Money Laundering:

Making Bad Money Good

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Extremist Propaganda in Social Media: A Threat to Homeland Security (CRC Press)
Threat Level Red: Cybersecurity Research Programs of the U.S. Government (Auerbach Publications)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

Money laundering generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities. Money laundering facilitates a broad range of serious underlying criminal offenses and ultimately threatens the integrity of the financial system.

The United States Department of the Treasury is combating all aspects of money laundering at home and abroad, through the mission of the Office of Terrorism and Financial Intelligence (TFI). TFI utilizes the Department's many assets - including a diverse range of legal authorities, core financial expertise, operational resources, and expansive relationships with the private sector, interagency and international communities - to identify and attack money laundering vulnerabilities and networks across the domestic and international financial systems. In recent decades, U.S. law enforcement has encountered an increasing number of major financial crimes, frequently resulting from the needs for drug trafficking organizations to launder large sums of criminal proceeds through legitimate financial institutions and investment vehicles.

Cornerstone is Immigration and Customs Enforcement's (ICE) initiative to detect and close down weaknesses within U.S. financial, trade and transportation sectors that can be exploited by criminal networks. Law enforcement entities share criminal typologies and methods with businesses and industries that manage the very systems that terrorists and criminal organizations seek to exploit. This sharing of information allows the financial and trade community to take precautions in order to protect themselves from exploitation.

The El Dorado Task Force consists of more than 260 members from more than 55 law enforcement agencies in New York and New Jersey – including federal agents, state and local police investigators, intelligence analysts and federal prosecutors. The El Dorado Task Force is headquartered at the New York Special Agent in Charge Office and at other locations in the New York/New Jersey Metropolitan area. The Task Force targets financial crime at all levels. Task force agents educate the private financial sector to identify and eliminate vulnerabilities and promote anti-money laundering legislation through training and other outreach programs. Prosecutors use a full range of criminal and civil laws to prosecute targets and forfeit the proceeds of their illicit activity. The El Dorado Task Force uses a systems-based approach to investigating financial crimes by targeting vulnerabilities such as the Black Market Peso Exchange and commodity-based money laundering. ICE leads investigations against corrupt foreign public officials who have used U.S. financial institutions and other investment vehicles to facilitate criminal acts involving the laundering of proceeds from public corruption.

Trade-based money laundering is an alternative remittance system that allows illegal organizations the opportunity to earn, move and store proceeds disguised as legitimate trade. Value can be moved through this process by false-invoicing, over-invoicing and under-invoicing commodities that are imported or exported around the world. Criminal organizations frequently exploit global trade systems to move value around the world by employing complex and sometimes confusing documentation associated with legitimate trade transactions. ICE established the Trade Transparency Unit initiative to target trade-based money laundering worldwide.

History of Anti-Money Laundering Laws

Money laundering is the process of making illegally-gained proceeds (i.e. "dirty money") appear legal (i.e. "clean"). Typically, it involves three steps: placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean." Money laundering can facilitate crimes such as drug trafficking and terrorism, and can adversely impact the global economy.

In its mission to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity," the Financial Crimes Enforcement Network acts as the designated administrator of the Bank Secrecy Act (BSA). The BSA was established in 1970 and has become one of the most important tools in the fight against money laundering. Since then, numerous other laws have enhanced and amended the BSA to provide law enforcement and regulatory agencies with the most effective tools to combat money laundering. An index of anti-money laundering laws since 1970 with their respective requirements and goals are listed below in chronological order.

Bank Secrecy Act (1970)

Established requirements for recordkeeping and reporting by private individuals, banks and other financial institutions

Designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions

Required banks to (1) report cash transactions over $10,000 using the Currency Transaction Report; (2) properly identify persons conducting transactions; and (3) maintain a paper trail by keeping appropriate records of financial transactions

Money Laundering Control Act (1986)

Established money laundering as a federal crime

Prohibited structuring transactions to evade CTR filings

Introduced civil and criminal forfeiture for BSA violations

Directed banks to establish and maintain procedures to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA

Anti-Drug Abuse Act of 1988

Expanded the definition of financial institution to include businesses such as car dealers and real estate closing personnel and required them to file reports on large currency transactions

Required the verification of identity of purchasers of monetary instruments over $3,000

Annunzio-Wylie Anti-Money Laundering Act (1992)

Strengthened the sanctions for BSA violations

Required Suspicious Activity Reports and eliminated previously used Criminal Referral Forms

Required verification and recordkeeping for wire transfers

Established the Bank Secrecy Act Advisory Group (BSAAG)

Money Laundering Suppression Act (1994)

Required banking agencies to review and enhance training, and develop anti-money laundering examination procedures

Required banking agencies to review and enhance procedures for referring cases to appropriate law enforcement agencies

Streamlined CTR exemption process

Required each Money Services Business (MSB) to be registered by an owner or controlling person of the MSB

Required every MSB to maintain a list of businesses authorized to act as agents in connection with the financial services offered by the MSB

Made operating an unregistered MSB a federal crime

Recommended that states adopt uniform laws applicable to MSBs

Money Laundering and Financial Crimes Strategy Act (1998)

Required banking agencies to develop anti-money laundering training for examiners

Required the Department of the Treasury and other agencies to develop a National Money Laundering Strategy

Created the High Intensity Money Laundering and Related Financial Crime Area (HIFCA) Task Forces to concentrate law enforcement efforts at the federal, state and local levels in zones where money laundering is prevalent. HIFCAs may be defined geographically or they can also be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)

[Title III of the USA PATRIOT Act is referred to as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001]

Criminalized the financing of terrorism and augmented the existing BSA framework by strengthening customer identification procedures

Prohibited financial institutions from engaging in business with foreign shell banks

Required financial institutions to have due diligence procedures (and enhanced due diligence procedures for foreign correspondent and private banking accounts)

Improved information sharing between financial institutions and the U.S. government by requiring government-institution information sharing and voluntary information sharing among financial institutions

Expanded the anti-money laundering program requirements to all financial institutions

Increased civil and criminal penalties for money laundering

Provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern"

Facilitated records access and required banks to respond to regulatory requests for information within 120 hours

Required federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations

Intelligence Reform & Terrorism Prevention Act of 2004

Amended the BSA to require the Secretary of the Treasury to prescribe regulations requiring certain financial institutions to report cross-border electronic transmittals of funds, if the Secretary determines that such reporting is "reasonably necessary" to aid in the fight against money laundering and terrorist financing

2015 National Money Laundering Risk Assessment

The *2015 National Money Laundering Risk Assessment* (NMLRA) identifies the money laundering risks that are of priority concern to the United States. The purpose of the NMLRA is to explain the money laundering methods used in the United States, the safeguards in place to address the threats and vulnerabilities that create money laundering opportunities, and the residual risk to the financial system and national security. The terminology and methodology of the NMLRA is based on the guidance of the Financial Action Task Force (FATF), the international standard-setting body for anti-money laundering and counter-terrorist financing safeguards. The underlying concepts for the risk assessment are threats (the predicate crimes associated with money laundering), vulnerabilities (the opportunities that facilitate money laundering), consequence (the impact of a vulnerability), and risk (the synthesis of threat, vulnerability and consequence).

Threats

Money laundering[1] is a necessary consequence of almost all profit generating crimes and can occur almost anywhere in the world. It is difficult to estimate with any accuracy how much money is laundered in the United States. However, while recognizing the limitations of the data sets utilized, this assessment estimates that about $300 billion is generated annually in illicit proceeds. Fraud and drug trafficking offenses generate most of those proceeds.

Fraud encompasses a number of distinct crimes, which together generate the largest volume of illicit proceeds in the United States. Fraud perpetrated against federal government programs, including false claims for federal tax refunds, Medicare and Medicaid reimbursement, and food and nutrition subsidies, represent only one category of fraud but one that is estimated to generate at least twice the volume of illicit proceeds earned from drug trafficking. Healthcare fraud involves the submission of false claims for reimbursement, sometimes with the participation of medical professionals, support staff, and even patients. Federal government payments received illegally by check can be cashed through check cashing services, some of which have been found to be complicit in the fraud.

Use of the Internet to commit identity theft has expanded the scope and impact of financial fraud schemes. Personal identifying information and the information used for account access can be stolen through hacking or social exploits in which the victim is tricked into revealing data or providing access to a computer system in which the data is stored. A stolen identity can be used to facilitate fraud and launder the proceeds. Stolen identity information can be used remotely to open a bank or brokerage account, register for a prepaid card, and apply for a credit card.

Drug trafficking is a cash business generating an estimated $64 billion annually from U.S. sales. Mexico is the primary source of supply for some drugs and a transit point for others. Although there are no reliable estimates of how much money Mexican drug trafficking organizations earn overall (estimates range from $6 billion to $39 billion), for cocaine, Mexican suppliers are estimated to earn about 14 cents of every dollar spent by retail buyers in the United States. It is the thousands of low level drug dealers and distributors throughout the country who receive most of the drug proceeds.

The severing by U.S. banks of customer relationships with Mexican money exchangers (casas de cambio) as a result of U.S. enforcement actions against U.S. banks between 2007 and 2013, combined with the U.S. currency deposit restrictions imposed by Mexico in 2010, are believed to have led to an increase in holding and using drug cash in the United States and abroad, because of placement challenges in both countries. This shifted some money laundering activity from Mexico to the United States.

International organized crime groups target U.S. interests both domestically and abroad. The criminal activity associated with these groups includes alien smuggling, drug trafficking, extortion, financial fraud,

illegal gambling, kidnapping, loan sharking, prostitution, racketeering, and money laundering. Some groups engage in white-collar crimes and co-mingle illegal activities with legitimate business ventures.

Vulnerabilities

The size and sophistication of the U.S. financial system accommodates the financial needs of individuals and industries globally. The breadth of products and services offered by U.S. financial institutions, and the range of customers served and technology deployed, creates a complex, dynamic environment in which legitimate and illegitimate actors are continuously seeking opportunities.

This assessment finds that the underlying money laundering vulnerabilities remain largely the same as those identified in the 2005 United States Money Laundering Threat Assessment. The money laundering methods identified in this assessment exploit one or more of the following vulnerabilities:

- Use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds;
- Opening bank and brokerage accounts using nominees to disguise the identity of the individuals who control the accounts;
- Creating legal entities without accurate information about the identity of the beneficial owner; Misuse of products and services resulting from deficient compliance with anti-money laundering obligations; and
- Merchants and financial institutions wittingly facilitating illicit activity.

Cash (bank notes), while necessary and omnipresent, is also an inherently fungible monetary instrument that carries no record of its source, owner, or legitimacy. Cash generated from drug trafficking or fraud can be held or spent as cash. Alternatively, criminals can buy cashier's checks, money orders, nonbank wire transfers, prepaid debit cards, and traveler's checks to use instead of cash for purchases or bank deposits. Transactions with cash and cash alternatives can be structured to stay under the recordkeeping and reporting thresholds, and case examples demonstrate that some merchants will accept more than $10,000 in cash without reporting the transaction as required.

To move funds into an account at a bank or broker-dealer, case examples show criminals may use an individual, serving as a nominee, to open the account and shield the identities of the criminals who own and control the funds. Alternatively, the account may be opened in the name of a business that was created to hide the beneficial owner who controls the funds.

Trade-based money laundering (TBML) can involve various schemes that disguise criminal proceeds through trade-related financial transactions. One of the more common schemes is the Black Market Peso Exchange (BMPE) which involves money brokers making local currency available in Latin America and Asia for drug dollars in the United States. Another form of TBML involves criminals using illicit proceeds to purchase trade goods, both to launder the cash and generate additional profits.

Risks

Any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering or terrorist financing.[2] The size and complexity of the financial system in the United States, and the fertile environment for innovation, create legitimate and illegitimate opportunities. However, the potential money laundering risks are significantly reduced by anti-money laundering regulation, financial supervision, examination, and enforcement. The risks that remain, including those that are unavoidable, are:

- Widespread use of cash, making it difficult for authorities to differentiate between licit and illicit use and movement of bank notes;

- Structured transactions below applicable thresholds to avoid reporting and recordkeeping obligations;
- Individuals and entities that disguise the nature, purpose, ownership, and control of accounts;
- Occasional AML compliance deficiencies, which are an inevitable consequence of a financial system with hundreds of thousands of locations for financial services;
- Complicit violators within financial institutions; and
- Complicit merchants, particularly wholesalers who facilitate TBML, and financial services providers.

IRS Criminal Investigation

IRS Criminal Investigation (CI) is comprised of nearly 3,500 employees worldwide, approximately 2,500 of whom are special agents whose investigative jurisdiction includes tax, money laundering and Bank Secrecy Act laws. While other federal agencies also have investigative jurisdiction for money laundering and some bank secrecy act violations, IRS is the only federal agency that can investigate potential criminal violations of the Internal Revenue Code.

Compliance with the tax laws in the United States relies heavily on self-assessments of what tax is owed. This is called voluntary compliance. When individuals and corporations make deliberate decisions to not comply with the law, they face the possibility of a civil audit or criminal investigation which could result in prosecution and possible jail time. Publicity of these convictions provides a deterrent effect that enhances voluntary compliance.

As financial investigators, CI special agents fill a unique niche in the federal law enforcement community. Today's sophisticated schemes to defraud the government demand the analytical ability of financial investigators to wade through complex paper and computerized financial records. Due to the increased use of automation for financial records, CI special agents are trained to recover computer evidence. Along with their financial investigative skills, special agents use specialized forensic technology to recover financial data that may have been encrypted, password protected, or hidden by other electronic means.

Criminal Investigation's conviction rate is one of the highest in federal law enforcement. Not only do the courts hand down substantial prison sentences, but those convicted must also pay fines, civil taxes and penalties.

The Criminal Investigation strategic plan is comprised of three interdependent programs: Legal Source Tax Crimes; Illegal Source Financial Crimes; and Narcotics Related and Counterterrorism Financial Crimes. These three programs are mutually supportive and encourage utilization of all statutes within CI's jurisdiction, the grand jury process and enforcement techniques to combat tax, money laundering and currency crime violations. CI must investigate and assist in the prosecution of those significant financial investigations that will generate the maximum deterrent effect, enhance voluntary compliance and promote public confidence in the tax system.

Prosecution for Money Laundering Crimes

To be criminally culpable under 18 U.S.C. § 1956(a)(1), a defendant must conduct or attempt to conduct a financial transaction, knowing that the property involved in the financial transaction represents the proceeds of some unlawful activity, with one of the four specific intents discussed below, and the property must in fact be derived from a specified unlawful activity.

The actual source of the funds must be one of the specified forms of criminal activity identified by the statute, in 18 U.S.C. § 1956(c)(7), or those incorporated by reference from the RICO statute (18 U.S.C. § 1961(1)). Section 1956(c)(7)(B) includes in the list of specified unlawful activity certain offenses against a foreign nation. Thus, proceeds of certain crimes committed in another country may constitute proceeds of a specified unlawful activity for purposes of the money laundering statutes.

To prove a violation of § 1956(a)(1), the prosecutor must prove, either by direct or circumstantial evidence, that the defendant knew that the property involved was the proceeds of any felony under State, Federal or foreign law. The prosecutor need not show that the defendant knew the specific crime from which the proceeds were derived; the prosecutor must prove only that the defendant knew that the property was illegally derived in some way. See § 1956(c)(1).

The prosecutor must also prove that the defendant initiated or concluded, or participated in initiating or concluding, a financial transaction. A "transaction" is defined in § 1956(c)(3) as a purchase, sale, loan, pledge, gift, transfer, delivery, other disposition, and with respect to a financial institution, a deposit, withdrawal, transfer between accounts, loan, exchange of currency, extension of credit, purchase or sale safe-deposit box, or any other payment, transfer or delivery by, through or to a financial institution.

A "financial transaction" is defined in § 1956(c)(4) as a transaction which affects interstate or foreign commerce and: (1) involves the movement of funds by wire or by other means; (2) involves the use of a monetary instrument; or (3) involves the transfer of title to real property, a vehicle, a vessel or an aircraft; or (4) involves the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce.

PRACTICE TIP: The legislative history indicates, and several cases have held, that each separate financial transaction should be charged separately in an individual count. For example, if an individual earns $100,000 from offense. If he then withdraws $50,000, he commits a second offense. If he then purchases a car with the withdrawn $50,000, he commits a third offense. Each transaction should be charged in a separate count. Charging multiple financial transactions in a single count is duplicitous. See, e.g., United States v. Prescott, 42 F.3d 1165 (8th Cir. 1994); United States v. Conley, 826 F. Supp. 1536 (W.D. Pa. 1993).

In conducting the financial transaction, the defendant must have acted with one of the following four specific intents:

§ 1956(a)(1)(A)(i): intent to promote the carrying on of specified unlawful activity;

§ 1956(a)(1)(A)(ii): intent to engage in tax evasion or tax fraud;

§ 1956(a)(1)(B)(i): knowledge that the transaction was designed to conceal or disguise the nature, location, source, ownership or control of proceeds of the specified unlawful activity; or

§ 1956(a)(1)(B)(ii): knowledge that the transaction was designed to avoid a transaction reporting requirement under State or Federal law [e.g., in violation of 31 U.S.C. §§ 5313 (Currency Transaction Reports) or 5316 (Currency and Monetary Instruments Reports), or 26 U.S.C. § 6050I (Internal Revenue Service Form 8300)].

Prosecutions pursuant to 18 U.S.C. § 1956(a)(2) arise when monetary instruments or funds are transported, transmitted or transferred internationally, and the defendant acted with one of the requisite criminal intents (i.e., promoting, concealing, or avoiding reporting requirements). The intent to engage in tax violations is not included in § 1956(a)(2).

If the transportation, transmission or transfer was conducted with the intent to conceal the proceeds of specified unlawful activity or to avoid a reporting requirement, the prosecutor must show that the defendant knew the monetary instrument or funds represented the proceeds of some form of unlawful activity. However, if the transportation, transmission or transfer is conducted with the intent to promote the carrying on of specified unlawful activity, the prosecutor need not show that the funds or monetary instruments were actually derived from any criminal activity.

The transportation, transmission or transfer must cross the border -- either originating or terminating in the United States. That term includes all means of transporting funds or monetary instruments, including wire or electronic funds transfers, and the transfer of currency, checks, money orders, bearer securities and negotiable instruments.

Section 1956(a)(3) relates to undercover operations where the financial transaction involves property represented to be proceeds of specified unlawful activity. The proceeds in § 1956(a)(3) cases are not actually derived from a real crime; they are undercover funds supplied by the Government. The representation must be made by or authorized by a Federal officer with authority to investigate or prosecute money laundering violations. The representation may also be made by another at the direction of or approval of a Federal officer. It should be noted that the specific intent provisions in § 1956(a)(3) are slightly different from those in § 1956(a)(1). First, the intent to violate the tax laws is not included in this subsection. Second, subsections 1956(a)(3)(B) and (C) require that the transaction be conducted with the intent to conceal or disguise the nature, location, source, ownership or control of the property or to avoid a transaction reporting requirement, respectively, in contrast to subsections 1956(a)(1)(B)(i) and (ii), which only require that defendant know that the transaction is designed, in whole or in part, to accomplish one of those ends.

Violations of § 1956 have a maximum potential twenty year prison sentence and a $500,000 fine or twice the amount involved in the transaction, whichever is greater. The general sentencing provisions in 18 U.S.C. §§ 3551-3571 should also be consulted.

There is also a civil penalty provision in § 1956(b) which may be pursued as a civil cause of action. Under this provision, persons who engage in violations of subsections 1956(a)(1), (a)(2) or (a)(3) are liable to the United States for a civil penalty of not more than the greater of $10,000 or the value of the funds involved in the transaction. Copies of pleadings in § 1956(b) actions are available from the Section.

Prosecutions under 18 U.S.C. § 1957 arise when the defendant knowingly conducts a monetary transaction in criminally derived property in an amount greater than $10,000, which is in fact proceeds of a specified unlawful activity. Section 1957(f)(1) defines a monetary transaction as a "deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument . . . by, through, or to a financial institution (as defined in section 1956 of this title), including any transaction that would be a financial transaction under section 1956(c)(4)(B) . . . ." Section 1957 carries a maximum penalty of ten years in prison and maximum fine of $250,000 or twice the value of the transaction. There is no civil penalty provision.

The most significant difference from § 1956 prosecutions is the intent requirement. Under § 1957, the four intents have been replaced with a $10,000 threshold amount for each non-aggregated transaction and the requirement that a financial institution be involved in the transaction. Although the prosecutor need not prove any intent to promote, conceal or avoid the reporting requirements, it still must be shown that the defendant knew the property was derived from some criminal activity and that the funds were in fact derived from a specified unlawful activity.

There is extraterritorial jurisdiction for violations of § 1956 if: (1) the transaction or series of related transactions exceeds $10,000; and (2) the laundering is by a United States citizen, or, if by a foreign national, the conduct occurs in part in the United States. See § 1956(f). There is extraterritorial jurisdiction for violations of § 1957 if the defendant is a United States person. See § 1957(d).

Sections 1956 and 1957 include "attempts" as well as completed offenses. Conspiracies are indictable under 18 U.S.C. § 1956(h). It should be noted that, in October 1992, Congress added § 1956(g), which provides a separate offense for money laundering conspiracy. Since Congress inadvertently added two sections designated as § 1956(g), the conspiracy provision was redesignated § 1956(h) in September 1994. The conspiracy provision in § 1956(h) is modeled after the conspiracy provision in 21 U.S.C. § 846. Thus, it should not be necessary to plead overt acts in the indictment. However, the Section recommends that overt acts be included in the indictment if practicable. A set of indictment forms can be found in this Manual at 2106 et seq. Jury instruction forms begin at 2111. See also this Manual at 2100.

For a comprehensive review of the money laundering statutes and case law, please consult Chapter Three of the Money Laundering Federal Prosecution Manual (June 1994), prepared by the Asset Forfeiture and Money Laundering Section, Criminal Division. Additional resources available from the Section include a newsletter entitled The Money Laundering Monitor, money laundering caselists, sample indictments and jury instructions.

Money Laundering Around the World

Money laundering, both at the country and multilateral levels, remains a significant crime issue despite robust, multifaceted efforts to address it. While arriving at a precise figure for the amount of criminal proceeds laundered is impossible, some studies by relevant international organizations estimate it may constitute 2-5 percent of global GDP. It is a seemingly ubiquitous criminal phenomenon: money laundering facilitates many other crimes and has become an indispensable tool of drug traffickers, transnational criminal organizations, and terrorist groups around the world. Its nefarious impact is considerable: it contributes to the breakdown of the rule of law, corruption of public officials, and destabilization of economies, and it threatens political stability, democracy, and free markets around the globe.

For these reasons, the development and implementation of effective AML regimes consistent with international standards and the ability to meet evolving challenges is clearly vital to the maintenance of solvent, secure, and reliable financial, commercial, and trade systems. Reducing money laundering's threat to U.S. interests is a national security priority reflected in the 2018 National Security Strategy and the 2017 Executive Order 13773, Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking. To that end, the United States, a founding member of FATF, has worked within the organization, and with partner countries and FATF-style regional bodies, to promote compliance with the 49 Recommendations. It has also supported, through technical assistance and other means, the development and implementation of robust national-level AML regimes in jurisdictions around the world.

The 2019 edition of the Congressionally-mandated International Narcotics Control Strategy Report, Volume II: Money Laundering focuses on the exposure to this threat – in the specific context of narcotics-related money laundering – of jurisdictions around the world. As with past reports, it provides a review of the AML legal and institutional infrastructure of each jurisdiction, highlights the most significant steps each has taken to improve its AML regime, describes key vulnerabilities, and identifies each jurisdiction's capacity to share information and cooperate in international investigations. The report also highlights the United States government's provision of AML-related technical assistance.

In view of the experience of jurisdictions included in the 2019 report, identification and reporting of suspicious transactions, identification of the true beneficial owners of legal entities and transactions, and frameworks and practices for international cooperation on money laundering investigations and prosecutions remain as germane today as when the FATF was created.

As new technologies come into use, various crimes, including money laundering, continue to evolve and pose new challenges for societies, governments, and law enforcement. New technologies create opportunities for exploitation by criminals and terrorists. For example, in Africa, South Asia, and some other parts of the world, use of mobile telephony to send and receive money or credit has outstripped owning a bank account. The rapid growth of global mobile payments (m-payments) and virtual currencies demands particular attention in the AML sphere. The risk that criminal and terrorist organizations will co-opt m-payment services is real, particularly as the services can manifest less than optimal financial transparency. Similarly,

virtual currencies are growing in popularity and expanding their reach. For example, key MSBs are exploring how to incorporate virtual or crypto currency (blockchain platform) payments to expedite remittances to locations around the world. Regulators and law enforcement are beginning, in some jurisdictions, to respond to the use of such anonymous e-payment methodologies, but their rapid development poses challenges on the policy, legal, and enforcement levels. Mexico and China have added virtual currency platforms and dealers as covered entities for AML supervision purposes, while Cayman Islands is among the jurisdictions taking action to develop legislation to address their use, and the British Virgin Islands issued a public advisory regarding the risk of investing in virtual currencies. Although virtual currencies are currently illegal in India, the government is exploring a regulatory regime for their use.

Corruption is both a significant by-product and a facilitating crime of the international drug trade and transnational organized crime. While corruption risks occur in any country, the risks are particularly high in countries where political will may be weak, institutions ineffective, or the country's AML infrastructure deficient. Encouragingly, the 2019 Report again highlights action several governments are taking to more effectively address corruption and its links to money laundering. As with money laundering, while legislative and institutional reforms are an important foundation, robust and consistent enforcement is also key, though often lacking. Jamaica, Senegal, Serbia, and Uzbekistan all enacted legislation to address corruption and/or PEPs. Sint Maarten charged a member of parliament with bribery, tax evasion, and money laundering. Argentina and Ecuador continue to investigate and prosecute corruption cases. Malaysia's new government has taken action to prosecute a number of former government officials, including a former prime minister, who allegedly were involved in misappropriations from the state-owned development fund.

The transparency of beneficial ownership remains a central focus for AML, arising in the discussions of multilateral fora such as FATF as well as in coverage of some recent high-level corruption allegations. Shell companies are used by drug traffickers, organized criminal organizations, corrupt officials, and some regimes to launder money and evade sanctions. "Off-the shelf" IBCs, purchased via the internet, remain a significant concern, by creating a vehicle through which nominee directors from a different country may effectively provide anonymity to the true beneficial owners. While the 2019 Report reflects that beneficial ownership transparency remains a vulnerability in many jurisdictions, the report also highlights significant steps taken by various jurisdictions on the issue. Cyprus issued circulars to banking, credit, payment, and virtual money institutions advising them to be extra vigilant against shell companies and to avoid doing business with them. To increase the transparency of company ownership, Peru enacted legislation to mandate the disclosure of beneficial ownership. Cyprus and Serbia have new laws addressing centralized records of beneficial owners. Additionally, in an effort to increase transparency, increasing numbers of jurisdictions, such as Argentina and Curacao, are concluding tax information sharing agreements. Others, such as Pakistan, Panama, and Russia are beginning to share financial information under the OECD's Multilateral Competent Authority Agreement. Here in the United States, on May 11, 2018, a new Treasury Department rule on beneficial ownership went into effect, requiring covered entities to identify and verify the identities of beneficial owners of legal entities.

The year 2018 saw increasing scrutiny at the international level of economic citizenship programs, which are also vulnerable to money laundering activity and must be closely monitored and regulated to prevent their abuse by criminals. U.S. law enforcement remains highly concerned about the expansion of these programs due to the visa-free travel and ability to open bank accounts accorded to participating individuals; other vulnerabilities, as well as good practices in countermeasures, have been analyzed in the various 2018 studies and publications on the issue. While Turkey eased its requirements for economic citizenship, St. Kitts and Nevis now uses a regional central clearing house under the auspices of the Caribbean Community to properly vet candidates. Antigua and Barbuda and St. Lucia have established their own vetting units.

Although new technologies are gaining popularity, money launderers continue to use offshore centers, FTZs, and gaming enterprises to launder illicit funds. These sectors can offer convenience and, often, anonymity to those wishing to hide or launder the proceeds of narcotics trafficking and other serious crimes. While the appeal of these institutions translates into their continued appearance across many of the jurisdictions that appear in the 2019 INCSR, many jurisdictions are taking measures to reduce vulnerabilities. In recent years, Dominica revoked the licenses of eight offshore banks. Macau is taking a more stringent approach toward the licensing and supervision of gaming junket promoters. Bahamian gaming authorities can observe operations, including account transactions, in real time from remote locations. In its second criminal prosecution involving money laundering charges, Vietnam prosecuted over 90 defendants associated with a prohibited online gaming enterprise.

To help address these issues, in 2018, the United States continued to mobilize government experts from relevant agencies to deliver a range of training programs, mentoring, and other capacity building support. U.S. government agencies also, in many cases, provided financial support to other entities to engage in complementary capacity-building activities, leveraging those organizations' unique expertise and reach. These U.S.-supported efforts build capacity to fight not only money laundering but also other crimes facilitated by money laundering, including narcotics trafficking, in partner jurisdictions. Depending on the jurisdiction, supervisory, law enforcement, prosecutorial, customs, FIU personnel, and private sector entities benefitted from the U.S.-supported programs. As the 2019 INCSR reflects, these efforts are resulting in an increase in investigations, prosecutions, and convictions, more robust institutions, and stronger compliance with international standards, in addition to raising awareness of cutting edge, emerging issues, such as abuse of new technologies, and sharing good practices to address them.

Looking ahead, FATF's recent focus on the identification of the methodologies currently used by human trafficking networks and terrorist financing and recruiting efforts will likely lead members of FATF and the FATF style-regional bodies to emphasize their endeavors in these areas. FATF notes the continued use of bulk cash smuggling and MVTS transactions in these areas, while crowdfunding is a new source of funding for small terrorist cells or lone wolves.

While the 2019 INCSR reflects the continued vulnerability to narcotics trafficking-related money laundering around the world, including in the United States, it also demonstrates the seriousness with which many jurisdictions are tackling the issue and the significant efforts many have undertaken. Though the impact of the aforementioned efforts manifests through increased

enforcement, there is much more to be done in that regard – the gap between de jure progress and implementation and enforcement in some jurisdictions is one of the most concerning observations of the report. The Department of State, working with our U.S. and international partners, will continue to support foreign assistance activities, diplomatic engagement, and law enforcement partnerships to promote compliance with international norms and strengthen capacity to combat money laundering, drug trafficking, and transnational organized crime.

During 2018, U.S. law enforcement and regulatory agencies provided training and technical assistance on money laundering countermeasures, financial investigations, and related issues to their counterparts around the globe. The programs provided the necessary tools to recognize, investigate, and prosecute money laundering, financial crimes, terrorist financing, and related criminal activity. U.S. agencies supported courses in the United States as well as in the jurisdictions of the program beneficiaries. Depending on circumstances, U.S. agencies provided instruction directly or through other agencies or implementing partners, unilaterally or in collaboration with foreign counterparts, and with either a bilateral recipient or in multijurisdictional training exercises. The following is a representative, but not necessarily exhaustive, overview of the capacity building provided and organized by sponsoring agencies.

Board of Governors of the Federal Reserve System (FRB)
The FRB conducts a Bank Secrecy Act (BSA) and OFAC compliance program review as part of its regular safety-and-soundness examination. These examinations are an important component in the United States' efforts to detect and deter money laundering and terrorist financing. The FRB monitors its supervised financial institutions' conduct for BSA and OFAC compliance. Internationally, during 2018, the FRB conducted training and provided technical assistance to banking supervisors on AML topics during four seminars: one in Sao Paulo, Brazil; one in Cairo, Egypt; one in Washington, D.C.; and one in Abuja, Nigeria. Countries participating in these FRB initiatives were Armenia, Brazil, Cote d'Ivoire, Egypt, Ghana, Hong Kong, India, Kenya, Korea, Lebanon, Lesotho, Liechtenstein, Mexico, Mongolia, Nigeria, Pakistan, Singapore, Sri Lanka, Sudan, Uganda, and Zimbabwe.

Department of Homeland Security Customs and Border Patrol (CBP)
The Trade and Cargo Academy provided two hours of money laundering training to 69 graduates of Basic Import Specialist Training in calendar year 2018. At the Border Patrol Academy, the Office of Chief Counsel taught a one-hour block on currency and monetary instrument reporting violations and unlicensed money transmitters. CBP conducted a bulk cash smuggling program in Peru in December 2018.

U.S. Immigration and Customs Enforcement
In Fiscal Year 2018, the ICE Homeland Security Investigations Illicit Finance and Proceeds of Crime Unit (IFPCU) conducted AML trainings focused on typologies, methodologies, and approaches to combat illicit finance. IFPCU provided technical training and presentations to representatives from the following foreign law enforcement partners: Canada, Colombia, France, Germany, South Korea, Europol, INTERPOL, the World Customs Organization, the Five Eyes Law Enforcement Group, and the FATF. In an effort to support the anticorruption efforts of the Government of Ecuador, in December 2018, ICE provided anticorruption training to members of the Ecuadorian National Police, Attorney General's Office, and the Ecuadorian Customs Service.

Trade Transparency Units (TTU)
The TTU, housed within the ICE National Targeting Center, provides critical exchange of trade data with numerous countries. The TTU has information sharing agreements with 14 countries to facilitate the identification of transnational criminal organizations utilizing TBML schemes to repatriate proceeds generated from multiple illegal activities, including drug and human smuggling, customs fraud, and intellectual property rights violations. The TTU methodology, which provides U.S. law enforcement and international partners with subject matter expertise, training, and investigative tools to combat TBML and third-party money launderers, is internationally recognized as a best practice to address TBML.

ICE continues to expand the network of operational TTUs, which now includes Argentina, Australia, Brazil, Chile, Colombia, Dominican Republic, Ecuador, France, Guatemala, Mexico, Panama, Paraguay, Peru, Philippines, UK, and Uruguay. The U.S. TTU is actively engaged with several countries in Asia and Southeast Asia regarding MOU discussions to establish a TTU.

Drug Enforcement Administration (DEA)
The Office of Global Enforcement, Financial Investigations Section (OGF) at DEA Headquarters serves as DEA's lead body for coordinating DEA's efforts across domestic and foreign offices with respect to the targeting of the financial aspects of drug trafficking organizations (DTO). OGF works in conjunction with DEA field offices, foreign counterparts, and the interagency community to provide guidance and to support a variety of investigative tools, as well as to provide oversight on DEA's undercover financial investigations. OGF facilitates cooperation between countries, resulting in the identification and prosecution of money laundering organizations operating on behalf of DTOs, as well as the seizure of assets and denial of revenue around the world. OGF regularly briefs and educates United States government officials and diplomats, foreign government officials, and military and law enforcement counterparts regarding the latest trends in money laundering, narcoterrorism financing, international banking, offshore corporations, international wire transfer of funds, and financial investigative tools.

In conjunction with the DEA Office of International Training, OGF conducts training for DEA field offices, as well as foreign counterparts, in order to share strategic ideas and promote effective techniques in financial investigations. During 2018, OGF participated in and led a number of workshops and strategy sessions focused on money laundering trends, engagement with financial institutions, guidance and overview on undercover money laundering operations, virtual currency, and investigative case coordination.

DEA has prioritized a financial component in its investigations and has made this component a key element of Priority Target Operations, the Domestic Cartel Initiative, and Organized Crime Drug Enforcement Task Force investigations. DEA has dedicated financial investigative teams across its domestic offices as well as foreign-based DEA teams in Mexico, Peru, and Colombia that have conducted local training programs. For example, in 2018, DEA offered a one-day money laundering course for Ecuadorian National Police officers/commanders, prosecutors, and personnel from the FIU.

Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation (FBI) provides training and/or technical assistance to national law enforcement personnel globally. Training and technical assistance programs enhance host country law enforcement's capacity to investigate and prosecute narcotics-related money laundering crimes. The FBI has provided workshops introducing high-level money laundering techniques used by criminal and terrorist organizations. The training may focus on topics such as a foundational understanding of drug trafficking investigative and analytical techniques and tactics, money laundering and public corruption, or terrorism financing crimes and their relationship to drug trafficking as a support for terrorism activities.

Anti-Money Laundering (AML) Source Tool for Broker-Dealers

Date: October 4, 2018

This research guide, or "source tool," is a compilation of key AML laws, rules, orders, and guidance applicable to broker-dealers. Several statutory and regulatory provisions, and related rules of the securities self-regulatory organizations (SROs), impose AML obligations on broker-dealers. A wealth of related AML guidance materials is also available. To aid research efforts into AML requirements and to assist broker-dealers with AML compliance, this source tool organizes key AML compliance materials and provides related source information.

When using this research "tool" or guide, you should keep the following in mind:

First, securities firms are responsible for complying with all AML requirements to which they are subject. Although this research guide summarizes some of the key AML obligations that are applicable to broker-dealers, it is not comprehensive. You should not rely on the summary information provided, but should refer to the relevant statutes, rules, orders, and interpretations.

Second, AML laws, rules, and orders are subject to change and may change quickly. Statutes that include AML-related provisions may be amended from time to time, and new statutes may be enacted which include AML-related provisions. The information summarized in this guide is current as of October 4, 2018. In addition, please note that in July 2007, the SEC approved the establishment of the Financial Industry Regulatory Authority (FINRA). FINRA consolidated the former NASD and the member regulation, enforcement, and arbitration operations of NYSE Regulation. The Source Tool reflects the historical issuance of AML rules and guidance by the NASD and NYSE as well as new rules and guidance issued by FINRA.

Finally, you will find a list of telephone numbers and useful websites at the end of this guide. If you have questions concerning the meaning, application, or status of a particular law, rule, order, or guidance, you should consult with an attorney experienced in the areas covered by this guide.

This compilation was prepared by staff in the Office of Compliance Inspections and Examinations (OCIE), Securities and Exchange Commission. The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed in this document are those of the staff and do not necessarily represent the views of the Commission, or other Commission staff.

TABLE OF CONTENTS

The following topics are addressed in this guide:

1. The Bank Secrecy Act

The Bank Secrecy Act (BSA), initially adopted in 1970, establishes the basic framework for AML obligations imposed on financial institutions. Among other things, it authorizes the Secretary of the Treasury (Treasury) to issue regulations requiring financial institutions (including broker-dealers) to keep records and file reports on financial transactions that may be useful in investigating and prosecuting money laundering and other financial crimes. The Financial Crimes Enforcement Network (FinCEN), a bureau within Treasury, has regulatory responsibilities for administering the BSA.

Rule 17a-8 under the Securities Exchange Act of 1934 (Exchange Act) requires broker-dealers to comply with the reporting, recordkeeping, and record retention rules adopted under the BSA.

***Source Documents*:**

- **Bank Secrecy Act:** The Bank Secrecy Act is codified at 31 U.S.C. §§ 5311 *et seq.* and is available at:

  http://www4.law.cornell.edu/uscode/html/uscode31/usc_sup_01_31_08_IV_10_53_20_II.html
- **Bank Secrecy Act Rules:** The rules adopted by Treasury implementing the BSA are located at 31 C.F.R. Chapter X and are available at:
  http://edocket.access.gpo.gov/2010/pdf/2010-25914.pdf
  31 C.F.R. Chapter X is comprised of a "General Provisions Part" and separate financial-institution-specific parts for those financial institutions subject to FinCEN regulations. The General Provisions Part (Part 1010) contains regulatory requirements that apply to more than one type of financial institution, and in some cases, individuals. The financial-institution-specific parts contain regulatory requirements specific to a particular type of financial institution. The financial-institution-specific part that pertains to broker-dealers is Part 1023 (31 C.F.R. §§ 1023.100 *et seq.*).
- **Exchange Act Rule 17a-8:** 17 C.F.R. § 240.17a-8.

2. The USA PATRIOT Act

The USA PATRIOT Act was enacted by Congress in 2001 in response to the September 11, 2001 terrorist attacks. Among other things, the USA PATRIOT Act amended and strengthened the BSA. It imposed a number of AML obligations directly on broker-dealers, including:

- AML compliance programs;
- customer identification programs;
- monitoring, detecting, and filing reports of suspicious activity;
- due diligence on foreign correspondent accounts, including prohibitions on transactions with foreign shell banks;
- due diligence on private banking accounts;
- mandatory information-sharing (in response to requests by federal law enforcement); and
- compliance with "special measures" imposed by the Secretary of the Treasury to address particular AML concerns.

Source Document:

- **USA PATRIOT Act:** Title 3 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 296 (2001). The full text of the USA PATRIOT Act is available at: http://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

3. AML Programs

Section 352 of the USA PATRIOT ACT amended the BSA to require financial institutions, including broker-dealers, to establish AML programs. Broker-dealers can satisfy this requirement by implementing and maintaining an AML program that complies with SRO rule requirements.

An AML program must be in writing and include, at a minimum:

- policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and its implementing rules;
- policies and procedures that can be reasonably expected to detect and cause the reporting of transactions under 31 U.S.C. 5318(g) and the implementing regulations thereunder;
- the designation of an AML compliance officer (AML Officer), including notification to the SROs;
- ongoing AML employee training; and
- an independent test of the firm's AML program, annually for most firms.
- risk based procedures for conducting ongoing customer due diligence which should include, but not be limited to: 1) understanding the nature and purpose of customer relationships to be able to develop a risk profile and 2) conducting ongoing monitoring to identify and report suspicious transactions as well as maintaining and updating customer information, including beneficial ownership information for legal entity customers.

Source Documents:

- **AML Program Rule:** 31 C.F.R. § 1023.210 .
- **Final Rule Release:** 67 Fed. Reg. 21110 (April 29, 2002)
- **SEC Order Approving FINRA AML Compliance Program Rule:** Exchange Act Release No. 83154 (September 10, 2009). See also 74 Fed. Reg. 47630 (September 16, 2009).
- **Joint Guidance Issued by FinCEN, SEC, and other Federal Regulators:**
  - Guidance on Obtaining and Retaining Beneficial Ownership Information (Mar 2010)
- **FINRA AML Compliance Rules and Related Guidance**

- FINRA Rule 3310: Anti-Money Laundering Compliance Program
- Supplementary Material 3310.01: Independent Testing Requirements
- Supplementary Material 3310.02: Review of Anti-Money Laundering Compliance Person Information

- **Other Related Guidance:**
  - NTM 02-21: NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Compliance Programs Required by Federal Law (April 2002).[1]
  - NTM 02-78: NASD Adopts Amendments to Rule 3011 to Require Members to Provide to NASD Contact Information for an Anti-Money Laundering Compliance Person(s) (November 2002).
  - NTM 06-07: SEC Approves Amendments to Anti-Money Laundering Compliance Program Rule and Adoption of Interpretative Material (February 2006).
  - NTM 17-40: FINRA Provides Guidance to Firms Regarding AntiMoney Laundering Program Requirements Under FINRA Rule 3310 Following Adoption of FinCEN's Final Rule to Enhance Customer Due Diligence Requirements for Financial Institutions Effective Date.
  - NTM 18-19: FINRA Amends Rule 3310 to Conform to FinCEN's Final Rule on Customer Due Diligence Requirements for Financial Institutions.
  - *FINRA Small Firm Template:* The template provides model language for AML program compliance and supervisory procedures and is available on the FINRA website at: http://www.finra.org/industry/anti-money-laundering-template-small-firms.
  - *FINRA AML Frequently Asked Questions*: The Qs and As are available on the FINRA website at: http://www.finra.org/industry/faq-anti-money-laundering-faq
- **Historical Source Documents:**
  Please note that the NYSE and NASD rules noted below have now been incorporated into a new FINRA Rule 3310 (see above). The information below is provided for historical purposes, and may still contain useful guidance.
  - **SEC Order Approving Initial NASD and NYSE AML Compliance Program Rules:**
    - Exchange Act Release No. 45798 (April 22, 2002). *See also* 67 Fed. Reg. 20854 (April 26, 2002).
  - **NYSE AML Compliance Program Rules and Related Guidance:**
    - NYSE Rule 445: Anti-Money Laundering Compliance Program.
    - *SEC Release Approving NYSE Amendment to Rule 445*: Exchange Act Release No. 53176 (January 25, 2006). *See also* 71 Fed. Reg. 5392 (February 1, 2006). (The rule amendments refine AML compliance program requirements relating to independence, testing, and AML Officer notifications.)
    - *Other Related NYSE Guidance:*
      - IM-02-16: Anti-Money Laundering Compliance Requirements (April 12, 2002).
      - IM 02-21: Approval of New Rule 445 — Anti-Money Laundering Compliance Program (May 6, 2002).
      - IM 03-48: Rule 445 — Initial Anti-Money Laundering Audit (October 23, 2003).
      - IM 06-04: Amendments to Rule 445 (February 3, 2006).

4. Customer Identification Programs

Section 326 of the USA PATRIOT Act amended the BSA to require financial institutions, including broker-dealers, to establish written customer identification programs (CIP). Treasury's implementing rule requires a broker-dealer's CIP to include, at a minimum, procedures for:

- obtaining customer identifying information from each customer prior to account opening;
- verifying the identity of each customer, to the extent reasonable and practicable, within a reasonable time before or after account opening;
- making and maintaining a record of information obtained relating to identity verification;
- determining within a reasonable time after account opening or earlier whether a customer appears on any list of known or suspected terrorist organizations designated by Treasury;[2] and
- providing each customer with adequate notice, prior to opening an account, that information is being requested to verify the customer's identity.

The CIP rule provides that, under certain defined circumstances, broker-dealers may rely on the performance of another financial institution to fulfill some or all of the requirements of the broker-dealer's CIP. For example, in order for a broker-dealer to rely on the other financial institution the reliance must be reasonable. The other financial institution also must be subject to an AML compliance program rule and be regulated by a federal functional regulator. The broker-dealer and other financial institution must enter into a contract and the other financial institution must certify annually to the broker-dealer that it has implemented an AML program. The other financial institution must also certify to the broker-dealer that the financial institution will perform the specified requirements of the broker-dealer's CIP.

Source Documents:

- **Customer Identification Program Rule:** 31 C.F.R. § 1023.220.
- **Final Rule Release:** Exchange Act Release No. 47752 (April 29, 2003). *See also* 68 Fed. Reg. 25113 (May 9, 2003)
- **Other Related Documents:**
  - *Proposed Rule:* Exchange Act Release No. 46192 (July 12, 2002). *See also* 67 Fed. Reg. 48306 (July 23, 2002).
  - Treasury Department Provides Guidance on Compliance with Section 326 of the USA PATRIOT ACT: *PO-3530* (October 11, 2002).[3]
  - *Withdrawal of the Notice of Proposed Rulemaking; Anti-Money Laundering Programs for Investment Advisers:* 73 Fed. Reg. 65568 (October 30, 2008).
- **FinCEN Guidance:**
  - Guidance: Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations (FIN-2008-G002; March 4, 2008)
  - Ruling: Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution (FIN-2008-R008; June 3, 2008)
- **SEC Staff Guidance:**
  - Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule (October 1, 2003). (The Q&A provides staff guidance regarding when a broker-dealer maintaining an "omnibus account" for a financial intermediary may treat the financial intermediary as the "customer" for CIP purposes.)

- *No-Action Letters to the Securities Industry Association* ("SIA") (February 12, 2004; February 10, 2005; July 11, 2006; January 10, 2008; January 11, 2010; January 11, 2011; January 9, 2015; and December 12, 2016). (The letters provide staff guidance regarding the extent to which a broker-dealer may rely on an investment adviser to conduct the required elements of the CIP rule, prior to such adviser being subject to an AML rule. Among other things, the 2015 letter provides additional details regarding the reasonableness of a broker-dealer's reliance on an investment adviser and also includes a requirement that the investment adviser promptly report to the broker-dealer potentially suspicious or unusual activity detected as part of the CIP being performed on the broker-dealer's behalf.)
- Staff Q&A Regarding Broker-Dealer CIP Rule Responsibilities under the Agency Lending Disclosure Initiative (April 26, 2006). (The Q&A provides staff guidance on the application of the CIP rule to the Agency Lending Disclosure Initiative.)
- National Exam Risk Alert — Master/Sub Accounts (September 29, 2011)

- **NYSE Guidance:**
  - IM 02-46: Compliance with Section 326 ("Verification of Identification") of the USA Patriot Act (October 31, 2002).
  - IM 03-32: Customer Identification Programs For Broker-Dealers (July 14, 2003).
- **NASD Guidance:**
  - NTM 02-50: Treasury and SEC Request Comment on Proposed Regulation Regarding Broker/Dealer Anti-Money Laundering Customer Identification Requirements (August 2002).
  - NTM 03-34: Treasury and SEC Issue Final Rule Regarding Customer Identification Programs for Broker/Dealers (June 2003).
  - NASD Customer Identification Program Notice (2003).
  - NASD Comparison of the AML Customer Identification Rule and the SEC's Books & Records Customer Account Records Rule (2003).
- **FINRA Guidance:**
  - Regulatory Notice 10-18: Master Accounts and Sub-Accounts (April 2010)

5. Beneficial Ownership and Customer Due Diligence ("CDD")

Covered financial institutions are required to establish and maintain written procedures that are reasonably designed to identify and verify beneficial owners of legal entity customers and to include such procedures in their anti-money laundering compliance program required under 31 U.S.C. 5318(h) and its implementing regulations.

Legal entity customer means a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account.

Beneficial owner means each of the following:

(1) Each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer; and

(2) A single individual with significant responsibility to control, manage, or direct a legal entity customer, including:

(i) An executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or

(ii) Any other individual who regularly performs similar functions.

(3) If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner for purposes of paragraph (d)(1) of this section shall mean the trustee. If an entity listed in paragraph (e)(2) of this section owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, no individual need be identified for purposes of paragraph (d)(1) of this section with respect to that entity's interests.

Source Documents:

- **Beneficial Ownership Requirements for Legal Entity Customers:** 31 C.F.R. §1010.230
- **Final Rule Release:** 81 Fed. Reg. 29398 (May 11, 2016)
- **FinCEN Guidance**
  - FAQs Regarding Customer Due Diligence Requirements for Financial Institutions (July 19, 2016)
  - FAQs Regarding Customer Due Diligence Requirements for financial Institutions (April 3, 2018)
- **FINRA Guidance**
  - NTM 17-40: FINRA Provides Guidance to Firms Regarding Anti-Money Laundering Program Requirements Under FINRA Rule 3310 Following Adoption of FinCEN's Final Rule to Enhance Customer Due Diligence Requirements for Financial Institutions Effective Date.

6. Correspondent Accounts: Prohibition on Foreign Shell Banks and Due Diligence Programs

Overview: Sections 312, 313, and 319 of the USA PATRIOT Act, which amended the BSA, are inter-related provisions involving accounts called "correspondent accounts." These inter-related provisions include prohibitions on certain types of correspondent accounts (those maintained for foreign "shell" banks) as well as requirements for risk-based due diligence of foreign correspondent accounts more generally.

A *"correspondent account"* is defined as: "any formal relationship established for a foreign financial institution to provide regular services to effect transactions in securities."

A "foreign financial institution" includes: (i) a foreign bank (including a foreign branch or office of a U.S. bank); (ii) a foreign branch or office of a securities broker-dealer, futures commission merchant, introducing broker in commodities, or mutual fund; (iii) a business organized under

foreign law (other than a branch or office of such business in the U.S.) that if it were located in the U.S. would be a securities broker-dealer, futures commission merchant, introducing broker in commodities, or a mutual fund; and (iv) a money transmitter or currency exchange organized under foreign law (other than a branch or office of such entity in the U.S.).

In addition, Treasury has clarified that, for a broker-dealer, a "correspondent account" includes:

- accounts to purchase, sell, lend, or otherwise hold securities, including securities repurchase arrangements;
- prime brokerage accounts that clear and settle securities transactions for clients;
- accounts for trading foreign currency;
- custody accounts for holding securities or other assets in connection with securities transactions as collateral; and
- over-the-counter derivatives contracts.

Prohibitions on Foreign Shell Banks: A broker-dealer is prohibited from establishing, maintaining, administering, or managing "correspondent accounts" in the U.S. for, or on behalf of, foreign "shell" banks (*i.e.*, foreign banks with no physical presence in any country). Broker-dealers also must take steps to ensure that they are not indirectly providing correspondent banking services to foreign shell banks through foreign banks with which they maintain correspondent relationships. In order to assist institutions in complying with the prohibitions on providing correspondent accounts to foreign shell banks, Treasury has provided a model certification that can be used to obtain information from foreign bank correspondents. In addition, broker-dealers must obtain records in the United States of foreign bank owners and agents for service of process (Sections 313 and 319 of the USA PATRIOT Act).

***Source Documents*:**

- **Shell Bank Prohibition**: 31 C.F.R. § 1010.630. *See also* 31 C.F.R. § 1010.605 (definitions).
- **Final Rule Release:** 67 Fed. Reg. 60562 (September 26, 2002).
- **Other Rule-Related Documents:**
  - Interim Guidance: 66 Fed. Reg. 59342 (November 27, 2001).
  - Proposed Rule: 66 Fed. Reg. 67460 (December 28, 2001).
- **FinCEN Guidance:**
  - FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 (February 3, 2006).
  - FIN-2008-G001: Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment (January 30, 2008).
  - Ruling: Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution (FIN-2008-R008; June 3, 2008)

Due Diligence Regarding Foreign Correspondent Accounts: A broker-dealer is required to establish a risk-based due diligence program (that is part of its AML compliance program) for any "correspondent accounts" maintained for foreign financial institutions. The due diligence program, which is required to be a part of the broker-dealer's overall AML program, must include appropriate, specific, risk-based policies, procedures, and controls reasonably designed

to enable the broker-dealer to detect and report, on an ongoing basis, any known or suspected money laundering conducted through or involving any foreign correspondent account (Section 312 of the PATRIOT Act).

Treasury has finalized a related rule that states when enhanced due diligence on foreign financial institutions is required.

***Source Documents*:**

- **Correspondent Account Due Diligence Rule:** 31 C.F.R. § 1010.610. *See also* 31 C.F.R. § 1010.605 (definitions).
- **Final Rule Release**: 71 Fed. Reg. 496 (January 4, 2006).
- **Enhanced Due Diligence Final Rule:** 72 Fed. Reg. 44768 (August 9, 2007).
- ***Other Rule-Related Documents:***
    - Enhanced Due Diligence Re-Proposed Rule: 71 Fed. Reg. 516 (January 4, 2006).
    - Proposed Rule: 67 Fed. Reg. 37736 (May 30, 2002).
    - Interim Final Rule: 67 Fed. Reg. 48348 (July 23, 2002).
- **Joint Guidance Issued by FinCEN, SEC, and other Federal Regulators:** Guidance on Obtaining and Retaining Beneficial Ownership Information (Mar 2010)
- **FFIEC AML Examination Manual — February 2015,** [4] available at: https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf
- **FinCEN Guidance:**
    - Fact Sheet: Section 312 of the USA PATRIOT Act (December 2005).
    - FIN-2006-G009: Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (May 10, 2006).
    - FIN-2008-A002: Guidance to Financial Institutions on the Continuing Money Laundering Threat Involving Illicit Iranian Activity (March 20, 2008).
    - FIN-2008-A003: Guidance to Financial Institutions on the Money Laundering Threat Involving the Turkish Cypriot Administered Area of Cyprus (March 20, 2008).
    - FIN-2008-A004: Guidance to Financial Institutions on the Money Laundering Threat Involving the Republic of Uzbekistan (March 20, 2008).
- ***NYSE Guidance*:**
    - IM 02-34: Special Due Diligence for Correspondent Accounts and Private Banking Accounts (August 1, 2002).
    - IM 06-50: Effective Dates for Section 312 of the USA PATRIOT Act (July 3, 2006).

7. Due Diligence Programs for Private Banking Accounts

Section 312 of the USA PATRIOT Act amended the BSA to, among other things, impose special due diligence requirements on financial institutions, including broker-dealers, that establish, maintain, administer or manage a private banking account or a "correspondent account" in the United States for a "non-United States person." Treasury's regulations provide that a "covered financial institution" is required to maintain a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving a "private banking account" that is established, maintained, administered or managed in the U.S. by the financial institution. In addition, the regulations set forth certain minimum requirements for the

required due diligence program with respect to private banking accounts and require enhanced scrutiny to any such accounts where the nominal or beneficial owner is a "senior foreign political figure."

The regulations define a "private banking account" as an account that: (a) requires a minimum deposit of assets of at least $1,000,000; (b) is established or maintained on behalf of one or more non-U.S. persons who are direct or beneficial owners of the account; and (c) has an employee assigned to the account who is a liaison between the broker-dealer and the non-U.S. person.

The definition of "senior foreign political figure" extends to any member of the political figure's immediate family, and any person widely and publicly known to be a close associate of the foreign political figure as well as any entities formed for the benefit of such persons (such persons are commonly referred to as PEPs, or Politically Exposed Persons).

Broker-dealers providing private banking accounts must take reasonable steps to:

- determine the identity of all nominal and beneficial owners of the private banking accounts;
- determine whether any such owner is a "senior foreign political figure" and therefore subject to enhanced scrutiny that is reasonably designed to detect transactions that may involve the proceeds of foreign corruption;
- determine the source of funds deposited into the private banking account and the purpose and use of such account;
- review the activity of the account as needed to guard against money laundering; and
- report any suspicious activity, including transactions involving senior foreign political figures that may involve proceeds of foreign corruption.

***Source Documents*:**

- **Private Banking Due Diligence Rule:** 31 C.F.R. § 1010.620 *See also*: 31 C.F.R. § 1010.605 (definitions).
- **Final Rule Release:** 71 Fed. Reg. 496 (January 4, 2006).
- **Other Rule-Related Documents:**
  - Proposed Rule: 67 Fed. Reg. 37736 (May 30, 2002).
  - Interim Final Rule: 67 Fed. Reg. 48348 (July 23, 2002).
- **Joint Guidance Issued by FinCEN, SEC, and other Federal Regulators:** Guidance on Obtaining and Retaining Beneficial Ownership Information (Mar 2010)
- **FFIEC AML Examination Manual — February 2015,** available at: https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf
- **FinCEN Guidance:**
  - Fact Sheet: Section 312 of the USA PATRIOT Act (December 2005).
  - FIN-2006-G009: Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (May 10, 2006).
- **NYSE Guidance:**
  - IM 02-34: Special Due Diligence for Correspondent Accounts and Private Banking Accounts (August 1, 2002).
  - IM 06-50: Effective Dates for Section 312 of the USA PATRIOT Act (July 3, 2006).

8. Suspicious Activity Monitoring and Reporting

Section 356 of the USA PATRIOT Act amended the BSA to require broker-dealers to monitor for, and report, suspicious activity (so-called SAR reporting).

Under Treasury's SAR rule, a broker-dealer is required to file a suspicious activity report if: (i) a transaction is conducted or attempted to be conducted by, at, or through a broker-dealer; (ii) the transaction involves or aggregates funds or other assets of at least $5000; and (iii) the broker-dealer knows, suspects, or has reason to suspect that the transaction: (a) involves funds or is intended to disguise funds derived from illegal activity, (b) is designed to evade requirements of the BSA, (c) has no business or apparent lawful purpose, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, or (d) involves the use of the broker-dealer to facilitate criminal activity.

Broker-dealers must report the suspicious activity using a form Treasury has issued for the securities and futures industry, the SAR-SF (also referred to as FinCEN Form 101). The form, which is confidential, includes instructions.

Broker-dealers must maintain a copy of any SAR-SF filed and supporting documentation for a period of five years from the date of filing the SAR-SF.

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers should immediately notify law enforcement in addition to filing a SAR-SF. In addition, if a firm wishes to report suspicious transactions that may relate to terrorist activity, in addition to filing a SAR-SF, the firm may call FinCEN's Hotline at 1-866-556-3974. [5]

***Source Documents*:**

- ***SAR Rule:*** 31 C.F.R. § 1023.320.
- **Proposed Rule**: 66 Fed. Reg. 67670 (December 31, 2001).
- **Final Rule Release:**67 Fed. Reg. 44048 (July 1, 2002).
- **Other Rule Related Documents**
  - Final Rule Release: Confidentiality of Suspicious Activity Reports (December 3, 2010).
  - Final Rule Release: Technical Amendment moving the SAR Confidentiality Rule from 31 C.F.R. 103 to the 31 C.F.R. Chapter X
- **SAR-SF: FinCEN Form 101.**
  BSA E-Filing System
- **FinCEN Guidance:**
  - SAR Bulletin Issue No. 4 - Aspects of Financial Transactions Indicative of Terrorist Funding (January 2002).
  - Unauthorized Disclosure of Suspicious Activity Reports (August 18, 2004).
  - Interpretative Release No. 2004-02 — Unitary Filing of Suspicious Activity and Blocking Reports 69 Fed. Reg. 76847 (December 23, 2004).
  - FIN-2006-G014: Potential Money Laundering Risks Related to Shell Companies (November 9, 2006).

    - Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (January 20, 2006).[6]
    - FIN-2007-G003: Suspicious Activity Report Supporting Documentation (June 13, 2007).
    - FIN-2007-G002: Requests by Law Enforcement for Financial Institutions to Maintain Accounts (June 13, 2007).
    - Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (October 10, 2007).
    - Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption (April 17, 2008).
    - Sharing Suspicious Activity Reports by Securities Broker-Dealers, Mutual Funds, Futures Commission Merchants, and Introducing Brokers in Commodities with Certain U.S. Affiliates (November 23, 2010).
    - Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates (November 23, 2010).
    - Guidelines for Completing FinCEN Form 101 (April 2011)
    - *SAR Activity Reviews:* These are available on FinCEN's website at: www.fincen.gov[7]
- **NYSE Guidance:**
    - IM 02-64: USA PATRIOT Act Updates: Section 356 Requirement to Report Suspicious Transactions; Deadline Extension for Sections 313 and 319 (December 24, 2002).
- ***NASD Guidance*:**
    - NTM 02-47: Treasury Issues Final Suspicious Activity Reporting Rule for Broker/Dealers (August 2002).
    - NTM 02-21: NASD Provides Guidance to Member Firms concerning Anti-Money Laundering Compliance Programs Required by Federal Law (April 2002). (This includes a list of "red flags" that may be useful in identifying possible money laundering.)[8]

9. Other BSA Reports

Broker-dealers have other reporting obligations imposed by the BSA. They include:

Currency Transaction Reports (CTRs): Broker-dealers are required to file with FinCEN a CTR for any transaction over $10,000 in currency, including multiple transactions occurring during the course of the same day. A broker-dealer must treat multiple transactions as a single transaction if the broker-dealer has knowledge that the transactions are conducted by or on behalf of the same person and result in either cash in or cash out totaling more than $10,000 during any one business day. A CTR filing is made using a Currency Transaction Report, FinCEN Form 104 (formerly IRS Form 4789).

Reports of Foreign Bank and Financial Accounts (FBARs): Broker-dealers are required to file reports of foreign bank and financial accounts if the aggregate value of the accounts exceeds $10,000. FBARs are filed with Treasury using Form TD F 90-22.1.

Reports of Currency or Monetary Instruments (CMIRs): Broker-dealers must report any transportation of more than $10,000 in currency or monetary instruments into or outside of the U.S. on a Report of International Transportation of Currency or Monetary Instruments, FinCEN Form 105 (formerly Customs Form 4790). CMIRs are filed with the Commissioner of Customs.

***Source Documents*:**

- **CTR:** 31 C.F.R. §§ 1010.311, 1010.306, 1010.312.
  - BSA E-Filing System.
- **FBAR:** 31 C.F.R. §§1010.350, 1010.306, 1010.420.
  - Form TD F 90-22.1.
  - Final Rule: 76 Fed Reg 10234 (February 24, 2011).
- **CMIR:** 31 C.F.R. §§ 1010.340, 1010.306.
  - FinCEN Form 105.
- **FinCEN Guidance:**
  - FinCEN Ruling 2003-1: Regarding the Aggregation of Currency Transactions Pursuant to 31 CFR Section 103.22 (October 3, 2002).
  - Guidance on Interpreting Financial Institution Policies in Relation to Recordkeeping Requirements under 31 C.F.R. 103.29 (November 2002).
  - FinCEN Ruling 2005-6: Suspicious Activity Reporting (Structuring) (July 15, 2005).
- ***NYSE Guidance*:**
  - IM 86-2: Revised Currency Transaction Report (January 29, 1986).
  - IM 89-5: Reporting of Suspicious Transactions Under the Money Laundering Control Act of 1986 (January 20, 1989).
  - IM 89-14: Amendments to Bank Secrecy Act Regulations Relating to Currency Transactions (March 22, 1989).

10. Records of Funds Transfers

Under the "joint rule" and "travel rule," broker-dealers must keep records of funds transfers of $3000 or more (such as wire transfers), including certain related information (such as name, address, account number of client, date and amount of wire, payment instructions, name of recipient institution, and name and account information of wire payment recipient). The "travel rule" also requires that certain information obtained or retained by the transmittor's financial institution "travel" with the transmittal order through the payment chain.

Source Documents:

- **Joint Rule:** 31 C.F.R. § 1010.410(e).
- **Travel Rule:** 31 C.F.R § 1010.410(f).
- **Other Rule-Related Documents:**
  - *Advance Notice of Proposed Rulemaking:* 71 Fed. Reg. 35564 (June 21, 2006).
- **FinCEN Guidance:**
  - FinCEN Advisory: Funds Transfers: Questions & Answers (June 1996).[9]
  - FinCEN Advisory: Funds "Travel" Regulations: Questions & Answers (January 1997).[10]
  - FinCEN Advisory: Funds "Travel" Regulations: Questions & Answers (November 2010).

11. Information Sharing with Law Enforcement and Financial Institutions

Two provisions relating to information sharing were added to the BSA by the USA PATRIOT Act. One provision requires broker-dealers to respond to *mandatory* requests for information made by FinCEN on behalf of federal law enforcement agencies. The other provides a safe harbor to permit and facilitate *voluntary* information sharing among financial institutions.

Mandatory Information Sharing: Section 314(a) Requests: FinCEN's BSA information sharing rules, under Section 314(a), authorize law enforcement agencies with criminal investigative authority to request that FinCEN solicit, on the agency's behalf, certain information from a financial institution, including a broker-dealer. These requests are often referred to as "Section 314(a) information requests." Upon receiving a Section 314(a) request, a broker-dealer is required to search its records to determine whether it has accounts for, or has engaged in transactions with, any specified individual, entity, or organization. If the broker-dealer identifies an account or transaction identified with any individual, entity or organization named in the request, it must report certain relevant information to FinCEN. Broker-dealers also must designate a contact person (typically the firm's AML compliance officer) to receive the requests and must maintain the confidentiality of any request and any responsive reports to FinCEN.

Source Documents:

- ***Section 314(a) Rule:*** 31 C.F.R. § 1010.520.
- ***Rule Release:*** 67 Fed. Reg. 60579 (September 26, 2002).
- **Proposed Rule Release:** 74 Fed. Reg. 58926 (November 16, 2009).
- **Final Rule Release: Broadening Access to the 314(a) program**- 75 Fed. Reg. 6560 (February 10, 2010).
- ***FinCEN Guidance:***
    - Treasury Issues Moratorium on Section 314(a) Information Requests (November 26, 2002).
    - FinCEN to Reinstate USA PATRIOT Act Section 314(a) Information Requests (February 6, 2003).
    - Implementation of Web-based 314(a) Secure Communication System (February 4, 2005).
    - FinCEN 314(a) Fact Sheet (April 5, 2011).
    - Changing your Point of Contact for 314(a) (November 5, 2010).
- ***NYSE Guidance:***
    - IM 02-58: Temporary Moratorium on Information Requests Under Section 314 of the USA Patriot Act (December 26, 2002).
    - IM 03-3: Lifting of the Temporary Moratorium on Information Requests Under Section 314 of the USA Patriot Act (February 20, 2003).
- ***NASD Guidance:***
    - NTM 02-80: Development Regarding Treasury Information Requests Under Section 314 of the PATRIOT Act (December 2002).

Voluntary Information Sharing Among Financial Institutions: Section 314(b): A separate safe harbor provision encourages and facilitates voluntary information sharing among participating financial institutions. The safe harbor provision, added to the BSA by Section 314(b) of the USA PATRIOT Act, protects financial institutions, including broker-dealers, from certain liabilities in connection with sharing certain AML related information with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities. Treasury's implementing regulations require that a financial institution or association of financial institutions that intends to share information pursuant to the regulations must file an annual notice with FinCEN, maintain procedures to protect the security and confidentiality of the information, and take reasonable steps to verify that the financial institution or association of financial institutions with which it intends to share the information has filed the required notice with FinCEN. This may be done by checking a list

that FinCEN makes available. A notification form and instructions for submitting a notification form (initial or renewal) are available on FinCEN's website.

Source Documents:

- ***Section 314(b) Rule:*** 31 C.F.R. § 1010.540.
- ***Final Rule Release:*** 67 Fed. Reg. 60579 (September 26, 2002).
- ***Rule-Related Documents:***
  - *Interim Final Rule*: 67 Fed. Reg. 9874 (March 4, 2002).
- **314(b) Notice Form:** (http://www.fincen.gov/314b.pdf).
- ***FinCEN Guidance:***
  - Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (June 16, 2009).

12. Special Measures Imposed by the Secretary of the Treasury

Section 311 of the USA PATRIOT Act amended the BSA to authorize the Secretary of the Treasury to require broker-dealers to take "special measures" to address particular money laundering concerns. The Secretary of the Treasury may impose special measures on foreign jurisdictions, financial institutions, or transactions or types of accounts found to be of "primary money laundering concern." There are five "special measures," including prohibiting U.S. financial institutions from opening or maintaining certain correspondent accounts. In addition, FinCEN issued a rule proposal on November 28, 2011, which, if adopted, will impose special measures against the Islamic Republic of Iran.[11]

Source Documents:

- **Section 311 Information:** Information about Section 311 is generally available at:
  - www.fincen.gov.
  - Section 311 Special Measures
- ***NYSE Guidance:***
  - IM 07-34: NASD and NYSE Joint Release Regarding Special Measures against Specified Banks Pursuant to Section 311 of the USA Patriot Act (April 18, 2007).
  - IM 06-58: NYSE and NASD Joint Release Regarding Special Measures Against Specified Banks Pursuant to Section 311 of the USA Patriot Act (August 14, 2006).
- ***NASD Guidance:***
  - NTM 07-17: NYSE and NASD Joint Release Regarding Special Measures Against Specified Banks Pursuant to Section 311 of the USA Patriot Act (April 2007).
  - NTM 06-41: NASD and NYSE Joint Release on Section 311 of the USA PATRIOT Act (August 2006).

13. OFAC Sanctions Programs and Other Lists

OFAC is an office within Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorism sponsoring organizations, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under

Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction.

OFAC's sanctions programs are separate and distinct from, and in addition to, the AML requirements imposed on broker-dealers under the BSA.

As a tool in administering sanctions, OFAC publishes lists of sanctioned countries and persons that are continually being updated. Its list of Specially Designated Nationals and Blocked Persons (SDNs) lists individuals and entities from all over the world whose property is subject to blocking and with whom U.S. persons cannot conduct business. OFAC also administers country-based sanctions that are broader in scope than the "list-based" programs.

In general, OFAC regulations require broker-dealers to:

- block accounts and other property or property interests of entities and individuals that appear on the SDN list;
- block accounts and other property or property interests of entities and individuals subject to blocking under OFAC country-based programs; and
- block or reject unlicensed trade and financial transactions with OFAC-specified countries, entities, and individuals.

Broker-dealers must report all blockings and rejections of prohibited transactions to OFAC within 10 days of being identified and annually. OFAC has the authority to impose substantial civil penalties administratively. To guard against engaging in OFAC prohibited transactions, one best practice that has emerged entails "screening against the OFAC list." OFAC has stated that it will take into account the adequacy of a firm's OFAC compliance program when it evaluates whether to impose a penalty if an OFAC violation has occurred. Firms should be aware of other lists, such as the Financial Action Task Force ("FATF") list of non-compliant countries (the "NCCT list"). If transactions originate from or are routed to any FATF-identified countries, it might be an indication of suspicious activity.[12]

Source Documents:

- **OFAC Guidance:**
  - Program information, including the SDN list and countries subject to OFAC sanctions, is available on the OFAC website at: www.treas.gov/ofac
  - Foreign Assets Control Regulations for the Securities Industry (April 29, 2004).
  - Economic Sanctions Enforcement Guidelines (73 FR 51933; September 2, 2008)
  - Opening Securities and Futures Accounts from an OFAC Perspective (November 5, 2008)
  - Risk Factors for OFAC Compliance in the Securities Industry (November 5, 2008)
  - Economic Sanctions Enforcement Guidelines (November 9, 2009)
  - *OFAC Frequently Asked Questions*, available on the OFAC website at: http://www.treas.gov/offices/enforcement/ofac/faq/index.shtml [13]
- **FinCEN Guidance:**
  - *Interpretive Release No. 2004-02-Unitary Filing of Suspicious Activity and Blocking Reports*. *See also* 69 Fed. Reg. 76847 (December 23, 2004).

- ***NASD Guidance*:**
  - NTM 01-67: Executive Order Targeting Terrorists (October 2001).
  - *OFAC Search Tool*: This tool is available as a hyperlink, called OFAC's SDN List, and is available on the FINRA website.
- ***NYSE Guidance:***
  - IM 95-45: Department of Treasury List of Specifically Designated Narcotics Traffickers (October 25, 1995).
  - IM 96-11: Updated Listing of The Department of Treasury "Specially Designated Nationals and Blocked Persons" (April 1, 1996).
  - IM 97-10: Updated Listing of the Department of Treasury "Specially Designated Nationals and Blocked Persons" (February 7, 1997).
  - IM 97-28: Updated Listing of the Department of Treasury "Specially Designated Nationals and Blocked Persons" (May 20, 1997).
  - IM 01-26: Terrorism Executive Order and Updated Listing of the Department Of Treasury "Specially Designated Nationals and Blocked Persons" (September 24, 2001).
  - IM 01-35: Updated Listing of the Department of Treasury Specially Designated Nationals and Blocked Persons (October 19, 2001).
  - IM 01-39: Updated Listing of the Department of Treasury "Specifically Designated Nationals and Blocked Persons" (November 21, 2001).
- **Other Lists:**
  Other lists of countries supporting international terrorism may be available at:
  - U.S. State Dept.: www.state.gov/s/ct
  - FATF: www.fatf-gafi.org.
  - FinCEN High Intensity Financial Crimes Areas Designation is at: https://www.fincen.gov/hifca.

14. Selected Additional AML Resources

- **SEC Staff Materials:**
  - Kevin Goodman, "Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance" (June 18, 2015)
  - OCIE/NEP Risk Alert: Broker-Dealer Controls Regarding Customer Sales of Microcap Securities (October 9, 2014)
  - OCIE/NEP Risk Alert: Master/Sub Accounts (September 29, 2011)
  - Richards, Lori, "Anti-Money Laundering in 2006: It's the Total Mix," Remarks before the Securities Industry Association Conference on Anti-Money Laundering Compliance (March 29, 2006).
  - Carlo di Florio, Keynote address at the SIFMA Anti-Money Laundering Seminar (March 3, 2011).
  - David W. Blass, Broker-Dealer Anti-Money Laundering Compliance — Learning Lessons from the Past and Looking to the Future" (February 29, 2012)
- **FinCEN Materials:**
  - FinCEN Advisories/Bulletins/Fact Sheets
  - 2015 National Money Laundering Risk Assessment
  - 2015 National Terrorist Financing Risk Assessment
  - Remarks of James H. Freis, Jr., Director, FinCEN, before the SIFMA Anti-Money Laundering Compliance Conference (March 5, 2008).
- **FATF Materials:**
  - Money Laundering and Terrorist Financing in the Securities Sector (October 2009)

- Anti-money Laundering and Counter-Terrorist Financing Measures: Mutual Evaluation of the United States (December 2016)

- **Selected AML Enforcement Cases:**
  - *In the Matter of Pinnacle Capital Markets, LLC and Michael A. Paciorek,* Exchange Act Release No. 62811 (September 1, 2010).
  - *In the matter of Ronald S. Bloomfield, Robert Georgia, Victor Labi, John Earl Martin, Sr., and Eugene Miller,* Exchange Act Release No. 61988 (April 27, 2010).
  - FINRA Hearing Panel Decision in Department of Enforcement v.Sterne, Agee, & Leach, Inc. (March 5, 2010).
  - *Securities and Exchange Commission v. Todd M. Ficeto, Florian Homm, Colin Heatherington, Hunter World Markets, Inc., and Hunter Advisors, LLC, et al.*, Litigation Release No. 21865 (February 25, 2011)
  - FINRA Fines Firms $750,000 for Inadequate Anti-Money Laundering Programs, Other Violations: Penson Financial Services Fined $450,000 for Inadequate Review of Hundreds of Thousands of Trades a Day; Pinnacle Capital Markets Fined $300,000 for Failing to Verify Foreign Customer Identities and to Detect and Report Suspicious Activity (February 2, 2010).
  - Scottrade Fined $600,000 for Inadequate Anti-Money Laundering Program (October 26, 2009).
  - FINRA: Letter of Acceptance, Waiver and Consent: Scottrade, Inc. (October 26, 2009).
  - FINRA Fines Three Firms Over $1.25 Million for Failing to Detect, Investigate and Report Suspicious Transactions in Penny Stocks (June 4, 2009).
  - FINRA: Letter of Acceptance, Waiver and Consent: Legent Clearing LLC (June 4, 2009).
  - FINRA: Letter of Acceptance, Waiver and Consent: J.P. Turner & Co., LLC; S. Cheryl Bauman; Robert S. Meyer (June 4, 2009).
  - FINRA: Letter of Acceptance, Waiver and Consent: Park Financial Group, Inc., Gordon Charles Cantley, David Farber (June 4, 2009).
  - *In the Matter of Ferris, Baker Watts, Inc.*, Exchange Act Release No. 59372 (February 10, 2009).
  - E*Trade Units Fined $1 Million for Inadequate Anti-Money Laundering Program (January 2, 2009).
  - FINRA Expels Barron Moore and Takes Disciplinary Actions Against Seven Individuals for Illegal Sales of Unregistered Penny Stocks (September 3, 2008).
  - *In the Matter of E*Trade Clearing LLC and E*Trade Securities LLC,* Exchange Act Release No. 58250 (July 30, 2008).
  - FINRA: Letter of Acceptance, Waiver and Consent: Southwest Securities, Inc. (July 18, 2008).
  - FINRA: Letter of Acceptance, Waiver and Consent: Citigroup Global Markets Inc. (June 5, 2008).
  - FINRA: Letter of Acceptance, Waiver and Consent: James I. Black (May 9, 2008).
  - *In the Matter of Park Financial Group, Inc. and Gordon C. Cantley,* Exchange Act Release No. 55614 (April 11, 2007) and Exchange Act Release No. 56902. (December 5, 2007).
  - FINRA Expels Franklin Ross, Inc. for Systemic Violations of Anti-Money Laundering Rules (November 5, 2007).
  - RBC Dain Rauscher, New York Stock Exchange Hearing Panel Decision 07-44 (March 23, 2007).
  - NASD vs. NevWest Securities Corporation, Sergey Rumyantsev, and Anthony M. Santos (March 13, 2007).

    - NASD Fines Bank of America Investment Services, Inc. $3 Million for Failing to Comply with Anti-Money Laundering Rules in Connection with High Risk Accounts (January 29, 2007).
    - John Pettus, New York Stock Exchange Hearing Panel Decision 06-082 (August 9, 2006).
    - *In the Matter of Crowell, Weedon & Co.*, Exchange Act Release No. 53847 (May 22, 2006).
    - Oppenheimer & Co. Inc., New York Stock Exchange Hearing Panel Decision 05-181 (December 29, 2005). *See also* In the Matter of Oppenheimer & Company, New York, New York, United States of America Department of the Treasury Financial Crimes Enforcement Network No. 2005-4 (December 29, 2005).
    - Bear Stearns & Co. Inc., New York Stock Exchange Hearing Panel Decision 05-163 (December 22, 2005).
    - In the Matter of Hartsfield Capital Securities, Inc., United States of America Department of the Treasury Financial Crimes Enforcement Network No. 2003-05 (November 24, 2003).
- **FFIEC AML Examination Manual — February 2015 Update,**[14] available at: https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf

Money Laundering & Bank Secrecy Act (BSA) Statistical Data

Since actions on a specific investigation may cross fiscal years, the data shown in cases initiated may not always represent the same universe of cases shown in other actions within the same fiscal year.

Money Laundering Investigations	FY 2016	FY 2015	FY 2014
Investigations Initiated	1201	1436	1312
Prosecution Recommendations	1010	1301	1071
Indictments/Informations	979	1221	934
Sentenced	668	691	785
Incarceration Rate*	84.1%	84.1%	82.2%
Average Months to Serve	62	65	66

Bank Secrecy Act (BSA) Investigations	FY 2016	FY 2015	FY 2014
Investigations Initiated	504	613	809
Prosecution Recommendations	411	519	677
Indictments/Informations	399	533	608
Sentenced	449	557	535
Incarceration Rate*	74.8%	72.4%	74.8%
Average Months to Serve	36	31	35

BSA statistics include investigations from Suspicious Activity Report (SAR) Review Teams, violations of BSA filing requirements, and all Title 31 and Title 18-1960 violations.
*Incarceration includes confinement to federal prison, halfway house, home detention, or some combination thereof.
Data Source: IRS Criminal Investigation Management Information System.

Money Laundering in the News

FinCEN Penalizes U.S. Bank National Association for Violations of Anti-Money Laundering Laws February 15, 2018

Bank capped number of alerts rather than invest resources to investigate suspicious activity

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN), in coordination with the Office of the Comptroller of the Currency, and the U.S. Department of Justice, today announced the assessment of a $185 million civil money penalty against U.S. Bank for willful violations of several provisions of the Bank Secrecy Act (BSA). U.S. Bank's obligation will be satisfied by payment of $70 million to the U.S. Department of the Treasury with the remaining amount satisfied by payments in accordance with the DOJ's actions. Since 2011, U.S. Bank willfully violated the BSA's program and reporting requirements by failing to establish and implement an adequate anti-money laundering program, failing to report suspicious activity, and failing to adequately report currency transactions.

Banks are required to conduct risk-based monitoring to sift through transactions and to alert staff to potentially suspicious activity. Instead of addressing apparent risks, U.S. Bank capped the number of alerts its automated transaction monitoring system would generate to identify only a predetermined number of transactions for further investigation, without regard for the legitimate alerts that would be lost due to the cap.

"U.S. Bank is being penalized for willfully violating the Bank Secrecy Act, and failing to address and report suspicious activity. U.S. Bank chose to manipulate their software to cap the number of suspicious activity alerts rather than to increase capacity to comply with anti-money laundering laws," said FinCEN Director Kenneth A. Blanco. "U.S. Bank's own anti-money laundering staff warned against the risk of this alerts-capping strategy, but these warnings were ignored by management. U.S. Bank failed in its duty to protect our financial system against money laundering and provide law enforcement with valuable information."

U.S. Bank systemically and continually devoted an inadequate amount of resources to its AML program. Internal testing by U.S. Bank showed that alert capping caused it to fail to investigate and report thousands of suspicious transactions. Instead of removing the alert caps, the bank terminated the testing. U.S. Bank also allowed, and failed to monitor, non-customers conducting millions of dollars of risky currency transfers at its branches through a large money transmitter. In addition, U.S. Bank filed over 5,000 Currency Transaction Reports (CTRs) with incomplete or inaccurate information, impeding law enforcement's ability to identify and track potentially unlawful behavior.

U.S. Bank also had an inadequate process to handle high-risk customers. As a result, customers whom the bank identified or should have identified as high-risk were free to conduct transactions through the bank, with little or no bank oversight. By not having an adequate process in place to address high-risk customers, U.S. Bank failed to appropriately analyze or report the illicit financial risks of its customer base. These failures precluded the bank from adequately

addressing the risks that such customers posed, including filing timely suspicious activity reports that law enforcement investigators rely upon to recognize and to pursue financial criminals.

FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws April 18, 2019

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) has assessed a civil money penalty against Eric Powers for willfully violating the Bank Secrecy Act's (BSA) registration, program, and reporting requirements. Mr. Powers failed to register as a money services business (MSB), had no written policies or procedures for ensuring compliance with the BSA, and failed to report suspicious transactions and currency transactions.

Mr. Powers operated as a peer-to-peer exchanger of convertible virtual currency. As "money transmitters," peer-to-peer exchangers are required to comply with the BSA obligations that apply to MSBs, including registering with FinCEN; developing, implementing, and maintaining an effective AML program; filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs); and maintaining certain records.

"Obligations under the BSA apply to money transmitters regardless of their size," said FinCEN Director Kenneth A. Blanco. "It should not come as a surprise that we will take enforcement action based on what we have publicly stated since our March 2013 Guidance—that exchangers of convertible virtual currency, such as Mr. Powers, are money transmitters and must register as MSBs. In fact, there were indications that Mr. Powers specifically was aware of these obligations, but willfully failed to honor them. Such failures put our financial system and national security at risk and jeopardize the safety and well-being of our people, as well as undercut responsible innovation in the financial services space."

Mr. Powers advertised his intent to purchase and sell bitcoin on the internet. He completed transactions by either physically delivering or receiving currency in person, sending or receiving currency through the mail, or coordinating transactions by wire through a depository institution. Mr. Powers processed numerous suspicious transactions without ever filing a SAR, including doing business related to the illicit darknet marketplace "Silk Road," as well as servicing customers through The Onion Router (TOR) without taking steps to determine customer identity and whether funds were derived from illegal activity.

Mr. Powers conducted over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single CTR. For instance, Mr. Powers conducted approximately 160 purchases of bitcoin for approximately $5 million through in-person cash transactions, conducted in public places such as coffee shops, with an individual identified through a bitcoin forum. Of these cash transactions, 150 were in-person and were conducted in separate instances for over $10,000 during a single business day. Each of these 150 transactions necessitated the filing of a CTR.

FinCEN notes that this is its first enforcement action against a peer-to-peer virtual currency exchanger and the first instance in which it has penalized an exchanger of virtual currency for

failure to file CTRs. FinCEN also notes that since his infractions, Mr. Powers has cooperated with FinCEN efforts. In addition to paying a $35,000 fine, Mr. Powers has agreed to an industry bar that would prohibit him from providing money transmission services or engaging in any other activity that would make him a "money services business" for purposes of FinCEN regulations.

FinCEN Penalizes Texas Bank for Violations of Anti-Money Laundering Laws Focusing on Section 312 Due Diligence Violations November 01, 2017

WASHINGTON, D.C. – The Financial Crimes Enforcement Network (FinCEN) today announced the assessment of a $2 million civil money penalty against Lone Star National Bank (Lone Star) of Pharr, Texas for willfully violating the Bank Secrecy Act (BSA). The action underscores the dangers that institutions face when taking on international correspondence activities without properly equipping themselves to manage such business. As noted in FinCEN's assessment, among other lapses, Lone Star failed to comply with section 312 of the USA PATRIOT Act, which imposes specific due diligence obligations with respect to correspondent banking.

Many of the lapses in Lone Star's BSA compliance were previously covered in an earlier action by the Office of the Comptroller of the Currency (OCC), but FinCEN's action focusing on the bank's 312 violations specifically highlights the need for a financial institution to avoid taking on international business for which it is not prepared. Lone Star's Mexican financial institution customer was moving millions of dollars through Lone Star in a manner inconsistent with the parameters of a relationship which, at the outset, required greater scrutiny. Lone Star failed to identify and consider public information about the foreign bank owner's alleged involvement in securities fraud. It also failed to verify the accuracy of assertions by the foreign bank with respect to source of funds, purpose of the account, and expected activity.

"Lone Star plainly failed to ask obvious due diligence questions in connection with its foreign bank account relationship, and did not follow up on inconsistencies in answers to the questions that it did ask," said FinCEN Acting Director Jamal El-Hindi. "Notwithstanding the fact that the OCC already fined the bank, FinCEN's assessment takes into account the penalties specifically applicable under FinCEN's Section 312 authority. Smaller banks, just like the bigger ones, need to fully understand and follow the 312 due diligence requirements if they open up accounts for foreign banks. The risks can indeed be managed, but not if they are ignored."

With respect to many of the deficiencies noted in FinCEN's assessment, the OCC entered into a Consent Order and a Memorandum of Understanding with Lone Star in 2012. Lone Star continued to have severe programmatic anti-money laundering (AML) deficiencies through 2012, 2013, and 2014. As a result, in 2015, the OCC issued a Consent Order for a Civil Money Penalty in the amount of $1 million against Lone Star. Lone Star's previous penalty payment to the OCC will be credited to FinCEN's assessment and the bank will pay an additional $1 million to satisfy its obligation to FinCEN.

FinCEN recognizes that Lone Star has expended considerable resources to respond to the findings regarding its BSA program and to promote compliance with the OCC's Consent Order. Lone Star is no longer engaging in the correspondent banking activities for which it was ill prepared. The bank has contracted outside consultants to conduct independent testing, conduct customer due diligence and suspicious activity lookbacks, and has expanded its BSA compliance organization.

DFS Fines Western Union $60 Million For Violations Of New York's Anti-Money Laundering Laws And For Ignoring Suspicious Transactions To Locations In China
January 4, 2018

- DFS Investigation Finds Western Union Failed to Implement and Maintain Anti-Money Laundering Compliance Between 2004 and 2012
- Western Union Executives and Managers Willfully Ignored and Failed to Disclose Illegal Conduct by Agents Who Engaged in Fraud and Suspicious Transactions to China Which May Have Aided Human Trafficking
- DFS Requiring Western Union to Designate a Compliance Point of Contact and Submit Plan to Ensure Adequate Anti-Money Laundering and Anti-Fraud Controls, Including Requiring All Agents to Adhere to U.S. Regulatory and Anti-Money Laundering Standards

Financial Services Superintendent Maria T. Vullo today announced that Western Union has agreed to pay a $60 million fine as part of a consent order with the New York State Department of Financial Services (DFS) for violations of New York Bank Secrecy Act (BSA) and anti-money laundering laws (AML). An investigation by DFS found that, for more than a decade, Western Union failed to implement and maintain an anti-money laundering compliance program to deter, detect and report on criminals' use of its electronic network to facilitate fraud, money laundering and the illegal structuring of transactions below amounts that would trigger regulatory reporting requirements. In addition, the DFS investigation discovered that senior Western Union executives and managers willfully ignored, and failed to report to DFS, suspicious transactions to Western Union locations in China by several high-volume agents in New York, other states and around the world, including money transfers that may have aided human trafficking. DFS licenses and regulates money transmitters in New York State and is the sole regulator for Western Union in New York State.

"Western Union executives put profits ahead of the company's responsibilities to detect and prevent money laundering and fraud, by choosing to maintain relationships with and failing to discipline obviously suspect, but highly profitable, agents," said Superintendent Vullo. "DFS will not tolerate unlawful activity that undermines anti-money laundering laws and endangers the integrity of our financial system."

The DFS investigation found that between at least 2004 and 2012, Western Union willfully failed to implement and maintain an effective anti-money laundering program to deter, detect, and report on suspected criminal fraud, money laundering, and illegal "structuring" schemes. Structuring occurs when a party executes financial transactions in a specific pattern, like

breaking up a larger sum into smaller transactions. The purpose of structuring typically is to avoid triggering the obligation of a money transmitter like Western Union to file reports with the federal government required by the BSA, or to avoid the money transmitter's own requirements for providing certain types of identification and other evidence of the legitimacy of the financial transaction.

Western Union has a prior history of compliance issues. In 2002, DFS's predecessor agency, the New York State Banking Department, conducted an examination of the company and determined that it failed to establish effective procedures to monitor its agents, detect suspicious transactions, and file suspicious activity reports. In addition, in a January 2017 agreement with the U.S. Department of Justice, Western Union admitted to federal criminal offenses of willfully failing to implement an effective anti-money laundering program under the Bank Secrecy Act, and aiding and abetting wire fraud.

In today's announcement, DFS said that several Western Union executives and managers knew about or willfully ignored improper conduct involving "NY China Corridor agents." Moreover, even after the U.S. Department of Justice launched an investigation of Western Union in 2012, and the company became aware of the full scope of the misconduct involving the NY China Corridor Agents, the company waited two years to disclose this information to the DFS.

The NY China Corridor agents include a small business located in Lower Manhattan, one in Sunset Park, Brooklyn, and another in Flushing, Queens. Despite their small size, these agents were some of Western Union's largest agent locations in the world by transaction volume – and thus some of the most profitable for the company.

The Lower Manhattan agent, a small travel agency that offered Western Union money transmission services, processed more than 447,000 transactions totaling more than $1.14 billion between 2004 and 2011. The Sunset Park location appears to be owned by the spouse of the owner of the Lower Manhattan location. The two agents were among the biggest Western Union agents in the entire country.

The Sunset Park location, a small business that sold wireless cellphone services to consumers, and also offered Western Union money transmission services, processed more than 302,000 transactions, totaling more than $600 million, between 2005 and 2011. Almost all of the more than $1.7 billion transfers processed in this time period processed by the Lower Manhattan and Sunset Park agents were transmitted to China. According to federal law enforcement authorities, at least 25 to 30 percent of these transactions showed indications of illegal structuring.

Between 2004 and 2012, the Flushing location processed more than 735,000 transactions, totaling more than $1.2 billion, most of which were sent to China. The sheer number and size of transactions processed by these agents, which were small independent stores each with a small number of employees, stood out as strong indicators of significant money laundering risk.

Western Union had extensive evidence indicating repeated suspicious, improper, or illegal conduct by these agents. The company conducted almost two dozen compliance reviews of the Lower Manhattan and Sunset Park agents during the relevant time period. On each occasion,

Western Union compliance staff found clear deficiencies with AML rules and internal company policies. However, senior managers intervened in the disciplinary to push for special treatment for problematic agents that were the highest fee generators, including failing to suspend them. In New York, these tended to be the NY China Corridor agents.

In 2008, Western Union paid the owner of the Lower Manhattan location a $250,000 bonus to renew his contract with the company, despite the agent's numerous compliance violations. The owner of the Lower Manhattan location later admitted to law enforcement agents that he knew that at least some customers used Western Union's money transfer services to pay debts to human traffickers based in China, and structured transactions to avoid identification and reporting requirements and thus evade scrutiny.

Western Union pays agents a commission for each money transfer the agent processes. It may also pay an agent bonuses and other compensation based on transaction volume. The company can terminate or suspend any agent or agent location for a variety of reasons, but especially for compliance reasons.

Western Union, which has more than 2,800 agent locations in New York State, has been licensed by DFS since 1990. In 2016, New York agents processed more than 18 million consumer-to-consumer financial transactions, totaling more than $4 billion. Transactions involving New York agents in 2016 yielded $224 million in revenue for Western Union, resulting in gross profits to the company of approximately $50 million.

Western Union must submit a written plan to DFS within 90 days that is designed to ensure the enduring adequacy of its anti-money laundering and anti-fraud programs. Western Union must also submit a written progress report to DFS detailing the form and manner of all actions taken to secure compliance with the provisions of this Order, and the results of any such actions at six, twelve, eighteen, and twenty-four months from the date of the Consent Order.

MoneyGram International Inc. Agrees to Extend Deferred Prosecution Agreement, Forfeits $125 Million in Settlement with Justice Department and Federal Trade Commission Thursday, November 8, 2018

Company also Agrees to Implement Additional Anti-Fraud and Anti-Money Laundering Program Compliance Enhancements in Agreements with Federal Authorities

MoneyGram International Inc. (MoneyGram), a global money services business headquartered in Dallas, Texas, has agreed to extend its deferred prosecution agreement and forfeit $125 million due to significant weaknesses in MoneyGram's anti-fraud and anti-money laundering (AML) program resulting in MoneyGram's breach of its 2012 deferred prosecution agreement (DPA). In addition to the monetary payment and extension of the deferred prosecution agreement, the company must enhance its anti-fraud and AML compliance programs.

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney David J. Freed of the Middle District of Pennsylvania, Federal Trade

Commission (FTC) Chairman Joseph Simons and Postal Inspector-in-Charge Daniel B. Brubaker of the U.S. Postal Inspection Service (USPIS) Philadelphia Division made the announcement.

A two-count felony criminal information was filed on Nov. 9, 2012, in the Middle District of Pennsylvania charging MoneyGram with willfully failing to maintain an effective AML program and aiding and abetting wire fraud. The government agreed to defer prosecution on the information for five years provided MoneyGram complied with the DPA. Today's amendment to the agreement will extend the term of the DPA for 30 months.

According to court documents filed in 2012, MoneyGram was involved in consumer fraud schemes perpetrated by corrupt MoneyGram agents and others. In the fraud scams, which generally targeted the elderly and other vulnerable groups, perpetrators contacted victims in the United States and falsely posed as victim's relatives in urgent need of money, falsely promised large cash prizes, or promised items for sale over the internet at deeply discounted prices. The perpetrators required the victims to send funds through MoneyGram's money transfer system.

According to the joint motion filed today to extend and amend the DPA, MoneyGram breached its 2012 DPA. During the course of the DPA, MoneyGram experienced significant weaknesses in its AML and anti-fraud program, inadequately disclosed these weaknesses to the government, and failed to complete all of the DPA's required enhanced compliance undertakings. As a result of its failures, MoneyGram processed at least $125 million in additional consumer fraud transactions between April 2015 and October 2016.

Today, as a result of MoneyGram's breach of the DPA, the government filed a motion to extend all the terms of MoneyGram's DPA and amend and enhance MoneyGram's compliance requirements pursuant to the DPA. In addition, MoneyGram agreed to forfeit $125 million, which the department intends to return to victims of fraud through the Justice Department's Victim Compensation Program. Under the terms of the extension, the government has agreed to continue to defer prosecution for a period of 30 months, after which time the government would seek to dismiss charges if MoneyGram has complied with the agreement.

As part of the amendment to and extension of the DPA, MoneyGram has agreed to additional enhanced compliance obligations, including creating policies or procedures:

to block certain reported fraud receivers and senders from using MoneyGram's money transfer system within two days of receiving a complaint identifying those individuals;
to require individuals worldwide to provide government-issued identification to send or receive money transfers;
to monitor all money transfers originating in the United States in its anti-fraud program; and
to terminate, discipline, or restrict agents processing a high volume of transactions related to reported fraud receivers and senders.

In a related case, MoneyGram agreed to settle contempt allegations by the FTC filed today in the U.S. District Court for the Northern District of Illinois, alleging that MoneyGram violated its 2009 order with the FTC. The FTC alleges that MoneyGram failed to implement the comprehensive fraud prevention program mandated by the 2009 order, which requires the

company to promptly investigate, restrict, suspend, and terminate high-fraud agents. According to the FTC, MoneyGram was aware for years of the high levels of fraud and suspicious activities involving certain agents, including large chain agents, but failed to promptly conduct required reviews or suspend or terminate agents, as required by the 2009 order.

In resolving the FTC allegations, MoneyGram agreed to a monetary judgment of $125 million and to an expanded and modified order that will supersede the Commission's 2009 order and apply to money transfers worldwide. The modified order requires, among other things, that the company block the money transfers of known perpetrators of fraud schemes and provide refunds to fraud victims in circumstances where its agents fail to comply with applicable policies and procedures. In addition, the modified order includes enhanced due diligence, investigative, and disciplinary requirements.

The USPIS and the U.S. Attorney's Office for the Middle District of Pennsylvania have been investigating and prosecuting consumer fraud schemes using MoneyGram's money transfer system since 2007. To date, the U.S. Attorney's Office of the Middle District of Pennsylvania has charged 37 MoneyGram agent owners for conspiracy, money laundering and fraud-related violations. Twenty-eight of those charged have been convicted.

USPIS's Philadelphia Division's Harrisburg, Pennsylvania Office investigated the case. Senior Trial Attorney Margaret A. Moeser of the Criminal Division's Money Laundering and Asset Recovery Section's Bank Integrity Unit and Assistant U.S. Attorney Kim Douglas Daniel of the Middle District of Pennsylvania are prosecuting the case. The department appreciates the significant cooperation and assistance provided by the FTC in this matter.

Bank Sentenced for Obstructing Regulators, Forfeits $368 Million for Concealing Anti-Money Laundering Failures Friday, May 18, 2018

SAN DIEGO – Rabobank, National Association, a California subsidiary of the Netherlands-based Coöperatieve Rabobank U.A., was sentenced today before U.S. District Judge Jeffrey T. Miller for conspiring to impair, impede, and obstruct its primary regulator, the Department of the Treasury's Office of the Comptroller of the Currency (OCC), by concealing deficiencies in its anti-money laundering program.

Judge Miller sentenced Rabobank to pay the statutory maximum fine of $500,000 after taking account of Rabobank's forfeiture of $368,701,259 as well as a two-year term of probation. Today's half million dollar criminal fine coupled with Rabobank's forfeiture of $368,701,259 stands as the largest monetary penalty paid by a criminal defendant in the history of the Southern District of California.

In imposing sentence, Judge Miller noted that Rabobank's conduct essentially amounted to "stiff-arming the OCC, and completely failing in its responsibility to its customers and the nation."

"The U.S. Attorney's Office is intent on securing the border and preventing the laundering of narco-dollars through financial institutions like Rabobank," said U.S. Attorney Adam L. Braverman. "In doing so we will safeguard our communities and protect our citizens from drug traffickers and corporate criminals alike."

"Rabobank's branches on the Mexican border processed hundreds of millions of dollars in suspicious transactions likely tied to international narcotics trafficking, organized crime, and money laundering," said Acting Assistant Attorney General John P. Cronan. "Instead of filing reports that would have alerted law enforcement to the suspicious activity, as required by law, the bank looked the other way and then compounded its misconduct by conspiring to cover-up its failures and deceiving its regulator. Today's sentence and the related forfeiture demonstrate that the Department of Justice will use all the tools at our disposal to combat drug trafficking and transnational crime—including prosecuting financial institutions that turn a blind eye to illicit proceeds moving through their customers' accounts."

"It is the responsibility of Homeland Security Investigations ("HSI") to monitor and investigate activity which exploits the global infrastructure, to include financial systems. This complex investigation revealed, and Rabobank admits, that Rabobank was aware of the extreme risk that it was processing hundreds of millions of dollars related to transnational crime and international money laundering – activity which plagues the Southwest Border," said Dave Shaw, Special Agent in Charge for HSI in San Diego. "This plea and significant forfeiture sends a strong message to financial institutions that this activity will not be tolerated."

"Rabobank's sentencing today is a victory for all Americans and sends a strong message about the need for transparency in banking and ultimately contributes to the fight against money laundering," stated IRS Criminal Investigation's Special Agent in Charge, Los Angeles Field Office, R. Damon Rowe. "IRS-Criminal Investigation works diligently with our law enforcement partners to ensure funds obtained through illegal means do not find their way into our financial institutions."

Today's sentence follows Rabobank's February 7, 2018, guilty plea for conspiring with several former executives to defraud the United States by unlawfully impairing and impeding the OCC's ability to regulate the bank and obstructing its examination of Rabobank's Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program. In connection with that guilty plea, Rabobank admitted that between 2009 and 2012 it implemented BSA/AML policies and procedures that precluded and suppressed legally-mandated investigations into potentially suspicious account activity, much of which was conducted by cross-border customers and through accounts that Rabobank had previously designated "High-Risk."

As a result of its BSA/AML failures, Rabobank admitted that certain customer accounts were involved in not less than $368,701,259 in suspicious transactions that were either unreported or untimely reported to the Financial Crimes Enforcement Network (FinCEN), as required by the BSA. These transactions along the southwest border included high-volume cash deposits and withdrawals, check transactions, electronic transfers, and wire transfers that were consistent with illegal activity such as trade-based money laundering, bulk cash smuggling, structuring, and the black market peso exchange.

Rabobank's branches in Imperial County were heavily dependent on cash sourced from Mexico – cash the bank knew was likely tied to narcotics trafficking and organized crime. In particular, Rabobank's Calexico, California branch, located approximately two blocks from the U.S.-Mexico border, was the highest performing branch in the Imperial Valley region due to its receipt of cash from Mexico. Rabobank continued soliciting cash-intensive customers from Mexico, while failing to employ appropriate BSA/AML policies and procedures to address the heightened risk, until approximately May 2013, when Rabobank placed a moratorium on originating new account relationships for Mexico-based businesses entities.

Rabobank also admitted that the bank and its executives corruptly obstructed the OCC's 2012 examination by responding to the OCC's February 2013 initial report of examination with false and misleading information about the state of Rabobank's BSA/AML program and by making false and misleading statements to the OCC regarding the existence of reports developed by a third-party consultant that described the deficiencies and resulting ineffectiveness of Rabobank's BSA/AML program. Rabobank also demoted or terminated two of its employees who provided information to the OCC.

The case is being prosecuted by Assistant U.S. Attorneys Daniel C. Silva, Mark W. Pletcher, and David J. Rawls from the Southern District of California, and Trial Attorneys Kevin G. Mosley and Maria Vento of the Criminal Division's Money Laundering and Asset Recovery Section. The investigation team included HSI, IRS, and the Financial Investigations and Border Crimes Task Force (the "FIBC"), a multiagency Task Force based in San Diego and Imperial Counties, and funded by the Treasury Executive Office of Asset Forfeiture ("TEOAF"). The investigation occurred in parallel with regulatory investigations by the OCC, Office of General Counsel, and FinCEN, Enforcement Division

16 Parents Involved in College Admissions Scandal Indicted by Federal Grand Jury in Boston Defendants indicted on fraud and money laundering charges Tuesday, April 9, 2019

BOSTON – Sixteen parents involved in the college admissions scandal were charged today in Boston in a second superseding indictment with conspiring to commit fraud and money laundering in connection with a scheme to use bribery to cheat on college entrance exams and to facilitate their children's admission to selective colleges and universities as purported athletic recruits.

The defendants, all of whom were arrested last month on a criminal complaint, are charged with conspiring with William "Rick" Singer, 58, of Newport Beach, Calif., and others, to bribe SAT and ACT exam administrators to allow a test taker to secretly take college entrance exams in place of students, or to correct the students' answers after they had taken the exam, and with bribing university athletic coaches and administrators to facilitate the admission of students to elite universities as purported athletic recruits.

The second superseding indictment also charges the defendants with conspiring to launder the bribes and other payments in furtherance of the fraud by funneling them through Singer's

purported charity and his for-profit corporation, as well as by transferring money into the United States, from outside the United States, for the purpose of promoting the fraud scheme.

The following defendants were charged in the second superseding indictment with one count of conspiracy to commit mail and wire fraud and honest services mail and wire fraud and one count of conspiracy to commit money laundering:

Gamal Abdelaziz, 62, aka "Gamal Aziz," of Las Vegas, Nev.;
Diane Blake, 55, of Ross, Calif.;
Todd Blake, 53, of Ross, Calif.;
I-Hsin "Joey" Chen, 64, of Newport Beach, Calif.;
Mossimo Giannulli, 55, of Los Angeles, Calif.;
Elizabeth Henriquez, 56, of Atherton, Calif.;
Manuel Henriquez, 56, of Atherton, Calif.;
Douglas Hodge, 61, of Laguna Beach, Calif.;
Michelle Janavs, 48, of Newport Coast, Calif.;
Elisabeth Kimmel, 54, of Las Vegas, Nev.;
Lori Loughlin, 54, of Los Angeles, Calif.;
William McGlashan, Jr., 55, of Mill Valley, Calif.;
Marci Palatella, 63, of Hillsborough, Calif.;
John Wilson, 59, of Lynnfield, Mass.;
Homayoun Zadeh, 57, of Calabasas, Calif.; and
Robert Zangrillo, 52, of Miami, Fla.

Three parents—David Sidoo, 59, of Vancouver, Canada; Gregory Colburn, 61, of Palo Alto, Calif.; and Amy Colburn, 59, of Palo Alto, Calif.—were previously indicted in connection with the scheme.

An arraignment date has not yet been scheduled. Case information, including the status of each defendant, charging documents and plea agreements are available here: https://www.justice.gov/usao-ma/investigations-college-admissions-and-testing-bribery-scheme.

The charge of conspiracy to commit mail and wire fraud and honest services mail and wire fraud provides for a maximum sentence of 20 years in prison, three years of supervised release, and a fine of $250,000 or twice the gross gain or loss, whichever is greater. The charge of conspiracy to commit money laundering provides for a maximum sentence of 20 years in prison, three years of supervised release, and a fine of $500,000 or twice the value of the property involved in the money laundering. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Examples of Money Laundering Investigations - Fiscal Year 2015

The following examples of Money Laundering Investigations are written from public record documents on file in the courts within the judicial district where the cases were prosecuted.

California Woman Sentenced for Role in Offshore Sweepstakes Scheme
On Aug. 11, 2015, in Asheville, North Carolina, Patricia Diane Clark, of Sacramento, California, was sentenced to 130 months in prison and ordered to pay $642,032 in restitution and to forfeit the same amount jointly with her co-defendants. Clark pleaded guilty to conspiracy to commit wire fraud, wire fraud and conspiracy to commit money laundering. According to court documents, from about 2007 through February 2013, Clark and her co-conspirators called U.S. residents from Costa Rican call centers, falsely informing them that they had won a cash "sweepstakes." The victims, many of whom were elderly, were told that in order to receive the prize, they had to send money for a purported "refundable insurance fee." Clark picked up money from the victims and sent it to her co-conspirators in Costa Rica. Clark also managed others who picked up money from the victims in the US and she kept a portion of the victims' payments. Once the victims sent money, Clark's co-conspirators contacted the individuals again and falsely informed them that the prize amount had increased, either because of a clerical error or because another prize winner was disqualified. The victims then had to send more money to pay for "new" fees to receive the larger sweepstakes prize. The attempts to collect additional money from the victims continued until an individual either ran out of money or discovered the fraudulent nature of the scheme. Clark, along with her co-conspirators, was responsible for approximately $640,000 in losses to more than a hundred U.S. citizens.

Businessman Sentenced for Conspiracy to Misbrand a Product for Human Consumption, Money Laundering
On Aug. 5, 2015, in Providence, Rhode Island, Tayfun Karauzum, of Newport Beach, California, was sentenced to 60 months in prison and three years of supervised release. On Jan. 30, 2015, Karauzum pleaded guilty to conspiracy to misbrand a product for human consumption and money laundering. According to court documents, Karauzum manufactured, marketed and distributed for human consumption Potion 9, a product containing butanediol, an industrial solvent that rapidly metabolizes into gammahydroxybutyric acid (GHB) – commonly referred to as a "club drug" or "date rape drug." Karauzum was the owner of Max American Distribution LLC in Newport Beach, California, through which he marketed and distributed between $1 million and $2.5 million dollars' worth of Potion 9 through online sales and dietary supplement companies. Karauzum caused nearly 13.5 million milliliters of the misbranded product Potion 9 to be manufactured and available for distribution. Karauzum routinely transferred proceeds from the sale of Potion 9 sales in increments in excess of $10,000 from his business' PayPal account into a personal bank account.

Former Pharmacy Operator Sentenced for Structuring Bank Deposits
On Aug. 3, 2015 in Huntington, West Virginia, Kofi Ohene Agyekum, former owner and operator of A+ Care Pharmacy in Barboursville, West Virginia, was sentenced to 64 months in prison. Agyekum also agreed to forfeit to the United States more than $2.3 million plus a Lexus. Agyekum pleaded guilty in May 2015 and admitted to avoiding the federal reporting requirement by making deposits in an amount less than $10,000 and making the deposits in multiple bank

accounts in various area banks. Federal banking laws aimed at identifying criminal activity require financial institutions to report cash transactions of more than $10,000 to federal authorities. Structuring, or dividing cash transactions into amounts less than $10,000, is a common technique used by criminals to avoid triggering the reporting requirements and the detection of the underlying crimes. It was found that the funds Agyekum structured were derived from the illegal distribution of oxycodone from A+ Care Pharmacy.

North Carolina Man Sentenced for Theft of Government Funds
On July 29, 2015, in Greensboro, North Carolina, Juan Francisco Martinez, of Concord, was sentenced to 24 months in prison, three years of supervised release and ordered to pay $2,999,905 in restitution to the IRS. According to court documents, from April 2010 through September 2012, U.S. Treasury refund checks bearing out-of-state payee addresses were negotiated through Martinez's business bank accounts. The vast majority of these refund checks were fraudulently obtained through the submission of false tax returns and the legitimate refund checks processed through the accounts had been stolen. These refund checks often contained payee addresses from New York, New Jersey, Pennsylvania, and other locations outside North Carolina.

Former Ringleader of Albuquerque-Based Drug Trafficking Organization Sentenced
On July 28, 2015, in Albuquerque, New Mexico, Christopher Roybal, the former leader of an Albuquerque-based drug trafficking organization, was sentenced to 168 months in prison, five years of supervised release and required to pay a $184,080 money judgment. On Feb. 25, 2015, Roybal pleaded guilty to five counts of a second superseding indictment, charging him with participating in a cocaine trafficking conspiracy, three money laundering conspiracies, and a substantive money laundering offense. In entering his guilty plea, Christopher Roybal admitted that between Aug. 2011 and Dec. 2012, he conspired with others to distribute kilogram quantities of cocaine in Albuquerque and Las Vegas, N.M. He also admitted participating in three conspiracies that laundered the proceeds of his drug trafficking organization. One conspiracy involved the transportation of drug proceeds from Albuquerque to California to pay for marijuana that was distributed by Christopher Roybal's organization. The second and third conspiracies involved the laundering of Christopher Roybal's drug proceeds through accounts at a bank and a credit union. As part of his plea agreement, Roybal agreed to forfeit his Albuquerque residence and a 1967 Chevrolet Camaro. The charges filed in the case were the result of a 16-month multi-agency investigation into a drug trafficking organization headed by Roybal. Roybal was one of the 19 defendants charged in Dec. 2012, with drug trafficking and money laundering charges in a 60-count indictment. The indictment was superseded twice; first in Feb. 2014, to add a 20th defendant and a witness tampering charge, and again in Sept. 2014, to add another witness tampering charge and a heroin trafficking charge.

Ohio Man Sentenced for Over $1.1 Million Unemployment Fraud
On July 27, 2015, in Cleveland, Ohio, Juan Sanders was sentenced to 139 months in prison. He previously pleaded guilty to conspiracy to commit mail and wire fraud, wire fraud, aggravated identity theft and money laundering. According to court documents, from about September 2011 to January 2014, Sanders and others conspired to defraud state unemployment offices in Ohio, California, North Carolina, Massachusetts and Illinois. Sanders fraudulently obtained personal identifying information from unsuspecting individuals to submit fraudulent claims for

unemployment insurance benefits. Sanders also created state unemployment insurance accounts for multiple fictitious employers and then filed claims from "employees" who had been purportedly laid off by the fictitious companies. Sanders caused benefit debit cards for the "employees" of these fictitious companies to be mailed to various addresses in Ohio. Once the benefits were loaded or reloaded onto the debit cards, Sanders and his co-conspirators used the debit cards at various ATMs in Ohio to withdraw the fraudulently obtained money. As a result of this scheme, approximately $1,174,767 in fraudulent unemployment benefits were paid from state agencies in North Carolina ($572,170), Ohio ($261,509), Illinois ($144,240), California ($129,600) and Massachusetts ($67,248).

Former New York Stockbroker Sentenced for Financial Fraud Schemes
On June 25, 2015, in Central Islip, New York, Mark Hotton, a former Long Island stockbroker, was sentenced to 135 months in prison, three years of supervised release and ordered to pay $5,750,000 in restitution. On July 30, 2013, Hotton pleaded guilty to conspiring to launder the illicit proceeds of almost two decades of fraud. According to court documents, between January 1995 and October 2012, Hotton used funds he obtained from a series of securities fraud schemes, mail fraud schemes and other crimes to promote his continuing illegal conduct. Throughout the conspiracy, Hotton also laundered proceeds of his frauds to pay employees cash wages, thereby avoiding federal withholding taxes intended for Social Security, Medicare and Medicaid. Hotton also laundered funds to avoid required payments to union pension and benefit funds. Additionally, Hotton pleaded guilty to additional fraudulent conduct arising from the financing of the proposed Broadway play "Rebecca."

California Woman Sentenced in Connection with Bank Fraud
On July 24, 2015, in Helena, Montana, Erika Rae Brown, of San Diego, California, was sentenced to 56 months in prison, three years of supervised release and ordered to pay approximately $3.7 million in restitution which represents money Brown owes to a bank and the United States Department of Agriculture (USDA). On March 19, 2015, Brown pleaded guilty to money laundering in connection with a bank fraud scheme. According to court records, Brown obtained a four-million dollar bank loan based on a series of fraudulent representations about a data storage facility project she claimed she was working on. In January 2009, the bank forwarded the data company's loan application to the USDA. Following representations by one of Brown's associates regarding the project, the USDA committed to guarantee the loan. As part of the parameters for the loan, the bank required proof that companies were interested in using the data storage facility. Brown submitted false letters to the bank from several well-known national companies that purportedly wanted to use the data storage in addition to a number of cashier's checks and invoices in an effort to show that the company was in fact spending capital on the project. In reality, no national companies were interested and the checks were altered version of checks Brown had written for other expenses. A financial analysis of the loan proceeds revealed that Brown used the money for personal expenses, including $128,135 in rent for a Laguna Beach house and $5,825 for two Rolex watches. The bank foreclosed on the property in August 2013.

Former Bank Branch Manager Sentenced for Cashing Fraudulently Obtained Tax Refund Checks

On July 22, 2015, in Manhattan, New York, Edwin Mejia was sentenced to 44 months in prison, three years of supervised release and ordered to pay $442,642 in forfeiture and $442,642 in restitution. In December 2014, Mejia pleaded guilty to theft of public funds and aggravated identity theft in connection with his participation in a scheme to cash more than $400,000 in fraudulently obtained federal tax refund checks issued in other people's names. According to court documents, Mejia worked at branches of a bank in Yonkers and Manhattan. Mejia initially was a banker and later became the branch manager of multiple branches of the bank. From 2010 through 2013, Mejia participated in a scheme to fraudulently obtain and cash tax refund checks issued by the United States Treasury. The fraudulent refund checks were generated by the filing of false and fraudulent tax returns in the names of other people. As part of this scheme, Mejia helped facilitate the cashing of the fraudulent refund checks. Mejia cashed the fraudulent checks himself or by paying a co-conspirator to do so.

Two Colombian Citizens Sentenced for International Money Laundering Conspiracy
On July 20, 2015, in Miami, Florida, Leonardo Forero Ramirez and Ubaner Alberto Acevedo Espinosa were sentenced to 37 months and 18 months in prison, respectively, and ordered to serve one year of supervised release. Both defendants previously pleaded guilty to conspiracy to commit money laundering. According to court documents, both Acevedo and Forero were Colombian citizens residing in Bogota. During 2008 and 2009, Acevedo handled customer accounts at a stock brokerage firm that offered accounts that could be used by customers to receive deposits, wire transfers, and other credit or money, and to disburse the funds through wire transfers and cash or other withdrawals. The stock brokerage firm was authorized to receive funds in U.S. dollars, provided that they were properly documented and justified as being for legitimate business transactions. Forero was one of Acevedo's customers. During the course of his participation in this scheme, Forero received approximately $1.2 million from IRS undercover accounts that he passed on to the people designated to receive it. Acevedo was involved in the transfer of approximately $335,000 from IRS undercover accounts in the United States to the stock brokerage firm in Colombia, and the conversion of the dollars into pesos and the subsequent withdrawal of the monies by Forero. Both Acevedo and Forero knew that the money was derived from criminal activity.

Financial Advisor Sentenced for Stealing Over $1.1 Million from His Clients
On July 15, 2015, in Norfolk, Virginia, Joshua Ray Abernathy, of Chesapeake, was sentenced to 90 months in prison, three years of supervised release and ordered to pay $1,181,755 in restitution to his victims and to forfeit all of the proceeds from his offense. Abernathy pleaded guilty on March 13, 2015 to mail fraud and unlawful money transactions. According to court documents, Abernathy, a licensed broker and financial advisory, engaged in a six-year Ponzi scheme. Abernathy convinced his clients to transfer funds from legitimate IRA accounts to his company "Omega Investment Group." Abernathy claimed that he could invest the funds in "puts" and "calls" and reap fantastic returns. In reality, Abernathy invested only a tiny portion of the money in his personal E*Trade account and used the majority of the monies to fund his extravagant lifestyle including paying for living expenses, home furnishings, restaurants, sporting goods, electronics, clothing and entertainment. Abernathy also spent substantial investor funds for personal travel and vacations as well as using client monies to rent luxury automobiles. After spending all of the client funds and with investors asking questions, Abernathy walked in to the FBI and confessed to running the Ponzi scheme.

Michigan Doctor Sentenced for Providing Medically Unnecessary Chemotherapy to Patients
On July 10, 2015, in Detroit, Michigan, Farid Fata, M.D., of Oakland Township, was sentenced to 540 months in prison and ordered to forfeit $17.6 million. Fata, a Detroit area hematologist-oncologist, pleaded guilty in September 2014 to 13 counts of health care fraud, one count of conspiracy to pay or receive kickbacks and two counts of money laundering. According to court documents, Fata was a licensed medical doctor who owned and operated a cancer treatment clinic, Michigan Hematology Oncology P.C. (MHO), which had various locations in Michigan. He also owned a diagnostic testing facility, United Diagnostics PLLC, located in Rochester Hills, Michigan. Fata prescribed and administered unnecessary aggressive chemotherapy, cancer treatments, intravenous iron and other infusion therapies to 553 individual patients in order to increase his billings to Medicare and other insurance companies. Fata then submitted approximately $34 million in fraudulent claims to Medicare and other insurers for these unnecessary treatments. Furthermore, Fata used the proceeds of the health care fraud at his medical practice, MHO, to promote the carrying on of additional health care fraud at United Diagnostics, where he administered unnecessary and expensive positron emission tomography (PET) scans for which he billed a private insurer.

Pennsylvania Man Sentenced for Violating Federal Drug, Gun and Money Laundering Laws
On July 7, 2015, in Pittsburgh, Pennsylvania, Omali P. McKay, a citizen of Trinidad who formerly resided in Lower Burrell and in Arnold, was sentenced to 180 months in prison, five years of supervised release and ordered to forfeit vehicles, a residence and $272,000 in cash. McKay was previously convicted of violating federal narcotics, firearms and money laundering laws. According to court documents, McKay conspired with others from 2006 to Aug. 25, 2012, to distribute five to 15 kilograms of cocaine and 280 to 840 grams of crack cocaine. Also, McKay admitted possessing with intent to distribute one kilogram of cocaine seized from his Lower Burrell residence on Aug. 25, 2012, while simultaneously possessing an assault rifle in furtherance of the drug crime. Finally, McKay admitted to conspiring with three others to launder his drug trafficking proceeds. He used those laundered funds to purchase the Lower Burrell residence for $243,000 in cash in August 2011.

New York Man Sentenced for Money Laundering Conspiracy
On July 3, 2015, in Albany, New York, Michael Elcox, of Ghent, was sentenced to 37 months in prison and three years of supervised release. Elcox pleaded guilty in March 2015 for his role in a conspiracy to launder the proceeds of an illegal marijuana distribution network. The conspiracy involved routing illegal proceeds through various bank accounts and moving cash from New York to Florida. Federal agents seized more than $300,000 in cash, representing the proceeds of Elcox's illegal marijuana distribution, from locations in New York and Florida.

Minnesota Man Sentenced for Defrauding Investors
On June 26, 2015, in Minneapolis, Minnesota, Sean Meadows, of Eden Prairie, was sentenced to 300 months in prison and three years of supervised release for using his financial planning and asset management firm, Meadows Financial Group (MFG), to operate a long-term Ponzi scheme. Meadows pleaded guilty on Dec. 11, 2014 to wire fraud, mail fraud, and transaction involving fraud proceeds. According to the plea and documents filed in court, Meadows operated MFG, through which he sold insurance and investment products to clients in Minnesota, Indiana,

Arizona, and elsewhere. From 2007 until April 2014, Meadows successfully solicited a total of at least $13 million from more than 100 clients for a purported investment managed by MFG. The defendant falsely told victims that he would use their funds to purchase bonds, real estate, or other legitimate third-party investments. Meadows lured victims into removing funds from their retirement and other savings accounts by promising high rates of returns – up to 10 percent annually – when, in fact, he did not invest their funds and did not have a legitimate means by which to make interest payments. Instead, Meadows used funds from new investors to make interest and/or principal repayments to existing investors and to pay personal expenses. Among the victims Meadows defrauded are senior citizens and the disabled, poor or terminally ill. Victims were left in financial ruin because they lost their financial security, retirement funds, their ability to support their families, and in some cases, their ability to pay for cancer treatments.

Former Senior Executive of Qualcomm Sentenced for Insider Trading and Money Laundering
On June 26, 2015, in San Diego, California, Jing Wang, of Del Mar, California, was sentenced to 18 months in prison and fined $500,000 for his role in a three-year insider trading scheme. Wang, former Executive Vice President and President of Global Business Operations for Qualcomm Inc., pleaded guilty in July 2014 to insider trading, money laundering and obstruction of justice. In connection with his plea, Wang made three, separate insider trades using a brokerage account in the name of his British Virgin Island (BVI) shell company, Unicorn Global Enterprises. First, in early 2010, prior to Qualcomm's announcement of a dividend increase and stock repurchase, Wang bought company stock valued at approximately $277,000. Then in December 2010, while attending Qualcomm's Board of Directors meeting in Hong Kong, and hours after the Board approved a non-public offer to purchase Atheros, Wang purchased stock in Atheros. A few weeks later, he directed his stockbroker, Gary Yin, to sell the Atheros stock, for approximately $481,000, and purchase Qualcomm stock one day before the company announced record earnings. Wang transferred the illegal proceeds from Unicorn's account to an account of a new BVI shell company he controlled. He obstructed justice by creating a false cover story in which he and Yin would blame Wang's brother Bing Wang, who resides in rural China, for the insider trading and ownership of the Unicorn Account. Yin pleaded guilty to conspiring to obstruct justice and launder money, and is scheduled to be sentenced at a later date. Bing Wang has been charged in connection with the scheme, and is wanted on an international arrest warrant.

North Carolina Land Developer Sentenced in $23 Million Bank Loan Scheme
On June 25, 2015, in Asheville, North Carolina, Keith Vinson, of Arden, was sentenced to 216 months in prison for his role in a scheme involving the failed land development deal of Seven Falls, a golf course and luxury residential community in Henderson County, North Carolina. Vinson was also ordered to serve three years of supervised release and to pay $18,384,584 in restitution in the amount of. A federal jury convicted Vinson in October 2013 of conspiracy, bank fraud, wire fraud, and money laundering conspiracy. According to court documents, beginning in 2008, Vinson and his co-defendants conspired and obtained money from several banks through a series of straw borrower transactions in order to funnel monies to Vinson and his failing development of Seven Falls. In order to advance this scheme Vinson and his co-conspirators, including Avery Ted "Buck" Cashion III, Raymond M. "Ray" Chapman, and others, recruited local bank officials including George Gordon "Buddy" Greenwood and Ted Durham, who at the time were presidents of two different banks. When bank officials realized

that they had reached their legal lending limits with respect to some of the straw borrowers, additional straw borrowers were recruited to the scheme and more straw borrower loans were made to them. Additional straw borrower loans were also necessary to keep loans current, a scheme known as "loan kiting." The loan kiting scheme became necessary when conspirators were unable to make payments on loans made early in the scheme. Seven Falls and another luxury residential golf development by Vinson named "Queens Gap" failed, resulting in millions in property losses. In addition, both banks failed and were taken over by the FDIC. Vinson's co-conspirators were previously sentenced for their roles in the scheme.

Maryland Man Sentenced for Stealing from a Charity

On June 19, 2015, in Baltimore, Maryland, William Peters, of Glen Burnie, was sentenced to 18 months in prison, three years of supervised release and ordered to forfeit and pay restitution of $4 million. Peters previously pleaded guilty to conspiring to commit mail and wire fraud and conspiring to commit money laundering. According to his plea, Peters was a board member of a charity that provided financial support to Native American communities and individuals. Peters and co-conspirator Brian J. Brown, the former president of the charity, falsely represented that if the charity funded Charity One, Inc., a nonprofit corporation Brown created and controlled, Charity One would use the funds for scholarships for American Indians. Peters used his board membership position to cause the charity to execute a series of endowment agreements in which the charity agreed to fund Charity One with $1 million per year for five years. However, Peters and Brown distributed the proceeds of their fraud scheme to themselves. Peters created and controlled a corporation called August First, Inc., which he used to receive and distribute to himself $950,244 of the fraud proceeds. Brown created and controlled a corporation called Aria Inc. to receive and distribute to himself $3,011,751 of the proceeds. Peters and Brown falsely characterized the funds as consulting fees on their federal income tax returns filed for 2006 to 2009 in order to conceal the source of these funds. Peters has agreed that the actual loss to the charity is $4 million. Brian Brown, of Beaverton, Oregon, was sentenced in Oregon on May 7, 2015 to 37 months in prison.

Colorado Man Sentenced to Prison for Investment Fraud Scheme

On June 18, 2015, in Denver, Colorado, Gary Snisky, of Longmont, Colorado was sentenced to 84 months in prison, three years supervised release and ordered to pay $2,531,032 in restitution to the victims. Snisky pleaded guilty on Jan. 5, 2015 to mail fraud and money laundering charges. Snisky's co-conspirator, Richard Greeott, was previously sentenced to six months in prison for his significantly smaller role in the scheme. According to court documents, from 2009 through 2011, Snisky operated Colony Capital in Colorado, which purported to be a private equity firm offering investment opportunities in bonds, futures trading, and other offerings. In 2011, Snisky shut down Colony Capital and formed Arete, which operated in a similar manner. As part of his scheme, Snisky repeatedly falsely told financial advisors and investors that he was an "institutional trader" who was "on Bloomberg," which Snisky claimed made him part of an elite group of people who could "make markets" and who had access to lucrative opportunities to which ordinary investors did not have access. From July 2011 through January 2013, Snisky offered investors a "proprietary value model" which was based on using the investors' money to purchase Ginnie Mae bonds. Throughout 2012, Snisky continued to make false assurances about the safety of investing in the Bond Program despite the fact that Snisky knew that he had not purchased any Ginnie Mae bonds as promised. Snisky sent fabricated account statements to

investors that falsely reflected that their money had been invested in the bonds as promised. Additionally, in 2010, Snisky asked Greeott to develop an algorithm to support a fully-automated trading system for trading in the futures market. The algorithm was never implemented however, Snisky falsely led investors, potential investors, and financial advisors to believe the algorithm was being used, to profitably trade in the futures market. Based on these false representations, several victims invested money in Snisky's futures trading program. The net loss Snisky caused to investors in the bond and futures trading programs was $5,226,965.

Salesman Sentenced for Role in Bribes-For-Test-Referrals Scheme Involving New Jersey Clinical Lab

On June 17, 2015, in Newark, New Jersey, Len Rubinstein, of Holmdel, was sentenced to 37 months in prison, one year of supervised release and ordered to forfeit $250,000 and pay a $10,000 fine. Rubinstein previously pleaded guilty to one count of conspiracy to commit bribery and one count of money laundering for his role in a long-running and elaborate scheme operated by Biodiagnostic Laboratory Services LLC (BLS), of Parsippany, New Jersey, its president and numerous Associates. According to court documents, from May 2012 through April 2013, Rubinstein agreed with BLS president David Nicoll, of Mountain Lakes, his brother, Scott Nicoll, of Wayne, and others to pay doctors to refer patients to BLS for testing of blood specimens. Rubinstein paid cash bribes to doctors as part of the conspiracy. Rubinstein admitted he used Delta Consulting Group LLC – an entity he controlled – to hide the money he received from BLS and used to make bribe payments to doctors.

California Man Sentenced for Defrauding Investors Out of Almost $1 Million

On June 16, 2015, in Portland, Oregon, Bryan Scott Gunn, of Victorville, California, was sentenced to 20 months in prison, three years of supervised release and ordered to pay $939,308 in restitution. According to court documents, Gunn executed schemes conning investors out of almost $1 million. For the first scam, Gunn convinced his victims to invest more than $500,000 in an alleged heavy equipment leasing company, Republic Funding LLC, promising a high rate-of-return. During the scheme, Gunn showed the investors documentation that falsely showed the alleged company was profitable. Gunn diverted the investors' money for his personal use. When the investors began to seek a return on their investment and began to challenge Gunn's claims about the alleged business, he started his second swindle. Gunn created two fictitious companies, a few fictitious employees, and a fictitious attorney, including corresponding email accounts, to conceal his fraud. Gunn told the investors that he had sold the equipment leasing business' portfolio to one of his fictitious companies, CMC Funding. When the investors sought payment from the sale of the portfolio, Gunn explained that CMC Funding had filed for bankruptcy and that its assets, including the portfolio, were being purchased by Fidelity LLC, Gunn's other fictitious entity. Gunn, using letters and emails, posed as employees of Fidelity and as an attorney, and falsely claimed that costs associated with the bankruptcy needed to be paid before the investors could receive any payment for the alleged purchase of the portfolio. The investors paid more than $411,000 in an attempt to recover some of their investment. Gunn continued to use their money to live lavishly. At one point, in an attempt to appease the investors, Gunn created and gave two bogus checks to the investors as a payout. The checks, one for $314,113 and the other for $1,169,887, appeared to be issued from CMC Funding and to be drawn on an account at a Federal Credit Union. After depositing the checks, the investors quickly learned that the checks were fraudulent and that the account at the Federal Credit Union did not exist.

Day Trader Sentenced for Investment Fraud Scheme

On June 16, 2015, in Pocatello, Idaho, Michael Justin Hoopes, of Rexburg, Idaho, was sentenced to 24 months in prison, three years of supervised release, and ordered to pay $620,000 in restitution. Hoopes pleaded guilty on Feb. 24, 2015 to wire fraud and monetary transactions in property derived from specified unlawful activity. According to the plea agreement, from 2007 through February 2011, Hoopes engaged in a scheme to defraud investors in various investment opportunities he offered. Specifically, Hoopes solicited investors to provide him with capital he represented would be use in his commodities futures day trading activities and to invest in Connected Lyfe, a publicly traded company. Hoopes misrepresented to investors that he earned returns in excess of 20 to 25 percent, that he would invest all of the capital they provided in day trading and pay them from the profits generated by their investments, and he would receive personal compensation only from profits he made above the 20 to 25 percent return. Hoopes provided false monthly account statements to investors documenting the purported positive returns. In reality, he used much of the capital he received for personal expenses and paying "positive" returns to existing investors primarily from the capital raised from new investors. Hoopes received in excess of $9 million from investors and misappropriated approximately $620,000 for his own personal use. Contrary to monthly account statements showing positive returns, he lost most of the remainder day trading and in other failed investments. Hoopes was also ordered to forfeit shares of Connected Lyfe in his possession.

Former Executive Director of Choctaw Nation Sentenced for Theft, Money Laundering and Tax Fraud

On June 1, 2015, in Muskogee, Oklahoma, Jason Brent Merida, of Fort Towson, Oklahoma, was sentenced to 144 months in prison, two years of supervised release and ordered to pay $545,000 in restitution to the Choctaw Nation of Oklahoma and $32,149 in restitution to the IRS. Merida was convicted by jury trial on Nov. 20, 2014 for conspiracy to commit theft or bribery of programs receiving federal funds, theft by an employee or officer of a tribal government receiving federal funds, conspiracy to commit money laundering and tax fraud. According to court documents, Merida, the former Executive Director of Construction for the Choctaw Nation of Oklahoma, conspired to corruptly demand, solicit and receive cash, trips, a Cadillac Escalade, cattle guards, and other things of value in excess of the $5,000 from subcontractors performing work on Choctaw Nation construction projects. Merida, in concert with others, submitted and approved false invoices from subcontractors allowing him to steal, embezzle and fraudulently convert in excess of $500,000 in funds from the Choctaw Nation of Oklahoma which were used to purchase items for Merida and others. Merida also willfully failed to report the proceeds of the fraud on his federal income taxes in 2009 and 2010. Merida was the eighth person to date to be convicted as part of this investigation and prosecution. Seven additional defendants have been sentenced to terms ranging from 60 months in prison to 3 years' probation.

Creator and Operator of the "Silk Road" Website Sentenced

On May 29, 2015, in Manhattan, New York, Ross Ulbricht, aka "Dread Pirate Roberts," of San Francisco, California, was sentenced to life in prison and ordered to forfeit $183,961,921. On Feb. 5, 2015, Ulbricht was found guilty of distributing narcotics, distributing narcotics by means of the Internet, conspiring to distribute narcotics, engaging in a continuing criminal enterprise, conspiring to commit computer hacking, conspiring to traffic in false identity documents, and

conspiring to commit money laundering. According to court documents, Ulbricht created Silk Road in January 2011, and owned and operated the underground website until it was shut down by law enforcement authorities in October 2013. Silk Road served as a sophisticated and extensive criminal marketplace on the Internet where unlawful goods and services, including illegal drugs of virtually all varieties, were bought and sold regularly by the site's users. While in operation, Silk Road was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to more than 100,000 buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions. Ulbricht sought to anonymize transactions on Silk Road by operating Silk Road on a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the networks' users. Ulbricht also designed Silk Road to include a Bitcoin-based payment system that concealed the identities and locations of the users transmitting and receiving funds through the site.

Car Dealer Sentenced for Money Laundering
On May 27, 2015, in Buffalo, New York, Jerry Robbins, of Cheektowaga, was sentenced to 63 months in prison. Robbins was previously convicted of money laundering and failure to report cash transactions of $10,000 or more. According to court documents, Robbins, owner of Finish Line Auto, in Buffalo, helped drug dealers launder proceeds of their illicit business by purchasing high end used cars. During these sales, the drug dealers would pay Robbins cash for cars ranging in price from $10,500 to $45,000. Robbins used the name of another person in sales and title paperwork to disguise the true purchaser and source of the money. In an effort to conceal the amount of money received for the sale of the car, Robbins listed that only a small deposit was received from the third party nominee, when in fact, the drug dealers had paid cash in full for the car. For each of these types of transactions, Robbins also failed to file the required forms with the Internal Revenue Service indicating the receipt of over $10,000 cash for the sale of the car.

Louisiana Man Sentenced for Money Laundering
On May 20, 2015, in New Orleans, Louisiana, Richard Zanco, of Slidell, Louisiana, was sentenced to 30 months in prison and three years of supervised release. Zanco previously pleaded guilty to money laundering. According to court documents, about May 2012, Zanco learned that someone had opened a brokerage account in his name and used that account to acquire collateralized mortgage obligations (CMOs), a type of bond, by fraudulent means. Even though he knew that the CMOs did not belong to him, Zanco gained control of the accounts and arranged for the interest proceeds of the CMOs to be diverted to other financial accounts under his control. Between March 11, 2013 and Sept. 19, 2013, Zanco illegally used the funds, in the amount of about $343,998 to engage in a variety of financial transactions, including the purchase of multiple automobiles and one or more boats.

Man Sentenced for Swindling Millions from Persons in Golf Course Scheme
On May 18, 2015, in Reno, Nevada, Scott H. Summerhays, formerly of the South Lake Tahoe, was sentenced to 234 months in prison, three years of supervised release and ordered to pay $1.4 million in restitution. Summerhays pleaded guilty in February 2014 to 14 counts of wire fraud, seven counts of money laundering, two counts of identity theft, and one count of aggravated

identity theft. According to the court records, during 2008 to 2010, Summerhays represented to potential investors that he was purchasing the Genoa Lakes Golf Club located west of Gardnerville, Nev. for $17 million and needed a short term loan to complete the deal because his own money was tied up in a trust. Summerhays also represented to the potential investors that he solicited funds for oil and gas investments in Texas and owned over $30 million in Berkshire, Las Vegas Sands and MGM stocks. Summerhays showed some of the investors a fraudulent investment account statement. Summerhays also claimed that he was in partnership with Las Vegas Sands owner Sheldon Aldelson, and showed potential investors a partnership agreement containing the forged signature of Adelson. In reality, Summerhays had no investment portfolio, and Adelson had no any partnerships with him. Using this scheme, Summerhays was able to convince 11 persons to loan him money for the golf course, totaling approximately $3.6 million. None of the investors were repaid and they lost all of the money they loaned Summerhays.

Final Defendant Sentenced in Decade Long Psychic Swindle Case
On April 30, 2015, in Portland, Oregon, Blancey Lee, of Portland, was sentenced to 24 months in prison, three years of supervised release, and ordered to pay $2,599,809 in restitution to the victim, for his role in a conspiracy to commit money laundering and his filing of false personal income taxes for 2012. Co-defendants, Rachel Lee, of Canby, Oregon was previously sentenced to 100 months in prison and ordered to pay $15,490,978 in restitution. Porsha Lee, of Northern California, was previously sentenced to 33 months in prison and ordered to pay $12,822,262 in restitution. According to court records, the victim met Rachel Lee in 2004 when he visited her Psychic Shop. At the time, Blancey Lee and Rachel Lee lived together as a couple at the Psychic Shop and presented themselves as husband and wife. Between 2004 and 2006, Rachel Lee fostered a friendship with the victim for the purpose of extracting money from him. As a result of her lies and the trust she established with the victim, Rachel Lee assumed a role as paid care giver to the victim's elderly father by 2007. Trusting her to act in his best interest, the victim also turned over all personal and business account control to Rachel Lee. While controlling the victim's finances, Rachel Lee, Blancey Lee, and their families lived in a million-dollar home in the Portland West Hills purchased with the victim's money. Rachel Lee recruited members of her family to play key roles in the fraud scheme. Between 2007 and 2011 Rachel Lee directed the victim to incrementally liquidate investments accounts totaling approximately $3.8 million dollars. After depleting the victim's investment account, Rachel Lee convinced the victim he owed substantial taxes and needed to sell his family's Tree Farm. At Rachel Lee's direction, the Tree Farm properties were sold for a total of approximately $12.3 million dollars. Rachel Lee, Blancey Lee, and Lee family members spent the victim's fortune on a luxury lifestyle. By the time of Rachel Lee's arrest and indictment in May 2014, the victim held less than $250,000 in accounts under his control. Through the initiation of forfeiture proceedings, a Bentley, Ferrari, Bel-Air, and 10 real properties have already been returned to the victim, and efforts are underway to restore to the victim the $1.9 million in cash seized and forfeited from bank accounts. The government is initiating civil forfeiture proceedings to liquidate numerous Rolexes and other designer goods purchased by the defendants and will provide those proceeds to the victim.

Former Foundation Chairman and Spouse Sentenced for Embezzling More Than $1.1 Million
On April 28, 2015, in Louisville, Kentucky, Charles Muir was sentenced to 46 months in prison and one year of supervised release. Diana Muir was sentenced to six months in prison and one

year of supervised release. Both previously pleaded guilty to interstate transportation of stolen property and money laundering. According to court documents, Charles Muir was the chairman of the Woodcock Foundation, a charitable organization associated with the Episcopal Church of Louisville, Kentucky. Diana Muir owned and controlled DBM-Dental Direct of Louisville. Between April 2007 and June 2011, the Muirs unlawfully transferred or caused to be transferred approximately $1,141,030 that had been stolen or taken by fraud from the Woodcock Foundation, a charitable trust providing college scholarships. The funds were transferred from a bank in Louisville, Kentucky, to locations outside of Kentucky. In addition, the Muirs conducted financial transactions involving the proceeds of the fraud by depositing checks from the Woodcock Foundation into a DBM Dental bank account to disguise the nature of the transactions. During the four year period, the couple withdrew approximately $262,000 by ATM at a casino in Indiana and in total withdrew more than $365,000 in cash.

North Carolina Man Sentenced for Structuring Financial Transactions
On April 27, 2015, in Raleigh, North Carolina, James Dino Wills, of Wilson, North Carolina, was sentenced to 102 months in prison, three years of supervised release and ordered to forfeit $733,882. Wills also agreed to file amended federal income tax returns for the tax years 2008 through 2013 and to pay any taxes owed. Wills pleaded guilty on May 7, 2014 to structuring financial transactions to evade the filing of currency transaction reports (CTRs). Federal law requires banks and other financial institutions to file CTRs with the U.S. Treasury Department for all cash transactions exceeding $10,000. According to court documents, Wills operated a business in the Rocky Mount and Wilson, North Carolina areas from 2008 to 2013 and received payments for services primarily in the form of checks. These checks were deposited into his business accounts at two financial institutions. Wills then structured cash withdrawals from these accounts in order to avoid the filing of CTRs. From 2008 to 2013, he structured $755,764 in cash transactions. Wills was prosecuted for the same offense in 1998.

Law School Graduate Sentenced for Conspiring to Launder Drug Money
On April 23, 2015, in Kansas City, Kansas, Mendy Read-Forbes, a law school graduate, was sentenced to 240 months in prison. Read-Forbes, of Platte City, Mo., was pleaded guilty to one count of conspiracy. According to court documents, in March 2012, Read-Forbes began meeting with an agent posing as a drug dealer. Read-Forbes, a law school graduate who was not licensed to practice law, operated Forbes & Newhard Credit Solutions, Inc., a nonprofit corporation registered in Missouri to provide educational and social welfare services. The agent told Read-Forbes he had assets to conceal from the sale of marijuana. She said she could use her legal training and her connections with federal attorneys and law enforcement officers to help him launder the money. She told the agent she would launder his cash by running it through her business. The plan also involved her listing the agent as an employee of her business and putting him on her company's board of directors. As part of the scheme, she created a fictitious company called Maximus Lawn Care LLC. Over the course of the investigation, she laundered more than $200,000 in purported drug funds. She also agreed to invest $40,000 of her money with the agent for the purchase of marijuana.

Tennessee Businesswoman Sentenced for Fraud and Money Laundering Violations
On April 20, 2015, in Knoxville, Tennessee, Joyce Allen, of Louisville, Tennessee, was sentenced to 360 months in prison and three years of supervised probation. Allen was ordered to

pay $20,711,371 in restitution as well as a court-ordered forfeiture of the same cash amount. In September 2014, Allen was found guilty by jury trial of charges contained in a superseding indictment against Allen and five other individuals associated with Benchmark Capital, Inc. (Benchmark). According to court documents, the purpose of Benchmark was to defraud investors by taking their funds in exchange for worthless and nonexistent investments, and paying a portion of the funds received to earlier investors under the guise of paying dividends, interest and mortgage payments, thereby encouraging new investors to entrust their funds to Benchmark. Allen was the president of J. Allen and Associates, Inc., based in Louisville. Through her business, Allen induced individuals to pay funds to her in exchange for annuity investments with Benchmark, knowing that these funds would not be placed with Benchmark or any other company for investments, but converted to personal use by Allen and her other co-conspirators. The other five individuals named in the superseding indictment pleaded guilty and have been previously sentenced.

Prominent Businessman for Private Consulting Group Sentenced after Bilking Elderly Victim of $1.1 Million

On March 31, 2015, in Portland, Oregon, Robert L. Keys was sentenced to 70 months in prison, three years of supervised release, and ordered to pay $1.1 million in restitution. Keys pleaded guilty on Sept. 9, 2014 to wire fraud, money laundering, and bankruptcy fraud. At the plea hearing, the government contended that in 2008, as Keys' business ventures were failing, he turned to one of his long-term clients, a widow in her mid-80s, and persuaded her to loan $1.1 million to co-defendant William Kearney, now deceased. Keys lied to his client about the terms of the loan, such as the existence of treasury bonds as collateral for the loan, and he failed to disclose important facts to her in order to fraudulently obtain money for his benefit and that of Kearney. Keys also received over $100,000 in kickbacks as part of the scheme. Those kickbacks were wired to him by Kearney the day after Keys persuaded his client to loan Kearney the $1.1 million. In addition, Keys and his wife filed for bankruptcy in 2010, and Keys fraudulently attempted to discharge $148 million in debt by lying to the Bankruptcy Court, concealing assets and income, and filing false documents with the Court.

Florida Man Sentenced For $100 Million Surety Bond Fraud Scheme

On March 24, 2015, in Atlanta, Georgia, Eric Campbell, of Orange Park, Florida, was sentenced to 57 months in prison, three years of supervised release and ordered to pay $1,904,376 in restitution. Campbell pleaded guilty on Oct. 20, 2014 to operating a multi-million dollar surety bond fraud scheme. According to court documents, from August 2012 until July 2013, Campbell used several corporations to sell fraudulent surety bonds on construction projects. Surety bonds are three party bonding agreements in construction projects where a surety company assures the project owner that a contractor will perform a construction contract. Campbell fraudulently held himself out to contractors and government agencies as having the authority to execute or issue surety bonds on behalf of Federal Insurance Company and Pacific Indemnity Company, affiliates of the Chubb group. To perpetuate the scheme, Campbell created fraudulent surety bonds, embossed the bonds using a counterfeit seal and forged the signatures of Chubb group officials. Campbell and his associates issued bonds with a face value of more than $100 million and received premium payments of more than $2.2 million during the course of the fraud. Many of these funds were then deposited into bank accounts owned and under the control of Campbell. In addition to financial losses, Campbell's fraud scheme caused delays in several construction

projects and compromised the construction bidding process because contracts were sometimes awarded to unqualified construction companies.

Former University Employee Sentenced On Fraud Charges
On March 19, 2015, in Rochester, New York, Debra Bulter, of Penfield, was sentenced to 36 months in prison, three years of supervised release and ordered to pay restitution totaling $4,285,637. Bulter was previously convicted of conspiracy to commit mail fraud and money laundering. According to court documents, Bulter worked as the Program Administrator for the Department of Anesthesiology at the University of Rochester in Rochester (the Department). From 2001 through 2012, CGF Anesthesia Associates, P.C. (CGF), contracted with the Department to provide anesthesiologists at medical facilities served by the Department. From 2007 to 2009, Bulter deceived the Department into making fraudulent payments of $930,000 to two doctors from CGF and $530,000 to CGF. The two doctors each executed fraudulent contracts with the Department worth more than $3,000,000 with the assistance of Bulter. The scheme caused the Department to divert compensation of $2,410,015 actually earned by CGF to the two doctors. For the years 2010 through 2012, CGF was deceived into paying $1,169,606 to Bulter's business, DJA Solutions, LLC. Bulter also caused the Department to make a fraudulent and unauthorized loan to a doctor working for the Department. Bulter disguised various payments to the doctor as extra compensation resulting in total fraudulent payments to the doctor of $510,726. From October 2012 to May 2012, Bulter also caused the Department to pay a former employee $7,168. Doron Feldman, of Williamsville, New York, one of the two doctors with CGF, was sentenced to 24 months in prison and ordered to pay $1,617,000 in restitution.

Maine Man Sentenced for Drug Trafficking and Money Laundering
On March 18, 2015, in Portland, Maine, David Jones, of Portland, was sentenced to 110 months in prison and three years of supervised release for distributing marijuana and money laundering. According to court documents, from August 2011 through October 2013, Jones obtained hundreds of pounds of marijuana from an out-of-state source and distributed it in Maine. In October 2013, agents seized $291,981 from a storage unit Jones rented, $92,104 from an associate's apartment and $6,278 from Jones' residence. Agents also seized two boats, a truck, several motorcycles, two trailers, numerous pieces of electronic recording equipment and jewelry. All the seized cash and items were forfeited. Jones also laundered $216,500 of his drug proceeds through other financial transactions.

Ohio Couple Sentenced for $2.3 Million Student Loan Fraud
On March 11, 2015, in Cleveland, Ohio, John "Richard" Ceroni, of Canton, was sentenced to 69 months in prison and Adale "Marie" Cernoni was sentenced to 55 months in prison. They were ordered to pay more than $2.3 million in restitution. The Ceronis previously pleaded guilty to conspiracy to commit mail fraud and conspiracy to launder money. Richard Ceroni also pleaded guilty to obstruction. According to court documents, the Ceronis were co-founders of Carnegie Career College. From at least 2003, Carnegie College held itself out to the public as a private not-for-profit college. From June 2007 through May 2012, the Ceronis fraudulently obtained approximately $2.3 million from the Department of Education by submitting applications for SFA funds that stated students at Carnegie College had obtained valid high school diplomas. They also falsely told prospective students they would earn a valid high school diploma at the same time they attended Carnegie College and that such a diploma would be paid for by a

"scholarship from a church" in order to increase enrollment and access to SFA funds. The Ceronis recruited students who had not earned high school diplomas or G.E.D. certificates, and thus were not eligible for SFA funds. The couple also submitted fraudulent financial aid documents to the Department of Education. They used online high schools, including Australia-based Adison High School, to purchase fake high school diplomas and coursework transcripts for students who were not required to attend any classes or complete any coursework. The Ceronis comingled fraudulently obtained money in several accounts and used that money to fund personal expenditures and expand Carnegie College.

Two Men Sentenced for Roles in Cross-Country Marijuana Distribution Ring
On March 9, 2015, in Phoenix, Arizona, two defendants were sentenced for their roles in a cross-country marijuana distribution ring. Darius Blackwell, of Mesa, Ariz., was sentenced to 110 months in prison and Grady Blackwell, of Lithonia, Ga., was sentenced to 60 months in prison. Both defendants previously pleaded guilty to conspiracy to possess marijuana with intent to distribute and conspiracy to commit money laundering. According to their plea agreements, the Blackwells participated in a conspiracy to distribute marijuana using the United States Postal Service. Their organization purchased marijuana in Arizona, mailed it throughout the United States, primarily to Georgia, and then arranged for the proceeds to be sent back to Arizona. Shipping records and seizures show that at least 50 kilograms of marijuana were mailed in this fashion. In addition, seven bank accounts were opened in March 2012 for the purpose of receiving and transferring the proceeds of the scheme. Nearly $410,000 was deposited into these accounts and over $395,000 was withdrawn.

Suspended Attorney Sentenced for Using Law Firm to Launder Drug Money
On March 9, 2015, in Minneapolis, Minnesota, Robert David Boedigheimer was sentenced to 60 months in prison and three years of supervised release. Boedigheimer was convicted by jury on June 17, 2014, of using his law firm to launder drug money, lying to investigators, and encouraging his brother-in-law to lie to federal investigators. As proven at trial, Boedigheimer had his own personal injury practice since 1995. The law firm and Boedigheimer began to experience financial problems in 2006. As proven at trial, Boedigheimer's brother-in-law, Brandon Lusk, was a distributor of high-end marijuana in and around Rochester, Minn. Boedigheimer approached Lusk for a cash loan. Lusk agreed to provide many loans to Boedigheimer, on the condition that the Boedigheimer repay the loans, plus interest, in checks issued from his law firm. Ultimately, Boedigheimer created a "no-show" job for Lusk at the law firm, which paid Lusk $48,000 per year. Lusk's no-show job was entirely paid for through drug proceeds that Lusk funneled to Boedigheimer, and which were laundered through the law firm. Between March 26, 2010 and Jan. 28, 2011, nine payroll cash advances were provided by Lusk, ranging from $5,000 to $10,000 each, and totaling approximately $55,000. In exchange, Lusk received payroll checks from the law firm. In March 2011, Lusk lost his source of income as a marijuana distributor when his supplier was under investigation. Lusk and a marijuana distribution associate approached the Boedigheimer for help in obtaining legal representation. Lusk was eventually interviewed by the US Attorney's office, before which Boedigheimer advised Lusk not to tell investigators about the money laundering arrangement between the two of them. Lusk then withheld information from investigators about his employment and the disposition of the drug proceeds. Lusk was sentenced to 30 months in prison for distribution of marijuana and money laundering.

Sham Church Director and Professed "Enforcer" Sentenced for Looting Church
On March 6, 2015, in Boston, Massachusetts, Edward J. MacKenzie, Jr., of Weymouth, was sentenced to 144 months in prison, three years of supervised release, and ordered to pay $754,569 in restitution. In October 2014, MacKenzie pleaded guilty to 13 counts, including RICO conspiracy, racketeering, mail fraud, wire fraud and money laundering in connection with his decade-long scheme to siphon off considerable financial assets of a church located in the Beacon Hill area of Boston. According to court documents, in 2003, MacKenzie became the "Director of Operations" at the church, a position that had not previously existed and paid him a salary as high as $200,000 per year. In order to drain the church of its assets, he began voting himself and his associates into positions of authority within the church, and consolidated and fortified his control by, among other things, changing the church's by-laws for his own benefit. MacKenzie was able to gain control over substantial church assets, including an 18-story apartment building in downtown Boston, because the church had a small number of voting members, many of whom were elderly. After obtaining control, MacKenzie stole church funds through a combination of fraud, deceit, theft, and bribery. Moreover, MacKenzie intimidated and threatened individuals who were employed by the church by, among other things, providing them with signed copies of his 2003 autobiography, Street Soldier: My Life as an Enforcer for Whitey Bulger and the Boston Irish Mob. In the autobiography, MacKenzie admitted to a lengthy criminal history, including burglary, robbery, armed assault, and narcotics trafficking. MacKenzie's crimes cost the church millions of dollars and deprived the needy who relied on its charity.

Arizona Man Sentenced on Drug and Money Laundering Charges
On Feb. 10, 2015, in Phoenix, Arizona, Carlos Antonio Garcia-Hurtado was sentenced to 168 months in prison and five years of supervised release. Garcia-Hurtado pleaded guilty on Oct. 6, 2014 to conspiracy to possess with intent to distribute marijuana and conspiracy to launder monetary instruments. According to the plea agreement, around June 2010 to on or about Dec. 10, 2013, Garcia-Hurtado was in agreement with others to receive and distribute marijuana from Mexico. The marijuana was brought from Mexico through the desert into Arizona by backpackers and then Garcia-Hurtado coordinated the distribution of bulk quantities of marijuana within the United States and the return of the drug proceeds to Mexico. Garcia-Hurtado also admitted to paying for a property, which is titled in his wife's name, with the proceeds from the drug trafficking and money laundering conspiracies.

Texas Men Sentenced in Drug Distribution Conspiracy
On Feb. 9, 2015, in Wichita Falls, Texas, Rodolfo Trevino, of Wichita Falls, was sentenced to 97 months in prison. In June 2014, Trevino pleaded guilty to one count of conspiracy to possess with the intent to distribute cocaine base and one count of money laundering. Trevino was also ordered to forfeit a residence, two vehicles, a firearm and assorted ammunition. In mid-December 2014, co-defendant Rene Villastrigo, Jr., also of Wichita Falls, was sentenced to 30 months in prison. He pleaded guilty to one count of conspiracy to possess with the intent to distribute cocaine. According to court documents, beginning in 2012 and continuing to April 18, 2014, Trevino and Villastrigo conspired with others to possess with the intent to distribute cocaine and cocaine base. Trevino traveled frequently to McAllen, where he recruited another individual to transport drugs from McAllen to Wichita Falls. Trevino also recruited Villastrigo to

rent a residence in Wichita Falls to store and repackage the drugs for distribution. Trevino deposited the drug proceeds he acquired into bank accounts in Wichita Falls and withdrew those deposits in the McAllen area, intending for these financial transactions to conceal his drug trafficking activity.

Former Pharmacist Sentenced for Role in Drug Distribution Scheme and Money Laundering
On Feb. 5, 2015, in Detroit, Michigan, Waleed Yaghmour, a Dearborn pharmacist, was sentenced to 72 months in prison and ordered to forfeit $973,177 for conspiracy to illegally distribute prescription pills and money laundering. In March 2013, Waleed Yaghmour was charged with 43 others in a health care fraud and drug distribution scheme. According to court documents, Sardar Ashrafkhan and others, who owned home health agencies, provided kickbacks, bribes and other illegal benefits to physicians in exchange for prescriptions for patients with Medicare, Medicaid and private insurance. The prescriptions were for controlled substances such as oxycodone (Oxycontin). Patient recruiters or "marketers" would pay kickbacks and bribes to patients in exchange for the patients' permitting the pharmacies and physicians to bill their insurers for medications and services that were medically unnecessary and/or never provided. During the conspiracy, prescriptions were presented to the Sav-Mart Pharmacy in Detroit, which was owned and operated by Yaghmour, as well as several other pharmacies. Yaghmour knew that the controlled substances he dispensed for these fraudulent prescriptions had no legitimate medical purposes. Yaghmour dispensed at least 1,500 oxycodone 100,000 hydrocodone and 100,000 alprazolam doses as part of the scheme. Yaghmour received nearly $2 million in cash payments for illegally dispensing the controlled substances. Many of the defendants charged in the indictment have been convicted by pleas and have been sentenced already.

South Carolina Man Sentenced for Money Laundering, Drug Trafficking
On Feb. 5, 2015, in Charleston, South Carolina, Hadden Andre Smith was sentenced to 144 months in prison, four years of supervised release and ordered to forfeit over $248,000 that authorities seized from his residence. Smith pleaded guilty on July 31, 2012 to conspiracy to possess with intent to distribute cocaine and marijuana, possession of firearms in furtherance of a drug trafficking crime, and conspiracy to launder money. According to court documents, upon executing a search warrant at Smith's residence, law enforcement officers found approximately $248,000 cash, 1.8 kilograms of marijuana, two firearms and drug packaging paraphernalia. Further investigation revealed that Smith used the drug proceeds to purchase several vehicles and had the vehicle titles put in the name of third parties to disguise the true ownership of the property.

Charity Fundraiser Sentenced for Fraud Against Veterans
On Feb. 3, 2015, in Indianapolis, Indiana, Scott M. Gruber was sentenced to 48 months in prison and three years of supervised release. On Aug. 21, 2014, Gruber pleaded guilty to two counts of mail fraud and one count of structuring to evade reporting requirements. As part of his plea, Gruber agreed to pay $365,750 to a legitimate veterans' charity and forfeit two vehicles. According to court documents, in late 2009, Scott Gruber changed his business, Independent Promotions, Inc., into a professional fundraiser/solicitor business for a specific charity - Purple Hearts Veterans Foundation, a charity owned and operated by his brother. Gruber would solicit funds and deposit the funds into Independent Promotion's account and then convert the cash into

an official check payable to Purple Hearts. Gruber's brother then sent Gruber a Purple Hearts' business check for 80% of the donations transmitted. Between January 2010 through August 2011, Gruber received approximately $437,669 in checks from Purple Hearts as his 80% fundraising fee. Additionally, Gruber retained approximately $116,192 in cash collections that were never forwarded to Purple Hearts. From the total amount of $553,861, Gruber paid 40% of the collections to his solicitors and used another 25% to run his fraudulent business. Gruber's brother did not expend the 20% received in support of veteran's causes but rather made minimal expenses in support of veteran's causes. From Purple Heart's account, less than 8% of the collected proceeds were expended in what might possibly be considered a benefit to a soldier or veteran. Gruber followed the same process to purportedly raise funds for Service Connected Disabled Veterans of America (SCDVA), a charity established in the name of a friend, retaining 85% of the fundraising proceeds. Gruber received approximately $491,791 as his 85% fee from SCDVA. From his 85%, Gruber paid 40% of the collections to his solicitors and used another 25% to run his fraudulent business. From SCDVA's account, $4,500, which represents less than 1% of the collected proceeds, were expended to benefit soldiers or veterans.

Connecticut Man Sentenced for Role in Coast-to-Coast Cocaine Trafficking Ring

On Feb. 3, 2015, in Hartford, Connecticut, Jermaine Jenkins, formerly of Newington, was sentenced to 72 months in prison and four years of supervised release. On Oct. 14, 2014, Jenkins pleaded guilty to conspiracy to distribute and to possess with intent to distribute 500 grams or more of cocaine, and conspiracy to commit money laundering. According to court documents, Jenkins participated in a drug trafficking organization that involved individuals in California using the U.S. Mail and commercial carriers to send large quantities of cocaine to co-conspirators in the Hartford area who sold the narcotics for profit. Joseph Miller of Los Angeles, formerly of East Hartford, sent kilogram parcels of cocaine from California to Jenkins, Luther Nance and their associates in Connecticut. Jenkins, Nance and others then distributed the cocaine, or converted the cocaine into crack for street sale. Certain co-conspirators traveled to California with a large amount of cash to finance the purchase of cocaine. Co-conspirators also made numerous cash deposits into local bank accounts, as well as wire transfers. The cash deposits were made at several branches of the same bank in the Hartford area in amounts of less than $10,000 in order to evade the bank's currency transaction reporting requirements. Miller and Nance have pleaded guilty and await sentencing.

Former Liberty Reserve IT Manager Sentenced for Operating an Unlicensed Money Transmitting Business

On Jan. 30, 2015, in New York, New York, Maxim Chukharev, a citizen of Russia and resident of Costa Rica, was sentenced to 36 months in prison in connection with his work for Liberty Reserve, a company that operated one of the world's most widely used digital currency services. Chukharev pleaded guilty in September 2014 to conspiring to operate an unlicensed money transmitting business. According to court documents, Chukharev was primarily responsible for maintaining Liberty Reserve's technological infrastructure and for implementing systems designed to create the false appearance that Liberty Reserve had an effective anti-money laundering program. Chukharev created and implemented a system designed to hide information about Liberty Reserve's users and the sources of its business from the company's Costa Rican regulatory agency. By design, the system provided mostly "fake" statistics about Liberty Reserve's business to the agency, in order to give the appearance that Liberty Reserve had an

effective anti-money laundering program. Beginning in January 2012, Chukharev took over responsibilities in the day-to-day management of Liberty Reserve's technical operations, including the maintenance and operation of its website. The fact that Liberty Reserve had not registered as a money transmitting business under U.S. law was a vital component of its success as a system used to launder funds derived from, or intended to promote, criminal activity.

First of Two Massachusetts Brothers Sentenced for Oxycodone Trafficking Scheme
On Jan. 22, 2015, in Boston Massachusetts, Joshua M. Gonsalves, of Dennisport, was sentenced to 240 months in prison, five years of supervised release and ordered to forfeit $1,522,372 and property. In October 2014, Gonsalves was convicted of oxycodone conspiracy, money laundering conspiracy and money laundering. According to court documents, Gonsalves and his brother, Stanley D. Gonsalves participated in a three-year conspiracy involving the distribution of hundreds of thousands of 30-milligram oxycodone pills generating over $5 million in proceeds. The conspiracy's couriers transported multi-thousand-pill loads of 30-milligram oxycodone pills from South Florida up to New England, first by plane and later by car. The primary object of the related money laundering conspiracy was to use the millions of dollars in drug proceeds to purchase additional oxycodone pills and to pay the ongoing expenses of the oxycodone conspiracy. Stanley D. Gonsalves, of Sandwich, was convicted of oxycodone trafficking conspiracy, money laundering conspiracy and 17 substantive money laundering charges. Stanley Gonsalves' sentencing has been scheduled.

North Carolina Man Sentenced for Role in Federal Racketeering Conspiracy
On Jan. 20, 2015, in Charlotte, North Carolina, Travis Bumpers, of Charlotte, was sentenced to 66 months in prison and three years of supervised release. Bumpers pleaded guilty in March 2013 to RICO conspiracy to commit securities fraud, bank fraud, wire fraud and money laundering conspiracy. According to court documents, Bumpers engaged in multiple mortgage fraud transactions, arranging for a straw buyer, providing down payment money, and receiving more than $800,000 in kickback money through a sham corporation. Bumpers also engaged in extensive investment fraud, defrauding approximately 70 victims out of more than $4.6 million. Four other defendants have received sentences ranging from an eight month split sentence to 46 months in prison.

Bitcoin Exchanger Sentenced for Selling Nearly $1 Million in Bitcoins for Drug Buys on Silk Road
On Jan. 20, 2015, in Manhattan, New York, Robert M. Faiella, of Fort Myers Beach, Florida, was sentenced to 48 months in prison, three years of supervised release and ordered to forfeit $950,000. Faiella, an underground Bitcoin exchanger, pleaded guilty in September 2014 to operating an unlicensed money transmitting business. According to court documents, from about December 2011 to October 2013, Faiella ran an underground Bitcoin exchange on Silk Road, a website that served as a sprawling and anonymous black market bazaar where illegal drugs of virtually every variety were bought and sold regularly by the site's users. Operating under the username "BTCKing," Faiella sold Bitcoins – the only form of payment accepted on Silk Road – to users seeking to buy illegal drugs on the site. Upon receiving orders for Bitcoins from Silk Road users, he filled the orders through BitInstant, a company based in New York. BitInstant was designed to enable customers to exchange cash for Bitcoins anonymously, that is, without providing any personal identifying information, and charged a fee for its service. Faiella obtained

Bitcoins with BitInstant's assistance, and then sold the Bitcoins to Silk Road users at a markup. With the knowledge and active assistance of Charles Shrem, the Chief Executive Officer of BitInstant, Faiella exchanged nearly $1 million in cash for Bitcoins for the benefit of Silk Road users, so that the users could, in turn, make illegal purchases on Silk Road. Faiella's co-defendant, Shrem, was sentenced to two years in prison on Dec. 19, 2014.

Pennsylvania Man Sentenced for Drug Distribution and Conspiracy to Commit Money Laundering

On Jan. 20, 2015, in Harrisburg, Pennsylvania, Ronald Belciano, of Newtown Square, was sentenced to 63 months in prison and four years supervised release. In February 2014, Belciano pleaded guilty to conspiracy to distribute 100 kilograms of marijuana in and through central Pennsylvania and conspiracy to commit money laundering between December 2007 and November 2011. According to court documents, in 2011 Belciano rented a vehicle and paid a co-conspirator to drive the vehicle, containing $1,184,340 in U.S. currency, from Pennsylvania to California to pay for marijuana, some of which was grown on Belciano's 190 acre property in Northern California. Agents obtained a search warrant for one of Belciano's homes; during the search, agents located $2,582,920 in U.S. currency and 1.5 kilograms of marijuana. Law enforcement agents later located 68 kilograms of marijuana, $316,800 in U.S. currency and 59 paintings valued at over $600,000 in a storage locker and at a co-conspirator's farm which was used to warehouse and distribute the marijuana transported from California to Pennsylvania. The assets seized and forfeited in this case included a residence, a 190-acre property in Laytonville, California, artwork appraised at over $619,000 and $4,084,060 in U.S. currency.

Man Sentenced for Roles in Multi-Million Dollar Fraud Schemes

On Jan. 15, 2015, in Columbus, Ohio, Haider Zafar, formerly of Dublin, Ohio, was sentenced to 72 months in prison, three years of supervised release and ordered to pay $15,723,034 in restitution, of which $2,083,565 is payable to the IRS. Zafar also agreed to a forfeiture money judgment of $10,115,000. Zafar previously pleaded guilty to wire fraud, money laundering, filing a false federal income tax return and failing to file federal income tax returns in connection with a $10.1 million fraud scheme involving false representations about investments in Pakistani real estate. According to court documents, Zafar, told the primary victim of his real estate scheme that his uncle was the Minister of Defence of Pakistan and was responsible for acquiring land on behalf of the Pakistani government. Zafar recruited the victim to be his partner in purchasing such land before the Pakistani government did, saying they would then sell the land to the government at a greatly inflated price. Between January 2008 and February 2010, Zafar prompted his victim to wire $10,115,000 into accounts controlled by Zafar. In another scheme, Zafar pleaded guilty to five counts of wire fraud for fraudulently obtaining $3,524,469 from seven victims associated with the Miami Heat professional basketball franchise. Zafar fraudulently obtained a Miami Heat premium three-season ticket package, which cost $1,055,000, approached several investors and promised various fraudulent investment opportunities. He ultimately obtained in excess of $3,500,000 from his Miami fraud scheme. Finally, Zafar reported a taxable income of zero on his 2007 federal income tax return, omitting $221,500 in taxable income. Zafar also earned more than $10 million from his fraud scheme between 2008 and 2010, but did not file income tax returns.

CPA Hedge Fund Manager Sentenced for Role in $40 Million Ponzi Scheme

On Jan. 15, 2015, in Charlotte, North Carolina, Jonathan D. Davey, of Newark, Ohio, was sentenced to 252 months in prison, three years of supervised release and ordered to pay $21,815,407 in restitution. In February 2013, a federal jury convicted Davey of securities fraud conspiracy, wire fraud conspiracy, money laundering conspiracy and tax evasion. According to court documents and today's sentencing hearing, Davey, a certified public accountant and registered investment advisor, served as the "Administrator" for numerous hedge funds for the Black Diamond Ponzi Scheme, an investment fraud scheme that deprived 400 victims of more than $40 million. Davey collected over $11 million from victims with his own hedge fund, "Divine Circulation Services," by falsely stating that he had done proper due diligence on Black Diamond and that he was operating a legitimate hedge fund with significant safeguards, when, in reality, neither claim was true. As the Black Diamond scheme began to collapse, Davey and his co-conspirators collected over $5 million from new victim investors for the cash account and used this money to make payments to old investors and to themselves. Davey controlled most funds and wires and published a website for victims that reflected fake high returns. By the end of the scheme, the website falsely reflected over $120 million in supposed value for victim-accounts, when in reality the funds were less than $1 million. Davey also used an elaborate network of shell companies to evade taxes and commit money laundering with the proceeds of the Ponzi scheme. Ten other defendants have been sentenced in this case to terms ranging from 40 years to six months in prison. In addition, in April 2011, a criminal bill of information and a Deferred Prosecution Agreement were filed against CommunityONE Bank, N.A., related to its failure to file a suspicious activity report about the Black Diamond scheme and failing maintain an effective anti-money laundering program. The bank agreed to pay $400,000 toward restitution to victims of the Ponzi scheme that operated through accounts maintained at the bank.

Former CEO of Bitcoin Exchange Company Sentenced for Helping to Sell Nearly $1 Million in Bitcoins for Drug Buys on Silk Road

On Dec. 19, 2014, in Manhattan, New York, Charlie Shrem, of New York, was sentenced to 24 months in prison, three years of supervised release and ordered to forfeit $950,000. Shrem pleaded guilty in September 2014 to knowingly transmitting nearly $1 million in Bitcoins intended to facilitate drug trafficking on the "Silk Road" website, a black-market international cyber business, designed to enable users to buy and sell illegal drugs anonymously and beyond the reach of law enforcement. According to court documents, Shrem was the Chief Executive Officer of BitInstant, and from about August 2011 until about July 2013, when BitInstant ceased operating, he was also its Compliance Officer, in charge of ensuring BitInstant's compliance with federal and other anti-money laundering (AML) laws. Shrem was also the Vice Chairman of the Bitcoin Foundation, a foundation dedicated to promoting the Bitcoin virtual currency system. Shrem's co-defendant, Robert M. Faiella, ran the underground Bitcoin exchange on the Silk Road website. Shrem was fully aware that Silk Road was a drug-trafficking website and he also knew that Faiella was operating a Bitcoin exchange service for Silk Road users. Nevertheless, Shrem knowingly allowed Faiella to use BitInstant's services to buy Bitcoins for his Silk Road customers; personally processed Faiella's orders; gave Faiella discounts on his high-volume transactions; failed to file a single suspicious activity report with the United States Treasury Department about Faiella's illicit activity and deliberately helped Faiella circumvent BitInstant's AML restrictions. Faiella, pleaded guilty in September 2014, and his sentencing has been scheduled for a later date.

Colorado Man Sentenced for Role in Mortgage Fraud Scheme
On Dec. 16, 2014, in Denver, Colorado, Peter V. Capra, of Littleton, was sentenced to 144 months in prison, three years of supervised release and ordered to pay over $9 million in restitution. Capra was convicted on March 21, 2014, on fourteen counts of wire fraud, two counts of mail fraud, and ten counts of money laundering. According to court documents and evidence presented at trial, Capra was the President of Golden Design Group, Inc. (GDG), a company which built and sold houses. Capra was also the registered agent for Distinctive Mortgages, LLC, which provided mortgages to some of the customers buying houses from GDG. From January 2005 through July 2008, Capra and others executed a scheme to defraud several mortgage lenders through applications for residential mortgage loans and related documents associated with real estate purchases. Capra structured transactions involving GDG homes to allow buyers to receive substantial amounts of the lenders' money at the time of closing without the knowledge of the lenders. He also sold a large volume of homes to otherwise unwilling or unqualified buyers. Capra netted over $11,000,000 as a result of his scheme. Loan applications for the buyers were submitted through several different mortgage brokers which contained materially false and fraudulent representations about the buyers' income, liabilities, source of down payment, and intent to occupy the properties as their primary residences. At closing, funds ranging from $85,000 to over $200,000 were distributed to the buyers in ways that prevented the lenders from discovering that these funds were actually going to the buyers; these funds were not disclosed in the HUD-1 closing statements or were disguised in those statements.

Virginia Attorney Sentenced for Mail Fraud and Unlawful Monetary Transactions
On Dec. 16, 2014, in Norfolk, Virginia, David R. Flynn, of Norfolk, was sentenced to 71 months in prison, three years of supervised release and ordered to pay $2,296,657 in restitution. Flynn pleaded guilty on April 23, 2014 to mail fraud and unlawful monetary transactions. According to the plea agreement, Flynn, an attorney licensed to practice law in Virginia and owner of Assured Title of Virginia, LLC in Virginia Beach, stole over $2 million from real estate trust accounts in order to cover up problems with his escrow account that dated back to 2008. Flynn also used the stolen funds to pay a personal credit card, to travel to tropical destinations, sometimes paying for friends to join him, and on at least one occasion, to charter a private plane.

Pennsylvania Attorney Sentenced for Defrauding Clients of Over $6 Million
On Dec. 16, 2014, in Harrisburg, Pennsylvania, Wendy Weikal-Beauchat was sentenced to 180 months in prison and ordered to pay $6,365,913 in restitution and $6,341,451 in forfeiture. On Nov. 15, 2014, Weikal-Beauchat pleaded guilty to wire fraud and money laundering in connection with the misuse of her clients' funds. According to court documents, Weikal-Beauchat, who has since been disbarred, was an attorney with the Gettysburg firm of Beauchat and Beauchat, concentrating on estate, trust, and long-term care planning. Beginning in 2007, Weikal-Beauchat diverted approximately $6 million from a trust account she maintained for her clients at a bank. Weikal-Beauchat used the proceeds to operate her law firm, for vacations and other personal expenses. She falsely represented she could invest in certificates of deposit with high interest rates as a result of her "special relationship" with the bank. She generated bogus bank CDs and distributed them to her clients to further mislead them.

Maine Attorney Sentenced for Money Laundering Conspiracy

On Dec. 16, 2014, in Portland, Maine, Gary Prolman, Esq., of Saco, was sentenced to 24 months in prison and two years of supervised release for conspiracy to launder marijuana trafficking proceeds. Prolman pleaded guilty on April 29, 2014. According to court documents, between 2011 and October 2013, David Jones and others illegally distributed hundreds of pounds of marijuana in Maine and elsewhere. Between June and September 2012, Prolman laundered about $177,500 worth of those drug proceeds by: (1) taking cash from Jones to purchase an interest in Prolman's sports agency business; (2) illegally structuring cash deposits and cashier's check purchases to avoid federal currency reporting requirements; and (3) using structured cashier's checks to jointly purchase real estate with Jones in a transaction where only Prolman's name appeared on the deed as the owner.

Real Estate Developer Sentenced for Defrauding His Business Partners

On Dec. 15, 2014, in Santa Ana, California, William Warren Geary, a real estate developer, was sentenced to 18 months in prison and ordered to pay $891,791 in restitution to investors. In September 2014, Geary pleaded guilty to conspiracy to commit mail fraud and money laundering. According to court documents, between August 2009 and April 2010, Geary, along with his bookkeeper, devised a scheme to defraud his business partners in connection with two capital calls he requested for tenant improvements to their joint real estate development. Geary along with nine other limited partners, purchased Ocean Walk Shoppes (OWS), a shopping center in Daytona Beach, Florida. In August 2009, Geary sent a letter to the OWS limited partners seeking $900,000 in capital contributions to complete tenant improvements for two prospective new tenants of OWS. The partners sent Geary $616,791 in response. In October 2009, Geary sent another letter requesting an additional $350,000 for additional tenant improvements. The OWS limited partners sent Geary another $270,000. Instead of using the funds as promised, Geary and his bookkeeper caused almost $900,000 of OWS funds to be used for Geary's personal benefit.

Convicted Ponzi Schemer Sentenced on New Fraud and Money Laundering Charges

On Dec. 15, 2014, in Trenton, New Jersey, Eliyahu Weinstein, of Lakewood, was sentenced to 135 months in prison, 111 months of which will be served concurrently with a previous sentence and 24 months to be served consecutively. His total sentence for the two schemes is 24 years in prison. In addition, Weinstein was ordered to pay $6.2 million restitution and forfeiture. Weinstein previously pleaded guilty to conspiracy to commit wire fraud, committing wire fraud while on pretrial release and money laundering. According to court documents, in February 2012, Weinstein and his fellow conspirators offered a pair of investors (the "Facebook victims") the opportunity to purchase large blocks of Facebook shares prior to the company's initial public offering, or IPO, in May 2012. The Facebook victims wired millions of dollars that the conspirators then misappropriated. Weinstein and his conspirators also persuaded the Facebook victims to invest $2.83 million in the purported purchase of an apartment complex, "Belle Glade Gardens," in Florida. However, Weinstein and his conspirators redirected the money to accounts that they controlled, returned $1.8 million to the Facebook victims as a purported return on investment and used the remaining money for their own purposes. In July 2012, Weinstein approached another group of investor victims (the "Florida condominium victims") and told them he had the opportunity to purchase the notes on seven condominiums in Florida. Weinstein did not use this money to purchase the notes on the Florida condominiums; instead, Weinstein and his conspirators converted the money to their own use. Throughout the scheme, Weinstein

was already under indictment and on pretrial release. Weinstein pleaded guilty on Jan. 3, 2013, admitting he ran a Ponzi-style real estate investment fraud scheme that caused $200 million in losses and then laundered the proceeds of the scheme. Weinstein was previously sentenced on Feb. 25, 2014, to 264 months in prison and ordered to pay more than $200 million in restitution and forfeiture to the victims of his scheme.

Chief Technology Officer of Liberty Reserve Sentenced for Fraud

On Dec. 12, 2014, in Manhattan, New York, Mark Marmilev, of Brooklyn, was sentenced to 60 months in prison, three years of supervised release and fined $250,000. Marmilev pleaded guilty in September 2014 to conspiring to operate an unlicensed money transmitting business that he knew involved the transmission of funds derived from criminal activity. In conjunction with the sentencing, a civil forfeiture complaint was filed seeking the forfeiture of two businesses located in Brooklyn, and the forfeiture of his interest in a pizzeria located in the Coney Island area of Brooklyn. According to the complaint, Marmilev purchased these business interests using more than $1.6 million in Liberty Reserve proceeds. Marmilev was a longtime associate of Liberty Reserve founder Arthur Budovsky and served as Liberty Reserve's chief technology officer. In that role, Marmilev was principally responsible for designing and maintaining Liberty Reserve's technological infrastructure. Liberty Reserve was incorporated in Costa Rica in 2006 and billed itself as the Internet's "largest payment processor and money transfer system." Liberty Reserve was created, structured, and operated to help users conduct illegal transactions anonymously and launder the proceeds of their crimes. It emerged as one of the principal money transfer agents used by cybercriminals around the world to distribute, store, and launder the proceeds of their illegal activity. Marmilev worked for Liberty Reserve for years despite knowing that the business was used extensively to process criminal transactions. Marmilev even promoted Liberty Reserve to criminals on Internet discussion forums, where, using aliases, he touted Liberty Reserve's lack of anti-money laundering policies and its tolerance for, as he put it, "shady businesses." Before being shut down by the U.S. government in May 2013, Liberty Reserve had more than five million user accounts worldwide, including more than 600,000 accounts associated with users in the United States, and processed tens of millions of transactions through its system, totaling more than $16 billion in funds. These funds encompassed suspected proceeds of credit card fraud, identity theft, investment fraud, computer hacking, child pornography, narcotics trafficking, and other crimes.

Ohio Man Sentenced for Role in Cocaine Distribution Ring

On Dec. 11, 2014, in Columbus, Ohio, Stephen A. Cagle was sentenced to 36 months in prison and ordered to forfeit $142,020 in cash and $14,800 in lieu of vehicles seized on his property, as well as at least 13 firearms. Cagle pleaded guilty on May 21, 2014 to conspiracy to distribute a controlled substance and money laundering. According to court documents, on about January 2010 through September 2011, Cagle and others were part of a large scale narcotics organization involved in importing, manufacturing and distributing cocaine. Specifically, Cagle was responsible for distributing multiple kilograms of cocaine. Cagle was also involved in operating an unlicensed money transmitting business, often transporting several hundreds of thousands of dollars from Ohio to Texas. While executing a search warrant at Cagle's residence in September 2011, investigators discovered more than 5 kilograms of cocaine, several firearms, more than $142,000 in cash and several vehicles.

South Dakota Woman Sentenced in Drug and Money Laundering Conspiracies
On Dec. 8, 2014, Sioux Falls, South Dakota, Faith Ashely Rasmussen was sentenced to 80 months in prison and four years of supervised release. Rasmussen pleaded guilty on Sept. 2, 2014, to conspiracy to distribute marijuana and conspiracy to commit money laundering. According to court documents, from approximately January 2012 to December 2013, Rasmussen received marijuana through the mail in South Dakota from her source of supply in California. When the amounts of marijuana became too large to mail, Rasmussen had co-conspirators drive to California and back to South Dakota with large quantities of marijuana. In addition, Rasmussen deposited the proceeds of marijuana sales into her bank account in South Dakota. She also deposited drug sales proceeds into the account of her source of supply, and instructed a co-conspirator to deposit marijuana proceeds into her account. She never deposited more than $10,000 in cash per occasion to intentionally avoid bank reporting requirements.

Defendant Sentenced for Money Laundering Charge Involving Tax Fraud
On Dec. 8, 2014, in Miami, Florida, Price Jules was sentenced to 57 months in prison and three years of supervised release. Jules previously pleaded guilty to one count of money laundering. According to court documents, the IRS uncovered a pattern of approximately 1,285 attempted fraudulent tax claims seeking approximately $5.7 million in refunds. There were approximately $629,942 in cash withdrawals and approximately $34,000 in ATM withdrawals from the bank accounts that Jules controlled. Jules knew that the laundered money was the proceeds of tax fraud because he received approximately $180,000 of tax fraud directly into his personal E-Trade account and approximately $73,000 into his personal bank account. In addition, Jules spoke about engaging in tax fraud and offered to launder the proceeds of tax fraud for a fee. None of the individuals or estates of individuals listed on the tax returns received any money.

New Jersey Man Sentenced for Role in Multi-Million Dollar Real Estate Investment Scheme
On Dec. 8, 2014, in Trenton, New Jersey, Alex Schleider, of Lakewood, was sentenced to 12 months and one day in prison, three years of supervised release and ordered to pay restitution of $613,200 and forfeiture of $363,200. Schleider previously pleaded guilty to wire fraud. According to court documents, Schleider, along with Eliyahu Weinstein, of Lakewood, and others persuaded victims to invest in the purported purchase of an apartment complex, “Belle Glade Gardens,” in Florida. They told the victims that Weinstein could purchase Belle Glade Gardens at a discounted price and immediately flip it at a substantial profit. Schleider and Weinstein further told the victims that Weinstein had already placed $2.5 million in the trust account of a Miami law firm for the transaction; if the victims contributed another $2.5 million toward the transaction, those funds would remain in escrow until the deal closed and the victims would be repaid within 60 days. The victims wired $2.83 million to complete the Belle Glades Gardens transaction, however, Schleider and Weinstein redirected the money to accounts that they controlled, returned $1.8 million to the victims as a purported return on a prior Facebook investment, and used the remaining money for their own purposes.

Wisconsin Businessman Sentenced for Bank Fraud and Theft from Pension Fund
On Dec. 3, 2014, in Madison, Wisconsin, Christian Peterson was sentenced to 84 months in prison and ordered to pay $816,168 in restitution to Greenwoods State Bank. Peterson was convicted by jury trial in May 2014 for bank fraud, money laundering and making false statements to banks. According to evidence given at the trial, between 2006 and 2007, Peterson

committed two acts of bank fraud and made false statements to banks by lying to a bank about the purpose of a wire transfer of funds taken from Maverick, Inc.'s $6.25 million business line of credit to a casino in Las Vegas, and by lying to Greenwoods State Bank in Lake Mills, Wisconsin, about the purpose of a $1.1 million loan for real estate development in Fitchburg. In addition to his convictions for bank fraud, money laundering and making false statements to banks, Peterson was convicted of stealing his former employees' 401(k) account funds and using the money to pay his former wife $7,500 in alimony and to lend himself $10,000.

Former Attorney Sentenced for Money Laundering

On Dec. 3, 2014, in Kansas City, Missouri, James C. Wirken, of Kansas City, was sentenced to 13 months in prison and ordered to pay a $4,000 fine. On May 12, 2014, Wirken pleaded guilty to one count of money laundering. Wirken was a lawyer and principal at The Wirken Law Group until he surrendered his law license in 2012 and was disbarred by the Missouri Supreme Court. According to court documents, Wirken withdrew money from his law firm's trust account, which was being held for the benefit of a client, and deposited the funds into his law firm's operating account. Wirken wrote six checks between December 2009 and Jan. 13, 2010, totaling $116,730 and used the funds for his personal benefit. All of the transactions were conducted without the client's consent. Wirken's law firm was engaged in a long-term, unethical Ponzi-type business model that spanned over many years. As early as 2007, Wirken began improperly borrowing substantial amounts of money from clients, and then he refused to pay his clients back. Wirken borrowed over $800,000 from at least seven clients from 2007 to 2012.

Former Apple Executive Sentenced for Defrauding Apple in Kickback Scheme and Laundering the Proceeds

On Dec. 1, 2014, in San Jose, California, Paul S. Devine was sentenced to 12 months and one day in prison, three years of supervised release and ordered to pay $4,464,664 in restitution. Devine pleaded guilty on Feb. 28, 2011, to wire fraud, conspiracy to commit wire fraud, money laundering and engaging in transactions with criminally-derived property. According to the plea agreement, beginning in approximately February 2007, Devine engaged in a scheme to defraud Apple of money or property as well as to defraud Apple of its right to his honest services. Devine had been a Global Supply Manager at Apple from 2005 until August 2010. Devine's job gave him access to confidential internal Apple information. In the course of the scheme, Devine transmitted confidential information, such as product forecasts, pricing targets, and product specifications, to suppliers and manufacturers of Apple parts. In return, the suppliers and manufacturers paid Devine kickbacks. The scheme enabled the suppliers and manufacturers to, among other things, negotiate more favorable contracts with Apple than they would have been able to obtain without the confidential information. Devine received kickbacks as wire transfers into bank accounts that he opened for that purpose in the U.S. and South Korea, including accounts in the name of a shell corporation, CPK Engineering. Devine knowingly transferred the proceeds of the wire fraud between his various accounts, including CPK Engineering accounts, in order to conceal and disguise the nature, location, source, ownership, and control of the proceeds. Devine agreed to forfeit $951,552 in proceeds of the fraud and a vehicle, all of which were seized by the FBI and IRS at the time of his arrest. Devine also agreed to forfeit $612,407 in proceeds of the fraud, which he transferred from overseas bank accounts and deposited with the clerk of the District Court following his arrest.

Indiana Man Sentenced on Money Laundering Charges
On Nov. 26, 2014, in South Bend, Indiana, Jeffrey Miller, of Osceola, was sentenced to 135 months in prison, two years of supervised release and ordered to pay $1,086,222 in restitution. Miller previously pleaded guilty to the interstate transportation of stolen goods and money laundering. According to court documents, from approximately June 2012 through January 2014, Miller stole copper wire from his former employer, an RV manufacturer located in Elkhart, Indiana. Miller then sold the copper to scrapyards after transporting the copper wire across the state line from Indiana to Michigan locations. He used these illegal funds to gamble at various casinos. Miller deposited cash into his bank account when he won at the casino because then he was able to justify to the bank where the cash came from. He avoided putting money from his sells of stolen copper wire directly into his bank accounts because he did not want to justify the source of the cash. In addition, Miller intentionally made bank deposits of cash below $10,000 to avoid the filing of currency transaction reports.

Ohio Man Sentenced for Investment Fraud
On Nov. 24, 2014, in Cleveland, Ohio, Anthony Davian was sentenced to 57 months in prison and ordered to pay $1,787,679 in restitution, as well as forfeit property. Previously, Davian pleaded guilty to one count of securities fraud, two counts of mail fraud, four counts of wire fraud, and seven counts of money laundering. According to court documents, Davian used his hedge fund, Davian Capital Advisers, LLC, to promote and sell securities to at least 20 investors between 2008 and 2013, resulting in $1.8 million in overall investor loss. Davian purported to sell securities in the form of shares in the various funds he created and controlled, including Davian Capital, Rubber City Gravity, Rubber City Pure Alpha, Cleveland Precious Metals Fund, and others. Instead, he used the investors' monies to pay earlier investors, enrich himself and pay off personal expenses. Davian persuaded investors' into giving him hundreds of thousands of dollars by claiming to manage hundreds of millions of dollars to make himself appear more sophisticated than he really was and by falsifying client account statements.

Former Bank CEO Sentenced for Bank Fraud and Money Laundering
On Nov. 24, 2014, in Wilmington, Delaware, James A. Ladio, was sentenced to 24 months in prison and ordered to pay restitution of $700,000. Ladio pleaded guilty on Dec. 17, 2013, to two counts of bank fraud and two counts of money laundering. According to court documents, Ladio was the founder and former CEO of Midcoast Community Bank, Inc. ("Midcoast"). On two occasions, Ladio convinced existing MidCoast customers to apply for commercial loans, ostensibly for valid business purposes. The true purpose of the loans, however, was to allow those MidCoast customers to loan money to Ladio. Ladio had been involved in a decade-long "loan-swap" arrangement with former Wilmington Trust Co. ("WTC") Market Manager Brian Bailey, in which the two men provided more than twenty (20) loans to each other totaling in excess of $1.5 million. In June 2010, WTC called Ladio's loans and required him to enter into a Global Restructuring Agreement (the "Agreement"). Ladio engaged in the nominee loan scheme in substantial part to make interest and principal payments under the Agreement.

Convenience Store Owners Sentenced for Selling Synthetic Cannabinoids, Money Laundering
On Nov. 21, 2014, in Tulsa, Oklahoma, Iqbal Makkar, of Bentonville, Arkansas, was sentenced to 97 months in prison, and Gaurav Sehgal, of Grove, Oklahoma, was sentenced to 84 months in prison. Additionally, both were ordered to forfeit their interests in two convenience stores,

various property and currency valued at over $3,475,535. A joint and several criminal forfeiture money judgment of $2,584,981was also levied and restitution of more than $6,000 was ordered. Both were convicted of conspiracy to distribute controlled drug analogues, possession of Schedule 1 controlled substance analogue with intent to distribute, maintaining drug-involved premises, and money laundering. According to court documents, from November 2011 to January 2013, Makkar and Sehgal operated the "Gitter Done Station" convenience store in Grove, Oklahoma, for the purpose of storing and distributing the controlled substance analogue known as XLR11. The men were charged with depositing funds from the illegal sales and distributions of the controlled substance analogues into a checking account in Missouri.

Ohio Man Sentenced for Criminal Schemes Centered Around IHOP Restaurants

On Nov. 21, 2014, in Toledo, Ohio, Mazen Khdeer, of Sylvania, was sentenced to 57 months in prison and two years of supervised release. Khdeer was also ordered to pay $1.3 million in restitution and forfeit two properties. Khdeer previously pleaded guilty to 13 counts, including money laundering, malicious use of fire, conspiracy to harbor aliens, identity theft, conspiracy to commit health care fraud and filing false claims. According to court documents, Khdeer was the last of 18 people to be sentenced for their roles in a series of criminal schemes that centered around seven IHOP restaurants owned by Tarek "Terry" Elkafrawi in northwest Ohio and Indiana. The schemes resulted in losses of more than $3 million. In 2008, the Findlay IHOP burned as the result of arson started by a co-conspirator at the direction of Elkafrawi and Khdeer to facilitate an insurance fraud scheme. Additionally, Khdeer used two identities to split his salary from the restaurants between two paychecks, creating lower reportable income for both identities. Using those identities, he claimed approximately $140,000 in Medicaid payments and $35,000 in food stamps and welfare benefits from the state of Ohio. Khdeer and Elkafrawi created a false property company to which Khdeer paid "rent" to Elkafrawi to show a lower income. Elkafrawi was sentenced to eight years in prison.

International Drug Dealer Sentenced to Prison

On Nov. 19, 2014, in Raleigh, North Carolina, Andrew Wayne Landells, of Jamaica, was sentenced to 180 months in prison, three years of supervised release and ordered to pay a money judgment of $1,000,000 and forfeit his interest in several properties located in New Jersey and Florida. Landells previously pleaded guilty to conspiracy to launder monetary instruments. According to court documents, Landells directed the activities of his estranged wife, and at least seven co-conspirators to assist him in the trafficking marijuana from Mexico throughout, New York, Florida, Virginia, Arizona, and North Carolina. Landells then used the drug proceeds to purchase luxury vehicles and residences, and to rent residences in others' names. In order to disguise the source of the proceeds from his illegal activities, Landells also operated sham companies purporting to be in the candle manufacturing business. Landells distributed up to 1,000 kilograms of marijuana and laundered money from drug proceeds through the straw purchase of at least seven pieces of real property, thirteen motor vehicles, and four businesses, all with a combined value of over $1,000,000.

Missouri Man Sentenced for Stealing Money from ATMs

On Nov. 18, 2014, in Kansas City, Missouri, Anthony T. Civella, Jr., was sentenced to 24 months in prison and ordered to pay $70,000 in restitution, in addition to the restitution that has already been paid. On Feb. 27, 2014, Civella pleaded guilty to bank larceny and money

laundering. According to court documents, from 2011 through 2013, Civella owned and operated a company called C Management Group, LLC, which serviced 35 ATMs in the Kansas City, Missouri, metropolitan area. Civella stole $330,040 from the ATMs by obtaining a maintenance code to access the machines. Civella moved money between the ATM machines in order to conceal the theft from the bank. He then comingled the stolen money from the ATMs by depositing most of the cash into his personal checking account at a credit union.

California Man Sentenced for Running Ponzi Scheme

On Nov. 17, 2014, in Sacramento, California, James Berghuis was sentenced to 168 months in prison for orchestrating a Ponzi scheme in the Sacramento area that defrauded family members, friends, and other acquaintances of more than $2.7 million. On Oct. 18, 2013, a jury convicted Berghuis of four counts of mail fraud, four counts of wire fraud, and one count of money laundering. According to evidence presented at trial, between 2005 and 2008, Berghuis convinced certain investors to take out home equity loans to make investments. Berghuis promised these investors he would use their money to invest in hard-money loans, real estate transactions, or the purchase of real estate franchises. He also offered several victims a deed of trust on his commercial property, promising each that they would be in second position on the title. However, Berghuis used investors' money to pay back other investors and to buy himself luxury goods, including several Mercedes Benz cars. Some victims lost their homes or continue to pay on mortgages they took out to make their investments with Berghuis.

Colorado Man Sentenced on Charges Related To Stealing Telecommunications Equipment, Money Laundering

On Nov. 14, 2014, in Tulsa, Oklahoma, Jesse Michael Greenwald, of Colorado, was sentenced to 84 months in prison, three years of supervised release and ordered to pay restitution of $4,419,125 on charges related to stealing and selling millions of dollars' worth of Verizon Communications telecommunications equipment. Greenwald pleaded guilty on Aug. 13, 2014, to conspiring to commit money laundering. Scott Gollan, and Michael Greenwald, both of Bastrop, Texas, and James Pennoyer, of Tulsa have also pleaded guilty to charges arising from the thefts from Verizon and are awaiting sentencing. According to court documents, from July 2009 to May 2014, Pennoyer was a contract employee at the Verizon Communications warehouse in Tulsa, and aided the other defendants in stealing telecommunications equipment from the warehouse. The defendants transported the stolen equipment to Colorado Springs, Colorado, and stored it in a facility to be sold at a later date. Much of the equipment was sold to a company in North Carolina, which made substantial payments to Greenwald and his co-conspirators. The conspirators, including Greenwald, then used the funds to engage in illegal monetary transactions of more than $10,000 each.

Illinois Man Sentenced on Drug and Money Laundering Offenses

On Nov. 13, 2014, in East St. Louis, Illinois, Demarcus L. Freeman, of East Alton, was sentenced to 151 months in prison and ordered to forfeit $10,000. On Aug. 7, 2014, Freeman pleaded guilty to distribution of cocaine base ("crack cocaine"), possession with intent to distribute cocaine base and money laundering. According to court documents, Freeman sold crack cocaine in Wood River, Illinois, on May 13, 2013 and again on June 4, 2013. On July 8, 2013, Police seized nine ounces of crack cocaine from Freeman which he admitted owning. Freeman also opened a credit union account in the name of a relative. Freeman laundered the

proceeds of his drug dealing through the account, in an attempt to disguise the source of the money. Freeman laundered over $60,000.

Costa Rica Based Telemarketing Fraud Results in Prison Terms for Two

On Oct. 30, 2014, in Charlotte, North Carolina, Glen Adkins Jr., of San Diego, California, was sentenced to 300 months in prison and Warren F. Tonsing Jr., of St. Paul, Minnesota, was sentenced to 144 months in prison. Both were ordered to pay $2.4 million in restitution, joint and several with their co-defendants. Adkins and Tonsing were convicted in August 2013 of wire fraud and money laundering. According to court documents, the defendants schemed to defraud United States residents, most over the age of 55, out of millions of dollars by deceiving them into believing that each had won a large monetary prize in a "sweepstakes contest." Both defendants worked in a Costa Rica-based call center that used computers to make telephone calls over the internet to victims in the United States. This process allowed the defendants and their co-conspirators to disguise the originating location of the calls. Victims were informed that the callers were from a federal agency and that to receive their "prize" they had to wire thousands of dollars to Costa Rica for a purported "refundable insurance fee." As long as the victims continued to pay, the co-conspirators continued to solicit more money from them in the form of purported fees. To date, 46 defendants have been convicted for their participation in similar Costa Rican telemarketing schemes.

Former Arkansas Business Developer Sentenced For Fraud

On Oct. 28, 2014, in Fort Smith, Arkansas, Brandon Lynn Barber, of New York, New York, was sentenced to 65 months in prison and three years supervised release. On July 31, 2013, Barber pleaded guilty to conspiracy to commit bankruptcy fraud, conspiracy to commit bank fraud and money laundering. According to court documents, from approximately 2005 through 2009, Barber was involved in several schemes to defraud banks, creditors and the Federal Bankruptcy Court. Barber provided false financial information and statements to banks for loans to finance the Legacy Condominium building and the Bellafont project in Fayetteville. Barber also concealed assets and income from creditors and the bankruptcy court by transferring funds to other co-defendants or accounts controlled by them and using those funds for his own personal benefit and expenses.

Former Boeing Procurement Officer and two Sub-Contractors Sentenced on Federal Fraud Charges

On Oct. 27, 2014, in St. Louis, Missouri, Deon Anderson, a former Boeing Procurement Officer, was sentenced to 20 months in prison. William P. Boozer, of Hacienda Heights, California, was sentenced to 18 months in prison. Robert Diaz, Jr., of Alta Loma, California, was sentenced to 15 months in prison. Anderson pleaded guilty in June 2014 to three counts of mail fraud, one count of wire fraud and one count of currency structuring. Co-defendants Boozer and Diaz previously pleaded guilty to related charges in connection with a bribery/kickback scheme involving Boeing military aircraft parts. According to court documents, between November 2009 and February 2013, Boozer requested Anderson provide him with non-public competitor bid information and historical price information in connection with Boeing military aircraft part purchase order requests for quotes. Anderson gave the information to Boozer to be used in preparing and submitting bids on behalf of Globe Dynamics in response to approximately sixteen different Boeing requests for quotes, in exchange for cash payments. Of the sixteen bids Globe Dynamics

was awarded seven purchase orders to supply United States military aircraft parts to Boeing totaling in excess of $1,500,000. The net benefit to Globe Dynamics on those seven purchase orders was approximately $116,339. Beginning in May 2011 and continuing through April 2013, Anderson provided Diaz and another individual with non-public competitor bid information and historical price information in connection with one and more Boeing military aircraft part purchase order requests for quotes. They used that information in preparing and submitting bids on behalf of J.L. Manufacturing to Boeing for approximately nine different Boeing requests for quotes. Of the those nine, J.L. Manufacturing was awarded seven purchase orders to supply United States military aircraft parts to Boeing totaling in excess of orders totaled approximately $2,052,746. In exchange for that information they made cash payments to Anderson. On more than one occasion, Anderson structured cash deposits into his personal checking account to conceal his bribe scheme.

California Man Sentenced for Money Laundering

On Oct. 24, 2014, in Muskogee, Oklahoma, David Lewis McDowell, of Riverside, California, was sentenced to 51 months in prison, ordered to pay approximately $2,500,000 in restitution and to forfeit $3,000,000. In March, 2014, McDowell pleaded guilty to money laundering. According to court documents, from about June 25, 2008 through Nov. 9, 2009, McDowell devised a scheme to defraud investors by fraudulently representing and promising that a company had a system that could produce ethanol at a commercial production rate sufficient to sell commercially. Based upon those fraudulent and material representations, his actions caused victims to send money to be invested in this company. In addition, McDowell caused money derived from wire fraud to be transferred from accounts at a bank.

Three Chiropractors Sentenced in Staged Automobile Accident Scheme

On Oct. 14, 2014, in West Palm Beach, Florida, three chiropractors were sentenced for their participation in a massive staged automobile accident scheme. Kenneth Karow, of West Palm Beach, was sentenced to 132 months in prison; Hermann J. Diehl, of Miami, was sentenced to 108 months in prison; and Hal Mark Kreitman, of Miami Beach, was sentenced to 96 months in prison. Karow was convicted of 48 counts of mail fraud and 11 counts of money laundering. Diehl was convicted of two counts of mail fraud and three counts of money laundering. Kreitman was convicted of 21 counts of mail fraud and two counts of money laundering. According to court documents, between October 2006 and December 2012, the defendants and their co-conspirators staged automobile accidents and caused the submission of false insurance claims through chiropractic clinics they controlled.

Three Sentenced in Illegal Gambling Operation in Guam

On Oct. 8, 2014, in Hagatna, Guam, three individuals were sentenced in a criminal conspiracy to conduct an illegal gambling business at the former MGM Spa in Tamuning. Jimmy Hsieh was sentenced to 24 months in prison and ordered to pay a $423,640 money judgment. In addition, Hsieh agreed to forfeit $178,113 from personal accounts and that three of his condos are subject to possible forfeiture proceedings. Hsieh pleaded guilty to gambling conspiracy and money laundering. William Perez, the manager and supervisor of the MGM poker operation in 2010, was sentenced to six months in prison, six months home confinement and three years of supervised release for conspiring to operate the illegal gambling business. Pauline Perez was sentenced to one year of probation and community service. According to court documents, from

at least January 2006 until December 2010, the defendants conspired to offer card games of chance, including baccarat and poker, at the MGM Spa building. The defendants took a percentage of the winnings from each game. They knowingly conducted financial transactions involving the proceeds from the illegal gambling operation.

Washington Man Sentenced for Operating Unlicensed Money Transmitting Business
On Oct. 6, 2014, in Seattle, Washington, Pavel Rombakh was sentenced to 24 months in prison and ordered to forfeit cash and property worth $510,000. Rombakh, who immigrated to the United States from Ukraine in the 1990's, pleaded guilty in May 2014 to operating an unlicensed money transmitting business. According to court documents, over a five year period, Rombakh received wires of more than $150 million from overseas and then wired the funds back out to other accounts. Many of the wires originated in Russia and Cyprus and were promptly re-wired to England, Latvia, the United Arab Emirates, and China. Rombakh kept a small percentage of the funds as his fee.

Illinois Man Sentenced for Money Laundering and Wire Fraud
On Oct. 3, 2014, in Springfield, Illinois, Brian J. Fields, of Belleville, was sentenced to 27 months in prison, three years of supervised release and ordered to pay $98,800 in restitution. Fields previously pleaded guilty to money laundering and wire fraud. According to court documents, Fields conspired with a person in Nigeria to defraud United States citizens by sending counterfeit checks and money orders to people in several schemes (such as a "Secret Shopper" scam). The schemes resulted in victims receiving the counterfeit check or money order, depositing it into their own bank account, and then at the direction of Fields, the victim would wire transfer legitimate funds to Fields. By the time the person learned the check or money order was worthless, they had already sent the money to Fields. When Fields received the victims' money, he would keep a portion for himself. Then to further the scheme, Fields would send the remaining funds to a person located in Nigeria.

Caribbean-Based Investment Advisor and Attorney Sentenced for Using Offshore Accounts to Launder and Conceal Funds
On Oct. 3, 2014, in Washington, DC, Eric St-Cyr, an investment advisor, and Patrick Poulin, an attorney, were each sentenced to 14 months in prison and three years of supervised release for conspiring to launder monetary instruments. St-Cyr and Poulin, both Canadian citizens, along with Joshua Vandyk, a U.S. citizen, previously pleaded guilty. Vandyk was sentenced on Sept. 5, 2014, to 30 months in prison. According to court documents, Vandyk, St-Cyr and Poulin conspired to conceal and disguise the nature, location, source, ownership and control of property believed to be the proceeds of bank fraud, specifically $2 million. Vandyk, St-Cyr and Poulin assisted undercover law enforcement agents posing as U.S. clients in laundering purported criminal proceeds through an offshore structure designed to conceal the true identity of the proceeds' owners. Vandyk and St-Cyr invested the laundered funds on the clients' behalf and represented that the funds would not be reported to the U.S. government. Poulin established an offshore corporation for the undercover agents. Upon request from the U.S. client, Vandyk and St-Cyr liquidated investments and transferred money, through Poulin, back to the United States. According to Vandyk and St-Cyr, the investment firm would charge clients higher fees to launder criminal proceeds than to assist them in tax evasion.

North Carolina Man Sentenced for Conspiracy, Mail Fraud, and Money Laundering
On Oct. 2, 2014, in Raleigh, North Carolina, Thomas L. Kimmel was sentenced to 264 months in prison, three years of supervised release and ordered to pay over $16.5 million in restitution. On June 26, 2014, Kimmel was convicted of conspiracy, mail fraud, and money laundering. According to court documents, Kimmel solicited about $20 million for Sure Line Acceptance Corporation from investors. Most of these investors found out about Sure Line through financial conferences that Kimmel gave at churches relating to Biblical principles of finance and getting out of debt. Most of the victims never received any of their principal back. Kimmel would typically spend a few minutes of each conference telling investors about a 12% collateralized note program. Kimmel's statements about Sure Line were false and that the collateralized note program was a Ponzi scheme.

Former Sheriff's Deputy Sentenced for Laundering $40 Million in Drug Proceeds
On Oct. 1, 2014, in McAllen, Texas, Robert Ricardo Maldonado, of Weslaco, Texas, was sentenced to 144 months in prison and three years of supervised release. Maldonado, a former deputy with the Hidalgo County Sheriff's Office, pleaded guilty on May 12, 2014, to conspiracy to commit money laundering. According to court documents, from 2001 to November 2013, Maldonado transported $40 million worth of drug proceeds. Maldonado was paid a percentage of the total amount of the currency transported. He then utilized these funds to purchase various properties and assets.

Utah Resident Sentenced for Role in Investment Fraud Scheme
On Oct. 1, 2014, in Salt Lake City, Utah, Armand R. Franquelin, of Liberty, Utah, was sentenced to 57 months in prison, three years of supervised release and ordered to pay $6,566,596 in restitution. In September 2014, Martin Pool was sentenced to 78 months in prison. Franquelin and Pool pleaded guilty in May 2014 to securities fraud and money laundering in connection with an investment fraud scheme related to a real estate project in Vernal, Utah. According to court documents, from 2006 to 2010, Franquelin and Pool persuaded investors to convert their traditional IRAs to self-directed IRA accounts and invest their funds in a residential real estate project known as Haven Estates. This was accomplished by inducing the investors to direct funds to their company, The Elva Group, in return for notes promising monthly interest payments at annual rates between 8 and 20 percent. In reality, investors' funds were used for purposes other than the development of Haven Estates. Investors were not told of encumbrances already in place on Haven Estates. Eventually, Haven Estates was foreclosed. Investors' funds were used by Pool and Franquelin and their associates for their personal benefit and to pay interest to earlier investors as Ponzi payments. The Ponzi payments had the effect of lulling the earlier investors, persuading them to leave their funds in the company and inducing them to renew their promissory notes from time to time. The payments also enticed new investors to invest.

Common Abbreviations Related to Money Laundering

1988 UN Drug Convention	1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
AML	Anti-Money Laundering
APG	Asia/Pacific Group on Money Laundering
ARS	Alternative Remittance System
BMPE	Black Market Peso Exchange
CBP	Customs and Border Protection
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CFT	Combating the Financing of Terrorism
CTR	Currency Transaction Report
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DHS/HSI	Department of Homeland Security/Homeland Security Investigations
DNFBP	Designated Non-Financial Businesses and Professions
DOJ	Department of Justice
DOS	Department of State
EAG	Eurasian Group to Combat Money Laundering and Terrorist Financing
EC	European Commission
ECOWAS	Economic Community of West African States
EO	Executive Order
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Department of the Treasury's Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FTZ	Free Trade Zone
GABAC	Action Group against Money Laundering in Central Africa
GAFILAT	Financial Action Task Force of Latin America
GDP	Gross Domestic Product
GIABA	Inter Governmental Action Group against Money Laundering
IBC	International Business Company
ILEA	International Law Enforcement Academy
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
INL	Bureau of International Narcotics and Law Enforcement Affairs
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service, Criminal Investigations
ISIL	Islamic State of Iraq and the Levant
KYC	Know-Your-Customer
MENAFATF	Middle East and North Africa Financial Action Task Force
MER	Mutual Evaluation Report
MLAT	Mutual Legal Assistance Treaty
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOU	Memorandum of Understanding

MSB	Money Service Business
MVTS	Money or Value Transfer Service
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
OAS	Organization of American States
OAS/CICAD	OAS Inter-American Drug Abuse Control Commission
OECD	Organization for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control
OPDAT	Office of Overseas Prosecutorial Development, Assistance and Training
OTA	Office of Technical Assistance
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TBML	Trade-Based Money Laundering
TTU	Trade Transparency Unit
UNCAC	United Nations Convention against Corruption
UNGPML	United Nations Global Programme against Money Laundering
UNODC	United Nations Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution
UNTOC	United Nations Convention against Transnational Organized Crime
USAID	United States Agency for International Development

Definitions of Money Laundering Terms

419 Fraud Scheme: An advanced fee fraud scheme, known as "419 fraud" in reference to the fraud section in Nigeria's criminal code. This specific type of scam is generally referred to as the Nigerian scam because of its prevalence in the country. Such schemes typically involve promising the victim a significant share of a large sum of money, in return for a small up-front payment, which the fraudster claims to require in order to cover the cost of documentation, transfers, etc. Frequently, the sum is said to be lottery proceeds or personal/family funds being moved out of a country by a victim of an oppressive government, although many types of scenarios have been used. This scheme is perpetrated globally through email, fax, or mail.

Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT): Collective term used to describe the overall legal, procedural, and enforcement regime countries must implement to fight the threats of money laundering and terrorism financing.

Bearer Share: A bearer share is an equity security that is solely owned by whoever holds the physical stock certificate. The company that issues the bearer shares does not register the owner of the stock nor does it track transfers of ownership. The company issues dividends to bearer shareholders when a physical coupon is presented.

Black Market Peso Exchange (BMPE): One of the most pernicious money laundering schemes in the Western Hemisphere. It is also one of the largest, processing billions of dollars' worth of drug proceeds a year from Colombia alone via TBML, "smurfing," cash smuggling, and other schemes. BMPE-like methodologies are also found outside the Western Hemisphere. There are variations on the schemes involved, but generally drug traffickers repatriate and exchange illicit profits obtained in the United States without moving funds across borders. In a simple BMPE scheme, a money launderer collaborates with a merchant operating in Colombia or Venezuela to provide him, at a discounted rate, U.S. dollars in the United States. These funds, usually drug proceeds, are used to purchase merchandise in the United States for export to the merchant. In return, the merchant who import the goods provides the money launderer with local-denominated funds (pesos) in Colombia or Venezuela. The broker takes a cut and passes along the remainder to the responsible drug cartel.

Bulk Cash Smuggling: Bulk cash refers to the large amounts of currency notes criminals accumulate as a result of various types of criminal activity. Smuggling, in the context of bulk cash, refers to criminals' subsequent attempts to physically transport the money from one country to another.

Cross-border currency reporting: Per FATF recommendation, countries should establish a currency declaration system that applies to all incoming and outgoing physical transportation of cash and other negotiable monetary instruments.

Counter-valuation: Often employed in settling debts between hawaladars or traders. One of the parties over-or-undervalues a commodity or trade item such as gold, thereby transferring value to another party and/or offsetting debt owed.

Currency Transaction Report (CTR): Financial institutions in some jurisdictions are required to file a CTR whenever they process a currency transaction exceeding a certain amount. In the United States, for example, the reporting threshold is $10,000. The amount varies per

jurisdiction. These reports include important identifying information about accountholders and the transactions. The reports are generally transmitted to the country's FIU.

Customer Due Diligence/Know Your Customer (CDD/KYC): The first step financial institutions must take to detect, deter, and prevent money laundering and terrorism financing, namely, maintaining adequate knowledge and data about customers and their financial activities.

Egmont Group of FIUs: The international standard-setter for FIUs. The organization was created with the goal of serving as a center to overcome the obstacles preventing cross-border information sharing between FIUs.

FATF-Style Regional Body (FSRB): These bodies – which are modeled on FATF and are granted certain rights by that organization – serve as regional centers for matters related to AML/CFT. Their primary purpose is to promote a member jurisdiction's implementation of comprehensive AML/CFT regimes and implement the FATF recommendations.

Financial Action Task Force (FATF): FATF was created by the G7 leaders in 1989 in order to address increased alarm about money laundering's threat to the international financial system. This intergovernmental policy making body was given the mandate of examining money laundering techniques and trends and setting international standards for combating money laundering and terrorist financing.

Financial Intelligence Unit (FIU): In many countries, a central national agency responsible for receiving, requesting, analyzing, and/or disseminating disclosures of financial information to the competent authorities, primarily concerning suspected proceeds of crime and potential financing of terrorism. An FIU's mandate is backed up by national legislation or regulation. The Financial Crimes Enforcement Network (FinCEN) is the U.S. financial intelligence unit.

Free Trade Zone (FTZ): A special commercial and/or industrial area where foreign and domestic merchandise may be brought in without being subject to the payment of usual customs duties, taxes, and/or fees. Merchandise, including raw materials, components, and finished goods, may be stored, sold, exhibited, repacked, assembled, sorted, or otherwise manipulated prior to re-export or entry into the area of the country covered by customs. Duties are imposed on the merchandise (or items manufactured from the merchandise) only when the goods pass from the zone into an area of the country subject to customs. FTZs may also be called special economic zones, free ports, duty-free zones, or bonded warehouses.

Funnel Account: An individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.

Hawala: A centuries-old broker system based on trust, found throughout South Asia, the Arab world, and parts of Africa, Europe, and the Americas. It allows customers and brokers (called hawaladars) to transfer money or value without physically moving it, often in areas of the world where banks and other formal institutions have little or no presence. It is used by many different cultures, but under different names; "hawala" is used often as a catchall term for such systems in discussions of terrorism financing and related issues.

Hawaladar: A broker in a hawala or hawala-type network.

International Business Company (IBC): Firms registered in an offshore jurisdiction by a non-resident that are precluded from doing business with residents in the jurisdiction. Offshore entities may facilitate hiding behind proxies and complicated business structures. IBCs are frequently used in the "layering" stage of money laundering.

Integration: The last stage of the money laundering process. The laundered money is introduced into the economy through methods that make it appear to be normal business activity, to include real estate purchases, investing in the stock market, and buying automobiles, gold, and other high-value items.

Kimberly Process (KP): The Kimberly Process was initiated by the UN to keep "conflict" or "blood" diamonds out of international commerce, thereby drying up the funds that sometimes fuel armed conflicts in Africa's diamond producing regions.

Layering: This is the second stage of the money laundering process. The purpose of this stage is to make it more difficult for law enforcement to detect or follow the trail of illegal proceeds. Methods include converting cash into monetary instruments, wire transferring money between bank accounts, etc.

Legal Person: A company, or other entity that has legal rights and is subject to obligations. In the FATF Recommendations, a legal person refers to a partnership, corporation, association, or other established entity that can conduct business or own property, as opposed to a human being.

Mutual Evaluation (ME): All FATF and FSRB members have committed to undergoing periodic multilateral monitoring and peer review to assess their compliance with FATF's recommendations. Mutual evaluations are one of the FATF's/FSRB's primary instruments for determining the effectiveness of a country's AML/CFT regime.

Mutual Evaluation Report (MER): At the end of the FATF/FSRB mutual evaluation process, the assessment team issues a report that describes the country's AML/CFT regime and rates its effectiveness and compliance with the FATF Recommendations.

Mobile Payments or M-Payments: An umbrella term that generally refers to the growing use of cell phones to credit, send, receive, and transfer money and virtual value.

Natural Person: In jurisprudence, a natural person is a real human being, as opposed to a legal person (see above). In many cases, fundamental human rights are implicitly granted only to natural persons.

Offshore Financial Center: Usually a low-tax jurisdiction that provides financial and investment services to non-resident companies and individuals. Generally, companies doing business in offshore centers are prohibited from having clients or customers who are resident in the jurisdiction. Such centers may have strong secrecy provisions or minimal identification requirements.

Over-invoicing: When money launderers and those involved with value transfer, trade-fraud, and illicit finance misrepresent goods or services on an invoice by indicating they cost more than they are actually worth. This allows one party in the transaction to transfer money to the other under the guise of legitimate trade.

Politically Exposed Person (PEP): A term describing someone who has been entrusted with a prominent public function, or an individual who is closely related to such a person.

Placement: This is the first stage of the money laundering process. Illicit money is disguised or misrepresented, then placed into circulation through financial institutions, casinos, shops, and other businesses, both local and abroad. A variety of methods can be used for this purpose, including currency smuggling, bank transactions, currency exchanges, securities purchases, structuring transactions, and blending illicit with licit funds.

Shell Company: An incorporated company with no significant operations, established for the sole purpose of holding or transferring funds, often for money laundering purposes. As the name implies, shell companies have only a name, address, and bank accounts; clever money launderers often attempt to make them look more like real businesses by maintaining fake financial records and other elements. Shell companies are often incorporated as IBCs.

Smurfing/Structuring: A money laundering technique that involves splitting a large bank deposit into smaller deposits to evade financial transparency reporting requirements.

Suspicious Transaction Report/Suspicious Activity Report (STR/SAR): If a financial institution suspects or has reasonable grounds to suspect that the funds involved in a given transaction derive from criminal or terrorist activity, it is obligated to file a report with its national FIU containing key information about the transaction. In the United States, SAR is the most common term for such a report, though STR is used in most other jurisdictions.

Tipping Off: The disclosure of the reporting of suspicious or unusual activity to an individual who is the subject of such a report, or to a third party. The FATF Recommendations call for such an action to be criminalized.

Trade-Based Money Laundering (TBML): The process of disguising the proceeds of crime and moving value via trade transactions in an attempt to legitimize their illicit origin.

Trade Transparency Unit (TTU): TTUs examine trade between countries by comparing, for example, the export records from Country A and the corresponding import records from Country B. Allowing for some recognized variables, the data should match. Any wide discrepancies could be indicative of trade fraud (including TBML), corruption, or the back door to underground remittance systems and informal value transfer systems, such as hawala.

Under-invoicing: When money launderers and those involved with value transfer, trade fraud, and illicit finance misrepresent goods or services on an invoice by indicating they cost less than they are actually worth. This allows the traders to settle debts between each other in the form of goods or services.

Unexplained Wealth Order (UWO): A type of court order to compel someone to reveal the sources of their unexplained wealth. UWOs require the owner of an asset to explain how he or she was able to afford that asset. Persons who fail to provide a response may have assets seized or may be subject to other sanctions.

UNSCR 1267: UN Security Council Resolution 1267 and subsequent resolutions require all member states to take specific measures against individuals and entities associated with the Taliban and al-Qaida. The “1267 Committee” maintains a public list of these individuals and entities, and countries are encouraged to submit potential names to the committee for designation.

UNSCR 1373: UN Security Council Resolution 1373 requires states to freeze without delay the assets of individuals and entities associated with any global terrorist organization. This is

significant because it goes beyond the scope of Resolution 1267 and requires member states to impose sanctions against all terrorist entities.

Virtual Currency: Virtual currency is an internet-based form of currency or medium of exchange, distinct from physical currencies or forms of value such as banknotes, coins, and gold. It is electronically created and stored. Some forms are encrypted. They allow for instantaneous transactions and borderless transfer of ownership. Virtual currencies generally can be purchased, traded, and exchanged among user groups and can be used to buy physical goods and services, but can also be limited or restricted to certain online communities, such as a given social network or internet game. Virtual currencies are purchased directly or indirectly with genuine money at a given exchange rate and can generally be remotely redeemed for genuine monetary credit or cash. According to the U.S. Department of Treasury, virtual currency operates like traditional currency, but does not have all the same attributes; i.e., it does not have legal tender status.

Zakat: One of the five pillars of Islam, translated as “alms giving.” It involves giving a percentage of one’s possessions to charity. Often compared to tithing, zakat is intended to help poor and deprived Muslims. The Muslim community is obligated to both collect zakat and distribute it fairly.