



Follow the Money: Civilizing the Darkweb Economy

By Tom Kellermann, Global Fellow

Introduction

Digital payment systems and financial services have become an essential part of modern technological infrastructure, growing exponentially over the past three decades and continuously innovating to meet the demands of the international financial system.¹ These systems and services have already revolutionized payments in many parts of the world. Research indicates that widespread adoption and use of digital financial services could provide access to an additional 1.6 billion unbanked and underbanked people.² By 2025, this could increase the GDPs of all emerging economies by 6 percent, or a total of \$3.7 trillion.

Despite the real utility that such innovation has delivered, however, the increasing digitization of

the global financial system has not been without its share of problems. The growing use of cyber as a domain for financial activity has inherently expanded the potential attack surface for would-be cyber criminals and the World Economic Forum now estimates that the cost to the global economy due to cybercrime is roughly \$445 billion a year.³

Yet despite this increased potential for wrongdoing, the pervasiveness of cybercrime that we observe today is not inevitable. Rather, this modern epidemic of cybercrime is sustained via the transfer of capital associated with virtual currencies.

While many digital services implement Anti-Money Laundering (AML) and Know Your Customer (KYC)

protocols, criminal entities have demonstrated innovative rigor in their efforts to continuously abuse the loopholes and take advantage of selective enforcement and defensive vulnerabilities that plague the financial services sector today. The international financial system is constantly facing new threats as technology proliferates and diversifies. Increasingly, individuals and syndicates use these systems to bypass traditional indicator and warning systems relied upon by regulators and law enforcement. According to a recent FBI statistic, “three in four money laundering cases involve digital currencies.”⁴ While digital currency is still a relatively specialized market, one continuous issue has been the increasing number of security breaches and thefts on digital currency exchange platforms.⁵ This is because there are few cryptocurrency exchanges that perform KYC procedures and basic security checks, both of which have been commonplace protocols in major exchanges for over a decade.⁶ Money laundering can easily take place in these virtual environments, as they can provide high levels of anonymity and low levels of detection.

Money laundering through digital currency and payment systems is just one example of illicit activity online. Other criminal markets include child pornography, weapons and drug sales, hackers and murder for hire, zero day exploits, and false identity documents. The advent of these criminal markets enabled by anonymous virtual currencies have created a global bazaar for criminals and organized crime to reach a mass global market.⁷

Collectively, these digital infrastructures represent a “3-legged stool” of illicit activity: it allows for the storage of illicit goods and services, it provides utility of financial vehicles to allow for the exchange of goods and services, and it develops techniques

to successfully transport the illicit goods and services around the world. The goal of this report is to “civilize” one leg of the stool—the utility of financial vehicles to allow for the exchange of illegal goods and services and the application of AML practices to curb cybercrime.

Before launching into potential policy prescriptions, however, in order to properly understand why virtual currencies are central to the increasing prevalence of cybercrime and the serious financial implications of this, it is useful to conceptualize what is meant by “digital currencies” and to examine innovation in the realm of virtual currencies and the underlying technology involved in payment systems.

Digital currency is distinct from common mediums of exchange because it is not funded by a central bank or government.

Digital Currencies 101:

Digital currency is defined as “digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency.”⁸ Digital currency is distinct from common mediums of exchange because it is not funded by a central bank or government. The borderless features of the Internet allow this privately issued currency to complete instantaneous transactions worldwide. In regard to digital currency, there are generally two main types: centralized and decentralized.

Centralized digital currency is stored in a central repository, where users can exchange the digital currency with other account holders.⁹ When con-

Definitions

- **Virtual Currency:** As defined by FATF this includes cryptocurrencies like bitcoin, but also a range of other digital payment systems like the Russian's WebMoney, the Chinese AliPay, and PayPal as well as many others.
- **Dark Web:** An Internet within the Internet of mainly anonymous sites which include many criminal markets and forums. Accessible through easy to obtain special software.
- **Deep Web:** Password protected and unindexed sites on the regular Internet which includes many criminal sites and forums.
- **Darkweb:** A term which collectively includes the criminal and terrorist sites on the Deep Web and the DarkWeb defined above.
- **Exchanges:** Serving to exchange fiat currency (dollars, euros...) for Virtual Currencies like bitcoin, WebMoney, stored value cards and many others these exchanges are currently regulated in the United States and some other countries. They are the key choke point in the use of these systems for illegal purposes.

verting conventional currency into digital currency, these central repositories typically partner with currency "exchangers," who are responsible for the conversion. A large quantity of digital currency is purchased from the central repository by the exchangers, who then credit the account holder after receiving the conventional currency. When account holders wish to convert their digital currency to a conventional currency, a reverse transaction is carried out back through the exchangers.

Decentralized digital currency, the most well-known of which is Bitcoin, has no central monetary authority and is instead exchanged through a peer-to-peer payment system consisting of its users' computers and devices.¹⁰ This means that the digital currency is a direct exchange, and there are no intermediaries. The digital currency is generated, or "mined," by a mathematical algorithm on computers which can execute complex number-crunching tasks.¹¹ The network of user computers is used to both mon-

itor and verify the creation and transfer of digital currency between users.¹² A log is maintained of every transaction between users, which is updated by user machines participating in the mining of this currency.

Since their creation, Internet-based virtual currencies such as bitcoin, the Chinese AliPay and Russian WebMoney systems have appreciated with incredible speed. Bitcoin's capitalization is \$100B globally, while WebMoney possesses that value in Russia alone.

Modernizations of Money Laundering and Virtual Currencies

Virtual currencies, alternative payments, and remittance systems have been major economic forces for the more than 3 billion people living in underdeveloped societies around the world.¹³ One of the

most significant aspects of these payment systems is that they “are part of a thriving ecosystem of not only virtual currencies but also other digital, mobile and stored value systems that cumulatively number in the thousands.”¹⁴ The ecosystem is revolutionizing payment capabilities through the financial inclusion and growth of regions such as Africa and South Asia.¹⁵ Take Kenya for example, which in 2007 launched M-Pesa—a mobile phone-based platform for the transfer of money and financial services.¹⁶ Today, 43 percent of Kenya’s GDP flows through M-Pesa which has over 237 million person-to-person transactions.¹⁷



But while most new financial technology (FinTech) is being used for legitimate purposes, they are ripe for abuse. According to Tom Glaessner, “while these sorts of financial services firms are important for purposes of efficiency, they also present substantial ‘operational risks’ in light of the dark web and lack incentives for proper intrusion detection.” Not surprisingly then, criminals are abusing digital currencies and alternative payment systems to fuel underground illicit economies and launder money across international borders.¹⁸ Trend Micro’s Chief Cybersecurity Officer Ed Cabrera states that, “global

money laundering schemes are estimated at 2% to 5% of global GDP, or roughly \$1-2 trillion annually and estimated in the United States at \$300 billion in illicit proceeds.”¹⁹

Many illicit transactions on the Dark Web take place using virtual currencies, like Bitcoin. However, the use of more anonymous cryptocurrencies is rapidly increasing and gaining market share, including Monero, Dash, and Zcash.²⁰ Many centralized virtual currencies and “the thousands of websites that buy and sell decentralized virtual currencies like bitcoin, lie outside of the western financial system’s network of detection points.”²¹ Suspicious Activity Reports (SARs) are not generated, and the sheer scale of potential criminal use of the financial services are unknown. Effective regulatory responses to virtual currencies continue to pose a significant challenge because they operate on a global scale and cut across the responsibilities of many different agencies.²²

The modernization of digital payment systems and internet-connected devices is also fueling the growth of both offenders and victims of child pornography.²³ While the vast majority of child sexual exploitation material (CSEM) is still produced by hands-on offenders, a growing number of Darkweb forums are facilitating the exchange of CSEM leading to an overall increase in volume of this material on the Darkweb.²⁴ Offenders are increasingly using these forums to produce, share, and distribute CSEM. Offenders are also producing CSEM for financial gain, particularly in the commercial production of Live Distant Child Abuse (LDCA)—where the offender pays “to direct the live abuse of children on a pre-arranged specific time-frame through video sharing platforms.”²⁵ Researchers have discovered

that crypto-currencies, such as Bitcoin, are purchasing CSEM ranging from \$1 to hundreds of dollars.²⁶ The UK's Internet Watch Foundation revealed that almost 200 child pornography websites accepted Bitcoin, and over 30 of these sites accepted *only* Bitcoin.²⁷ According to Scott Dueweke, it has been observed in the last year that many of these sites are now moving to the more anonymous cryptocurrencies, like Monero. Effective regulation of virtual currency exchanges, with KYC and AML rules that form a common identity standard, will help to combat child exploitation online and disrupt the provision of payments for cybercrime conspiracies.

In addition to organized crime, extremist organizations are also known to use cryptocurrency and alternative payment systems for operational purposes and to raise funds. Many of these payment services and cryptocurrencies offer true or relative anonymity. For many users, privacy rather than anonymity may be their primary interest, as they do not seek to hide illegitimate behavior. However, the anonymity offered by some of these systems facilitate illicit financial flows (IFF) as well as offering privacy. Advice is available on various social media platforms regarding jihadists' potential use of Dark Wallet, a bitcoin wallet that provides anonymity, and on how to set up an anonymous donation system to send money using bitcoin. This advice is clearly motivated to mask the provision of funds to ISIL.

This raises the necessity of increased regulation of digital money. From a macro perspective: during the past century global trade agreements, formal financial infrastructure and the legal norms underpinning these systems have been dominated by the West. The explosion of decentralized P2P (Napster, Bitcoin, etc.) systems has, and increasingly will, destabilize these centrally organized systems.

These P2P systems could be used to destabilize the global norms established by GATT, FATF, and other international agreements and structures upon which modern civilized society has been built. This is true not only because of criminal and transnational terrorist organizations' use of these systems, but because of potential systemic destabilization by nations states such as Russia (WebMoney), China (AliPay), and even North Korea (ransomware use of bitcoin and cryptocurrency exchange hacks). Russia just recently approved a cryptocurrency regulation framework, which would allow the government to "levy a 13% tax on individuals and organizations who attempt to trade their 'cryptorubles' for a fiat currency but cannot demonstrate that the coins were obtained legally."²⁸ This policy could allow Russia to profit from money laundering and other financial crimes.

This policy could allow Russia to profit from money laundering and other financial crimes.

Digital Currency: E-Gold and Liberty Reserve Case Studies

Few cases exemplify the historic nefarious utility of centralized digital currencies like that of two exchanges: E-Gold and Liberty Reserve. The centralized company E-Gold, a digital currency backed by gold, was founded in 1996. E-Gold was the first-of-its-kind, circulating a private currency around the globe and independent of government controls.²⁹ Customers could open accounts anonymously and complete quick, borderless transactions. By 2001, customer accounts for the company had grown to approximately 288,000 and held \$16 million in

value.³⁰ E-Gold's reserves of sovereign coins were converted into bars and transferred to bank vaults in London and Dubai. At its peak, E-Gold's reserves were valued at nearly \$85 million.

E-gold ran into several setbacks over the next few years, including system performance issues with the company's growing traffic load and cyber scammers launching phishing attacks to drain customer accounts.³¹ But the company rebounded in 2004 after scaling its infrastructure and deploying an anti-phishing remedy, growing its customer accounts to 3.5 million in 165 countries by 2005.³² Although the company was enjoying success, E-Gold caught the attention of U.S. law enforcement who discovered that the company was a money-transfer platform used by cyber criminals because the criminals could remain anonymous.

E-Gold had not been adhering to regulatory protocols, such as registering with the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) or authenticating the identity of its customers through KYC protocols.³¹ FBI and Secret Service agents raided E-Gold business locations in mid-December 2005, freezing the company's domestic bank accounts.³³ Authorities had discovered that cybercriminals were using E-Gold not only to transfer money worldwide, but also to park and accumulate value in the system. Over the next two years, the founder of E-Gold provided integral information to investigators on cyber criminals using his platform and assisted in tracking the criminals down for arrests. ¹

1 In April 2007, E-Gold executives were indicted on federal charges of money laundering and running an unlicensed money transmitting business. The executives plead guilty to the charges in 2008, but were spared jail time for unintentionally engaging in the illegal activity.

Though not backed by gold, Liberty Reserve was a centralized virtual currency service incorporated in 2006 in Costa Rica.³⁵ From 2009 through 2013, Liberty Reserve was a leading digital platform for cyber-criminals to launder money.³⁶ The company's more than one million customers could move money worldwide through its multiple layers of anonymity. Liberty Reserve customers could open an account using an email, name, and physical address. However, both the name and physical address could be fake, which was demonstrated by the criminal monikers "Russia Hackers" and "Hacker Account" found during the investigation.³⁷ The customer would then transfer money to a money "exchanger," who would deposit an equivalent amount of Liberty Reserve currency into the customer's account for a five percent transaction fee.³⁸ The majority of these exchangers were operating unlicensed money transmitting businesses and were concentrated in countries including Malaysia, Russia, Nigeria, and Vietnam, which had little government oversight.³⁹

When the money had been successfully exchanged into Liberty Reserve currency, Liberty Reserve customers could exchange the currency for any type of good or service, including stolen credit cards, drugs, and computer hackers for hire.⁴⁰ In addition to exchanges for goods and services, criminal transactions through Liberty Reserve included proceeds for drug trafficking, identity theft, computer hacking, and child pornography, to name a few.⁴¹ Liberty Reserve was also used to transfer funds and distribute proceeds among criminal associates in countries around the world including the United States, Vietnam, Nigeria, Hong Kong, and China.⁴²

Liberty Reserve was contacted by a Costa Rican agency known as Superintendencia General de Entidades Financieras (SUGEF) around 2009 to apply for a license to operate the money transmitting business. SUGEF, which was a financial regulating insti-

tution, refused to grant Liberty Reserve a license when the company sent in its application because Liberty Reserve lacked even basic AML controls. Liberty Reserve did not have KYC procedures, which included verifying the identity of the company's clients, nor did the company track suspicious activity within its system.⁴³

Liberty Reserve had failed to obtain the license to operate by 2011, and that same year a notice to financial institutions was issued by the U.S. Department of Treasury's FinCEN warning them about providing financial services to Liberty Reserve because it was "being used by criminals to conduct anonymous transactions to move money globally."⁴⁴ Within two weeks of obtaining this notice, Liberty Reserve informed SUGEF that the company had been sold and was no longer operating in Costa Rica. But the company just moved underground, continuing to work in Costa Rica and out of offices held in the name of shell companies owned by a Liberty Reserve executive.⁴⁵

When Liberty Reserve executives began emptying the bank accounts of Liberty Reserve and transferring millions of dollars from Costa Rica to shell companies in Cyprus and Russia, the Costa Rican government seized \$19.5 million left in Liberty Reserve Costa Rican bank accounts at the request of U.S. law enforcement.⁴⁶ When the U.S. government shut down Liberty Reserve in 2013, "it had more than 5 million user accounts worldwide, including more than 600,000 accounts associated with users in the United States, and had processed millions of transactions."⁴⁷ In January 2016, Liberty Reserve executives plead guilty to running a digital currency business used by criminals around the world that laundered more than \$250 million.⁴⁸

FinCEN was key in implementing regulatory action against Liberty Reserve, including targeting the

company as a primary money laundering concern and allowing for the imposition of special measures to be taken against Liberty Reserve.⁴⁹ These measures successfully eliminated the Liberty

Reserve currency from the U.S. financial system. In addition to FinCEN's regulatory success, the international community played a significant role in supporting the investigation process. The Liberty Reserve case demonstrated a global alliance to counter money-laundering and enhance transparency involving digital currency transactions. The following paragraphs describe several enforcement mechanisms that have made significant strides in AML and regulation of digital currencies worldwide.

These measures successfully eliminated the Liberty Reserve currency from the U.S. financial system.

Domestic and International Efforts to Improve Financial Security

Domestically, the Financial Crimes Enforcement Network (FinCEN) operates as the chief American Financial Intelligence Unit (FIU) and is the designated administrator of the Bank Secrecy Act (BSA) of 1970.⁵⁰ The BSA was established to help identify the source and movement of currency through the United States and into financial institutions, requiring U.S. financial institutions to establish AML programs and maintain records.⁵¹ The BSA has been integral in combating money laundering and acts as the primary federal AML law.⁵² FinCEN is currently working to determine the key vulnerabilities of virtual currency that could be exploited by illicit actors and developing a corresponding regulatory approach for industry to mitigate those vulnerabilities.⁵³ One ex-



ample of success in this endeavor is FinCEN's coordination with federal law enforcement in May 2015 to assess the first civil enforcement action against Ripple Labs Inc., a virtual currency exchanger, for failure to register with FinCEN as a money services business and uphold sufficient AML measures.⁵⁴ Presently, all cash seized as a result of money laundering is placed in the Treasury Forfeiture Fund (TFF) or the Department of Justice Assets Forfeiture Fund (AFF), depending on the law enforcement agencies involved in the seizure.

Internationally, the Financial Action Task Force (FATF) has been integral to worldwide efforts in combating AML/ATF through the production of its *Forty Recommendations* that facilitate regulatory reforms in these areas. These recommendations form the foundation for a coordinated response to threats on the financial system, as well as help to ensure a level playing field for those involved.⁵⁵ In a recent speech the FATF President, Santiago Otamendi,

highlighted the significance of FATF in working with the BIS Financial Stability Board to address the vulnerabilities of banks de-risking and de-marketing. These practices could lead to "financial exclusion and an increase in the risks of money laundering and terrorist financing, as well as indirectly encouraging the use of cash and informal or non-regulated channels."⁵⁶ Major financial institutions have been severing foreign banking clients, where money laundering and terrorist financing concerns are high, in an attempt to avoid compliance issues and manage risk. This is detrimental to regions around the world who have limited access to the global financial network, or have lost access entirely. With these banking clients severed from the global financial network, there is concern that criminals will launder money no longer through financial institutions but through underground or unregulated means.

The Strategic Opportunity for Action

Cyberspace is not a peaceful environment. In 2018 cybercrime conspiracies will become increasingly punitive and destructive. As the use of virtual currencies and financial systems continues to increase and innovate, so too does global crime. Fintech firms themselves present significant 'operational risks,' lacking the incentive for proper intrusion detection or KYC/AML protocols. Given that 50% of all crimes now have a cyber component, it is high time that we follow the money to create an international e-forfeiture fund. The modern epidemic of cybercrime and cyberespionage can also be mitigated through modernization of existing authorities to empower FATF, FinCEN and TFF to combat cyber-money laundering. Virtual currencies and other alternative payment systems that facilitate money-laundering associated with cybercrime, as well as terrorist financing, must be held to account. Every digital payment service should abide by KYC and cooperate in all law enforcement initiatives regarding cybercrime conspiracy, or it should be shut down. We can prioritize this effort through the establishment of an international Fund, maintained by the forfeiture of all money laundering and terrorist financing seizures. Proceeds from the Fund will be allocated specifically to critical infrastructure protection of the global financial system. The Fund would represent a global public/private partnership to combat money laundering using these alternative payment systems. Furthermore, creating global, enforceable rule sets through such a public/private partnership could help the private sector flourish and simultaneously meet the needs of the unbanked and underbanked throughout the world. Virtual currencies who refuse to *know their customers* or *freeze accounts* of those engaged in criminal conspiracies should be subject to Treasury Executive Office for Asset Forfeiture (TEOAF).

The strategic plan must be international in nature and thus incorporate the Bank of International Settlements. The Bank for International Settlements (BIS), an organization that has been at the forefront of fostering international coordination in the pursuit of monetary and financial stability for over eight decades. Established in 1930, this international financial entity is "owned by 60 member central banks, representing countries from around the world that together make up about 95% of world GDP."⁵⁷ The US, in cooperation with the BIS, could galvanize the international community to participate in AML efforts and create an incentive for partners to tackle corruption with international transparency. Global crime is facilitated by the use of cyber currencies, and more needs to be done to regulate and supervise digital payment systems and ensure basic KYC and information reporting protocols. The U.S., in partnership with the BIS, can incentivize the international community to participate in this effort by the capital gains that will ultimately be afforded as a result of hindering criminal activity from the illegal buying and selling of goods and services. Finally, due to lack of incentives for developing nations to participate, we must provide the proverbial "carrot." In order to facilitate international cooperation 40% of the funds forfeited must be distributed to the host countries critical infrastructure protection efforts or other international efforts to secure payment systems and e-governance. It is time to civilize cyberspace via thoughtful, strategic action.

Appendix:

FinCEN

FinCEN was originally created in 1990 to provide an intelligence and analytical network that would support investigations, detections, and prosecutions of both domestic and international money laundering. The mission of FinCEN was broadened in 1994 to include regulatory responsibilities and the organization merged with the Treasury Department's Office of Financial Enforcement (OFE) to create a single, unified AML agency.⁵⁸ Today, the mission of FinCEN "is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."⁵⁹

FinCEN works closely with law enforcement, industry, and international partners to regulate and protect the U.S. financial system.⁶⁰ Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) are two reporting streams that contribute to the majority of BSA data collected by FinCEN.⁶¹ These reporting streams are fulfilled by financial institutions which are required to report both suspicious transactions and cash transactions totaling more than \$10,000.⁶² This information provides FinCEN and other law enforcement agencies the necessary data "to detect and prevent money laundering, other financial crimes, and terrorism."⁶³ Highlighted by its then Acting Director Jamal El-Hindi, virtual currency is one of the current focus areas FinCEN is working to actively address.⁶⁴

FinCEN plays a key role in addressing new vulnerabilities of the current period of technological innovation and growth that characterize the financial industry. According to El-Hindi, "any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering

or terrorist financing."⁶⁵ In July of this year, FinCEN and the U.S. Department of Treasury launched its second supervisory action, assessing a civil monetary penalty of \$110,003,314 against Canton Business Corporation (BTC-e).⁶⁶ BTC-e was a foreign entity operating one of the largest virtual currency exchanges in the world, with activities in the United States.⁶⁷

The Genesis of FATF

The Financial Action Task Force (FATF) was established in 1989 at the G-7 Summit in Paris in response to growing concern over money laundering.⁶⁸ The original Task Force was convened by the G-7 member states, eight additional countries, and the European Commission. The major economic powers of the world came to realize that non-state actor groups who threatened the stability of their regimes were being empowered with asymmetrical capabilities due to their capacity to launder money. According to FATF, the objectives of the Task Force "are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a 'policy-making body' which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas."⁶⁹ Initial responsibilities of the Task Force included examining techniques and trends of money laundering and setting the measures that needed to be taken by the international community to combat money laundering. In 1990, FATF released its first *Forty Recommendations* which provided "a comprehensive plan of action needed to fight against money laundering."

Eight Special Recommendations were added to the report in 2001 in response to the fight against terrorist financing, with a ninth special recommendation published in 2004. FATF has conducted several comprehensive revisions of its *Forty Recommendations* in response to the continued evolution of money laundering techniques. The most current revised version of the FATF recommendations were published in 2012, which now include measures to deal with new threats including the financing of proliferation of weapons of mass destruction (WMD). The updated recommendations are also meant to be “clearer on transparency and tougher on corruption,” and have fully integrated the *Nine Special Recommendations* on terrorist financing with the measures against money laundering.

Presently, FATF has expanded to a total of 37 members and observers representing most major financial hubs around the world. There are also 31 additional regional and international organizations that are Observers or Associate Members of FATF and participate in its work.⁷⁰ The Task Force has a fixed lifespan which requires a specific decision by its Ministers to continue. The decision-making body of FATF, the Plenary, meets three times per year to discuss the progress of its members in implementing measures established by the FATF and to review tactics, techniques, and countermeasures of money laundering and terrorist financing criminals.⁷¹ The current mandate of FATF was adopted in April 2012 and extends to 2020. The threat from money laundering, terrorist financing, and WMD proliferation financing has never been greater. The FATF is now focused on ensuring the effectiveness of countries in implementing financial laws and the capacity of those countries to deal with these threats. The

FATF has had success with its methodologies in assessing whether countries are effectively preventing financial crime. Countries around the world are identifying and disrupting organized crime groups and terrorist networks, cutting them off from the financial system.⁷²

Forfeiture Laws

The Treasury Forfeiture Fund (TFF) is administered by the Treasury Executive Office for Asset Forfeiture (TEOAF), and was established in 1992 as a successor to the Customs Forfeiture Fund.⁷³ All forfeitures made by Treasury and participating law enforcement agencies are placed in the TFF, a special fund earmarked by law for specific purposes which are defined by Title 31 U.S.C. 9703.⁷⁴ Once property or cash is seized, the forfeiture process begins. The seized currency is initially deposited into a holding account and then transferred to the Fund as forfeited revenue.⁷⁵ The participating agencies of the TFF include: U.S. Immigration and Customs Enforcement (ICE), Internal Revenue Service Criminal Investigations Division (IRS-CI), U.S. Customs and Border Protection (CBP), U.S. Secret Service (USSS), and U.S. Coast Guard.

The forfeited cash or proceeds from forfeited property cannot be retained by any Treasury investigative agency.⁷⁶ Seized cash, unless being used as evidence, is deposited into the Suspense Account until the forfeiture is approved. If valued at \$5,000 or less, seized cash can be held with approval from the Attorney General, and amounts over \$5,000 can be held with approval from the Chief of the DOJ's Asset Forfeiture and Money Laundering Section.⁷⁷

First and foremost, the forfeiture revenue is obligated to meet the expenses of running the TFF.⁷⁸ Any unobligated balances remaining are deposited in the general fund of the Treasury of the United States and are available for the Secretary to allocate to any of the participating Treasury law enforcement agencies, as well as other law enforcement agencies that do not have forfeiture authority, such as FinCEN and the Tax and Trade Bureau.⁷⁹ Specifically, the proceeds of asset forfeiture from the TFF are allocated to fund programs or activities aimed at disrupting criminal activity, as well as enhance forfeiture capabilities.⁸⁰ The Secretary also has Discretionary Category Expenses, where the Secretary “has the discretion to make payments from the Fund for other specifically authorized expenses when the funds are appropriated for that purpose.”⁸¹

The Department of Justice also maintains an Asset Forfeiture Program (AFP).⁸² The Department of Justice Assets Forfeiture Fund (AFF) is a special fund within the Department of Treasury and was established by the Comprehensive Crime Control Act of 1984.⁸³ The AFF receives the proceeds of forfeited assets used to facilitate federal crimes.⁸⁴ The DOJ participants that contribute to the AFF include, but are not limited to the following agencies: Money Laundering and Asset Recovery Section (MLARS), Bureau of Alcohol, Tobacco, and Firearms and Explosives (ATF), Drug Enforcement Agency (DEA), and the Federal Bureau of Investigation (FBI).⁸⁵ The Attorney General has authorization to use the Fund to pay any expenses associated with forfeiture operations, as well as to finance general investigative expenses.⁸⁶ These authorized uses are detailed in Title 28 U.S.C.⁸⁷

Over the last ten years, the annual forfeiture revenue to the AFF has evolved into a multi-billion-dollar national program.⁸⁸ Most of this increase in forfeiture revenue can be attributed to large fraud and economic crime forfeiture cases.⁸⁹ The future of this Fund is hard to predict, however, due to unpredictable timing and outcome of judicial forfeiture processes. Large forfeiture cases (i.e. assets valued at \$20 million or more) are more volatile, but are an increasingly significant part of the AFF’s revenue as smaller seizures and forfeiture of non-cash assets appear to be in decline.⁹⁰ The Fund has three types of spending authority: Mandatory Budget Authority, Discretionary Budget Authority, and Super Surplus.⁹¹ Mandatory Authority is used to defray the cost of forfeiture related activities, victim compensation, and equitable share of the proceeds to state and local partners. Discretionary Authority funds non-forfeiture related activities, which fall under three categories: purchase of evidence, equipping of conveyances, and awards for information. Super Surplus represents the remaining balance of the Fund that the Attorney General is authorized to use “for any federal law enforcement, litigative/prosecutive, and correctional activity, or any other authorized purpose of the DOJ.”⁹²

Endnotes

- 1 T.S. “How does Bitcoin work?” *The Economist*, April 11, 2013, <http://www.economist.com/bitcoin-explained>
- 2 *Ibid.*
- 3 *Ibid.*
- 4 Scott Dueweke, “Hearing entitled Virtual Currency: Financial Innovation and National Security Implications.”
- 5 *Ibid.*
- 6 *Ibid.*
- 7 Daniel Runde, “M-Pesa and the Rise of the Global Mobile Money Market,” *Forbes*, August 12, 2015, <https://www.forbes.com/sites/daniel-runde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/#79ac1e615aec>
- 8 *Ibid.*
- 9 Ed Cabrera, “Risk and Reward of Alternative Payment Systems,” *Trend Micro*, October 26, 2016, <http://blog.trendmicro.com/risk-and-reward-of-alternative-payment-systems/>
- 10 *Ibid.*
- 11 Scott Dueweke, “Hearing entitled Virtual Currency: Financial Innovation and National Security Implications.”
- 12 *Ibid.*
- 13 Dong He, et al, “Virtual Currencies and Beyond: Initial Considerations,” *International Monetary Fund*, January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>
- 14 “European Union Serious and Organised Crime Threat Assessment 2017,” p. 31
- 15 *Ibid.*
- 16 *Ibid.*
- 17 Kristen Schweizer, “Bitcoin Payments by Pedophiles Frustrate Child Porn Battle,” *Japan Times*, October 10, 2014, <https://www.japantimes.co.jp/news/2014/10/10/world/crime-legal-world/bitcoin-payments-by-pedophiles-frustrate-child-porn-battle/#.WezF8EzMy3U>
- 18 *Ibid.*
- 19 Josiah Wilmoth, “Putin Approves Framework for ICO, Cryptocurrency Regulation,” *Cryptocoins News*, October 28, 2017, <https://www.cryptocoins-news.com/putin-approves-framework-for-ico-regulation/>
- 20 Kim Zetter, “Bullion and Bandits: The Improbable Rise and Fall of E-Gold,” *WIRED*, June 9, 2009, <https://www.wired.com/2009/06/e-gold/>
- 21 *Ibid.*
- 22 *Ibid.*
- 23 *Ibid.*
- 24 *Ibid.*
- 25 *Ibid.*
- 26 Seth Robbins, “Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash,” *InSight Crime*, June 4, 2013, <http://www.insightcrime.org/news-analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash>
- 27 “Sealed Indictment: United States v. Liberty Reserve S.A.”
- 28 *Ibid.*
- 29 Seth Robbins, “Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash.”

- 30 “Sealed Indictment: United States v. Liberty Reserve S.A.” 44 *Ibid.*
- 31 Seth Robbins, “Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash.” 45 *Ibid.*
- 32 “Sealed Indictment: United States v. Liberty Reserve S.A.” 46 *Ibid.*
- 33 *Ibid.* 47 *Ibid.*
- 34 *Ibid.* 48 <https://www.bis.org/about/index.htm?m=1%7C1>
- 35 *Ibid.* 49 “FinCEN—History,” Federation of American Scientists, <https://fas.org/irp/agency/ustreas/fincen/history.htm>
- 36 *Ibid.* 50 “Mission,” *Financial Crimes Enforcement Network*, <https://www.fincen.gov/about/mission>
- 37 *Ibid.* 51 “Statement of Acting Director Jamal El-Hindi before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance,” *Financial Crimes Enforcement Network*.
- 38 “Founder of Liberty Reserve Pleads Guilty to Laundering More Than \$250 Million through His Digital Currency Business,” *Department of Justice*, January 29, 2016, <https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital> 52 *Ibid.*
- 39 *Ibid.* 53 *Ibid.*
- 40 “Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern,” *Department of Treasury*, May 28, 2013, <https://www.fincen.gov/sites/default/files/shared/311--LR-NoticeofFinding-Final.pdf> 54 *Ibid.*
- 41 “History of Anti-Money Laundering Laws,” *Financial Crimes Enforcement Network*, <https://www.fincen.gov/history-anti-money-laundering-laws> 55 “Statement of Acting Director Jamal El-Hindi before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance,” *Financial Crimes Enforcement Network*, pg. 9
- 42 “Statement of Acting Director Jamal El-Hindi before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance,” *Financial Crimes Enforcement Network*, April 27, 2017, <https://www.fincen.gov/news/testimony/statement-acting-director-jamal-el-hindi-house-committee-financial-services> 56 “Statement of Acting Director Jamal El-Hindi before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance,” *Financial Crimes Enforcement Network*. pg. 11
- 43 *Ibid.* 57 Weinstein, Jason and Alan Cohn, “Significant FinCEN Action Against BTC-e, Implications for Virtual Currency Exchangers,” *Miami Legal Resources*, July 31, 2017, <http://www.miamilegalresources.com/files/124842499.pdf>
- 58 *Ibid.*
- 59 “History of the FATF,” *Financial Action Task Force*, <http://www.fatf-gafi.org/about/historyofthefatf/>

- 60 “Who We Are,” *Financial Action Task Force*, <http://www.fatf-gafi.org/about/whoweare/>
- 61 “Member Countries and Observers,” *Financial Action Task Force*, <http://www.fatf-gafi.org/faq/membercountriesandobservers/#d.en.11224>
- 62 “Who We Are,” *Financial Action Task Force*.
- 63 “Speech by FATF Executive Secretary,” *Financial Action Task Force*, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-apg-speech-july-2017.html>
- 64 “Resource Center: Asset Forfeiture,” *Department of Treasury*, <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Asset-Forfeiture.aspx>
- 65 “Terrorism and Financial Intelligence: Treasury Executive Office for Asset Forfeiture,” *Department of Treasury*, <https://www.treasury.gov/about/organizational-structure/offices/Pages/The-Executive-Office-for-Asset-Forfeiture.aspx>
- 66 “Treasury Forfeiture Fund,” *Department of Treasury*, https://www.treasury.gov/about/budget-performance/Documents/13_Treasury_Forfeiture_GTG.pdf
- 67 “Guidelines for Seized and Forfeited Property,” *Department of the Treasury*, July 2001, <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Asset-Forfeiture/Documents/redbook.pdf>
- 68 “39 CFR 233.7-Forfeiture authority and procedures,” *Cornell Law School*, <https://www.law.cornell.edu/cfr/text/39/233.7>
- 69 “31 U. S. Code 9705-Department of the Treasury Forfeiture Fund,” *Cornell Law School*, <https://www.law.cornell.edu/uscode/text/31/9705>
- 70 “Terrorism and Financial Intelligence: Treasury Executive Office for Asset Forfeiture,” *Department of Treasury*.
- 71 *Ibid.*
- 72 “Guidelines for Seized and Forfeited Property,” *Department of the Treasury*.
- 73 “Asset Forfeiture Program,” *Department of Justice*, <https://www.justice.gov/afp>
- 74 “U.S. Department of Justice Asset Forfeiture Program: FY 2017 Performance Budget Congressional Justification,” *Department of Justice*, <https://www.justice.gov/jmd/file/821291/download>
- 75 “The Fund,” *Department of Justice*, <https://www.justice.gov/afp/fund>
- 76 <https://www.justice.gov/afp/participants-and-roles>
- 77 “The Fund,” *Department of Justice*.
- 78 *Ibid.*
- 79 “U.S. Department of Justice Asset Forfeiture Program: FY 2017 Performance Budget Congressional Justification,” *Department of Justice*.
- 80 *Ibid.*
- 81 *Ibid.*
- 82 “U.S. Department of Justice Asset Forfeiture Program: FY 2018 Performance Budget Congressional Justification,” *Department of Justice*. <https://www.justice.gov/file/968796/download>
- 83 *Ibid.*

Acknowledgments

A special note of gratitude to Katherine Vockery as Lead Researcher and the following individuals who provided sage insights: Scott Dueweke; Meg King; Tom Glaessner.



Tom Kellermann





CEO of Strategic Cyber Ventures and serves as a Global Fellow for the Wilson Center.

digitalfutures@wilsoncenter.org

Over his career, Tom has acted as a trusted advisor to Fortune 100 clients and the U.S. government regarding their cybersecurity postures and the cyber threat landscape. Tom served as a Commissioner on the Congressionally Appointed Commission on Cybersecurity for the 44th Presidency. He has also served on the board of the National Cyber Security Alliance, The International Cyber Security Protection Alliance (ICSPA), and the National Board of Information Security Examiners Panel for Penetration Testing. Tom has held the positions of CISO at Trend Micro, Vice President for Cybersecurity at Trend Micro, Chief Technology Officer at AirPatrol Corporation, and Vice President of Security Awareness for Core Security. Previously, Tom was the Senior Data Risk Management Specialist for the World Bank Treasury Security Team, where he was responsible for internal cyber-intelligence and policy and for advising central banks around the world about their cyber-risk posture and layered security architectures. Tom was also an Adjunct Instructor in the School of International Service and the Kogod School of Business at American University for eight years.

The opinions expressed in this article are those solely of the author.

The Wilson Center

-  wilsoncenter.org
-  facebook.com/WoodrowWilsonCenter
-  [@TheWilsonCenter](https://twitter.com/TheWilsonCenter)
-  202.691.4000

Digital Futures Program

-  wilsoncenter.org/program/digital-futures-project
-  digitalfutures@wilsoncenter.org
-  facebook.com/WilsonCenterDFP
-  [@WilsonCenterDFP](https://twitter.com/WilsonCenterDFP)
-  202.691.4002

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027