Not surprisingly, this too good to be true investment attracted much investor's money into the OSGold digital currency system. When the entire scheme collapsed, many people believed that the OSGold digital currency system was nothing more than a method of funneling more investor monies into the Ponzi.

Compared to all other online digital gold currency systems at the time, OSGold was in a class by itself. There was no proof that any gold had ever existed backing the digital units. There were no office locations. Other than David Reed, an unknown person in the digital currency industry, no other principals were standing behind the ownership and operation of OSGold. Additionally, the gold was reported to be held by an offshore bank. No gold has ever been found connected to OSGold. Furthermore, the SSL certificate on the website identified the business location as a coastal city in North Carolina.

CN = www.osgold.com
O = Home Entrepreneur Network, Inc.
L = Fayetteville
S = North Carolina
C = US[7]

Anyone with experience in the digital gold industry recognized OSGold as a scam. However, by June 2, 2001, there were already six currency exchange agents listed on the OSGold website page entitled "Funding Your OSGold Account." These agents began building liquidity into the

marketplace for OSGold digital currency. This activity bolstered consumer confidence and was vital in creating a successful OSGold operation

The Shills

After the launch of the HYIP OSOpps, a large part of OSGold's legitimacy was gleaned from third-party independent digital currency exchange agents.

David Reed had originally gained liquidity through Ecommerce Exchange, Inc. as OSGold's main exchange agent business. However, during the period 2001–2003, the industry was expanding so rapidly; many new third-party independent exchange agents, seeking to earn a larger profit, also began buying, selling, and exchanging OSGold. Some of these agents became "approved OSGold exchange service providers." The OSGold website actively promoted these companies and agents. Being a recommended agent was, in essence, a financial bonus for being involved with OSGold.

A text link from the index page of OSGold.com led visitors to the promoted agents stating, "Fund your OSGold Account with your choice of our Approved Exchange Providers." Users connected to a page showing 17 independent exchange agents.[8] In return for their endorsement of OSGold through trading and exchange, David's website channeled new customers to the agents who generated substantial new agent revenue.

Dozens of independent third-party exchange agents, not listed on this page, also recognized an opportunity to make a profit through OSGold and began trading in this new digital currency. Without any knowledge or audit of OSGold assets, these agents carelessly reported to clients that precious metal backed the OSGold platform, and they believed the operation was legitimate. Seeing the increased activity between OSGold and the HYIP Ponzi OSOpps, many of these agents recognized the profitable market and effectively began shilling for OSGold.

At its start, OSGold was promoted on industry email lists, forums, and HYIP Ponzi sites. It was this activity by third-party agents that gave OSGold much of its legitimacy with consumers. It was OSOpps, David's HYIP Ponzi scheme that attracted thousands of new users to OSGold. The primary method of payment accepted by the OSopps Ponzi was OSGold. Consequently, anyone wanting to "invest" had to buy OSGold.

In June 2001, there were a half dozen exchange agents already buying and selling OSGold. Some of them were very well-known. The list of promoted OSGold agents June 2, 2001, included:

- Fastgold.net
- GoldNow.st
- Gold-Today.com
- Gold Pouch Express.com
- MyGoldBug.com
- CyberMidasGold.com
- EuroGoldLine.nl[9]

Most of those participating OSGold agents were leaving comments and engaging in discussions on digital currency forums either promoting OSGold or supporting David Reed. The following comment is from the e-gold list. Michael Moore posted this statement:

> Michael Moore, Operator of Gold-Today.com
> [e-gold-list] Re: Re osgold.com
> Michael Moore Wed, 21 Mar 2001
> I have received a email from David (with whom I am aquainted) and am satisfied this [OSGold] is a genuine site. I have indicated to David that on the basis of the info below and in his email, I would be pleased to be considered as a Market Maker for osgold.
> Kind regards, http://www.gold-today.com[10]

Shown here are comments from additional exchange agents who widely promoted the use and exchange of OSGold. The OSGold commission referral sign-up links were usually included in any comments by these agents.

On March 22, 2001, James Shupperd, the owner of FastGold.net, left this comment:

> Subject: Re: [e-gold-list] OSGOLD
> Date: Thursday, March 22, 2001
> As far as getting osgold converted to egold, there are already a few market makers that are doing that. I am one. This is the future of online payment systems, They are not trying to take E-gold down, but they would like to see e-gold have better customer service. OSGold, Standard Reserve, GoldMoney, and E-gold are just the beginning of what will probably be

> a saturated industry. I would rather have my money in a safe offshore haven, and have complete access to it. I also prefer Customer Service!! Give OSGold a try, soon it will be used by many more than you imagine. James Shupperd[11]

In April 2001, the well-known exchange agent, Graham Kelly from GoldNow.st added this comment to the e-gold list:

> April 2001 [e-gold-list]
> "We are now proud to be associated with OSGOLD! Our investigations of that company so far, has revealed that they are a surprisingly solid company, with a great vision, and huge customer acceptance! For a free OSGOLD Account, click on the link at the top of this page!"[12]

Later, in May 2001, Graham included this statement:

> [e-gold-list] OSGOLD performance figures
> Graham Kelly
> Wed, 02 May 2001
> Joyce, and interested others,
> I'm currently processing approx. 7–15% of all my daily orders thru OSGOLD per day, and I've never had a single problem (that couldn't be fixed!). Indeed, I get calls from OSG staff, asking if there's anything I need or want, to enable me to deliver gold quicker to the gold economy participants. Now, THAT's what I call customer service! Apparently, they now have over 13,000 customers, and according to my own records, they had a total of 958 spends from 00:14 to 06:05 (just under 6 hours, approx. midnight to 6 am, this morning), an approx. average of 159.66 spends per hour, or 2.661 spends per minute. Of course, this is only a fraction of the business that e-gold generated, but for a company that's less than 3 months old, not a bad record!
> Cheers!
> Graham Kelly CEO[13]

Independent third-party exchange agents, who do not spend money on advertising, need to attract new customers by expanding into new product markets. Exchanging OSGold along with the additional digital currency business that accompanied this activity translated into substantial income for agents who partnered with David Reed, OSGold, and the OSOpps Ponzi scam. If an existing agent's business had slowed, adding the new OSGold currency could double or triple exchange orders almost overnight. Partnering with OSGold was an opportunity to generate substantial new income for any exchange agent willing to take the risk.

In a February 2002 online interview, Michael Moore of Gold-Today.com stated that after adding OSGold, 90 days ago, his business has processed more than 100,000 AUD and is expected to continue processing OSGold estimating that annually the market should reach about 500,000 AUD.[14]

Monday, February 4, 2002 Planetgold.com: Interview of Michael Moore of Gold-Today.com

Despite a surge in new users across the digital currency industry, which began in 2001, consumers were not yet cutting up bank cards or closing checking accounts for digital gold currency. New customers entering the marketplace were associated with HYIP activity and had arrived in the business by investing in an HYIP Ponzi scam. Endorsing OSGold and thereby recommending OSOpps was not only generating new customers and earning profits for exchange agents, but was also expanding the digital currency industry.

In another online interview from February 2002, prominent independent exchange agent Eric Gaithman, who operated Gaithmans Gold Nation, Inc. (Gaithmans.com), stated that "Gaithmans has witnessed the following in gross sales for the period of January 1st, 2002 to February 17th, 2002: E-Gold 69.67%, OSGold 14.66%, Evocash 8.59%, E-Bullion 5.52%, (Other sales) 1.6%."[15]

Even David Reed, the operator of both OSGold and OSOpps, could be found shilling for his scams and openly posting public comments to the e-gold list. By April 2002, the OSGold website was promoting 16 partner exchange agents. Agents were now accepting national currency and digital currency in the open exchange of OSGold units. New customers did not have to send government-issued money to purchase OSGold; the digital currency was also now exchangeable with a long list of other digital currency products. Here is the list of exchange agents promoted from the OSGold website found April 8, 2002.

- AlliedDigitalCurrency.com
- CanX.ws (Canadian Exchange)
- EcurrencyExchange.com
- e-forexgold.com
- EuroGoldLine.nl
- Fastgold.net
- Gaithmans.com (Gaithmans Gold Nation)
- GoldEx.com.au
- Gold-n-days.com

- osg.Goldnow.st
- GoldPouchExpress.com
- Gold-Today.com
- Gold-Trader.com
- MyGoldBug.com
- QuickMetal.com
- TampaExchange.net

However, by March 2002, after being in operation around a year, the OSGold began to crumble. Just before the maturity date on one of the program's significant investments, the "interest payment" payouts to members abruptly ended.

As in all fraudulent Ponzi schemes, those operating the scheme reach a midway point in the life of that scam, where the income is no longer growing, and the outflow of funds is greater than the new money available from incoming investors. In the case of OSGold, March 2002 marked the maturity date of a large investor's funds, rumored to be an approximate $10 million. His attempted withdrawal of funds was unsuccessful. David Reed responded to complaints by stating that it was a temporary delay caused by minor technical issues. Identical to all other Ponzi scams in the world's history, news of the problem quickly spread. Unable to withdraw funds, investors panicked. In June 2002, David Reed simply disappeared into the night along with the investor's money.

Those operating the OSGold scheme had claimed to have bullion, gold certificates, or another form of precious metal assets backing the digital units. After the payouts had ended and OSGold was revealed to be a scam, users quickly learned that there was no gold. Both OSGold and OSOpps were complete frauds created for the sole purpose of stealing customer's money. By mid-2002, OSopps and OSGold had both gone offline. The money and the operator had vanished into thin air.

While the digital currency system had only survived for about 13 months, the financial and legal problems that David Reed had created would last for decades.

The Scam

Throughout the operation of OSGold and OSOpps, David Reed and his associates had been withdrawing large amounts of cash from the program and bank account connected to the scheme. With no required audits,

money service business registrations, or licensing procedures that may have caused the supervision of the OSGold business, David was free to move funds out of the system and into his pocket.

In later court documents, the FBI concluded from bank statements and ATM records that David Reed and his associates had withdrawn more than $12 million in cash through banks in Latvia, Mexico, and the USA. Reed and his family had fled to Mexico and were residing in Cancun. In his possession were the millions of US dollars, in cash, withdrawn from the OSGold and OSOpps schemes.

During that 2001 digital currency market, which observed no existing US financial regulations, government supervision, licensing, reporting requirements, or financial auditing, anyone could create a digital currency and misrepresent that financial product. In fact, David Reed, a US citizen living in Ocean Isle Beach, North Carolina, USA, had created a phony offshore digital gold system and a multimillion-dollar investment scheme out of thin air. Through the Internet, he had controlled all of the online digital currency accounts, the primary exchange agent, and even the foreign bank accounts that transacted funds on behalf of all of these entities.

He had purchased a paper Panamanian company online named One Groupe International, Inc. and had control over other offshore entities including Group Harbor Investments, Inc., Thunderbirth Investing Corp., and UMEX. He and his associates had opened and opened foreign bank accounts in jurisdictions such as Latvia, Panama, and Mexico. Finally, he had stolen approximately $13 million from around 60,000 OSGold users. A 2005 lawsuit filed in Washington State very accurately detailed the crime:

> This action involves a fraud as vast and far-reaching as the Internet itself. The Defendants' scheme was founded upon a fraudulent operation fronted by the sale of a nonexistent gold-backed Internet currency and was fueled by a mammoth "Ponzi" scheme disguised as a guaranteed high-yield investment program. As a result of this fraud, the accounts and investments of the victims of this elaborate fraud, once estimated to be valued in excess of $250,000,000.00, are now effectively worthless.[16]

Before he and his family had left the USA for Mexico, they had withdrawn the money, packed it into duffel bags and clothing, and then smuggled into Mexico. Using the cash, he later purchased local Cancun assets including a nightclub, shopping mall, and gymnasium.

The Foreign Banks

After the initial shock of the scam had passed, investors began searching for the guilty parties. The foreign banks that had processed the enormous amount of victims' money received much of the victims' focus. Two Latvian banks named Lateko and Parex had been directly involved in the Ponzi activity.

Debit Cards

Each institution had provided anonymous debit card accounts which were used to create liquidity for OSGold clients and also David Reed's criminal enterprise. The cost of this card to any new user was $99 with standard shipping.

According to court documents, Reed had entered into a partnership with a well-known exchange agent named Frank Zuchristian, who then opened bank accounts at both Lateko and Parex Banks in Riga, Latvia. The Lateko card account issued 2500 initial cards that functioned as sub-accounts of the primary bank account.

This option was the only card account directly linked to OSGold out-exchange. The cards were purchased from the domain www.cardaccounts.tv. This online business was linked with another paper Panamanian corporation named Thunderbirth Investing. According to statements from the FBI, this entity was also under the control of David Reed and his associates.

> And excerpted from Southern District Court of New York – Civil Action – 02 CV 8993:
>
> "72. As part of the OSGold/OSOpps programs, Defendant One Groupe issued debit cards through Defendant Reed and Mr. Zuchristian's joint-venture, Card Accounts. The system was set up so that the Exchange Makers, such as Mr. Zuchristian and Defendant Kelly, held "master accounts" in LATEKO Bank. The debit cards that were issued to the OSGold depositors and OSOpps investors drew from a series of anonymous "sub-accounts", held within the master accounts, that were identified only by the sub-account number. These sub-accounts belonged to the individual OSGold depositors and OSOpps investors. For these accounts to be funded, OSGold had to be converted to hard currency and then deposited to the LATEKO sub-accounts, generally a task completed by the Exchange Maker that had provided the card. The master account holder purchased a series of anonymous debit cards corresponding to these subaccounts."[17]

Latvian bank debit card programs, matched with digital currency exchanges, were very common. In this situation, a corporate bank account was opened on behalf of an exchange agent, and thousands of sub-accounts (ledgers) all feeding off that main corporate account were created for each card and sold to anyone willing to pay the $99 price for a card. Card holders were not required to present identification, and an individual user could possess multiple cards. Large deposits could be wired into the Latvia corporate account, and with convenient Internet access, any employee representing the card company could manually move amounts from the primary account into each card sub-account. This method allowed individual card holders access the digital currency value and funds through an ATM. This particular Latvian account entitled Thunderbirth Investing offering cards through Lateko Bank would later become a curious legal issue.

Just as debit cards were used in all other digital currency operations in the years between 2000 and 2006, each card represented a sub-account was manually loaded from the main bank account. OSGold account holders could sell the digital currency and receive funds through the Cirrus ATM network. Zuchristian operated the accounts by manually allocating funds to each card. In March 2002, as the OSGold scheme began to fail, David Reed abandoned the debit card accounts and any further deposits to the banks. By July 25, 2002, the cardaccounts.tv website had announced "… a total suspension of business until further notice."[18]

In the case of Parex Bank, a similar anonymous debit card account had been created. However, court documents showed that the bank only issued one OSOpps card. The Latvia bank mailed that card to Ecommerce Exchange, Inc., which was operated by David Reed.

Some of the most interesting legal digital currency Ponzi issues to ever be heard in a US court emerged because of the civil actions brought by those who had lost funds in OSGold and OSOpps.

The Complaints

Case Number: CV05-0706

Washington State, USA

In April 2005, seven investors who had lost money with OSGold came together and in a US court sued two of the Latvian banks that had been used by David Reed to extract stolen funds from the operation. It was the investors' claim that the banks had loaned their name to the scam and allowed the activity to continue without investigation. Their claim was

that the bank had been liable for their losses, and the amount approached $250,000,000. The case also named several of the exchange agents that had operated from foreign countries, as being directly involved or significantly aiding the fraudulent scheme.

In addition to One Groupe International, Inc., OSGold.com, OSOpps.com, David C. Reed, Randy L. Johnson, Jr., ECommerce Exchange, Inc., and the Lateko Bank in Latvia, the lawsuit included all of those agents that had irresponsibly promoted the use of OSGold. The third-party exchange agents named in this lawsuit included:

- James Shupperd of FastGold registered to a company in Oklahoma;
- Graham Kelly of GoldNow registered Nevada Company, place of business in Texas, and Graham was believed to be a resident of England perhaps living in New Zealand;
- Frank Zuchristian of Euro Gold Line;
- Eric Gaither of Gaithmans Gold Nation Ltd. in Indiana; and
- Michael Moore operator of Gold-Today in Australia.

Here is some selected text from that extensive legal document in the Washington State Case.

With David Reed gone and no public money to recover, angry victims turned to the only others parties present which were the banks and the exchange agents. The exchange agents had been some of the "front men" for the OSOpps Ponzi scam and the OSGold fraudulent online payment system. The agents that had been accepting hard-earned national money and exchanging it for fraudulent digital currency. They had directly profited from the partnership. The exchange agents were the direct connection between victim's money and David Reed's criminal activity. Without the agents and the banks, it may not have been possible to complete such an elaborate scheme. The Latvian banks that moved the victim's money in and out of the scam were also an obvious target.

In the US District Court Western District of Washington, an angry group of victims pleaded their case (No. CV05-0706). To a small degree, they were successful at extracting some funds from at least one agent. A jury trial was demanded, and the group listed the following claims:

> (RICO claims; federal and state securities violations; federal common law fraud; supplemental jurisdiction re* violation of Washington Unfair Business Practices Act claims; constructive trust; attorney's fees and costs; injunctive relief).

The suit focused on Michael Moore and Lateko Bank. Here is that text from the Complaint for Injunctive and Other Relief:

> 105. Defendant Moore, in his dealings as an approved Exchange Maker for OSGold and as a result of the direct link between the OSGold and Gold-Today websites, persuaded investors to deposit money into the OSGold system and/or purchase interests in OSOpps. In doing so, Defendant Moore collected a commission for his services, and voluntarily assumed a fiduciary duty to his clients.
>
> 107. Upon information and belief, Defendant Moore failed to conduct the most cursory due diligence required to protect his customers' interests
>
> 108. Defendant Moore's failure to conduct due diligence and his failure to warn investors regarding these misrepresentations caused Plaintiffs to continue to deposit and invest money in the One Groupe companies only to have these funds become irretrievable when OSGold and OSOpps collapsed.

The counts against Michael Moore were:

> COUNT I: Securities Exchange Act, 15 U.S.C. § 78j.
>
> COUNT II: Racketeer Influenced and Corrupt Organizations Act (RICO).
>
> COUNT IV: Aiding and Abetting Common Law Fraud.
>
> COUNT V: Negligent Misrepresentation.
>
> COUNT VI: Breach of Fiduciary Duty.
>
> COUNT IX: Deceptive Acts and Practices.
>
> COUNT X: Breach of Contract.
>
> COUNT XI: Unjust Enrichment.
>
> COUNT XII: Imposition of a Constructive Trust.

Many of the OSGold agents professed their innocence of any fraudulent intent. Most said their work only involved the exchange of national currency with no knowledge of the OSOpps HYIP scheme. Michael Moore of Gold-Today simply went out of business.

> James Shupperd, the operator of FastGold that for a period was the exclusive exchange agent for OSGold, acknowledged his involvement with David Reed and claimed that he had no participation in the HYIP Ponzi scheme OSOpps. He stated that during the summer of 2002 when he had learned of OSGold's financial difficulties, he discontinued exchange operations for the currency. He also acknowledged that at a later date, after the OSGold

closure, he exchanged approximately $3.5 million in cash funds for OSGold with principals of OSRecovery.[19]

While early legal results seemed to support the Plaintiffs' actions, both of these civil cases eventually fell apart in spectacular fashion. It was not until the beginning of 2009 that a small measure of closure came to the OSGold victims. On February 24, 2009, the US Attorney's Office for the Southern District of New York announced that FBI had arrested David Copeland Reed at his residence in Columbia, South Carolina. At just 38 years old, he was now headed to prison, and that fact alone made some of his victim's smile. The OSGold former customer's jubilation was posted on the Internet.

After years of living in Cancun, Mexico, David Reed's money ran out. He had purchased a nightclub, shopping mall, gymnasium, and other assets. However, elements of Mexican organized crime had moved in and taken over most of his business. David has been forced to return to the USA and accept a day job to support himself and his family. He had been quietly living in South Carolina when the FBI had located and arrested him in 2009.

An earlier 2002 lawsuit had been filed in New York State which included the OSGold exchange agents.

Case Number: 02-CV-8993
Southern District of New York, USA
US District Court for the Southern District of New York
Civil Action No. 02 CV 8993
Osrecovery, Inc.
Plaintiff,
v.
One Groupe International Inc.,
OSGOLD.com
David C. REED (co-founder of OSGold and OSOpps)
Randy L JOHNSON, Jr. (co-founder of OSGold)
James SHUPPERD (owner of Fastgold)
Graham KELLY (owner of GoldNow Corp.)
Eric GATHIER (owner of Gaithmans Gold Nation, Inc.)
Michael MOORE (owner of Gold-Today)
Rick YOUNG (head of International Negotiations Team)

The initial plaintiff in this 2002 civil action, OSRecovery, Inc., was a New York corporation representing the interests of approximately 3400 individuals all of whom had been an OSGold account holder or OsOpps investors. Since that original filing, several thousand more victims had joined as plaintiffs in amended complaints. OSRecovery, Inc. and the additional parties were referred to as numbered "Doe" plaintiffs throughout the litigation. According to New York Attorney Alec Sauchik, a partner in the law firm MDRXLaw – Sauchik & Giyaur, P.C. (http://mdrxlaw.com/), this New York civil lawsuit, filed by Osrecovery, is the largest Internet fraud case in US history. The more than 3000 plaintiffs were seeking $250,000,000 in direct and $750,000,000 in punitive damages. The plaintiffs alleged that the Latvian bank acted as co-conspirator and intermediary.[20]

The Complaint alleged that defendants David C. Reed and others carried out a scheme to defraud investors. However, these One Groupe Defendants were not the only defendants named in the 2002 civil action. The angry investors were also alleging David Reed's group had acted in concert with the exchange agents (Shills) that had been directly involved in OSGold transactions. The complaint named all of the public exchange agents that had been promoting the use of OSGold and had been profiting from the digital currency exchange. The list included:

Ecommerce Exchange, Inc.;
Pinnacle Dynamics, LLC d/b/a FastGold, and its owner, James Shupperd;
GoldNow Corp. and its owner, Graham Kelly;
Euro Gold Line and its owner, Frank Zuchristian;
Gaithmans Gold Nation Ltd. and its owner, Eric Gaither; and
Gold-Today and its owner, Michael Moore.

Additionally, the plaintiff named other parties in the suit, including Lateko and Parex banks. The claim was that both banks had allegedly played a direct role in the debit card part of the scheme.

The Office of the US Attorney stated that between March 2001 and June 2002, customers had opened around 66,000 OSGold accounts and transferred at least approximately $12.8 million to three bank accounts controlled by David and his associates.[21]

The 2009 statement from an FBI press release was no surprise to anyone confirming that "Millions of dollars of the investors' and depositors'

money, including principal, have never been returned. No gold bullion reserves associated with OSGold have been located."[22]

David Copeland Reed was charged with one count of conspiracy to commit money laundering, one count of money laundering, and three counts of wire fraud.

> REED, 38, was arrested this morning in Columbia, South Carolina, where he moved recently after having lived in Mexico for years. REED is charged with one count of conspiracy to commit money laundering, one count of money laundering, and three counts of wire fraud. The conspiracy to commit money laundering count and money laundering count each carry a maximum sentence of 20 years in prison and a maximum fine of $500,000. Each wire fraud count carries a maximum sentence of 20 years in prison and a fine of $250,000, or twice the gross gain or loss from the offense. This case has been assigned to United States District Judge JOHN G. KOELTL. REED will be presented later today in Columbia, South Carolina.[23]

Both the FBI and the press were now referring to the case as the "Gold-Unit" Ponzi scheme.

The creation of OSGold had occurred during an active period of development in both digital currency and online HYIP scam community. The success of OSGold to rob victims of digital currency funds can be in part attributed to this unique period of new digital currencies. New customers entering the Internet marketplace and first discovering OSGold were encouraged by an amount of secondary "proof" of the company's legitimacy. Exchange agents that had openly participated in the OSGold marketplace had added validity to the digital currency that could not have been created through the digital currency company by itself. By endorsing OSGold and engaging in the exchange of OSGold for national currency financial agents, including the two Latvian banks, provided a "stamp of approval."

Notes

1. "Securities and Exchange Commission, Charis Johnson: Lifeclicks LLC; and 12Daily Pro," Gilardi & Co. LLC, accessed October 27, 2016, http://www.gilardi.com/pdf/AllenMatkinsApplication.pdf.
2. "Charis Johnson, Lifeclicks, LLC, and 12daily Pro: Lit. Rel. No. 19579/February 27, 2006," SEC.gov | Home, accessed August 18, 2015, http://www.sec.gov/litigation/litreleases/lr19579.htm.

3. "MLM.com—MLM Discussion Board—MLM Tools • View Topic—BBB Releases Warning About Stormpay" MLM.com | The Direct Sales Resource, accessed October 8, 2015, http://www.mlm.com/forum/viewtopic.php?t=8106&p=70748.
4. "Welcome to OSGold," Internet Archive: Wayback Machine, accessed November 18, 2015, https://web.archive.org/web/20021207092643/www.osgold.com/faq.php.
5. "Welcome to OSGold," Internet Archive: Wayback Machine, accessed May 15, 2015, https://web.archive.org/web/20020524093545/www.osgold.com/.
6. "[e-gold-list] Re: Public Announcement Regarding OSGold Links," The Mail Archive, accessed August 14, 2015, https://www.mail-archive.com/e-gold-list@talk.e-gold.com/msg04096.html.
7. "[e-gold-list] OSGold = Suspicious," The Mail Archive, accessed April 3, 2016, https://www.mail-archive.com/e-gold-list%40talk.e-gold.com/msg06291.html.
8. "Welcome to OSGold," Internet Archive: Wayback Machine, accessed November 16, 2015, https://web.archive.org/web/20020408134427/www.osgold.com/approved_exchange_providers.php.
9. "OSGold.com," Internet Archive: Wayback Machine, accessed November 18, 2015, https://web.archive.org/web/20010602071525/www.osgold.com/howto/buy.html.
10. "[e-gold-list] OSGOLD Performance Figures," The Mail Archive, accessed October 16, 2015, https://www.mail-archive.com/e--gold-list%40talk.e-gold.com/msg03916.html.
11. "[e-gold-list] Re: OSGOLD," The Mail Archive, accessed October 17, 2015, https://www.mail-archive.com/e-gold-list@talk.e-gold.com/msg03073.html.
12. "Goldnow.st Welcome," Internet Archive: Wayback Machine April 2001, accessed October 15, 2014, https://web.archive.org/web/20010419190520/www.goldnow.st/.
13. "[e-gold-list] OSGOLD Performance Figures," The Mail Archive, accessed October 16, 2015, https://www.mail-archive.com/e--gold-list%40talk.e-gold.com/msg03916.html.
14. "Internet Archive Wayback Machine," Planetgold Interview Michael Moore 2002, accessed April 29, 2014, https://web.

archive.org/web/20020816065816/planetgold.com/interview.asp?SPID=20060375.
15. "Interview of Eric Gaithman of Gaithmans.com," Planetgold from Internet Archive, last modified February 18, 2002, https://web.archive.org/web/20020816065816/planetgold.com/interview.asp?SPID=48539574.
16. "Osrecovery, Inc. v. One Groupe Intern., Inc. | Leagle.com," Leagle.com | A Leading Provider of Copies of Primary Caselaw from All Federal Courts and All State Higher Courts, accessed January 29, 2015, http://www.leagle.com/decision/2004645305FSupp2d340_1610/OSRECOVERY,%20INC.%20v.%20ONE%20GROUPE%20INTERN.,%20INC.
17. "Osrecovery Inc 3050 3188 939 V. One Groupe International Inc LLC | FindLaw," Findlaw, accessed October 6, 2015, http://caselaw.findlaw.com/us-2nd-circuit/1269038.html.
18. "Card Accounts.TV—Your Private Banking Solution!" Internet Archive: Wayback Machine, accessed August 16, 2015, https://web.archive.org/web/20020725223902/cardaccounts.tv/.
19. "Osrecovery, Inc. v. One Groupe Intern., Inc. | Leagle.com," Leagle.com | A Leading Provider of Copies of Primary Caselaw from All Federal Courts and All State Higher Courts, accessed January 29, 2015, http://www.leagle.com/decision/2004645305FSupp2d340_1610/OSRECOVERY,%20INC.%20v.%20ONE%20GROUPE%20INTERN.,%20INC.
20. "Alec Sauchik's' Legal Cases—OSRecovery V. One Groupe Int'l 02-cv-8993 (USDC SDNY)—Avvo.com," Avvo.com -, accessed November 8, 2015, http://www.avvo.com/attorneys/10004-ny-alec-sauchik-1785896/legal_cases/30318.
21. "FBI—Arrest in Multi-Million-Dollar Internet "Gold-Unit" Ponzi Scheme," FBI, accessed January 18, 2015, https://www.fbi.gov/newyork/press-releases/2009/nyfo022409a.htm.
22. Ibid.
23. Ibid.

CHAPTER 9

GoldMoney

The GoldMoney system is said to combine modern Internet technology with the world's oldest form of money. GoldMoney is considered the "Cadillac" of digital gold companies. The digital gold currency that emerged from the GoldMoney platform was designed to be more efficient than existing fiat money and safer than conventional banks. GoldMoney was late entering the market, launching in 2001, five years after e-gold. The process of transferring money using GoldMoney should have attracted millions of new users seeking a monetary upgrade and access to a patented version of gold that utilized in everyday finance. The GoldMoney operators stated the belief that this original Internet version of money might power an entirely new global economy. However, over the past 15 years since 2001, this plan has not yet materialized.

In modern times, the accepted weight of a gold unit was the gram. E-gold, e-bullion, and others like GoldMoney denominated smaller units of digital currency in grams. In the patented and copyrighted GoldMoney business, 1 gram was named a "GoldGram^{tm}." These units are the standard unit of commerce and exchange on this platform. Similar to other digital gold products, a customer logging into the online GoldMoney account will see an amount of value denominated by weight and stated in GoldGrams (1 GoldGram = 1 gram of gold). However, unlike other digital gold currency that circulated before 2006, the operators of GoldMoney stated that one GoldGram may not be equal to another gram of gold under another company name. Differences in the underlying 400-oz gold bullion bars were occasionally a topic of contention. Unlike e-gold and

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_9

e-bullion, a GoldGram was not easily interchangeable with other brand names. GoldMoney customers could not deposit or exchange another brand of digital gold for value in a GoldMoney account.

The concept of using a digital form of gold in everyday payments was envisioned by Mr. James Turk around 1979. However, without the infrastructure to support his vision, GoldMoney remained on the drawing board until 1998. A digital format for gold and other precious metals could enable it to circulate as a functional currency. An electronic version of gold could overcome past issues that were preventing gold use as everyday currency in the modern world.

In the 1990s, the commercial Internet delivered an online digital platform that allowed GoldMoney to become a reality. GoldMoney is the registered business name of Net Transactions Limited. This company and its servers are located in St. Helier, Jersey, a British crown dependency in the English Channel near the northwestern tip of France. Jersey is considered a major international offshore financial center with modern data protection regulations.

GoldMoney's technology platform offered powerful e-commerce tools, including a merchant interface shopping cart program, tools for batch payments and automated merchant integration. If US shoppers and merchants had widely adopted GoldMoney as a conventional method of payment, the robust tools offered through the GoldMoney platform could have supported shopping centers across Europe and America. GoldMoney was a digital gold currency designed for e-commerce.

James Turk has authored monographs on the topics of money and banking. In 1987, he began publishing the Freemarket Gold & Money Report as an investment newsletter focusing on national currencies and precious metals. With the aim of helping readers better understand gold, money, and currency in August 2009, his investment newsletter moved online and became the Free Gold Money Report (FGMR). In 2004, he and John Rubino also co-authored The Coming Collapse of the Dollar. Mr. Turk's research, writings, videos, market updates, analysis, and podcasts blanket the Internet. He is one of the most knowledgeable and accessible people in the world of digital gold and precious metals.

Building a Better Mousetrap?

According to GoldMoney's creator and patent holder, James Turk, the GoldMoney platform was designed as a better version of existing modern currency. The GoldMoney software platform was created to facilitate

secure and efficient payments backed by gold bullion. Digital gold currency was an improved version of the world's popular national currency systems. One primary use of the GoldMoney platform was to be a currency for commercial transactions. The company's information portrays GoldMoney as a cheaper and more secure method of buying and selling goods or services. This new digital gold currency was a cost-effective way to complete secure cross-border global financial transactions. These new and improved digital gold transactions, across multiple time zones, would also present no settlement risk. He was awarded four patents for enabling gold to be circulated efficiently as a digital currency, and the company's aim had been to offer this more valuable currency to the global commercial world. Its makers discussed the GoldMoney system as potentially having a wide appeal which included its use as a tool for micropayments and multinational corporations engaged in global transfers. Operators promoted the system as a new single currency for a global audience.

During a presentation to the Gold Institute in late 2001, James Turk stated that it was logical, in his mind, for an electronic gold currency to be widely accepted and used for global e-commerce in the years ahead. His early vision forecast that customers would use digital gold currency in financial transactions, and some instances even perform better, thus replacing the use of national currency for certain domestic and international operations. GoldMoney was marketed as a powerful financial tool that would aid diverse unconnected groups of shoppers and business people around the globe to complete nearly instantaneous cost-effective financial transactions with each other using a digital version of gold. Referencing gold's historical role as money around the world, James Turk forecast that if consumer's adopted Internet tools for everyday payments that digital gold would be the shopper's first choice. The Internet had forged a new connectivity that had overcome past impediments, and again gold could be used as currency

In 2001, James Turk's vision included using GoldMoney digital currency in everyday commerce alongside local currency. His version of risk-free sound money digital currency could preserve purchasing power, facilitate trade, and efficiently settle business transactions.[1]

Again in the world of Internet pioneers, GoldMoney was someone's version of a better mousetrap. During the first ten years of GoldMoney's operation, the company widely promoted its new digital gold currency as a means of making online payments. The GoldMoney website described its

new service as a low-cost and reliable user-to-user (U2U) payment system that offered non-repudiable payments.[2]

From 2001 through 2011, GoldMoney accounts permitted the digital transfer of value from one customer to another (Precious Metal Payments). However, the ability to make payments was removed from the GoldMoney system in early 2012. Following an increase in US regulations regarding money service businesses, the company decided to discontinue this segment of business. The company mentioned other factors as having an impact on this decision, including the profitability and popularity of GoldMoney as a method of payment. However, a large part of the decision hinged on the strict new US regulations.

The payments feature remains functional only if both receiver and sender reside where the company is a licensed money services business, the country of Jersey. In the USA, GoldMoney has never been licensed as a money transmitter in any US state.

By 2011, with the influx of new US financial regulations, the GoldMoney website reflected the company's new mission by dropping all online payments content and prominently displaying how ownership of precious metals through GoldMoney was an excellent way to preserve purchasing power and buy physical gold, silver, palladium, and platinum online.

From the inspirational patent holder and inventor of digital gold currency, GoldMoney had devolved into an online precious metals seller offering metal storage services to its customers. Unlike other digital currency products that emerged during that early period, in 2015, GoldMoney is still in operation and still considered an exceptional company. However, the ability to use gold as a currency was a central part of the business's mission. The extensive company patents clearly illustrate this factor. The loss of the payment side of GoldMoney potentially leaves a large void in James Turk's original mission.

Created by Bankers

The online digital gold system, GoldMoney.com, opened to the public in early 2001. Mr. James Turk and his eldest son Geoff Turk created GoldMoney. James Turk had an extensive career in both banking and precious metals. He had spent more than 40 years working in the financial services industry, and that included positions at The Chase Manhattan Bank and the Abu Dhabi Investment Authority. When he and his son, along with other prominent financiers, formed the business, they under-

stood the valuable monetary role gold could play as a global financial asset. Through their collective experiences, it was well understood that GoldMoney was identified in legal terms as a financial institution. Decades of banking experience had led James Turk to operate GoldMoney with strict financial controls as a system that would not be exploited by users as other digital currency operations of that time. Unlike e-gold or e-bullion, there was no question that GoldMoney was a financial institution. Its operators managed the day-to-day operations and client accounts as would any conventional US financial institution.

From the first day of business in 2001 when consumers discovered GoldMoney, existing US financial regulations did not require the company to function as a regulated financial institution. Just as an industry had recognized e-gold, e-bullion from 1996 through 2006, US financial regulations had not yet recognized the activity of a digital gold currency issuer as requiring a license or government registration. This applied especially to any digital currency company operating from a foreign jurisdiction.

From 2001 to 2006, while GoldMoney was not required to follow any existing Bank Secrecy Act regulations or verify each customer's identification, the company voluntarily instituted in-house regulations including AML, KYC, and customer identification. As the digital gold currency industry leader, GoldMoney set the standard for governance and customer protection. Mr. Turk's decades of experience in the banking and financial services sector shaped the GoldMoney operation and its methods used for supervision of client accounts. GoldMoney voluntarily enforced the standard rules and regulations for a financial institution and operated similarly to a bank's customer compliance. Believing that the company's responsibility was to operate under the same supervision that existed for most US financial institutions, from 2001 until 2015, a new GoldMoney account required about as much information and verification as a regular US bank account. The GoldMoney Customer Acceptance Program (CAP) requires all new users to provide identification and source of funds just as required for a US bank account. In 2008, GoldMoney integrated its online customer verification process with Equifax Inc., a consumer credit reporting agency. New account identities were quickly verified online through the Equifax service.

The GoldMoney system could have easily operated just as e-gold had done, without verification or supervision. However, Mr. Turk's decades of banking experience and knowledge created a business that operated as a highly regulated financial institution. Unlike the e-gold or e-bullion plat-

forms, the accounting giant Deloitte & Touche annually audits GoldMoney precious metal holdings and security measures. GoldMoney has always maintained a strict KYC compliance and AML program. Since the digital precious metals company opened in 2001, all new client accounts, large or small, included verified customer identification.

The year 2008 began a major consumer shift from stocks and bank savings into precious metals. As a result of the economic crisis, GoldMoney enjoyed strong growth from the accumulation of new customer precious metal assets. Due to both company's regulatory and legal issues e-gold and e-bullion missed out on this huge monetary shift. Account holders looking to protect the value of their savings purchased precious metals through GoldMoney, and the increase in total assets held by the company was substantial.

Fifteen years after opening to the public, GoldMoney has never encountered any regulatory issues with the USA. In fact, a holdings balance with GoldMoney may even be subject to reporting under FACTA. Permanent US residents or citizens may be required to file a TD F 90-22.1 if the account value passes certain reporting levels.

GoldMoney conducts third-party audits of its precious metal holding and publically verifies that 100 percent of metal is always backing the digital units. Beginning in October 2010, GoldMoney even began using ultrasound technology to scan each gold bar and verify that it was free from foreign materials and defects. Any bar that did not meet the strict GoldMoney standard was melted down, assayed, and recast into a new clean bar.

GoldMoney is recognized as a money service business, licensed and regulated by the Jersey Financial Services Commission. All company financial statements are prepared according to International Financial Reporting Standards (IFRS), ISAE, and audited by Deloitte. The GoldMoney website offers an independent verification and audit reports page that contains access to third-party audits, certificates, and reports which independently verify the company and its customer assets. GoldMoney customers can also obtain the Deloitte & Touche audit report.

Unlike e-gold, GoldMoney clearly defined a Ponzi or pyramid scheme as fraudulent and illegal. The company had a zero-tolerance policy for any fraud. Unlike the HYIP Ponzi driven world of e-gold and e-bullion, former GoldMoney shareholders have included two publicly traded companies DRDGold (sold the company's interest in 2008) and IAMGOLD. In 2015, GoldMoney merged with BitGold, and the parent company GoldMoney

Inc. became listed on the Toronto Stock Exchange. BitGold is a gold payments technology company founded by Roy Sebag and Joshua Crumb.

In 2016, GoldMoney still offers an efficient and secure online method to buy and store gold, silver, platinum, and palladium. The Turks understand gold's usefulness as a financial asset and the role of gold as money, better than the majority of other financial experts in the world, including those working on Wall Street. GoldMoney customer precious metals are allocated to the account holder and at all times owned by the account holder, and not GoldMoney. GoldMoney "holds" the asset on behalf of the customer and is never the titled owner. Each user in the system owns their gold holdings. Even if the GoldMoney Company were to go bankrupt, customer gold holdings would not be affected.

This structure is beneficial for customers because the company's business activities can have no impact on the security of the precious metal.

However, GoldMoney's practice of assigning customer ownership is quite different from the past policies of e-gold. Within the e-gold system, the ownership of all precious metal was assigned to a trust. In fact, the e-gold Bullion Reserve Special Purpose Trust, which was domiciled in Bermuda, presented a clear separation of gold ownership between the digital units and the bullion. This separation was not the case with GoldMoney. Each gram of gold was legally attached to a user's account. This ownership is extended to the actual identification of different storage facilities in various countries. Clients owned grams tied to the certain private vault facilities and companies in the various country.

Critics of GoldMoney describe this ownership arrangement in a negative context. The critics have tried to explain if a client had a gram of gold held in UBS vaults in Switzerland, that because of the jurisdiction, that gram would be different from a gram of gold held elsewhere such as Scotia Mocatta's vault in New York City. Both of these grams would be distinct from a gold stored in GoldCorp's Perth vault location in Australia.

Since the 1990s, GoldMoney was awarded four patents for the technology and concepts of its online platform. Mr. Turk spent 20 years obtaining the four patents on his processes for the use of precious metals as an online method of payment. The patents acknowledge that GoldMoney has advanced the "prior art" of global online payments.

1. The first US Patent, No. 5,671,364, was filed in February 1993 and awarded in September 1997. It provides for a system and method enabling gold or other commodities (tangible assets) to circulate as

currency through an electronic medium book entry accounting system.

2. The second US Patent, No. 5,983,207, was awarded in November 1999. It provides for a system and method enabling gold or another commodity to privately circulate electronically as digital cash and facilitate micro-payments.
3. The third US Patent, No. 6,415,271, was awarded in July 2002. It provides for a system and method enabling gold or another commodity to privately circulate electronically as digital cash over wireless networks and by means of electronic devices such as smart cards.
4. The fourth US Patent, No. 7,143,062, was awarded in November 2006. It provides for a system and method enabling gold to circulate as digital cash through a global computer network such as the Internet and/or private communication networks. A comparison is made between this product and how physical cash circulates in the world.

Digital gold currency systems, such as GoldMoney e-gold, addressed settlement risk which is also known as "Herstatt risk." The term originates with the 1974 failure of the German Bank Herstatt. When regulators closed the bank, it had received actual foreign-currency receipts but not yet made any of the corresponding US dollar payments. The closure left counterparties with substantial losses and unable to collect their funds.

By designing a system of payments that used actual gold bullion in the transactions, any possibility of Herstatt risk could be eliminated. In a digital gold system, the purchase of goods is paid for with another physical commodity (gold) denominated by weight. Alternately, when a customer bought a product and paid with dollars or any other national currency, the receiving merchant is accepting Herstatt risk. In 2015, all national currencies are issued through debt making; this risk is unavoidable. Governments default on currency all the time! Whether the money is US Federal Reserve Notes or the euro, that merchant is accepting default risk. Gold has no such risk. One ounce of gold will always be 1 ounce of gold.

Gold bullion and other metals stored through GoldMoney were exceptionally safe. The business used a triple-check system, and all three participants were required to sign off anytime that precious metal was removed from the vault. Two of those three verifications were provided by reliable

and well-known firms that operated in the business for decades. Those companies were VIA MAT and Euro-Dutch Trust Company (EDT).

Storing customers' precious metal and removing it from the vault location involved GoldMoney, VIA MAT, and a commercial trust service named Euro-Dutch Trust Company (EDT). These multiple corporate oversights were arranged to prevent any arbitrary increase or decrease in the number of circulating GoldMoney digital units. VIA MAT and EDT made the actual changes, increasing or decreasing the number of GoldGrams in the system, and GoldMoney supervised the activity and guaranteed its accuracy.

Just as other digital currency companies had done, GoldMoney also differentiated itself from being a bank. GoldMoney's website, blog, and documents always pointed out that GoldMoney did not accept deposits. The precious metal creates no deposit liability that the company holds on behalf of its clients. This operation is contrary to a bank, which accepts deposits and then loans that money out.

GoldMoney also published the third-party reports which verified there is always a 1-to-1 ratio of precious metals to digital units. Clients could access these reports through the website.

Cambios

The businesses that exchanged national currency or precious metal to GoldMoney digital units (GoldGrams) were called Cambios. Agents operating through an agreement with GoldMoney were listed on the GoldMoney website. The listing of a Cambio on the website was not an endorsement of the service. The listings were for informational purposes.

From 2001 through 2003, there was just a handful of Cambios. However, many other unrecognized exchange agents accepted GoldMoney and swapped GoldGrams for another digital currency brand or out-exchanged it to national currency. While this activity of independent third-party agents was permitted, it was not promoted by GoldMoney. The majority of GoldMoney exchanges with national currency occurred through the GoldMoney website. Modern banking and money services, such as international wire transfers, eventually became popular features of the GoldMoney business. In 2016 there is even a GoldMoney debit card for ease of access to national currency from the newer GoldMoney system. Cambios also accepted and exchanged gold coins and bars for GoldGram

digital units. In April 2001, Cambios listed on the GoldMoney website included:

1. FideliTrade Inc., Wilmington, Delaware
2. Ormetal Inc., Quebec, Canada
3. Goldfinger Coin and Bullion Inc., Camarillo, California[3]

The last Cambio in this list, Goldfinger Coin and Bullion, Inc., was owned by James Fayed and his wife Pamela. In July 2001, James opened e-bullion.com as a digital currency extension of their precious metals business.

Over the years since GoldMoney began, critics will state that while e-gold moved into a more mainstream payment arena by allowing and promoting independent exchange agents, GoldMoney moved away from a payments platform and more toward an online precious metals dealer. From 2000 through 2010, GoldMoney move away from the independent Cambio model and back to being the primary exchange agent for national money. GoldMoney as the primary agent did not have to create liquidity for outside agents or a bustling payments industry. Liquidity, as required by clients, and banking benefits came from within the organization.

Why All the Patents?

The first appearance of GoldMoney.com digital gold currency was seen around November–December 1997 after the announcement of James Turk's first patent in the area of digital gold.

Here is the information release that appeared online in Mr. Turk's Freemarket Gold & Money Report, #212, from October 1997:

> U.S. Patent No. 5,671,364
>
> Originally Published in FGMR #212 on October 6, 1997 by James Turk
>
> I hope to use my patent to build a business over time based on the premise that Gold is money, and it can once again circulate as currency. I do not mean to use the word circulate as Gold coins once circulated. Gold coins are currency of the past. I'm talking about Gold currency of the future. My proposition is: When given a free choice of alternative currencies, good money drives out bad money. If I am right, and Gold once again circulates supplanting national currency, perhaps my proposition may come to be known as Turk's Law.[4]

James Turk is an accomplished banker and businessman. As inventor of digital gold currency, the GoldMoney business worked very hard to develop high-quality industry standards to ensure that the digital gold currency and the industry wide concept of digital gold would grow into a viable safe financial product. In a 2002 interview, he stated that GoldMoney would defend the patent rights if any other digital gold firm was envisioned to not be meeting the high-quality standards as created by GoldMoney. This has always been a puzzling point of view because e-gold had already been operating in the market for around five years before GoldMoney launched. Believing that GoldMoney's concept of digital gold currency was of such importance that it should be protected, October 31, 2001, GM Network Limited and Net Transactions Limited (GoldMoney) filed a civil case in the US District Court Southern District of New York which claimed that Dr. Douglas Jackson's e-gold was infringing on the following GoldMoney patents: US Patent No. 5,671,364 and US Patent No. 5,983,207. The Defendants were:

- E-Gold Ltd.
- DigiGold Ltd.
- Douglas Jackson Chairman OmniPay
- Barry Downey
- The Jackson Family Trust
- The Downey Family Trust

At the time, this lawsuit was considered a very serious expensive legal issue. The potential penalties were impressive. GoldMoney asked the court to declare that the Defendants had infringed on the GoldMoney patents. The lawyers for GoldMoney requested that the court permanently enjoin and restrain both e-gold and DigiGold from any further infringement. That would mean a total shutdown of the businesses. GoldMoney was also asking the court to require defendants to turn over all software, including the source code, used by e-gold and DigiGold, plus pay damages, times three, along with all attorney's fees (GM Network Limited vs. e-Gold Limited Civil Action No. 01 CV 9621).

By June 2002, e-gold had aggressively responded to the lawsuit and the legal brawl was becoming heated. Preparing for an expensive battle in court with lengthy discover, GoldMoney then filed for a stay. The judge declined and in September dismissed the entire claim without prejudice. While the GoldMoney team declared a type of victory, the company's

patents were referred back to the US patent office for re-examination. GoldMoney could have proceeded again with the case at any time in the future; however, GoldMoney never again pursued it. E-gold's legal expenses had been substantial. Questioned about the legal case in 2016, Douglas Jackson, co-founder of e-gold, responded with this statement:

> At the time Turk brought his patent action against e-gold he had been repeatedly apprised of the lack of merit. There was never any illusion that e-gold actually infringed on the Turk patents (Goldmoney, when actually launched, would not have infringed on his patent!). His explicit purpose was to damage e-gold with reputational assaults and legal costs. The legal cost aspect was two edged: he knew from hiring Charles Evans that we were chronically resource constrained. But he had finally gotten like-minded investors (Clifford Press, DRD) and saw an opportunity to bankrupt us with legal costs a) the case was dropped as soon as it reached the point where they were going to have to comply with discovery, b) the most important Turk patent was eventually re-examined and all the claims were shredded anyway.[5]

Throughout the company's history, GoldMoney formed alliances and partnerships with companies that provided critical investments and expansion during the development of the platform.

In September 2002, an alliance was created with Kitco Metals Inc., a very substantial precious metals dealer and online portal. Through this partnership, GoldMoney account holder were able to purchase physical precious metal from Kitco and pay using GoldGrams. Accounts with GoldMoney could also be funded with national currency by sending the money directly to Kitco. In reality, Kitco may have been considered a Cambio. The alliance was very successful at expanding the GoldMoney empire.

In February 2003, GoldMoney completed an additional financing with IAMGOLD Corporation. The funds were earmarked for future GoldMoney expansion. IAMGOLD is a major Canadian gold mining company that is publically traded on the Toronto and American stock exchanges.

In January 2004, GoldMoney sold a 14 percent stake of the business to a South African company named Durban Roodepoort Deep, Limited (DRD). This company had an existing ownership in GoldMoney, and the new purchase brought the company's ownership up to an approximately $2 million investment.

In July 2006, existing shareholder since 2003, Sprott Asset Management Inc. increased their ownership stake to 9.9 percent. The corporate involvement surrounding Mr. Turk's GoldMoney business was impressive and no doubt a reflection of his compliant operation. There were no such partnerships or alliances for any other unregulated digital currency company at the time.

In October 2007, GoldMoney announced a partnership through which it could offer UK precious metal GoldMoney customers a Self-Invested Personal Pension (SIPP), specifically designed for holding gold. The deal partnered with Berkeley Burke & Co Ltd. US customers could also now hold digital gold and silver GoldMoney units in an individual retirement account.

In December 2008, GoldMoney made a surprising announcement that the platform had implemented online identity verification through the Equifax credit services. This service streamlined the new account procedure for GoldMoney customers. Using this new verified screening mechanism, new US or UK clients could completely register and begin buying digital metal in under 20 minutes.

In just six short years, GoldMoney had grown into a powerhouse corporate organization integrated with banks, credit bureaus, and services a multitude of and corporate clients.

In the years 2007 through 2008 also signaled an economic crisis for the USA and the world. The price of gold moved from the mid-$600 range to $1000 per ounce. Because of the many bank bailouts, there was a dramatic renewed interest in precious metals. New customers and larger deposits flowed into the GoldMoney platform. From $337 million worth of bullion deposits in February 2008, to over 1 billion dollars' worth of gold and silver in August 2010.

In mid-2009, GoldMoney also partnered with Baird & Co. Operating from London, Baird & Co is a well-known historic precious metals company. This partnership allowed GoldMoney account holders to redeem digital gold units and take physical delivery of gold in convenient sized bars. Both 100-gram and 1-kilo bars were available to GoldMoney customers with pickup possible in the UK and 16 other countries.

Belief Versus Reality

Many users during that time had the belief that a digital gold currency would prove to be a better method of transacting business down the block or around the world. Certainly GoldMoney set out to be a preferred

method of online payment. Many projections from all digital currency operators from that early decade saw banks and legacy-clearing financial systems would be replaced by digital gold currency. Some owners, such as Mr. Turk, also believed that digital gold payment could have an impact of Internet commerce, just as the early operating systems had for the PC. If people adopted the Internet as a method for sending and receiving funds, then GoldMoney was to be well-received.

Unfortunately, through the years, the payment side of GoldMoney's business did not gain momentum. Digital gold currency did not have the effect of significantly diminishing the need for banks our outdated credit clearing systems. A new economy built around GoldMoney digital gold payments did not emerge. In fact, the history of GoldMoney illustrates that strict new US regulations and the lack of consumer interest in digital gold payments caused an eventual sale of the company. Douglas Jackson, co-founder of e-gold, had this comment on the GoldMoney's history as a payment platform.

> Goldmoney's "survival" stemmed from its failure to attract usage as a payment system. The fact that there was virtually no usage for actual commercial (or even personal) payments protected it from the hazards of customers abusing it for illicit purposes (in a publicly visible way). Customers that accept payment typically exert themselves to be visible online, exposing their warts to any observer seeking to find fault. This is especially so with commercial recipients.[6]

Mr. Turk's original combination of the world's oldest money and the Internet's innovative new technology did not outweigh the US consumers' desperate need for a plastic debit card and a mobile banking app.

The well-known UK company BullionVault, a GoldMoney competitor in the precious metals marketplace, researched and reviewed the past several years of the GoldMoney business. The finding was that in recent years GoldMoney sales had dropped more than 78 percent in just three years. In 2014, the company posted a loss of £9.4 million. From 2013 through 2015, GoldMoney net assets fell from £25.4 million to £13.1 million.[7]

In 2015, GoldMoney merged with new Canadian company named BitGold. In exchange for company stock in Bitgold, which is traded on the Toronto Stock exchange, GoldMoney was purchased and now operates from Canada. BitGold is an innovative new company and will continue the digital gold legacy started by James Turk. The company facts

and figures from BullionVault's review came from filing related to the publically traded BitGold stock.

Given gold's historical role as money, the expectation that an exciting new brand of secure digital gold currency will naturally attract a multitude of consumers seems very plausible. However, regarding personal finance, convenient methods of payment, and new technology, it seems more likely that the adoption of new digital currency "money" may only widely occur with those individuals that require the currency. The outright need for a payment solution, instead of the common desire for better alternatives, seems to be one of the driving forces behind the consumer adoption of private digital money. The "build a better mousetrap" simply does not fit the world of modern consumer payments. Consumers and businesses alike are not yet willing to give up the online banking, credit cards, and mobile payments in favor of commerce built around the digital gold currency. However, when paper fiat currency returns to its original value, as it always does, many citizens will be in desperate need of a secure and convenient version of gold as money.

Notes

1. "Internet Archive Wayback Machine," Internet Archive: Wayback Machine, accessed February 17, 2016, https://web.archive.org/web/20010909151328/www.goldmoney.com/public/news/presentation.htm.
2. "GoldMoney," Internet Archive: Wayback Machine, accessed January 28, 2015, https://web.archive.org/web/20010409174254/www.goldmoney.com/public/faqs/goldmoney.html.
3. "GoldMoney," Internet Archive: Wayback Machine, accessed February 15, 2015, https://web.archive.org/web/20010409095740/www.goldmoney.com/public/cambios.html.
4. "U.S. Patent No. 5,671,364," Free GoldMoney Report, accessed August 29, 2015, https://www.fgmr.com/us-patent-no-5671364/.
5. Douglas Jackson, Email question and answer interview, Melbourne, FL March 11, 2016.
6. Ibid.
7. "Bitcoin, BitGold, GoldMoney—and BullionVault | Gold News," Buy Gold & Silver Bullion Online | BullionVault, accessed February 27,2015,https://www.bullionvault.com/gold-news/bitgold-goldmoney-052720152.

CHAPTER 10

WebMoney Transfer

WebMoney Transfer is a Russian business. Operating from this jurisdiction offers the company certain operational and regulatory benefits not found in another area of the world, such as the USA. Russian money service businesses, banks, and financial institutions are not subject to strong state and federal financial regulations as US financial companies. This regulatory environment further adds to the importance of discussing the history of WebMoney Transfer and the company's products.

This brief glimpse into the history and operation of WebMoney Transfer is a vital segment of digital currency history. It is also important to note that WebMoney Transfer information and knowledge obtained from the Internet only details a slight portion of the company's global operations. Much of WebMoney Transfer's business transacts through brick-and-mortar operations, alongside the Internet. The company has strategically integrated its business with money transfer companies, digital kiosks, banks, and a global network of financial services companies. Since the company's inception, this uninterrupted partnering with existing financial businesses in more than 100 countries has also been a part of WebMoney Transfers growth and client acquisition. The WebMoney operation discussed in this book; however, understanding the colossal nature of the WebMoney Transfer global network involves visiting the countries and areas where the products are popular.

To truly understand how the features of WebMoney Transfer products create benefits and advantages for users requires knowledge of the local

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_10

and regional circumstances experienced by those populations. WebMoney is not a one-size-fits-all digital currency product. Each financial product created and supported by the company has a specific purpose for a set population of users. Each digital currency solves problems and fills the needs of different users.

The WebMoney Transfer operation is so massive, and there are so many successful products that any in-depth research into its successful history would fill several books. For that reason, the history of WebMoney Transfer discussed here will be very limited to a brief discussion of the products and operation, followed by the similarities and differences of WebMoney with other digital currency systems operating from 1996 to 2006. Just as in the case of GoldMoney, by highlighting some of the operational differences between other digital currency companies, an advantageous structure for a legal digital currency system becomes evident.

The WebMoney Transfer system is essentially a state-of-the-art software platform from which financial products are housed and operate. As WebMoney developed new, innovative financial products, the company adds it to the existing WebMoney Transfer software network. For more than a decade, this growth has fueled the growth WebMoney Transfer's global empire. After being introduced, some of these new products are quick to gain a large following of users from WebMoney's existing client base. However, most new products are rolled out for a specific audience with a distinct financial need for that payment product.

WebMoney purses meet the needs and requirements of local and global users. The accounts were free to open, inexpensive to operate, and more convenient than banks. Each local system was also very closely integrated with its local marketplace. Local vendors including cellular, cable television, shopping, and bill pay accepted WebMoney payments. In local markets, the digital currency became an everyday convenience for local merchants. This dramatic acceptance also contributed to the company's growth. It is important to remember that users were never required to have a bank account or credit card in order use the WebMoney Transfer system.

It is also worth noting that some of the success achieved by WebMoney Transfer came from partnering with existing financial businesses in various parts of the world. There is no faster way to grow a digital currency network than integrating it with existing successful payment products.

WMID

The WMID is the 12-digit number attached to a member's passport. It is a unique address within the WebMoney Transfer system. The WMID is not a secret hidden number; it identifies a member, and each user can share the WMID with others. Many users will list a WMID in the payment area on commercial website businesses.

Just as members compare the WebMoney Passport to a driver's license, the WMID could be viewed as the DL number. In this case, the ID is issued by the private Russian company, not by any government organization. However, it serves a similar purpose affording the holder privileged access to the WebMoney Transfer system. It is unique to that person.

A WebMoney Passport can have up to five WMID numbers attached to it. If one member receives a verified personal passport or higher level, up to four more WMIDs could be officially attached and would also be considered verified.

WebMoney Passports

It is the role of non-bank digital currency to provide access to vital financial tools otherwise not accessible to users blocked from using conventional financial institutions. A digital currency account should be available to anyone, anywhere in the world. Digital currency should provide instant access to financial services for people of all ages, races, and income levels. Finally, a true digital currency has no account limitation on transaction frequency or the amount of funds flowing through the account. Digital currency systems are all created to deliver these features and benefits. It is only jurisdiction regulatory considerations that change how a digital currency account operates. WebMoney Transfer has found a way to incorporate both regulation and monetary freedom into a digital currency online payment system.

WebMoney Transfer can provide these valuable services through an "alias" digital currency account while maintaining local financial regulatory compliance, a strict anti-money laundering program, and robust KYC measures. WebMoney Transfer accomplishes this demanding task through a digital identification tool called the WebMoney Passport.

Each WebMoney Transfer member has a WebMoney Passport. It is a digital certificate that is issued based on the personal data provided by the member. There are many kinds of WM Passports offering access to various products and services within the WebMoney Transfer system. Each one of

these "levels" represents a staggering accomplishment for an online payment or digital currency company:

- Alias passport
- Formal passport
- Initial passport
- Service passport
- Personal passport
- Merchant passport
- Operator passport
- Developer passport
- Registrar passport
- Guarantor passport
- Capitaller passport

Each different passport expands certain areas of client identification and verification. Various passports may also offer greater benefits within the WebMoney Transfer system. If a WM member wants to link a business to the WM Passport, then more identification is required. If a member wants to access financial tools, such as credit borrowing, additional verification is required. The more identification and verification provided by the member, the higher the passport level, the more services and interaction a user can access in the WebMoney Transfer platform.

The first level is the alias passport. It is the basic pseudonymous identification that is given instantly to all new users. The alias passport grants instant access to the WebMoney system. One of the significant features of true digital currency systems is the ability of new customers to sign instantly up and begin using the system moments later. This feature was inherent in all digital currency products during the decade 1996–2006, except of course GoldMoney. In 2016, this feature is still present in WebMoney Transfer alias passport account.

An alias passport requires no ID or verification. In other words, this first alias passport level is almost identical to an e-gold account. This account is not completely anonymous, as a physical cash transaction; however, using the correct combination of an online proxy and other privacy tools, this account can be operated in an anonymous manner. The alias passport is issued automatically upon registration and is free of charge to each new WebMoney Transfer member. The new member data requested for an alias passport includes name, address, phone number, and date of birth.

However, this data is never verified. Hence, the wallet's name is "alias." Also, there is no limit to the amount of funds that can move through this account.

When using WebMoney Transfer for personal or business transactions, the passport level of each user is openly provided. When executing a transaction in the WebMoney Transfer system, both parties are aware of the others WMID and passport certification.

A members' passport level can also be a partial clue to the legitimacy of that user. An alias passport that is transacting $50,000 a week in funds might be considered suspicious. Whereas an alias passport that is transacting under $40 each month for the past year could be regarded as a practical application of digital currency. The lack of requirements for an alias passport illustrates an advantageous feature of all true digital currency systems, including bitcoin.

Many users around the world:

1. Do not have access to conventional banks
2. Do not meet banks' identification and verification requirements
3. Cannot afford the fees and costs of a bank account.

In all of these cases, a simple digital currency account would better meet the needs of these types of clients. A WebMoney Transfer digital currency account, with an alias passport, is free, and the operation of the WebMoney account is inexpensive allowing access the lowest wage earners anywhere in the world. In particular, an alias account could also facilitate financial business for a person without the resources to obtain government-issued ID.

A customer with no government-issued ID, no access to a bank, and earning less than $2500 annual income would be very pleased to access the current free financial tools offered through the alias WebMoney Passport. Digital currency offers instant, easy access to financial instruments and services usually restricted to those bank accounts.

On the complete opposite end of the spectrum, a new WebMoney member in London, Munich, or Prague, depositing and spending $50,000 a month through an alias account, offers very different telltale signs about that members. Members living in metropolitan areas, with good cash flow, could obviously provide ID or access local banks. This type of alias passport account sends a message that the member does not want to be identified through a higher-level passport and may be trying to operate

anonymously. For these reasons and others, many services and colleagues of the WebMoney community will require customers to possess a high-level passport. The alias passport serves a critical function by providing access to those otherwise shut out of traditional financial services such as banks. However, this same easy access to any digital currency product can also be exploited by bad actors and criminal elements. Here are two of the more popular WebMoney Passports. It is important to note that identifying a customer in Russia requires a government-issued passport and not a driver's license as the case in America.

Formal Passport

This passport is issued free of charge when a member provides the necessary personal information, including their passport data. This information is received by the system, however, not verified. Receiving a formal passport permits an account to access to banking from within the WebMoney Transfer service:

- Add funds by bank wire
- The use of a prepaid card
- Automate funds acceptance from customers using the Merchant WebMoney Transfer service interfaces, in limited mode

After the issuance of a formal passport, more verification or a changing member circumstances will bring additional levels of verification, access, and fees.

Personal Passport

A personal passport is the main WebMoney Transfer passport and requires a small fee of $5 to $15. These members receive access to many more options within the system.

- Automated funds acceptance from customers using Merchant WebMoney Transfer service interfaces.
- Verification Centre Partner Program issuing initial passports.
- Publish news on different system websites www.webmoney.ru & www.megastock.ru.
- Restore WMID control using a simplified control model.

- Credit Exchange operations.
- Capitaller service operations (to create budget automation tools).
- The Internet resources registration in any Megastock directory sections.
- System consultant status.
- Star/Plus debit bank card and to use it to withdraw funds from the system.
- Create trading sites using the DigiSeller service.
- Submission of complaints against other system members in the System Arbitration without restrictions.[1]

In accordance with the WebMoney verification procedures, personal passports are issued either at an in-person meeting at an office location or in person with selected registrars. Notarized or apostilled documents and passports are always required.

Other than WebMoney Transfer, new digital currency systems did not offer this type of voluntary identification and verification. Clearly, e-gold or e-bullion could have structured similar levels of customer identification and level of access.

Bitcoin

This type of passport identification would be ideal for use in bitcoin and other cryptocurrency. As a stand-alone product, housed in the block chain, a free public identification file or document offering verification of a person or a business could solve many different issues now plaguing the commercial use of cryptocurrency. If a bitcoin user voluntarily decided to become verified, the merchant's obligation to collect that user identity documents would be limited to quick review of the user's public passport document and any private data access provided by the customer. If a user desires the anonymity of bitcoin, they may continue to use cryptocurrency as users now engage in pseudonymous bitcoin transactions around the world, without ID or verification. The WebMoney Passport system is a proven success that allows the privacy of nearly anonymous use and a level of customer verification found at a bank.

When receiving a payment from another WebMoney Transfer member, the WMID is not the number to provide the sender. To send and receive a payment, after obtaining the passport, that member must also have a WebMoney purse. The platform offers various digital currency

purses for commerce in many parts of the world. The company denominated each purse in a popular national currency that is suitable for business in some regions of the world. In addition to national currencies, the WebMoney platform includes a peer-to-peer credit purse, global payment solutions, APIs, merchant solutions, online billing, and local payment integration with other digital currency platforms and products. Since 1998, WebMoney Transfer has been the fastest-growing digital currency company in the world. No other company offers sophisticated and secure online payment choices from a single platform.

WebMoney Transfer

The WebMoney Transfer website went live in November 1998 with the WMZ purse, a digital wallet denominated in US dollars. Months earlier, the Russian economy and banking industry experienced a financial meltdown. The event became known as the 1998 ruble crisis or simply the "default." In addition to devaluing the Ruble currency, the Russian government defaulted on domestic debt and declared a moratorium on paying foreign creditors. This event caused several of Russia's largest banks to close. That list included Inkombank, Oneximbank, and Tokobank.

As each bank closed and shut out account holders, more and more Russian citizens lost their deposited saving. These victims totaled in the millions. Consequently, after the default, local banks were not considered safe by consumers, and across the region, people stopped using Russian banks.

This unfortunate financial situation in Russia, during the late 1990s, created a massive cash-driven local economy. Since the Ruble has crashed, most Russians were also now using US dollars. Local consumer markets functioned on both dollars and rubles. By 1999, there were millions of Russians with no electronic method to make payments and no savings deposit account. This combination of failed Russian banks and the extensive use of cash proved to be the ultimate consumer environment for the introduction of a digital currency system. This audience of users were the first to adopt WebMoney Transfer. The systems began in late 1998 offering a convenient and very inexpensive alternative to Russian banks. The platform's creators were quick to integrate local walk-in locations that accepted cash and exchanged digital currency. These independent exchange agents formed around Moscow and other parts of Russia. The business quickly caught on in other regions and countries. A small fee was charged to convert paper money into digital units. Users could

instantly transfer those units to any other WebMoney account in the area or around the world. When a customer needed cash, the exchange agents were happy to complete the transaction in reverse converting WMZ back into currency. WMZ represented the first online wallet for WebMoney digital funds. The WMZ represented dollars. As the local economy dictated, dollars were required for most transactions. Consequently, the first wallet created was the US dollar wallet.

In the 1990s, WebMoney transfer was "digital money" that functioned alongside the national money. The digital payments took the place of bank services for many people that had rejected banks or because of circumstances those persons had been shut out of conventional banking. Many rural WebMoney users simply did not have access to a bank or an ATM. However, all towns in Russia had a post, and WebMoney could be used for both sending and receiving funds through the post. The Russians, unlike many other designers of digital currency, created a product to fill an economic need. The WMZ wallet was a secure financial product that anyone with Internet access could use. There were no ID requirements, no deposit requirements, and no limit of the movement of funds through the account. Just like in the USA during that period, this new digital currency technology was brand-new and without government supervision or regulations. The new WebMoney financial infrastructure moved money over the Internet and not through any regulated financial institution, particularly any Russian bank.

The Russian bank crisis had created millions of people that needed this financial service, and the WebMoney Transfer non-bank Internet payment platform met those needs. These local Russian consumers offered a very identifiable market.

It is important to note that the launch of WebMoney Transfer in a consumer market that already held huge demand for a bank alternative is a very different product roll-out than any other digital currency system of the time. The WebMoney operators knew their target market and offered the exact products to meet their needs. At the time, there was no question about "who" would use their digital currency system.

Digital currency in the WebMoney system allowed any user to send local payments as easy as they could transfer funds around the globe. Users could also store funds online in the electronic system effectively creating a bank and savings account outside of the ailing Russian banks. Similar to other digital currency products, WebMoney transactions are non-repudiable, and it is not possible to reverse a transaction.

WebMoney digital currency units circulate online as WM units. The user can set up an online or mobile purse to accept and hold these units. Sending payments mean spending units from the purse.

Soon after the original WMZ dollar purse, a WMR Russian Ruble purse also came online. From that first day of business in 1998, the WMZ dollar purse has remained popular with users. Because of the need for a non-bank payment system, WebMoney was quickly adopted by both users and merchants in Russia.

Unlike all other digital currency systems of the period that introduced innovative currency products in search of users, WebMoney found the users and filled their payment needs. This point cannot be understated. With the hundreds of digital currency products now available through decentralized digital currency systems, it should be a priority for designers and operators to ask themselves, "who will use my currency," long before any new regime opens for use.

WebMoney has since introduced many additional digital currency products. Here is a list of various currencies offered through WebMoney Transfer system. Each currency has its e-purse; however, digital units from one purse cannot be deposited or exchanged for another through the WebMoney client software. If a user has WMZ and wants WMR, they must locate an independent agent, sell WMZ, and buy WMR. Each purse is mutually exclusive of the others, and a user cannot exchange between purses within the WebMoney platform.

Assets representing the value of each unit are held separately in a corporate vehicle that functions precisely for that jurisdiction. No purse is the same. Each is created to perform for the country in which it operates. Once again, the Russians are creating a product to fill a specific need. There is no mystery to why the company created each purse specifically designed for use in that country and no question to the target audience of local users. Russian innovation created these original online digital currency products. In 2016, it is the Russian systems still leading the world in payment innovation.

WebMoney system supports multiple purses secured by various resources and tangibles.

- WMR—equivalent to RUR, Russian Rubles (R-Purse)
- WMZ—equivalent to USD, US Dollars (Z-Purse)
- WME—equivalent to EUR, euros (E-Purse)
- WMU—equivalent to UAH, Ukrainian Hryvnias (U-Purse)

- WMB—equivalent to Belorussian Rubles (B-Purse)
- WMY—equivalent to Uzbek Sum (Y-Purse)
- WM-C and WM-D—WMZ equivalent for transactions on C- and D-purses (credit purses)
- WMG—equivalent of Gold Bullion (G-Purse)
- WMV—equivalent to prepaid transfer in Vietnamese Dongs (V-purse)
- WMX—Bitcoin Property Rights

WebMoney Transfer has built a multibillion-dollar empire on the ability to identify non-bank consumer markets. The wide variety of WM units caters to non-bank Internet users, and the company's marketing efforts do not include efforts to convert or compete with banks. The company's products fill the gaps left behind by big money banks. WM units serve those excluded from conventional banking.

This point, regarding "who" will use a digital currency and "why" is critical to understand when discussing online payment systems. WebMoney products target specific groups of non-bank users and are designed to work alongside national currency, not replace it. Other digital currency systems, such as e-gold, had no specific target group of users. It was a replacement for federal money. The e-gold system was designed to be a better mousetrap and compete head-to-head with government-issued money.

WebMoney Transfer operates the software platform responsible for the purses (accounts) and transactions between all of the digital currency products and platforms. The networks include account access from mobile devices, tablets, laptops, and personal computers. There are even some products that can be combined and used as a physical voucher.

The WebMoney system was created to operate separately from the public exchanges, insulated from payment risk. The operation's structure protects the stored financial assets from the exchange risks of dealing with day-to-day customer national money transactions. Similar to some other digital currency systems, there was no option for users to send funds to WebMoney Transfer. Third-party independent agents handled all exchange transactions.

An attractive design of the WebMoney structure is the business or corporate entity backing each the transaction platform.

WebMoney creates each business entity backing the various purses as complete separate corporate units independent of the software transaction platform. The purse structure is organized as a stand-alone legal entity best suited for convenient operation in that local jurisdiction. These are

all mutually exclusive entities and never share or commingle funds. Even with the over one million transactions occurring each day through the WebMoney platform, no funds from any purse are ever combined with assets from another currency purse. Each is a closed ledger circulating only those units denominated for that particular purse. All purses belonging to a single user are conveniently secured by the Keeper software assigned to the user's WMID registration number.

The design behind the WebMoney Purses is structured on a set of standardized interfaces for managing users' property rights. The business entity behind each purse is called the Guarantor. The user can create any number of purses across each platform. Value within the system and each purse are measured individual WM units that correspond to that specific purse.

The type of entity holding the value behind the digital units varies for each purse. Here are examples of each purse design and specific Guarantors that maintain the customer value.

Z-Purse: WMZ—Goods certificate, in USD;
Guarantor for WMZ
Amstar Holdings Limited
Postal address: 13 Upper Baggot Street, 2nd Floor, Dublin 4, Ireland[2]
WMZ-Certificate is an electronic accounting document certifying the right of the Buyer for the certain amount of acquired goods or services of the Supplier and granting the right to receive goods or services from the Supplier contrary to granting WMZ-Certificate without any cash settlements.[3]

E-Purse: WME—Electronic money in EUR;
Guarantor for WME
WebMoney Europe LTD
Postal address: Compass House, Vision Park, Chivers Way, Histon, Cambridge, CB24 9AD, England, UK[4]

WebMoney defines WME as electronic money denominated in euros. The value corresponding to a euro balance held in one or more segregated bank accounts in which the funds correspond to the balance in the WebMoney WME purse. These funds are segregated according to the provisions of the Electronic Money Regulations 2011.

> WebMoney Europe Ltd is authorized by the Financial Conduct Authority under the Electronic Money Regulations 2011 (Firm Ref. No. 900216) for the issuing of electronic money.[5]

This WME purse is the very popular European medium of exchange accessible for use across the European Union. It carries some specific user requirements and is not available to users residing in some regions of the world, including the USA.

There are transaction limits and document requirements that vary with the user's level of activity. Here are some examples.

User identification documents are not required if the total deposits during one calendar year to all WME purses registered to one WebMoney Passport do not exceed 2500 WME.

If the user's total WME incoming transactions exceed 2500 WME, the following documents and verification are required.

- A valid national passport or another ID document.
- Proof of residential address, for example, banks statement or utility bill, no older than three months.

For the user that has over 15,000 incoming WME transactions per calendar year, additional bank documents and source of funds are required.

Other WebMoney purses are designed and created for specific users in targeted area of the world. WebMoney identifies a group of users in need of these non-bank payment systems and crafts a highly convenient and useable purse for that group.

R-Purse: WMR—Bearer's bank cheque in Russian Rubles;
U-Purse: WMU—Bank account claims in UAH;
B-Purse: WMB—Electronic Belorussian Roubles;
K-Purse: WMK—A receipt for the right to receive EKZT from the guarantor for a certain amount;
G-Purse: WMG—Warehouse receipt for stock Gold in a certified storage area;
X-purse: WMX—Stored property rights to publish entries in the global public database of the bitcoin.org network.[6]

In May 2013, WebMoney introduced a new purse that used bitcoin. WMX identifies the purse. The digital units are termed property rights to publish entries in the distributed transaction database of the bitcoin.org

peer-to-peer network. The purse Guarantor stores bitcoin deposits. Just like other WebMoney units, a user can exchange them for any other WM unit through any third-party independent agent.

Each purse has been created around that specific jurisdiction for the optimal performance of a vehicle containing a value for those local customers. This structure is not a one-size-fits-all approach to global currency and offers a very different mechanism for the design and creation of a new digital currency. WebMoney establishes and releases new currency products to meet the needs of specific groups of users.

Building on the success of WebMoney products, new purses had to offer convenient and inexpensive customer access to the online stored digital funds. This is accomplished using a variety of methods of innovative products including:

Keeper Standard (Mini)

This client software is a regular website purse that is compatible with any browser, including mobile browsers. WebMoney Keeper Standard is a straightforward and convenient product that is available immediately after the registration. Access to the software requires a login and a password.

Keeper Mobile

This client is a straightforward and user-friendly application software for mobile devices, MacOS and Linux. It is used for the management of WebMoney purses and functions alongside Keeper WinPro or Keeper WebPro. It is available for Android, iOS, Windows Phone, Blackberry, Bada, and Java-enabled phones.

Keeper WebPro (Light)

This client software is a website purse with sophisticated extended functions. This version can be used alongside Keeper Standard and Keeper Mobile software.

Access to the purse is accomplished using any one of three options:

- A personal digital certificate
- Using a login and a password
- Authorization through the E-NUM service

E-NUM is a modern authorization system that requires enhanced information security. It is a convenient software system that allows users to store WM Keeper keys in its database. This procedure enables the secure use of WebMoney purses and services from virtually any computer.

There is statistics page for WebMoney transactions, showing transparent activity. It includes daily, weekly, and monthly totals for operations, new registrations, and active users. Statistics for March 26, 2016, show 10,112,673 from the first day of March. Total registrations in the WebMoney system were 30,982,268, and there were 231,422 active users in March. This section of the website also includes historical data and charts showing the number of cumulative transactions for certain periods.

Fees within the WebMoney Transfer system are much lower than those required by local banks. The system factors in smaller payments around the fifty- or one-hundred-dollar level. The goal of the scheme is not to replace national currency but to offer customers in a specific niche an alternative to banks. WebMoney welcomes small non-bank customers by providing inexpensive financial products that are useful in local commerce.

In the late 1990s and for several years after the introduction of WebMoney Transfer digital currency, the products were no regulated in Russia or other parts of the world. However, the organization recognized a need for common sense voluntary regulations over user account that would protect the system from being exploited by bad actors. HYIP type investments were never permitted; other "investment" accounts were also not permitted and closed by WebMoney administrators. Registration with the system also required acceptance of an anti-money laundering program. The WebMoney Passport requirements functioned as an excellent KYC platform and advanced customer security for the entire system. Partnership and cooperation among other financial companies, payment businesses, and industry organizations are a continuing practice of WebMoney Transfer. In 2009, WebMoney became a member of the Russian Electronic Money Association (REMA).

In 2016, non-bank populations around the world and areas of low credit card penetration are still top consumer markets for the introduction of digital currency products. WebMoney Transfer has been very successful in designing and introducing digital currency purses into these areas creating millions of new users. The basic Alias passport is still available without any identification documents. This ability to open and instantly use a digital currency account still represents one of the defining features of digital currency. There is also no restrictions or value transfer limits on the Alias user.

Notes

1. "Personal Passport—WebMoney Wiki," WebMoney Wiki—WebMoney, accessed January 7, 2015, https://wiki.wmtransfer.com/projects/webmoney/wiki/Personal_passport.
2. "Wmtransfer.com/System Subjects/Guarantors," WebMoney—Universal Payment System, accessed September 28, 2015, http://www.wmtransfer.com/eng/subjects/guarantors/index.shtml.
3. "Wmtransfer.com/Legal Information/Guarantors/Agreement on WMZ," WebMoney—Universal Payment System, accessed August 17, 2015, http://www.wmtransfer.com/eng/legal/garants/wmz.shtml.
4. "Wmtransfer.com/System Subjects/Guarantors," WebMoney—Universal Payment System, accessed November 18, 2015, http://www.wmtransfer.com/eng/subjects/guarantors/index.shtml.
5. "Wmtransfer.com/Legal Information/Guarantors/Agreement on WME," WebMoney— Universal Payment System, accessed December 15, 2015, http://www.wmtransfer.com/eng/legal/garants/wme.shtml.
6. "Wmtransfer.com/Description/Purse Types," WebMoney—Universal Payment System, accessed May 16, 2015, http://www.wmtransfer.com/eng/information/wmwallets/index.shtml.

CHAPTER 11

New FinCEN Rules

The two new FinCEN rules were:

- Definitions and Other Regulations Relating to Prepaid Access

On July 29, 2011, FinCEN published a final rule, renaming "stored value" as "prepaid access" and amending the BSA regulations relating to prepaid access (the "Prepaid Access Rule").[1]
On September 9, 2011, FinCEN extended the compliance date for certain provisions of the final Prepaid Access Rule. While initial requirements went into effect on September 27, 2011, the full compliance was not required until March 31, 2012.

- Definitions and Other Regulations Relating to Money Services Businesses

On July 18, 2011, FinCEN released the final rule, Definitions and Other Regulations Relating to Money Services Businesses (the "MSB Rule"). The rule more clearly defined which businesses qualify as Money Services Businesses (MSBs) and are therefore subject to anti-money laundering rules under the Bank Secrecy Act (BSA).[2]
The MSB Rule became effective on September 19, 2011. Compliance with the MSB Rule was not required until January 23, 2012.

When any new technology or financial product, such as digital currency, emerges within the global marketplace, the product or service may

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0_11

also present new risks that threaten America's financial system. A decade of rapid growth, coupled with the obvious lack of customer identification and account supervision, had produced some well-documented money laundering risks and regulatory abuses.

Digital financial products that were able to transfer funds outside conventional financial channels had become a common tool for the exploitation and misuse of the US financial system. The law enforcement community had begun to recognize the methods by which digital currency was being abused by bad actors.

As the industry continued to expand, regulatory agencies began crafting new rules designed to prevent these abuses. In 2009, barely a year after the e-gold guilty pleas, FinCEN moved ahead with new regulations. Unfortunately, the new regulations seemed to also crush any hope for the continued expansion of digital currency in the USA.

During that time, discussions with the law enforcement community highlighted how the innovative structure of Internet digital currency had inadvertently created barriers for investigating financial crimes. Early digital currency operator's lack of common sense supervision had also impeded the efforts of law enforcement in curtailing illegal activity.

Digital currency products were not the only new technology linked to criminal activity. Prepaid card products had been increasingly used for illicit purposes and illegal cross-border transactions.

The ease with which prepaid cards could be purchased combined with the velocity of money flowing through these products had made stored value cards very suitable for criminal activity and the movement of criminal proceeds, particularly across international borders.

Similar to digital currency value loaded to an ATM card, the cash proceeds of criminal activity were being loaded to prepaid card accounts and accessed from other parts of the world. Money was being loaded onto prepaid cards in Texas and withdrawn in Medellin, Colombia. The proceeds of credit card fraud occurring in the USA was being loaded onto cards using digital currency and withdrawn from ATMs in Moscow, Russia. Both prepaid cards and digital currency gave individuals the ability to distribute substantial amounts of money without being subject to the reporting requirements, recordkeeping, or customer identification that applies to bank customers.

By 2000, it was abundantly clear that US financial regulations had not kept pace with emerging prepaid technology or innovative digital currency products. FinCEN was now determined to change this situation

with comprehensive new rules that would properly categorize digital currency products as "prepaid access" (formerly stored value) and assign new strict regulation across the industry.

In September 2010, Mr. James Freis, Jr., acting Director of the US Department of the Treasury's Financial Crimes Enforcement Network, made this comment during a speech to the Money Transmitter Regulators Association regarding FinCEN's plans to shape the network's new regulations.

> A balance between expanding financial inclusion and ensuring financial transparency for law enforcement, while staying mindful of the obligations and costs to the industry in complying with regulatory requirements – and the related potential inconvenience passed down to customers.[3]

In July 2011, after a lengthy public comment period allowing industry feedback, FinCEN released two final rules that updated several critical definitions within the preexisting US financial regulatory framework. These updated US financial regulations had a permanent impact on the digital currency industry, for both domestic and international companies.

Full compliance with the new Prepaid Access Rule was required by March 31, 2012. The final rule illustrated that FinCEN had recognized the emergence of a more mature industry. Advances in technology and the needs for a more secure marketplace had warranted stronger supervision of prepaid access products including digital currency. The prepaid card business was moving to a higher level of supervision and regulation that had been occupied by all other US Money Service Business products. The new regulations were also dragging all digital currency products and companies along for the ride.

These new Bank Secrecy Act rules established that both digital currency issuers and exchange agents were subject US regulations as it applied to financial institutions. Under the BSA, these newly categorized MSBs had to implement anti-money-laundering programs, regularly make certain reports to FinCEN, and maintain records that would facilitate financial transparency. Additionally, companies, both domestic and foreign, had to fully identify all customers.

Digital currency companies were required to register with FinCEN and became subject to IRS examination for BSA compliance. Both domestic and foreign digital currency issuers and exchange agents, servicing US clients, were now required to:

- Establish written AML programs designed to prevent the company from being used to facilitate money laundering or terror funding activities;
- File Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs); and
- Maintain customer identification and client transaction records, including those relating to the purchase of certain monetary instruments with currency, transactions by currency dealers or exchangers, and certain transmittals of funds.[4]

Banks, credit card issuers, and existing financial service companies previously had the luxury of time, in which to establish compliance programs. Over months and even years, compliant financial institutions hired experienced employees who fine-tuned reporting techniques understood how to supervise client accounts. Banks and credit card companies already had sophisticated in-house software platforms that alerted the business to improper customer account activity. Over the decades, an entire global compliance industry had risen to meet the needs of those financial institutions.

However, new digital currency businesses, particularly those operated from foreign jurisdictions, did not have this luxury of time. Young digital currency companies and exchange agent businesses, many of which were single-person operations, were now required to develop and implement these new compliance procedures in just a matter of a few months.

A company such as GoldMoney, not headquartered in the USA, but engaged in the payments business with US clients, rejected the substantial costs of being licensed in each US state. A Russian organization such as WebMoney Transfer wanted to avoid the costs and hassles of vigorous compliance examinations and scrutiny from both federal and state regulatory agencies. This was a very intense change for digital currency companies. The two largest businesses at that time, WebMoney Transfer and GoldMoney, simply opted out of the US market. As both companies were domiciles in foreign jurisdictions, the cost of complying with the new BSA regulations was astronomical. Just the state money transmitter licensing costs would run in the millions of dollars. It was more economical to pull out of the US payments market, and for a time, WebMoney Transfer even blocked US IP addresses.

GoldMoney changed the company's digital platform and dropped any ability to send payments between GoldMoney customer accounts, outside of the company's home jurisdiction of Jersey. Changing the company's busi-

ness plan and structure allowed GoldMoney to continue doing business in the USA and avoid any money transmitter licensing requirements. These were dismal changes for GoldMoney. The company that, over the previous decade, had earned four patents for the process of using precious metal as a form of digital payment, was now backing away from that entire business model. Within the digital currency industry, GoldMoney's withdrawal from the payments business was analogous to Steve Jobs in 1978, deciding to pull out of the US computer market because of restrictive regulations.

The new FinCEN rules had forced issuers and agents to run from American customers, and many US digital currency users were also asking, "Is it worth it for me to use digital currency here in America?" Drastic changes and deep pockets were needed to compete and comply in the new US marketplace. America later received both of those features in the form of bitcoin cryptocurrency.

No centralized digital currency company was up for this challenge. Even WebMoney Transfer, a company that had been supporting US customers since the late 1990s, saw no benefits in complying with FinCEN's new rules. Fortunately for WebMoney, pulling out of the US market affected less than 1 percent of their total customer base. In researching this matter, it was not possible to find a single digital currency exchange agent, that operated from outside the USA, willing to comply with these new regulations. A majority of foreign exchange agents were now reluctant to even service anyone in the USA.

According to the new Prepaid Access Rule, all digital currency businesses, even exchange agents, were now subject to new registration, customer identification, verification, reporting, and recordkeeping obligations. Additionally, businesses had to adopt and maintain effective anti-money-laundering program and respond to law enforcement requests for information. In fact, a physical location in the USA was required for legal service.

These new regulations were designed to apply across a broad spectrum of existing products and future designs including those using magnetic stripe cards, Internet systems, fobs, and mobile phone networks. The final rule was crafted to be technology neutral and adaptable to a wide range of products and possible future technologies.

Prepaid Access

This rule expanded the definition of a money transmitter to include most digital currency products (Excluding Bitcoin):

> "Prepaid Access," which replaces the term "stored value" in the BSA rules, is defined as "[a]ccess to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number."
>
> The supplemental information to the Final Rule notes that the definition of "prepaid access" is modified from the proposal to recognize that Prepaid Access is not itself a device or vehicle, but that such a device or vehicle is a means through which prepaid funds are accessed.[5]

For the first time in history, this new rule had identified most digital currency as the type and category of financial products requiring any entity doing business with those products to be properly registered with the federal government and properly licensed at the state level. The Prepaid Access Rule identified digital currency as a "stored value" prepaid financial product.

The MSB Rule

> This rulemaking amends the current MSB regulations by:
>
> (1) ensuring that certain foreign-located persons engaging in MSB activities within the United States are subject to the BSA rules;
>
> (2) updating the MSB definitions to reflect past guidance and rulings, current business operations, evolving technologies, and merging lines of business; and
>
> (3) separating the provisions dealing with stored value from those dealing with issuers, sellers, and redeemers of traveler's checks and money orders.[6]

The new MSB Rule also added the phrase "other value that substitutes for currency" to the definition of "money transmitter services." A "money transmitter" is a type of money services business already covered by the Bank Secrecy Act Regulations. Digital currency qualifies as "other value" because either it has an equivalent value in national money or a digital unit functions as a substitute for national money.

A digital currency system that issues or transmits digital units of value from point A to point B is considered a money transmitter business. Any person who accepts national currency and delivers an amount of value in digital currency to another party is considered a money transmitter. A person accepting digital currency value from one party and transmitting that value to another party by any means is considered a money transmitter.

An important part of the new regulations stated that qualifying as an MSB does not depend on whether the person is licensed as a business or any other factors such as number of employees, or being engaged in a for-profit venture. The new rule clarified that it is the activity of the party that causes it to be characterized as an MSB.

More importantly, any financial party qualifies as an MSB based on its activity within the USA. No physical presence, office, branch, or agency was required. A digital currency company utilizing the Internet to service clients that resided in the USA was now considered a US Money Service Business. Overseas exchange agents and foreign digital currency issuers now faced the new reality that servicing US clients without the proper financial registrations and licensing was considered a crime.

Foreign digital currency companies engaged in business with any US clients either had to register and comply with the new regulations or exit the US market. Reporting, recordkeeping, and AML program requirements under the BSA applied to all digital currency companies anywhere in the world, if they were servicing any US customers. In 2012, registration and appointment of an agent for US service of legal process was also included in this program. GoldMoney sent out this email text to all customers:

> We are writing to advise you of a change of services we currently offer to our customers with a Full Holding. Since the launch of GoldMoney in 2001, we have continued to change and adapt to the global increase of compliance requirements for payment service providers. Due to this growing trend of regulation, we have decided to suspend the following services until further notice with an effective date of the 21st January 2012:
>
> - The facility to make and receive payments in precious metals to or from other GoldMoney Full Holding customers.
> - The facility to convert directly between the various currencies.
>
> Basic Holding owners do not have access to these features and are therefore not affected by this change.
>
> Our research has proven that our customers' use of the metal payments and currency exchange services is not significant and we trust that the suspension of these services will not be inconvenient for the majority of our customers.
>
> In accordance with our Customer Agreement, we are providing advance notice of this change to our services that will take effect on the 21st January 2012 at 12am local London time (GMT).[7]

These new rules established several critical changes to the US laws regulating digital currency products. The final rule, Definitions and Other Regulations Relating to Money Services Businesses, helped to more clearly define which digital currency businesses qualified as Money Services Businesses (MSBs) and were therefore regulated as a financial institution. These changes required digital currency issuers and exchange agents to abide by US legal requirements including a federal registration, state money transmitter licensing, and anti-money-laundering rules under the Bank Secrecy Act. The MSB Rule enabled both domestic and foreign digital currency companies, to more easily determine if their companies were engaged in money transmitting. The new rules also highlighted the activity of foreign digital currency companies "engaged" in business with US customers. This rule directly addressed the cross-border global nature of Internet digital currency systems. The rule also clearly stated that there was no threshold of activity for a money service business. Any entity that engages in money transmission in any amount is subject to the BSA rules.

The regulations were very clear on the new procedures and guidelines for all MSBs including previously unlicensed and unsupervised foreign digital currency exchange agents:

> FinCEN has issued regulations under the BSA implementing the record-keeping, reporting, and other requirements of the BSA with respect to these types of financial institutions. These regulations refer to these types of financial institutions as——money services businesses. Like other financial institutions under the BSA, MSBs must implement AML programs, make certain reports to FinCEN, and maintain certain records to facilitate financial transparency. MSBs are generally required to:
>
> (1) establish written AML programs that are reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities; (2) file Currency Transaction Reports and Suspicious Activity Reports; and
>
> (3) maintain certain records, including those relating to the purchase of certain monetary instruments with currency, transactions by currency dealers or exchangers (to be called——dealers in foreign exchange under this rulemaking), and certain transmittals of funds. Most types of MSBs are required to register with FinCEN13 and all are subject to examination for BSA compliance by the Internal Revenue Service (IRS).[8]

This US Treasury's new requirements arose out of a recognition that the Internet and other technological advances had made it increasingly pos-

sible for any residing in a foreign jurisdiction to offer MSB services over the Internet to customers residing in the USA.

With these new regulations, FinCEN was seeking to ensure that BSA rules apply to all persons engaging in these financial activities within the USA, regardless of their physical location.

The MSB Rule defined all US digital currency businesses now belonged in the category of money transmitter. FinCEN Director Freis remarked on this topic in 2010 at the Money Transmitter Regulators Association annual meeting:

> Let me clarify something critical here – the framework for money transmission – and that which we propose for prepaid access – is an activity-based test. More specifically, we are looking at the ability to introduce value – and to realize that value at some subsequent time, different place, by a different person, for a subset of the original amount, or some combination of the foregoing.[9]

As a money transmitter, businesses doing business in a particular state also require that state license and operate according to that state's requirements for money transmitters. Forty-eight US states and District of Columbia have money transmitter laws. These laws prohibit money transmitter businesses and activity without being licensed by the state or licensed as an authorized distributor of a money transmitting service, such as a Western Union office or MoneyGram agent.

The regulations are not uniform, and one state can have rules that considerably differ from another. Any money transmitter business engage in US business is likely to have applied and obtained different state financial license. The process involved with garnering all of these licenses is considerable and can take more than one year. The cost for all licenses is estimated at around $2 million. Consequently, the process and costs for a previously unlicensed foreign digital currency company, such as WebMoney or GoldMoney, to obtain the proper state licensing and comply with BSA regulations was a monumental task. In 2016, state agencies have the main responsibility for regulating money transmitting businesses. These regulations and agencies focus on consumer protection within each state's jurisdiction. Agencies of the federal government are most concerned with preventing money laundering and possible terror financing. The principal revisions in the new MSB Rule included an amended definition of a Money Service Business.

Definition of MSB

The Final Rule amended the definition of "money services business" at 31 CFR 1010.100(ff). An entity may now qualify as a money services business (MSB) under the Bank Secrecy Act (BSA) regulations based on its activities within the United States, even if none of its agents, agencies, branches or offices are physically located in the United States. The Final Rule arose in part from the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations. FinCEN seeks to ensure that the BSA rules apply to all persons engaging in covered activities within the United States, regardless of the person's physical location.

The MSB Rule amended the definition of an MSB to include a "person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the US," acting in the capacity of certain regulated activities, i.e. a dealer in foreign exchange, check casher, issuer or seller of traveler's checks or money orders, provider and seller of prepaid access, and/or money transmitter ("Regulated MSB Activity").[10]

Foreign-Located MSBs

The new MSB regulations addressed the global nature of financial crimes and the Internet. All foreign-located MSBs are considered financial institutions according to the BSA. All activity for clients in the USA must be recorded, and the MSB must comply with recordkeeping, reporting, and anti-money-laundering program requirements according to the BSA. These institutions must also register with FinCEN. The Final Rule requires that the foreign-located MSB also must appoint a person that resides in the USA as an agent for receiving service and legal notification from the court as it would be required with respect to comply with the BSA regulations.

Activity Threshold

The MSB regulations currently apply to persons engaged that exceed $1000 for any person in one day. The $1000 threshold remained unchanged by the MSB Rule. However, money transmitters are the exception to this rule. Money transmitters do not have an activity threshold. However, FinCEN indicated it is continuing to study the MSB activity thresholds and may consider future changes.

Penalties

Failure to comply with these new regulations subjected the foreign-located MSB to the same civil and criminal penalties for violations of the BSA as they applied for domestic MSBs.

Money Transmitter

The term money transmission service was amended to reflect "other value that substitutes for currency." Under the MSB Rule, a person who provides money transmission services or any other person engaged in the transfer of funds is a money transmitter.

Suspicious Activity Reporting

Consistent with the standard for reporting suspicious activity under the BSA, if a financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity or appears to be indicative of money laundering, terrorist financing, or other violation of law or regulation, the financial institution should file a SAR.

FinCEN did not directly address decentralized virtual currency, such as Bitcoin, until issuing Guidance in March 2013.

Notes

1. "FinCEN Issues Prepaid Access Final Rule Balancing the Needs of Law Enforcement and Industry," Welcome To FinCEN.gov, last modified July 26, 2011, https://www.fincen.gov/news_room/nr/html/20110726b.html.
2. "FinCEN Clarifies Money Services Businesses Definitions Rule Includes Foreign-Located MSBs Doing Business in U.S," Welcome To FinCEN.gov, last modified July 18, 2011, https://www.fincen.gov/news_room/nr/html/20110715.html.
3. "Prepared remarks of Director Freis, delivered at Money Transmitter Regulators Association 2010 annual meeting," The Financial Crimes Enforcement Network, accessed April 4, 2015, https://www.fincen.gov/news_room/speech/html/20100901.html.

4. "Msb.gov—Money Laundering Prevention," Welcome To FinCEN.gov, accessed February 5, 2016, https://www.fincen.gov/financial_institutions/msb/materials/en/prevention_guide.html.
5. "Federal Register, Volume 76 Issue 200 (Monday, October 17, 2011)," U.S. Government Publishing Office, accessed March 28, 2016, https://www.gpo.gov/fdsys/pkg/FR-2011-10-17/html/2011-26743.htm.
6. "Amendment to the Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Money Services Businesses," Welcome To FinCEN.gov, accessed September 15, 2015, https://www.fincen.gov/statutes_regs/frn/pdf/MSB_Final_Rule_Definition_and_OtherRegulations.pdf.
7. Carl Mullan, private email from GoldMoney, December 2011.
8. "Amendment to the Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Money Services Businesses," Welcome To FinCEN.gov, accessed September 15, 2015, https://www.fincen.gov/statutes_regs/frn/pdf/MSB_Final_Rule_Definition_and_OtherRegulations.pdf.
9. "Prepared Remarks of Director Freis, Delivered at Money Transmitter Regulators Association 2010 Annual Meeting," Welcome To FinCEN.gov, last modified September 1, 2010, https://www.fincen.gov/news_room/speech/html/20100901.html
10. "FIN-2012-A001," FinCEN.gov, accessed September 20, 2015, https://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A001.html.

Index

P.C. Mullan, *A History of Digital Currency in the United States*,
DOI 10.1057/978-1-137-56870-0