NATIONAL MONEY LAUNDERING RISK ASSESSMENT

2018

EXECUTIVE SUMMARY

The 2018 *National Money Laundering Risk Assessment* (2018 NMLRA) identifies the money laundering threats, vulnerabilities, and risks that the United States currently faces, updating the 2015 *National Money Laundering Risk Assessment* (2015 NMLRA).[1] Relevant component agencies, bureaus, and offices of Treasury, the Department of Justice (DOJ), the Department of Homeland Security (DHS), as well as U.S. regulatory agencies, participated in the development of the risk assessment. The 2018 NMLRA is based on interviews with relevant authorities as well as a review of federal and state public sector actions and analysis, and private sector research, issued since the 2015 NMLRA.

The United States continues to estimate that domestic financial crime, excluding tax evasion, generates approximately $300 billion of proceeds for potential laundering, based on the sources and analysis cited in the 2015 NMLRA.[2] Criminal prosecutions and law enforcement investigations indicate that most of the money earned from crime in the United States stays in the United States, but also that the United States is an attractive destination for illicit funds generated abroad.

The crimes that generate the bulk of illicit proceeds in the United States are fraud, drug trafficking, human smuggling, human trafficking, organized crime, and corruption. The many varieties of fraud, including bank fraud, consumer fraud, healthcare fraud, securities fraud, and tax refund fraud, are believed to generate the largest share of illicit proceeds. Healthcare fraud alone generates proceeds of approximately $100 billion annually. Prosecutions indicate that healthcare fraud often involves complicit healthcare professionals submitting fraudulent bills to insurers. Insurance payments and subsequent transactions may flow through the banking system and look indistinguishable from legitimate funds transfers. When payments are made by check the laundering can involve the help of complicit check cashers.

Law enforcement agencies have seen an increase in cybercrime, which encompasses a variety of illicit activity including phishing, malware attacks, and cyber-enabled crime such as credit card fraud, business e-mail compromise; and various types of consumer scams, including fake romance and lottery schemes, and employment offers that all inevitably involve the victim receiving requests for money. These internet-based crimes can be perpetrated from anywhere in the world, which, along with the universal presence of drug trafficking networks, has contributed to the rise of global money laundering syndicates that employ complicit merchants, financial services professionals, and individuals to launder illicit proceeds on behalf of a variety of criminals. These professional money launderers and networks then subsist independently of the criminals they serve, making them dangerous due to their adaptability.

---

[1] The three stages of money laundering are: (1) placement, in which illicit proceeds are introduced into the financial system; (2) layering, in which the criminal attempts to distance the proceeds from the crime through a series of transactions; and (3) integration, whereby the illicit funds re-enter the economy disguised as legitimate funds.

[2] The 2015 National Money Laundering Risk Assessment is available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

Mexico remains the dominant conduit for most illegal drugs entering the U.S. Professional money launderers often take possession of the drug proceeds in the U.S. and facilitate the laundering process. Such laundering can involve a combination of structured bank deposits, funnel accounts, and bulk cash smuggling. A typical scheme exemplifying how these money laundering methods work together involves the pooling of proceeds into a single account as the result of small cash deposits at bank branches throughout the country, then either wiring the collected funds to Mexico or withdrawing them in currency near the Southwest border for smuggling into Mexico. Another common method is trade-based money laundering, which involves using a cycle of money brokers and exporters of goods to disguise and move drug money. The sale of the goods effectively launders the money and provides drug suppliers with payment in local currency. Merchants who receive payment by check or wire for their goods may be unaware they are participating in a money laundering scheme, but some willingly accept drug cash and are aware they are complicit.

The nature of synthetic drug trafficking, and associated financial flows, has changed with the rise of China as a supplier of fentanyl and its analogues and precursors. China is the primary source of fentanyl and fentanyl analogues[3] and payments to China for these drugs are made by bank and non-bank wires as well as by virtual currencies. In October 2017 the Department of Justice announced its first indictments of Chinese nationals for fentanyl and fentanyl analogues trafficking in the United States.[4] After a series of deaths and overdoses that prompted the investigation, 32 defendants were charged, including Jian Zhang. The Attorney General noted: "[t]his was an elaborate and sophisticated conspiracy. They used the internet, about 30 different aliases, cryptocurrency, off-shore accounts, and encrypted communications, and they allegedly laundered funds internationally through third parties."[5] In April 2018 the Office of Foreign Assets Control (OFAC) followed with the designation of Zhang and others as Significant Foreign Narcotics Trafficker pursuant to the Kingpin Act blocking their U.S. assets and prohibiting transactions with them in the first such designation involving an alleged fentanyl trafficker. OFAC noted that money services businesses (MSBs) were also used to launder the proceeds.[6]

Virtual currencies, in addition to being the preferred form of payment for buying illicit drugs and other illicit goods online and paying the perpetrators of ransomware attacks, are also now used as a money laundering vehicle. Global money laundering syndicates have added the option of moving illicit proceeds into and through virtual currencies as another way to layer transactions in order to hide the origin of dirty money.

---

[3] Sean O'Connor, Fentanyl: China's Deadly Export to the United States, U.S.-China Economic and Security Review Commission, February 1, 2017.

[4] DOJ, Press Release, "Justice Department Announces First Ever Indictments Against Designated Chinese Manufacturers of Deadly Fentanyl and Other Opiate Substances", October 12, 2017, available at https://www.justice.gov/opa/pr/justice-department-announces-first-ever-indictments-against-designated-chinese-manufacturers.

[5] DOJ, Press Release, "Attorney General Sessions Announces New Indictments in International Fentanyl Case", April 27, 2018, available at https://www.justice.gov/opa/speech/attorney-general-sessions-announces-new-indictments-international-fentanyl-case.

[6] Treasury, Press Release, "Treasury Sanctions Chinese Fentanyl Trafficker Jian Zhang", April 27, 2018, available at https://home.treasury.gov/news/press-releases/sm0372.

The most significant money laundering risks in the United States include misuse of cash, complicit individuals and financial services employees, and lax compliance at financial institutions. These are the residual risks that are left after taking into consideration the scope and quality of U.S. anti-money laundering (AML) regulation, supervision, and enforcement. Although improvements can be made to diminish these risks, the fact they exist to some extent should not be considered surprising.

Anonymity in transactions and funds transfers is the main risk that facilitates money laundering. Criminal actors involved in drug trafficking, human smuggling and trafficking, illicit retail transactions, and various activities associate with organized crime continue to prefer U.S. currency-denominated cash due to its widespread use in the U.S. as well as its global use due its wide acceptance as a stable store of value and medium of exchange. Virtual currencies, when exchanger and administrators are unregulated, also provide anonymity and pose risks due to the speed they can be transmitted, disintermediation, global reach, and the lack of regulation and supervision in many jurisdictions. The risk of the misuse of cash and virtual currency is mitigated in the United States by the imposition of AML program, suspicious and currency transaction reporting, and customer recordkeeping requirements on financial institutions. In addition, businesses and individuals have cash reporting obligations in certain circumstances to mitigate the risks of using cash. But these obligations are only effective to the extent they are followed. Criminals seek out complicit merchants, professional, and financial services employees. The Department of Justice has increased its focus on complicit professionals, resulting in prosecutions of merchants facilitating trade-based money laundering (TBML), as well as attorneys and real estate agents. Individuals who abuse their professional position at financial institutions also are a money laundering risk. These individuals facilitate the opening of accounts, conduct funds transfers, and cash checks while knowingly failing to verify customer identification when required, maintain accurate transaction records, or file required reports.[7] Financial institutions with lax compliance programs also pose a money laundering risk.

Federal law enforcement agencies noted that misuse of legal entities posed a significant money laundering risk and that law enforcement efforts to uncover the true owners of companies can be resource-intensive, especially when those ownership trails lead overseas or involve numerous layers. The lack of obligation for certain financial institutions to identify the natural person(s) who own or control a corporate customer had allowed individuals to access financial services anonymously by acting through shell companies. While it is too soon to predict the full impact of Financial Crimes Enforcement Network (FinCEN) new Customer Due Diligence (CDD) rule, this money laundering risk should lessen as a result of their full implementation.[8]

---

[7] Title 31 of the U.S. Code, Section 5313, requires a financial institution to file a Currency Transaction Report (CTR) with FinCEN for each cash transaction or group of related cash transactions in a day that aggregate to more than $10,000. Willful failure to file a CTR is criminalized under Title 31 of the U.S. Code, Section 5322. Financial institutions in the United States are required to file a suspicious activity report to FinCEN under certain circumstances as specified by regulation.

[8] FinCEN issued final rules effective July 11, 2016 under the Bank Secrecy Act (BSA) to clarify and strengthen customer due diligence requirements for: banks; brokers or dealers in securities; mutual funds; and futures commission merchants and introducing brokers in commodities. The rules contain explicit customer due diligence requirements and include a new requirement to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. Covered financial institutions were required to come into compliance with these rules by May 11, 2018.

Finally, pursuing global money laundering syndicates requires U.S. law enforcement to partner with other countries to help trace illicit proceeds, identify relevant parties, collect evidence, and seize assets. A continuing money laundering vulnerability for the United States is that some countries lack the necessary authorities, capabilities, or motivation to help U.S. law enforcement pursue money laundering investigations with a nexus to the United States.

INTRODUCTION

The 2018 NMLRA updates the 2015 NMLRA.[9] This report identifies the most significant money laundering threats, vulnerabilities, and risks that the United States currently faces. It is based on a review of federal and state public sector analysis, enforcement actions, and guidance; as well as interviews with FinCEN staff, intelligence analysts, law enforcement agents, and prosecutors. The NMLRA uses all available information to identify as objectively as possible the priority money laundering risks to the United States.

Money laundering continues to be a significant concern because it facilitates and conceals crime and can distort markets and the broader financial system. The United States is particularly vulnerable to all forms of illicit finance because more than half of the world's trade is denominated in U.S. dollars.[10] Even trade transactions that do not involve a U.S. buyer or seller may involve the U.S. financial system. In addition, U.S. currency continues to be used globally.

METHODOLOGY

The terminology and methodology of the NMLRA are based in part on the guidance of the Financial Action Task Force, the international standard-setting body for anti-money laundering and countering the financing of terrorism (AML/CFT) safeguards. The following concepts are used in this risk assessment:

- **Threat**: These are the predicate crimes that are associated with money laundering. The environment in which predicate offences are committed and the proceeds of crime are generated is relevant to understanding why, in some cases, specific crimes are associated with specific money laundering methods.
- **Vulnerability**: This is what facilitates or creates the opportunity for money laundering. It may relate to a specific financial sector or product or a weakness in regulation, supervision, or enforcement. It may also reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity. The methods that allow for the most amount of money to be laundered most effectively or most quickly present the greatest potential vulnerabilities.
- **Risk**: Risk is a function of threat and vulnerability. It represents a summary judgment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement.

The first section of the NMLRA provides an overview of money laundering threats and related money laundering methods. The second section of the report goes into further detail on money laundering vulnerabilities and the residual risks, which are illustrated by a number of case examples.

[9] The 2015 NMLRA is available at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.
[10] SWIFT, Worldwide Currency Usage and Trends, December 2015.

PARTICIPANTS

This report incorporates published and unpublished research and the analysis, insights, and observations of managers and staff from U.S. government agencies, which also reviewed this report:

- Department of the Treasury
  - Internal Revenue Service Criminal Investigation (IRS-CI)
  - Internal Revenue Service Small Business/Self-Employed Division (SBSE)
  - Terrorism and Financial Intelligence (TFI)
    - Financial Crimes Enforcement Network (FinCEN)
    - Office of Foreign Assets Control (OFAC)
    - Office of Intelligence and Analysis (OIA)
    - Office of Terrorist Financing and Financial Crimes (TFFC)
- Department of Justice
  - Criminal Division
    - Computer Crime and Intellectual Property Section
    - Fraud Section
    - Money Laundering and Asset Recovery Section
    - Narcotics and Dangerous Drugs Section
    - Organized Crime and Gang Section
  - Drug Enforcement Administration (DEA)
  - Federal Bureau of Investigation (FBI)
  - Organized Crime Drug Enforcement Task Forces (OCDETF)
- Department of Homeland Security
  - Immigration and Customs Enforcement (ICE)
    - Homeland Security Investigations (HIS)
  - United States Secret Service (USSS)
- Staff of federal functional regulators[11]

[11] This includes staff of: the Commodity Futures Trading Commission (CFTC); Federal Deposit Insurance Corporation (FDIC); Board of Governors of the Federal Reserve System (Federal Reserve); National Credit Union Administration (NCUA); Office of the Comptroller of the Currency (OCC); and the Securities and Exchange Commission (SEC). SEC staff also sought input from the staff of the Financial Industry Regulatory Authority (FINRA), which is the largest self-regulatory organization for broker-dealers doing business with the public in the United States. CFTC staff also sought input from the staff of the National Futures Association, a self-regulatory organization, and the CME Group Inc., a leading derivatives marketplace.

SECTION 1. THREATS

In the context of this risk assessment, money laundering threats are the predicate crimes that generate illicit proceeds for laundering. The risk assessment identifies the most significant money laundering threats in the United States. Where reliable data exists, this section also identifies the proceeds of crime generated abroad that are laundered through or in the United States. Understanding the threat environment is essential to understanding the vulnerabilities that create money laundering opportunities.

A. FRAUD

Fraud is estimated to generate more illicit proceeds laundered in the United States than any other category of crime. It encompasses a wide range of criminal activity including healthcare, bank, consumer, securities, mortgage and tax refund fraud, and other crimes that are based on deception. A trend across most categories of fraud is the use of stolen identities. Healthcare fraud, tax refund fraud, bank fraud, and credit card fraud are a few of the categories of fraud that often involve using someone else's identifying information (e.g. Social Security number and account or credit card numbers) to perpetrate the crime.

1. Healthcare Fraud

The DOJ estimates that healthcare fraud alone generates tens of billions of dollars of illicit proceeds each year and "some estimates put the figure close to $100 billion a year."[12] The high daily volume of health care claims makes fraud detection a challenge. Medicare processes more than 4.5 million claims each day.[13] The often high cost of pharmaceuticals and medical devices and services can make large financial transactions seem ordinary and impede the discovery of crime.

Healthcare fraud schemes can be complex and involve complicit doctors and other medical professionals, so the money flows can mimic legitimate transactions from insurers to healthcare providers. In some cases, the fraudulent reimbursement claims are filed with insurers using stolen identities. Information can be stolen by healthcare professionals and resold on the black market, or may be stolen by hackers accessing medical databases.[14] In 2018, in the largest healthcare fraud enforcement action in DOJ's history, over 602 defendants, including 165 doctors, nurses, and other licensed medical professionals were charged in related healthcare fraud schemes involving more than $2 billion.[15]

---

[12] DOJ, Health Care Fraud Unit, available at https://www.justice.gov/criminal-fraud/health-care-fraud-unit.

[13] National Healthcare Anti-Fraud Association, The U.S. Health Care System and the Challenges of Fraud, September 2017, available at https://www.nhcaa.org/media/127538/nhcaa_ushealthcaresystem_2017.pdf; Medicare provides health insurance to people age 65 and older, as well as younger people with disabilities and certain diseases. Medicaid provides health insurance to low-income people. TRICARE is a health insurance program for members and veterans of the armed forces and their families.

[14] Medical Identity Theft, Coalition against Financial Fraud, available at http://www.insurancefraud.org/scam-alerts-medical-id-theft.htm#.UyXbF6hdWSo.

[15] DOJ, Press Release, "National Health Care Fraud Takedown Results in Charges Against 601 Individuals Responsible for Over $2 Billion in Fraud Losses", June 28, 2018, available at

A 2016 review by FinCEN of Supicious Activity Reports (SARs) noted certain activities by healthcare providers that were considered suspicious, including the healthcare principals using insurance payments for personal rather than professional purposes, or quickly moving (i.e., layering) insurance payments through accounts at the same or other financial institutions using various means to transfer the funds including cash withdrawals and deposits. See Table 1 below for a list of the types of healthcare providers most often cited in SARs reporting suspicion of healthcare fraud.

Table 1 – Top Ten Categories of Healthcare Professionals and Others Cited in SARs Marked by Filers as Indicating Potential Healthcare Fraud in a Study Sample (2016)[16]

Provider Type	Filing Count	Percentage of Healthcare Provider Types
Home Healthcare	123	12%
Doctor	95	10%
Pharmacist	72	7%
Assisted Living	38	4%
Chiropractor	35	4%
Radiologist	27	3%
Medical Supplies	23	2%
Rehabilitative Services	22	2%
Personal Fraud	267	27%
All Others	281	28%

State and federal authorities note that insurance payments to doctors and other healthcare professionals are typically made by check. Depending on the perpetrator of the fraud, insurance checks may be cashed at banks where the perpetrator holds an account. The account may be held in the name of a licensed medical professional or healthcare practice, or it may be held in the name of a shell company. Checks may also be cashed at a storefront check-cashing outlet, some of which have been found to be complicit in healthcare fraud. According to DOJ, even in states that require check cashers to verify and maintain customer identification records, complicit check cashers may knowingly record false customer identification so that their records will appear to be in order during on-site compliance examinations by state regulators.

2. Tax Refund Fraud

The IRS reports progress in combating tax refund fraud, which often involves the use of stolen identities to claim fraudulent tax refunds. Overall during the 2015-2017 period, the number of confirmed identity theft tax returns fell by 57 percent with more than $20 billion in taxpayer

https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-601-individuals-responsible-over.

[16] The provider type identified in the chart as "personal fraud" refers to situations in which individuals are suspected of hiding monetary assets in order to qualify for Medicaid coverage.

refunds being protected.[17] Tax refund fraud is typically not a sophisticated crime, but the volume of tax returns filed each year can make it difficult to identify fraudulent returns during processing. Almost 250 million tax returns were processed in fiscal year 2016.[18]

Fraudulent filers who use stolen identification to claim a tax refund may receive payment via prepaid card, paper check, or direct deposit to a U.S. bank account. Check cashers who knowingly cash IRS refund checks for individuals who are not the named beneficiaries have been prosecuted for money laundering. Criminals may also open bank accounts using false identification or the legitimate identifying information of witting accomplices or unwitting third parties, and then use these accounts to receive tax refunds.

IRS-CI has seen an evolution of organized crime groups acquiring, selling, and using stolen identities. In addition to tax refund fraud, stolen identities are used to facilitate other forms of fraud.

3. Cybercrime

In 2016, the FBI's Internet Crime Complaint Center (IC3) received 298,728 complaints from the public citing suspected criminal activity facilitated by the internet, with self-reported losses of more than $1.3 billion.[19] IC3 submits the information it receives to the FBI for investigation and compiles data and analytical reports. The complaints received by IC3 are likely only a fraction of the cybercrime occurring in the United States. For example, DOJ estimates only 15 percent of the nation's fraud victims, more broadly, report their crimes to law enforcement.[20]

Based on the complaints filed with IC3, the cyber-enabled crimes generating the largest losses were Business E-mail Compromise (BEC) and romance and confidence schemes (see Table 2). BEC involves criminals accessing business email accounts through hacking or social engineering[21], targeting employees with access to company finances in order to trick them into making wire transfers to bank accounts thought to belong to trusted partners. [22] According to the FBI, BEC is carried out by transnational criminal organizations that employ lawyers, linguists, hackers, and social engineers.[23]

---

[17] IRS, Press Release, February 8, 2018, available at https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft; Written Testimony of John A. Koskinen Before the Senate Finance Committee on the 2017 Filing Season and IRS Operations, April 6, 2017, available at https://www.irs.gov/newsroom/written-testimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operations-april-6-2017.

[18] IRS, Fiscal Year Return Projections for the United States: 2017–2024 (Publication 6292), available at https://www.irs.gov/pub/irs-soi/p6292.pdf.

[19] FBI, 2016 Internet Crime Report, available at https://pdf.ic3.gov/2016_IC3Report.pdf.

[20] DOJ, Financial Fraud Crime Victims, available at https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud.

[21] Social engineering is a non-technical technique that cybercriminals use to manipulate victims, using information or trust-building tactics, to convince the victim to share information or take/not take certain actions. For example, social engineering could be used by a hacker to persuade a victim to provide a password or identifying information.

[22] FinCEN Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes, FIN-2016-A003, September 06, 2016, available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003.

[23] FBI, Press Release, "Business E-Mail Compromise," available at https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise.

Victims of romance and confidence schemes are sometimes recruited by the perpetrators of the fraud to act as "money mules" to help launder stolen funds. According to the FBI, cyber criminals exploit three distinct groups of individuals when targeting victims and/or mules: people seeking companionship, job seekers looking for legitimate income, and job seekers looking for off-the-books income. Individuals victimized by fraudulent romance schemes are typically unaware that they are facilitating money laundering when they comply with requests to receive and forward funds which are actually illicit proceeds stolen from other victims. Similarly, individuals recruited online who are seeking employment can be exploited to receive and transfer illicit funds, believing their actions to be the function of a legitimate job. In some cases, individuals are recruited who either know they are facilitating illegal activity or choose not to ask.

In a 2016 FBI investigation, a romance fraud victim was convinced by the person he was corresponding with to open a bank account in order to receive funds transfers and then wire the money out as directed to other U.S. accounts and to an individual in Nigeria. The funds wired into the money mule's account came from the account of a company that had been the victim of a business e-mail compromise.

Table 2 – Select Reported Losses by Internet enabled Crime Type

IC3 Data for 2016		
Crime Type	**Reported Losses**	**Reported Victims**
Business and personal e-mail compromise	$360,513,961	12,005
Confidence fraud/romance schemes	$219,807,760	14,546
Employment schemes	$40,517,605	17,387
Phishing/vishing/smishing/pharming[24]	$31,679,451	19,465
Total	**$652,518,777**	**63,403**

Source: 2016 Internet Crime Report, https://pdf.ic3.gov/2016_IC3Report.pdf

Cyber criminals' use of money mules complicates law enforcement investigations by placing at the center of the money laundering activity individuals who know little or nothing of the underlying predicate activity and may, in fact, be victims themselves unaware they have been exploited. Determining whether a money mule is witting or unwitting can be a challenge.

B. DRUG TRAFFICKING

Estimating the size of the illegal drug market in the United States is difficult due to the lack of reliable data. The United Nations Office of Drugs and Crime (UNODC) calculated illicit drug

[24] These terms generally refer to the use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, or login credentials, or a combination of the three. For an overview of the myriad tactics used by cybercriminals, see https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud.

proceeds in the United States to be $64 billion in 2010.[25] However, another study using a different analytical model put the figure at $100 billion for the same period.[26] The 2015 NMLRA used the UNODC estimate of $64 billion. However, the illicit drug market has changed significantly since then with the increase in domestic marijuana production following legalization or reduction in penalties in many states, a rebound in cocaine sales, growth in the sale of heroin and synthetic opioids, an expanding market for methamphetamine, and the persistent creation, and sale of new synthetic psychoactive substances.[27] Given these market dynamics, the 2018 NMLRA is using $100 billion figure as a rough estimate of illicit drug proceeds in the U.S.

While much of the money generated in the United States from illegal drug retail sales stays in the U.S., money generated by wholesalers or larger transnational drug trafficking organizations leaves the United States. As noted in the 2015 NMLRA, as much as 70 percent of the revenue generated by cocaine is earned by mid-level wholesalers and retail dealers.[28] The drug money that leaves the United States typically flows to Colombia and Mexico, with Central American countries serving as transit points and intermediate money laundering hubs. Money laundering networks with ties to illegal drug sales in the United States operate out of Mexico, Venezuela, Guatemala, Colombia, Honduras, and Panama.

Money movement and laundering methods associated with drug trafficking continue to include bulk cash smuggling, which involves moving currency illicitly into or out of the country; TBML, which most often involves using illicit proceeds to buy goods for export, as the subsequent sale of the goods effectively launders the proceeds; misuse of financial services providers, by disguising the identity of the customer and/or the nature of the business relationship; and virtual currencies and other alternative payment methods, which can often be used anonymously. According to the DEA and HSI, bitcoin and other virtual currencies are used by individuals in the United States to pay for illegal drugs sold online. Virtual currencies are also being used by money launderers in the layering phase to transfer illicit proceeds internationally. Drug trafficking organizations use a variety of methods to move and launder illicit proceeds, but some drugs are associated with particular money laundering methods as noted below.

1. Marijuana

Marijuana remains the most commonly used illicit drug in the United States, yet marijuana-related arrests have declined since 2010 likely due to state-level decriminalization. Marijuana is illicitly cultivated in all 50 states, but Mexico remains the most significant foreign source for marijuana, and Mexican cartels control some of the cultivation in the United States. Marijuana at the retail level is typically a cash business. Traffickers use all available methods to move

[25] United Nations Office on Drugs and Crime, *Estimating Illicit Financial Flows Resulting From Drug Trafficking and other Transnational Organized Crimes,* October 2011, available at http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf .
[26] *What America's Users Spend on Illegal Drugs: 2000-2010*, prepared for the Office of National Drug Control Policy by the RAND Corporation, available at https://www.rand.org/pubs/research_reports/RR534.html.
[27] 2017 DEA National Drug Threat Assessment, available at https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf ; https://www.ice.gov/sites/default/files/documents/Speech/2017/170216allen.pdf.
[28] United Nations Office on Drugs and Crime, Globalization of Crime, 2010.

and/or launder marijuana proceeds, including bulk cash smuggling, TBML, and transfers via banks and MSBs.

2. Cocaine

Cocaine use in the United States increased between 2015 and 2016, according to DEA, and is likely to continue increasing due to growing cocaine production in Colombia, the primary source for cocaine seized and tested in the United States.[29] Mexican drug trafficking organizations dominate cocaine transportation throughout the United States. Retail-level distribution is carried out by local U.S. criminal groups and street gangs. DEA estimates that roughly $5 billion to $10 billion in cocaine proceeds are laundered back into Colombia each year.

3. Heroin and Synthetic Opioids

The abuse of controlled prescription drugs, heroin, and synthetic opioids such as fentanyl and fentanyl analogues, has spiked dramatically, according to DEA. Fentanyl is a licit synthetic opioid produced in the United States for use as a pain medication. Illicit fentanyl, fentanyl analogues, and their immediate precursors are generally produced in China, can be purchased online, and shipped directly to individual buyers in the United States or shipped to criminal organizations in Mexico, Canada, and the Caribbean for distribution in the United States. According to ICE-HSI, seizures of illicit fentanyl and other synthetic opioids at international mail facilities have increased over the last few years. Fentanyl is incredibly potent, and because it is relatively inexpensive to produce and the retail price is very high, fentanyl may be the most lucrative, efficient drug that cartels are selling.

FinCEN analysis of SARs has found indications that U.S.-based individuals buying fentanyl and fentanyl analogues online or importing the drug or its precursors from China and elsewhere are more likely to wire payments via a money transmitter than a bank. Mexican cartels coordinating fentanyl sales and distribution in the United States are more likely to generate illicit proceeds as cash from street sales. When the cash enters the banking system it becomes subject to detection, as banks monitor for suspicious activity, such as structured cash deposits and funnel accounts, among other things. Funnel accounts are used to accept cash deposits from bank branches around the country; the controllers of such accounts quickly dispose of the funds, transmitting them to Mexico or withdrawing them again in cash near the southwest border in order to smuggle them into Mexico.

Mexican cartels also use TBML to launder drug cash. Law enforcement notes the increasing prevalence of Chinese money laundering networks working with Mexican drug traffickers. These networks may use a combination of bulk cash smuggling, bank deposits in cash, wire transfers, and transactions through Mexican exchange houses to facilitate the ultimate receipt of pesos by Mexico-based traffickers.

[29] 2017 DEA National Drug Threat Assessment.

4. Methamphetamine

Most of the methamphetamine available in the United States is produced in Mexico and smuggled across the southwest border.[30] According to DEA, methamphetamine production laboratories had been on the rise in the United States, but aggressive enforcement and restrictions on the sale of precursor chemicals led to a decrease since 2004.[31] The passage of the Combatting Methamphetamine Epidemic Act of 2005 in the United States and the enforcement crackdown on laboratories manufacturing the drug pushed the production into Mexico. Mexican drug cartels are now overproducing high-purity methamphetamine, leading to record low prices. The cartels are attempting to boost demand and increase the price by expanding the methamphetamine market to the East Coast of the U.S.to bring the drug to new users. Mexican producers have to rely on Chinese sources for precursor chemicals, transited through Central America or Mexican ports, but are working on synthesizing the chemicals themselves. Methamphetamine is a cash business and methods of moving/laundering cash proceeds to Mexico to pay traffickers and acquire additional supply use the same methods cited for other illicit drugs sourced from Mexico, including bulk cash smuggling, structured cash deposits, funnel accounts, bank wires, and TBML. Domestic retail traffickers launder proceeds using cash, money orders, and structured bank deposits. In one recent case a methamphetamine trafficker also used casino slot machines to launder methamphetamine proceeds.[32] Methamphetamine and cash linked to its purchase and sale are often shipped directly through the mail or package delivery services, including by persons using aliases and fake/stolen identity documents.

5. Synthetic Psychoactive Drugs

Synthetic psychoactive drugs, such as MDMA (ecstasy) and synthetic cannabis, are created in laboratories. Each variety requires different precursor chemicals and scientific processes, and the drug formulas change to stay ahead of U.S. law.[33] According to DEA, most traffickers in the United States buy synthetic psychoactive drugs from suppliers in China, and to a lesser extent, India and parts of Europe. Payment is often made by money transmitter or virtual currency with the drugs delivered through the United States Postal Service or a package delivery service. These drugs are relatively inexpensive and are widely available online and on the street.

[30] 2017 DEA National Drug Threat Assessment.
[31] 2017 DEA Domestic Methamphetamine Threat Assessment Key Findings, available at https://www.dea.gov/ops/2017%20Domestic%20Methamphetamine%20Threat%20Assessment%20Key%20Findings.pdf.
[32] USA vs Patrick R. Brigaudin, U.S. District Court for the Western District of Missouri, Southern Division, United States' Motion for Pretrial Detention, Case 6:16-cr-03039-MDH, Filed 03/02/16. Brigaudin pleaded guilty to conspiracy to distribute methamphetamine and money laundering.
[33] Title 21 of the United States Code, the Controlled Substances Act, places substances regulated under federal law into one of five schedules based on the substance's medical use and potential for abuse. Activities related to such substances, such as production and distribution are criminalized.

C. HUMAN SMUGGLING

Human smuggling involves illegally transporting people, who have consented to their travel, into the United States and, potentially, the subsequent harboring of those individuals in the U.S. According to DHS OIS, increased border security has driven up the fees paid to smugglers to get migrants across the southwest border.[34] Interviews with migrants conducted by the U.S. Border Patrol (USBP) found that smuggling fees are often paid in stages, with initial fees required to approach staging locations along the southwest border and then a final payment at the destination. Smuggling fees for Mexicans and Central Americans reportedly have been as high as $1,200 for the initial staging payment and up to $8,000 at the final destination, but DHS OIS finds the average fee is approximately $4,000.

Payment is made to smugglers in a variety of ways depending on who is paying, the migrant being smuggled across the border or family members in the United States. SARs filed following FinCEN's 2014 human smuggling advisory frequently cite cash deposits into bank accounts or cash transfers through MSBs near the U.S.-Mexico border.[35] The bank deposits often involve suspected funnel account activity. In addition to cash and wires, USBP interviews with migrants found an increase in alternative forms of payment, including migrants being required to participate in smuggling controlled substances or other illicit items across the border or to work off debts upon arrival in the United States, as well as reports of harsh negotiations concerning payment plans with family members.

D. HUMAN TRAFFICKING

Human trafficking is exploitation of non-consenting persons, often across borders, which involves force, fraud, or coercion to recruit individuals to provide labor or services, including prostitution which may be prosecuted as sex trafficking. HSI estimates that human trafficking generates $32 billion annually.[36] The illicit finances involved with human trafficking are difficult to discern, as they can include profits made by the traffickers, payments made to bring them from one place to another, outlays for logistics, and then the proceeds generated by the further exploitation of the trafficking victim. For example, according to one study, cash is the most common form of payment in the underground commercial sex economy although credit and prepaid cards are also accepted.[37] DOJ, in announcing charges against a U.S. based online advertising website accused of facilitating prostitution and money laundering, stated that the site

---

[34] DHS, Office of Immigration Statistics, *Efforts by DHS to Estimate Southwest Border Security between Ports of Entry*, September 2017, available at https://www.dhs.gov/sites/default/files/publications/17_0914_estimates-of-border-security.pdf.

[35] FinCEN Advisory to Financial Institutions on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking — Financial Red Flags, FIN-2014-A008, September 11, 2014, available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a008.

[36] ICE, Press Release, "Using a financial attack strategy to combat human trafficking", January 29, 2015, available at https://www.ice.gov/news/releases/using-financial-attack-strategy-combat-human-trafficking.

[37] Estimating the Size and Structure of the Underground Commercial Sex Economy in Eight Major US Cities, Urban Institute, March 2014, available at https://www.urban.org/sites/default/files/alfresco/publication-pdfs/413047-Estimating-the-Size-and-Structure-of-the-Underground-Commercial-Sex-Economy-in-Eight-Major-US-Cities.PDF.

facilitated human trafficking.[38] According to a plea agreement of the website's co-founder, the site accepted credit cards and virtual currency, but had to misrepresent the nature of the business to the credit card companies and route the card payments through shell companies.[39]

E. CORRUPTION

Public corruption investigations encompass bribery, extortion, embezzlement, illegal kickbacks, and money laundering and can involve local, county, state, federal, and foreign officials. Even when the person paying the bribe is not a U.S. person, and the recipient is not a U.S. official, the conduct may violate federal laws, particularly the money laundering statutes if the proceeds are laundered through the U.S. financial system, and the Foreign Corrupt Practices Act.

IRS-CI, which focuses on the tax and money laundering aspects of corruption investigations working alongside the FBI and other law enforcement agencies, opened an average of 86 corruption-related investigations annually from FY 2014 to FY 2016.[40] According to DOJ, some corruption cases involve the laundering of assets worth billions of dollars and typically involve the use of shell companies and the help of lawyers and other professionals to arrange the purchase of real estate and luxury goods. As of January 2018, DOJ's Kleptocracy Asset Recovery Initiative had seized or restrained $3.5 billion worth of corruption proceeds.[41] In a single DOJ case currently under litigation, the amount at issue and alleged to be stolen through crimes related to a foreign jurisdiction's sovereign wealth fund is $4.5 billion.[42] In addition, DOJ has imposed fines, penalties, and forfeitures of more than $2 billion in foreign corruption cases in 2016 and 2017 alone.[43] The proceeds of purely domestic corruption offenses should not be minimized, but offenses involving foreign corruption can have a significant, negative impact on the U.S. financial system, including possibly skewing markets. By some estimates, the proceeds of corruption equal two percent of U.S. gross domestic product. The proliferation of corruption abroad can destabilize countries—creating economic and human rights refugees—waste U.S. aid and other financial support from donors, and pose national security challenges to the United States.

---

[38] DOJ, Press Release, "Backpage's Co-founder and CEO, As Well As Several Backpage-Related Corporate Entities, Enter Guilty Pleas", April 12, 2018, available at https://www.justice.gov/opa/pr/backpage-s-co-founder-and-ceo-well-several-backpage-related-corporate-entities-enter-guilty.

[39] United States v. Carl Allen Ferrer, CR-18-464-PHX-DJH (Plea Agreement), available at https://www.justice.gov/opa/press-release/file/1052531/download.

[40] IRS, Statistical Data - Public Corruption Investigations, available at https://www.irs.gov/compliance/criminal-investigation/statistical-data-public-corruption-investigations.

[41] M. Kendall Day, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Testimony before the Senate Committee on Banking, Housing, and Urban Affairs, January 17, 2018, available at https://www.banking.senate.gov/imo/media/doc/Day%20Testimony%201-17-18.pdf.

[42] DOJ, Press Release, "U.S. Seeks to Recover approximately $540 Million Obtained From Corruption Involving Malaysian Sovereign Wealth Fund", June 15, 2017, available at https://www.justice.gov/opa/pr/us-seeks-recover-approximately-540-million-obtained-corruption-involving-malaysian-sovereign.

[43] DOJ, Fraud Section Year in Review 2016, available at https://www.justice.gov/criminal-fraud/page/file/929741/download; DOJ, Fraud Section Year in Review 2017, available at https://www.justice.gov/criminal-fraud/file/1026996/download.

F. TRANSNATIONAL CRIMINAL ORGANIZATIONS

A number of Transnational Criminal Organizations (TCOs)[44] operate in the United States. Mexican and Russian TCOs operating in the U.S. remain priority threats, with African and Asian organizations becoming more significant each year. Drug cartels in Colombia, Peru, and throughout Central America also operate as independent TCOs.

1. African TCOs

According to the FBI, Nigerian criminal enterprises are the most significant of the African TCOs.[45] They are primarily engaged in drug trafficking and financial fraud, including business e-mail compromise schemes and various confidence scams in the United States. They commonly use money mule networks to launder proceeds. In a 2017 case that involved tens of millions of dollars in fraud proceeds, unsuspecting victims of online romance scams cashed counterfeit checks and money orders on behalf of the perpetrators and sent them the proceeds by non-bank wire transfers, and received and re-shipped merchandise purchased with stolen credit card numbers.[46]

2. Asian TCOs

According DEA's 2017 National Drug Threat Assessment (NDTA), Asian organized crime groups in the United States are prominent in money laundering for Mexican, Colombian, and Dominican drug trafficking organizations.[47] Money laundering tactics vary by organization with some using cash-intensive businesses in the United States to move drug proceeds into the financial system for laundering. Generally, Asian TCOs transfer funds to and from China and Hong Kong, using front companies as part of their international money movement schemes. Law enforcement agencies have reported interconnectivity between Chinese money laundering organizations and Mexican drug cartels.

According to the FBI, Asian TCOs also conduct traditional racketeering activities normally associated with organized crime—extortion, murder, kidnapping, illegal gambling, prostitution, and loansharking. They also smuggle persons; traffic heroin and methamphetamine; commit financial frauds; steal autos and computer chips; counterfeit electronics and clothing products; as well as money laundering.[48]

---

[44] Congress has defined the term "transnational organized crime" to refer self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary, or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption or violence or through a transnational organization structure and the exploitation of transnational commerce or communication mechanisms. See 10 U.S.C. § 284(i)(6).

[45] FBI, Transnational Organized Crime, available at https://www.fbi.gov/investigate/organized-crime.

[46] DOJ, Press Release, "Three Nigerians Sentenced in International Cyber Financial Fraud Scheme", May 25, 2017, available at https://www.justice.gov/opa/pr/three-nigerians-sentenced-international-cyber-financial-fraud-scheme.

[47] DEA, 2017 National Drug Threat Assessment.

[48] FBI, Transnational Organized Crime, available at https://www.fbi.gov/investigate/organized-crime.

3. Mexican and Colombian TCOs

Mexican TCOs dominate the U.S. drug trade and associated money movement. DEA investigations show that six major Mexican drug cartels maintain drug distribution cells in cities across the United States.[49] It is anticipated that Mexican TCOs will continue to grow in the United States through the expansion of distribution networks and relationships with intermediaries, such as U.S.-based Dominican traffickers and local gangs.

Colombian TCOs dominate the production and supply of the majority of cocaine shipped to U.S. markets. Colombian TCOs rely on their partnership with Mexican TCOs for the sale and distribution of wholesale quantities of cocaine and heroin in the United States. Smaller Colombian TCOs maintain direct cocaine and heroin routes into the United States through couriers and air cargo on commercial flights. Colombian TCOs also maintain a physical presence in the United States to facilitate the laundering of illicit proceeds.

The groups rely on bulk cash smuggling, TBML, and transactions conducted through financial institutions[50] to move their illicit proceeds. Professional money launderers can provide worldwide services to facilitate the movement of billions of dollars on behalf of both Mexican and Colombian cartels.[51]

On February 9, 2017, President Donald J. Trump issued Executive Order 13773, which directed the federal government to "ensure that Federal law enforcement agencies give a high priority and devote sufficient resources to efforts to identify, interdict, disrupt, and dismantle transnational criminal organizations[.]" It directs federal agencies to make combating TCOs a priority line of effort, develop new strategies to counter TCOs, and increase information sharing and international partnership efforts. The Attorney General also established an interagency Transnational Organized Crime Task Force in October 2018 and has designated the following criminal groups as top transnational organized crime threats: MS-1; Cartel de Jalisco Nueva Generacion (CJNG); Sinaloa Cartel; Clan del Golfo, and Lebanese Hezbollah.

4. Eurasian TCOs

According to the FBI, Eurasian TCOs engage in a wide range of criminal activity and have caused hundreds of millions of dollars in losses to U.S. businesses and investors.[52] The roots of Eurasian organized crime in the United States lie with the Vory V Zakone, or "Thieves-in-Law." The Thieves-in-Law is a global criminal organization, active in the United States. Based on SAR analysis, FinCEN has determined that Russian organized crime groups in the United States

[49] Sinaloa Cartel, Jalisco New Generation Cartel (Cartel Jalisco Nueva Generación, or CJNG), Juarez Cartel, Gulf Cartel, Los Zetas Cartel, and Beltran-Leyva Organization.
[50] In a four-year period, as a result of AML failures at just one financial institution with global operations, at least $881 million in drug trafficking proceeds—including proceeds of drug trafficking by the Sinaloa Cartel in Mexico and the Norte del Valle Cartel in Colombia—were laundered. See https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations.
[51] DOJ, Press Release, "Three Members Of International Organization Of Money Launderers For The Largest Drug Cartels Arrested", September 10, 2015, available at https://www.justice.gov/usao-edny/pr/three-members-international-organization-money-launderers-largest-drug-cartels-arrested.
[52] FBI, Transnational Organized Crime, available at https://www.fbi.gov/investigate/organized-crime.

engage in a variety of crimes including, illegal gambling, money laundering, and various types of fraud. SARs indicate suspicions of money laundering activity involving cross-border wires from bank accounts held by shell companies and TBML involving auto sales. In December 2017 OFAC designated the Thieves-in-Law, along with 10 individuals and two entities, pursuant to Executive Order 13581, which targets significant groups and their supporters.[53]

In 2017, DOJ settled a money laundering and civil forfeiture action associated with a $230 million tax refund fraud scheme committed by Russian organized crime against the Russian treasury. In a complex series of transactions, the $230 million was laundered through bank accounts in Russia and other countries, with a portion of the funds used to buy real estate in Manhattan.[54] The company accused of laundering the fraud proceeds agreed to pay $5.9 million.

[53] Treasury, Press Release, "Treasury Targets the "Thieves-in-Law" Eurasian Transnational Criminal Organization", December 22, 2017, available at https://home.treasury.gov/news/press-releases/sm0244.
[54] DOJ, Press Release, May 12, 2017, available at https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-59-million-settlement-civil-money-laundering-and.

SECTION 2. VULNERABILITIES AND RISKS

In the context of the 2018 NMLRA, a money laundering vulnerability is what facilitates or creates the opportunity for money laundering. Risk is a function of threat and vulnerability. It represents a summary judgment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement.

Vulnerabilities may relate to a specific financial sector or product or a weakness in regulation, supervision, or enforcement. It may also reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity. The methods that allow for the most amount of money to be laundered most effectively or most quickly present the greatest potential vulnerabilities.

Money launderers attempt to identify and exploit vulnerabilities, given the nature, location and form of their illicit proceeds. Money laundering methods shift and evolve in response to opportunities and changes in financial services, regulation, and enforcement.

A. CASH

U.S. currency remains a significant money laundering vulnerability because its use is often anonymous, despite reporting requirements for financial institutions, individuals, and persons engaged in a trade or business.[55] The Federal Reserve Board (FRB) estimates that between one-half and two-thirds of the value of all U.S. currency in circulation is held abroad.[56] This widespread use of U.S. currency internationally makes it difficult for authorities to know when someone is accumulating illicit cash or merely attempting to protect their life savings. Although identifying the illicit use of currency is difficult, the required reporting domestically, including SARs, provides FinCEN and law enforcement with useful indicators for criminal investigations and trend analysis.

1. Bulk Cash Smuggling

According to DEA, bulk cash smuggling remains one of the main methods Mexican drug cartels use to move illicit drug proceeds across the U.S. southwest border to Mexico. Bulk cash smuggling is used to move money into and out of the United States. The statute that governs bulk cash smuggling does require proof that a suspect intended to cross the border. However,

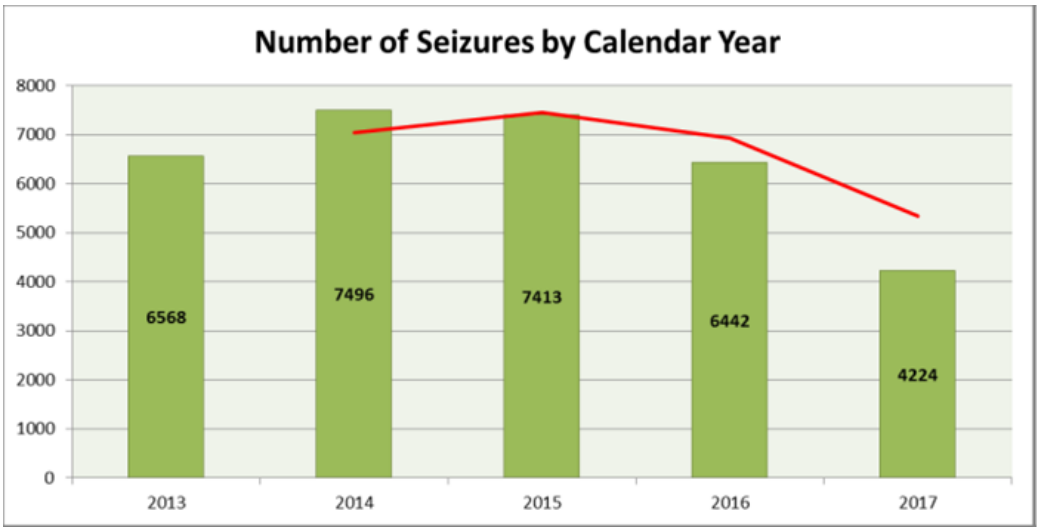
[55] A Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300) must be filed by each person engaged in a trade or business who, in the course of that trade or business, receives more than $10,000 in cash in one transaction or in two or more related transactions. A Currency Transaction Report must be filed by each financial institution for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction in currency of more than $10,000. A Report of International Transportation of Currency or Monetary Instruments must be filed by (1) Each person who physically transports, mails, or ships, or causes to be physically transported, mailed, or shipped currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside the United States or into the United States from any place outside the United States, and (2) Each person who receives in the United States currency or other monetary instruments In an aggregate amount exceeding $10,000 at one time which have been transported, mailed, or shipped to the person from any place outside the United States.

[56] Federal Reserve, available at https://www.federalreserve.gov/paymentsystems/coin_about.htm.

criminal organizations rely on complex transportation and smuggling networks to move and launder their illicit proceeds. Criminals frequently consolidate proceeds within the United States as an intermediary step to moving the cash out of the country. Retail drug traffickers and mid-level drug wholesalers operating within the United States retain most of their proceeds within the U.S., sending to the Mexican TCOs the amount needed to pay for their drug shipments. Additionally, as Mexican TCOs increasingly control more of the drug distribution network in the United States, they are able to claim a larger portion of the drug proceeds in the U.S.

Since 2013 there has been a steady decrease in the number of bulk cash seizures throughout the United States reported to the ICE-HSI National Bulk Cash Smuggling Center (see Table 3). This correlates with a decrease in the gross amount seized from an estimated $780 million in 2014 to $324 million in 2017 (see Table 4). The decrease in seizures could indicate that TCOs are increasing their use of other, more discreet, methods of moving illicit money such as TBML, or it could indicate that law enforcement is targeting other money laundering activities away from the borders. Nonetheless, in FY 2016, ICE-HSI arrested 575 individuals and seized more than $66.3 million associated with bulk cash smuggling.[57]

Table 3: **Bulk Currency Seizures, 2013 – 2017**



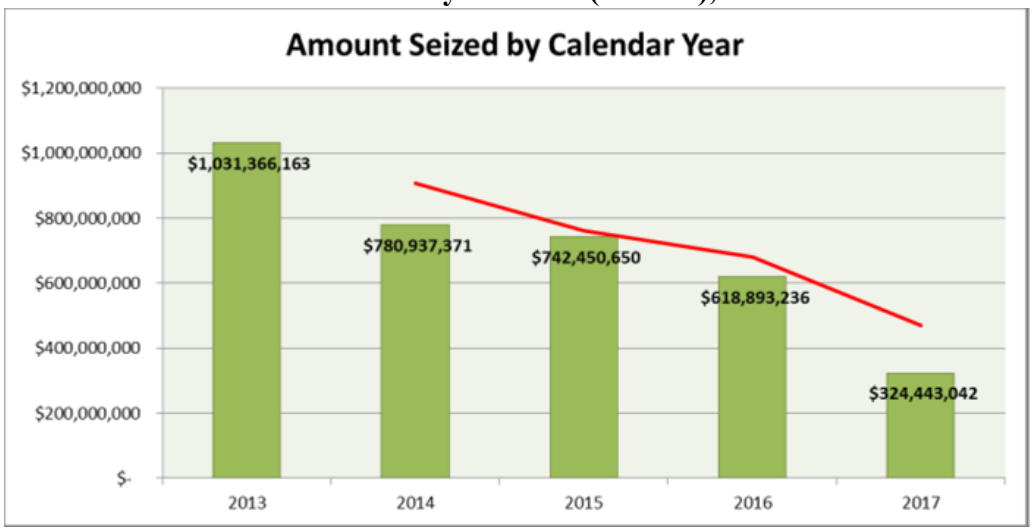
Source: ICE-HSI National Bulk Cash Smuggling Center

FinCEN issued a Geographic Targeting Order (GTO)[58] that modified the Report of International Transportation of Currency or Monetary Instruments (CMIR) requirements for armored car services in the San Diego area between August 2014 and February 2016, which, according to FinCEN analysis, appeared to show that certain armored car companies were knowingly involved in money laundering through their delivery of cash from Mexico to U.S. financial

[57] ICE, National Bulk Cash Smuggling Center, available at https://www.ice.gov/bulk-cash-smuggling-center.
[58] The Director of FinCEN may issue an order that imposes certain additional recordkeeping and reporting requirements on one or more domestic financial institutions or nonfinancial trades or businesses in a geographic area. These orders are known as Geographic Targeting Orders.

institutions.[59] Law enforcement information and financial institution reports to FinCEN suggest that much of this cash was not properly reported on CMIRs, indicating that armored car services and other common carriers of currency were misusing regulatory exemptions and filing incomplete or inaccurate reports.

Table 4: **Bulk Currency Seizures (in USD), 2013 – 2017.**



Source: ICE-HSI National Bulk Cash Smuggling Center

Case examples:

- In December 2017 in New York a flight attendant was charged with operating as an unlicensed money transmitter. The flight attendant had not declared more than $50,000 in cash found in his carry-on bag. According to ICE HSI, the flight attendant had been regularly shuttling cash illegally from New York to California.[60]
- In September 2017, in Texas, a married couple was sentenced for running a drug trafficking and money laundering organization that received marijuana shipments from Mexico for distribution in the Dallas area. They used couriers driving both personal vehicles and tractor trailers to transport the cash proceeds from the marijuana sales back to Mexico.[61]
- In August 2017, in Indiana, Pierre Burnett Jr. was sentenced for drug trafficking and money laundering. Burnett bought wholesale quantities of heroin and cocaine paying cash to Mexican suppliers who delivered the drugs in the U.S. and then smuggled the

[59] FinCEN, Press Release, August 1, 2014, available at https://www.fincen.gov/news/news-releases/fincen-and-mexican-counterpart-shine-spotlight-cross-border-cash-couriers. In 2010, Mexico established limits on the deposit of U.S. currency in Mexican financial institutions, which resulted in an increase in cash coming back to the United States from Mexico, via armored car and courier services for attempted placement in U.S. financial institutions. In 2014, in response, FinCEN issued guidance clarifying the circumstances under which the narrow exemption to the CMIR filing requirements apply and a ruling that determined that certain armored car activity would be considered as MSB activity.

[60] ICE, Press Release, December 19, 2017, available at https://www.ice.gov/news/releases/flight-attendant-charged-federal-court-airport-security-violations.

[61] DOJ, Press Release, December 20, 2017, available at https://www.justice.gov/usao-sdtx/pr/operation-trena-sin-trono-sends-leader-and-final-defendants-prison.

cash back to Mexico. Burnett sold the drugs to retail distributors for cash. The retail distributors sold the drugs online via the dark web with buyers paying in Bitcoin. The retail distributors sold the Bitcoin online receiving cash, which was sent to them through the U.S. Postal Service, or they were paid via a bank wire transfer.[62]

2. Structuring

Title 31, United States Code, section 5324(a) prohibits the evasion of certain currency transaction reporting and record-keeping requirements, including structuring schemes.[63] Generally speaking, structuring occurs when, instead of conducting a single transaction in currency in an amount that would require a report to be filed or record made by a domestic financial institution, the violator conducts a series of currency transactions, keeping each individual transaction at an amount below applicable thresholds to evade reporting or recording.[64] While this may effectively evade currency transaction report (CTR) or customer identification triggers, it does not always; sometimes, the financial institution may file a SAR in addition to the CTR. Both forms, and customer identification records, are used by law enforcement authorities to uncover a broad range of illegal activities including money laundering

Case examples:

- In November 2017, in New Mexico, two individuals were sentenced for healthcare fraud and aggravated structuring offences. The defendants submitted fraudulent reimbursement claims to Arizona's state Medicaid agency on behalf of their transportation company for providing non-emergency medical transportation to Arizona Medicaid recipients. They collected almost $2 million over two years, submitting more than 18,000 claims. Defendant Rosita Toledo was charged with aggravated structuring for conducting financial transactions involving the proceeds of the health care fraud in a manner that avoided the filing CTRs. From August 2011 to July 2013, the defendant conducted at least 200 cash withdrawals, each for several thousands of dollars but less than $10,000 and totaling at least $800,000, to avoid the filing of CTRs.[65]
- In 2015, in Las Vegas, Damien Williams was sentenced for drug trafficking, money laundering, and identity theft. Williams was selling codeine and marijuana. He used stolen identity information to obtain a Nevada identification card, rent an apartment, obtain a car loan, and open bank accounts. His distributors made structured deposits of approximately $856,000 in drug proceeds into the accounts from other states and

[62] DOJ, Press Release, August 9, 2017, available at https://www.justice.gov/usao-sdin/pr/dark-web-investigation-leads-conviction-indianapolis-drug-trafficker.
[63] 31 U.S.C. § 5324.
[64] CTRs are reports which must be filed by financial institutions on transactions involving more than $10,000 during any business day. Under the so-called aggregation rules, financial institutions must treat multiple transactions as a single transaction if the financial institution has knowledge that (1) they are by or on behalf of the same person, and (2) they result in either currency received (cash in) or currency disbursed (cash out) by the financial institution totaling more than $10,000 during any one business day.
[65] DOJ, Press Release, June 29, 2016, available at https://www.justice.gov/usao-nm/pr/san-juan-county-residents-facing-federal-health-care-fraud-charges, https://www.justice.gov/usao-nm/file/871746/download.

Williams made structured withdrawals to evade the CTR requirements and used them to further his drug trafficking activities.[66]

- In November 2015, a West Virginia man was sentenced to prison for a drug trafficking conspiracy and structuring monetary transactions to evade the reporting requirement.[67] The man was a manager of retail shops where he sold synthetic drugs, the proceeds of which he structured to avoid reporting more than $200,000 to the IRS.

Bank Secrecy Act Structuring Filing by Industry Type, for Calendar Years: 2015—2017[68]

STRUCTURING as SOLE CATEGORY				STRUCTURING as ONE of MULTIPLE CATEGORIES		
Year	Industry Type	Unique Count of BSAID where "Only Structuring" was identified	Total SAR Count	Year	Industry Type	Unique Count of BSAID where "Structuring As Whole or Part" was identified
2015	Casino/Card club	12,090	Unique SARs filed in CY2015 1,812,249	2015	Casino/Card club	20,070
2015	Depository institution	105,008		2015	Depository institution	299,793
2015	Housing GSE	6		2015	Housing GSE	21
2015	Insurance company	809		2015	Insurance company	1,185
2015	Loan or Finance Company	5		2015	Loan or Finance Company	52
2015	Money Services Business (MSB)	137,630		2015	Money Services Business (MSB)	361,995
2015	Other	2,692		2015	Other	7,779
2015	Securities/Futures	726		2015	Securities/Futures	1,386
	TOTAL	258,966			TOTAL	692,281
2016	Casino/Card club	14,665	Unique SARs filed in CY2016 1,975,643	2016	Casino/Card club	24,513
2016	Depository institution	94,776		2016	Depository institution	295,849
2016	Housing GSE	3		2016	Housing GSE	31
2016	Insurance company	579		2016	Insurance company	924
2016	Loan or Finance Company	7		2016	Loan or Finance Company	66
2016	Money Services Business (MSB)	203,274		2016	Money Services Business (MSB)	482,616
2016	Other	2,025		2016	Other	7,397
2016	Securities/Futures	490		2016	Securities/Futures	1,304
	TOTAL	315,819			TOTAL	812,700
2017	Casino/Card club	13,952	Unique SARs filed in CY2017 2,034,411	2017	Casino/Card club	22,652
2017	Depository institution	81,994		2017	Depository institution	278,592
2017	Housing GSE	1		2017	Housing GSE	30
2017	Insurance company	763		2017	Insurance company	1,271
2017	Loan or Finance Company	9		2017	Loan or Finance Company	103
2017	Money Services Business (MSB)	159,922		2017	Money Services Business (MSB)	471,730
2017	Other	6,367		2017	Other	26,972
2017	Securities/Futures	644		2017	Securities/Futures	1,655
	TOTAL	263,652			TOTAL	803,005

3. Funnel Accounts

The term funnel account refers to the use of a single bank account (or multiple bank accounts, at multiple banks) to collect deposits from various locations and individuals. Rather than

[66] IRS, Examples of Money Laundering Investigations, available at https://www.irs.gov/compliance/criminal-investigation/examples-of-money-laundering-investigations-fiscal-year-2016.

[67] DOJ, Press Release, November 10, 2015, available at https://www.justice.gov/usao-ndwv/pr/ohio-man-sentenced-selling-bath-salts-and-synthetic-drugs.

[68] Numbers reflect: 1) Instances where only the Category of Structuring was selected on the filed SAR; and 2) Instances where the Category of Structuring was one of multiple Categories selected on the filed SAR (e.g., Structuring and Fraud). Categories contain multiple suspicious activity options. Hence, if a SAR indicates one or multiple options selected within a Category, that Category is only counted once.

physically transporting the cash across a significant distance, criminals can make a series of deposits of illicit proceeds into one or numerous accounts from different branch locations or shared branches and then withdraw the money elsewhere, potentially across the country and often in a condensed time period.[69] Structuring may also be present in funnel accounts and the persons making the deposits are frequently money mules recruited especially for this purpose.

Law enforcement agencies have seen this activity associated with the movement of drug proceeds from around the country to the southwest border, where the money is withdrawn as cash and smuggled or wired into Mexico. Funnel accounts can also be used to pool the proceeds of a variety of crimes. According to a FinCEN review of SAR filings, human smuggling and human trafficking-related transactions often involved funnel account activity.

Following a FinCEN advisory in 2014,[70] some financial institutions with large branch networks amended their rules to require that individuals making deposits to personal accounts show identification. This may help to diminish the funnel account phenomenon by discouraging deposits by individuals who are not the account holder or authorized to access the account. According to FinCEN, Bank Secrecy Act (BSA) reporting from 2016 and 2017 indicates funnel account activity may be decreasing. Recently, some large banks have further amended their rules to prohibit deposits into another individual's account unless the depositor is also a joint-owner of the account.

Case examples:

- In 2017, in Florida, Benjamin Guerrero-Lantz and a co-defendant were convicted on drug trafficking and money laundering charges.[71] The men sent drug proceeds earned in Florida to an affiliated California-based marijuana trafficking organization. They structured cash deposits into accounts at Florida branches of at least eight banks, with the money withdrawn at branches in California. The group also laundered drug proceeds by buying $500 Western Union money orders and cars which they registered to nominees.
- In 2017, in Minneapolis, 21 people, including ten Thai nationals, were indicted on sex trafficking and money laundering charges. The organization allegedly trafficked women for sexual exploitation from Bangkok to cities across the United States. The organization dealt primarily in cash and engaged in rampant and sophisticated money laundering to promote, redistribute, and conceal illegal profits. Funnel accounts were used to launder and route cash from cities across the U.S. to the money launderers in Los Angeles, where the funds would be withdrawn and either wired to Thailand or transported as bulk cash or through the mail. Upon entry to the U.S., victims were often escorted by a member of the organization to a bank and instructed to open an account in her own name; once the account was open a member of the organization took control of the account and then

[69] Funnel accounts are distinct from concentration accounts, which are used legitimately by businesses, including banks, to consolidate daily cash flow activity from multiple locations into a single account.
[70] FinCEN Advisory on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, FIN-2014-A005, May 28, 2014, available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a005.
[71] DOJ, Press Release, June 1, 2017, available at https://www.justice.gov/usao-ndfl/pr/men-sentenced-multi-state-drug-trafficking-and-money-laundering-operation.

provided the account information to other co-conspirators to coordinate deposits throughout the United States.[72]

4. Virtual Currency

The legitimate use of, and speculation and investment in, virtual currency[73] is increasing, as is the use of Bitcoin and other virtual currencies by cybercriminals.[74] Darknet websites, such as the now-shuttered Silk Road and AlphaBay, allow users to buy and sell narcotics and other illicit goods and services online regardless of physical location with perceived or actual anonymity.[75] Transactions on these sites typically require use of virtual currency and the sites often provide an escrow service or other settlement system. Despite evidence of growing use, constraints of scale and liquidity, as well as market value volatility, suggest that at present virtual currency is not eclipsing the use of physical currency or the traditional financial system for large-scale money laundering. Recognition of the potential money laundering risk by the U.S. government led to the imposition of certain obligations on intermediaries that exchange fiat currency into virtual currency and vice versa. This relatively early action, as well as certain features of virtual currencies themselves—such as meticulous transaction records known as the blockchain—has helped law enforcement to uncover criminals' use of virtual currency for money laundering.

ICE-HSI forecasts that illicit use of virtual currency will accelerate due to its unique features and ongoing efforts to improve anonymity. Law enforcement investigations have shown that many virtual currency users who buy or sell illegal goods or exchange virtual currency on Darknet markets rely on technology that conceals their location and identity from law enforcement. Anonymizing software such as the Tor network used in conjunction with mixers and tumblers[76] can obscure the source and destination of virtual currency and frustrate law enforcement's efforts to link transactions to people, virtual currency wallets, or IP addresses.[77]

According to IRS-CI, Bitcoin alternatives or altcoins provide more anonymity than is available from Bitcoin because they do not post transactions to a public decentralized blockchain ledger. FinCEN notes that anonymity-enhanced cryptocurrencies (AECs) specifically designed to make virtual currency transactions untraceable and to provide near-impenetrable anonymity are increasingly being used on the Darknet.

---

[72] DOJ, Press Release, May 25, 2017, available at https://www.justice.gov/usao-mn/pr/twenty-one-additional-defendants-indicted-their-roles-thai-sex-trafficking-enterprise.
[73] For a definition of virtual currency, see https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[74] HSI Office of Intelligence analyzed 220 HSI investigations initiated from FY 2014 through FY 2016 and identified the use of virtual currency associated with illegal purchases of firearms, ammunition, and weapons; narcotics trafficking; and money laundering.
[75] Darknet content is not indexed by traditional search engines and requires unique software or authorization to access. See https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces and https://www.ice.gov/features/darknet.
[76] Tumbler and mixing services takes virtual currencies like bitcoin from many users, routes them through a complex funding path, and redistributes them so they no longer can be readily traced to a specific source. See https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities.
[77] Bitcoin and other virtual currencies rely on blockchain technology, a distributed public ledger containing an historical record of every transaction. Third-party services like mixers and tumblers can defeat the blockchain by obscuring the source, destination, and movement of the virtual currency. Some virtual currencies have built-in mixers.

Although the Darknet and virtual currencies allow for illicit cross-border transactions, eventually criminals exchange their virtual currency for fiat currency requiring the use of a virtual currency exchanger. In the United States, based on facts and circumstances, virtual currency exchangers and administrators are subject to the BSA.[78] Virtual currency administrators and exchangers outside of the jurisdiction of the United States typically do not have obligations comparable to the recordkeeping and reporting requirements under the BSA. In addition, international investigations, especially those involving advanced technology, can create challenges for law enforcement with respect to gathering evidence and information.

Case examples:

- In July 2017, DOJ announced the seizure of the then-largest online criminal marketplace, AlphaBay, which operated for over two years on the Darknet and was used to sell illegal drugs, among other things.[79] Five U.S. law enforcement agencies and authorities from six foreign countries participated in the investigation. According to the FBI, there had been more than $1 billion in transactions on Alphabay involving the use of Bitcoin and other virtual currencies including the AECs Monero and Zcash.[80] AlphaBay hosted more than 250,000 listings for illegal drugs and toxic chemicals and more than 100,000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and services associated with perpetrating fraud.
- In August 2017, an alleged AlphaBay vendor was indicted in Pennsylvania for the distribution of furanyl fentanyl,[81] under the name NARCOBOSS.[82] The defendant is alleged to have filled more than 7,800 orders from July 2016 to June 2017, most of it paid for with Bitcoin. ICE-HSI seized $154,000 from the defendant's accounts.[83]
- In July 2017, FinCEN, working in coordination with DOJ, assessed a $110 million penalty against BTC-e (a/k/a Canton Business Corporation) —one of the largest digital currency exchanges by volume in the world—for willfully violating U.S. AML laws. FinCEN also assessed a $12 million penalty against Russian national Alexander Vinnik, one of the operators of the foreign-based BTC-e, who was arrested in Greece.[84] Separately, a criminal investigation led by IRS, ICE-HSI, FBI, and USSS resulted in charges against Vinnik and BTC-e for operating an unlicensed MSB, money laundering,

[78] See https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[79] DOJ, Press Release, July 20, 2017, available at https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.
[80] FBI, Press Release, July 20, 2017, available at https://www.fbi.gov/news/stories/alphabay-takedown.
[81] Because fentanyl is synthesized, chemists can create a wide range of similar synthetic opioids ranging in potency. Furanyl fentanyl is among the more common fentanyl analogs. See https://www.dea.gov/druginfo/fentanyl-faq.shtml.
[82] DOJ, Press Release, August 3, 2017, available at https://www.justice.gov/usao-wdpa/pr/darby-man-charged-distributing-fentanyl.
[83] Written testimony of ICE Homeland Security Investigations Investigative Programs Assistant Director Matthew Allen, November 28, 2017 available at https://www.dhs.gov/news/2017/11/28/written-testimony-ice-senate-committee-judiciary-hearing-titled-s1241-modernizing.
[84] FinCEN, Press Release, available at https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.

and related crimes.[85] According to the indictment, between at least 2011 and 2017, BTC-e was used to launder more than $4 billion in illicit proceeds from a variety of crimes. BTC-e users allegedly openly discussed criminal activity on the site's user chat space and BTC-e's customer service representatives offered advice on how to process and access money obtained from illegal drug sales on Darknet sites. BTC-e also lacked basic AML controls and policies, including adequate internal controls to mitigate the risks presented by virtual currencies with anonymizing features.

5. Misuse of Legal Entities

Misuse of legal entities to hide a criminal beneficial owner or illicit source of funds had been reported by law enforcement as a common feature of money laundering and corruption schemes.[86] Bad actors consistently use shell companies to disguise criminal proceeds and U.S. law enforcement agencies have had no systematic way to obtain information on the beneficial owners of legal entities. The ease with which companies can be incorporated under state law, and how little information is generally required about the company's owners or activities, raises concerns about a lack of transparency. However, when a legal entity formed in the United States opens a U.S. bank account to launder domestic illicit proceeds, this has not proved to be a major impediment to law enforcement investigations although it may slow them down. It may significantly slow down investigations or require the use of more resource-intensive investigative techniques, but not stop them altogether. Additionally, not all U.S. states require the same level of information about their companies, and for companies formed in some states, investigators are may have very few leads to follow besides the name of a corporate registered agent.

Much more challenging for law enforcement are those circumstances in which funds deposited in the United States in an account held in the name of a legal entity are transferred abroad to an account also held in the name of a legal entity, or when funds originating abroad are transferred to the U.S., again to and from accounts held in the name of a legal entity. Complex ownerships structures featuring layers of corporate entities, trusts, or nominee owners—punctuated by the involvement of foreign natural or legal persons—also present investigative challenges. The shares of shell companies may also be transferred, which effectively changes the ownership of the companies' assets. Another related issue is shelf companies. They are essentially shell companies available "off the shelf," but which often have been incorporated in the past to make them appear "established" to outsiders; they are attractive to criminals looking for ready-to-use legal entities.

The DOJ has noted that FinCEN's recent CDD Rule will make it more difficult for criminals to circumvent the law through use of opaque corporate structures. Since May 2018, the CDD Rule has required covered financial institutions in the U.S. to collect and verify the personal information of the beneficial owners who own, control, and profit from companies when those companies open accounts. According to the DOJ, the collection of this information will generate

[85] https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged ; *United States v. BTC-e*, Superseding Indictment, Case No. CR 16-00227 SI (N.D. Cal. Jan. 17, 2017).
[86] ICE, Cornerstone Report: Third Party Money Launderers, Summer 2017, available at https://www.ice.gov/sites/default/files/documents/Report/2017/CSReport-13-4.pdf.

better law enforcement leads and speed up investigations.[87] Such information should become accessible to law enforcement through subpoenas to the financial institutions holding the information. In addition to slowing or otherwise hampering law enforcement investigations, asset seizures and forfeitures, and international cooperation, the lack of readily available beneficial ownership information also impaired a financial institution's CDD processes affecting its ability to identify suspicious activity.

Criminals also misuse front companies, which have legitimate operations allowing illicit proceeds to be comingled with earnings from legitimate operations. Unlike shell companies that usually have no employees, operations, or even a physical location other than a registered agent because they are mere "shells" to hold assets, front companies generate real economic activity. Front companies are used to commingle illicit proceeds with the earnings from legitimate business operations, whether those earnings are derived from running a restaurant, a nightclub, an exchange house, or any other type of business with consistent cash flow. For example, criminals do this by adding illicit cash with to the firm's legitimate cash earnings and depositing the combined amount in the firm's bank account. With the funds in the banking system, the illicit proceeds can be layered and integrated disguising their source. A variation on this money laundering method is merchants facilitating TBML by accepting drug money in payment for goods for export. When the drug cash is already in the banking system and payment is made by check, the transaction can be indistinguishable from a legitimate trade transaction. However, when merchants accept a large volume of cash directly as part of a TBML scheme but their business does not usually involve large cash deposits, banks may recognize and report the suspicious activity.

Case examples:

- In January 2018, in Tennessee, seven people were charged with operating pain management clinics and medical labs in Florida and Tennessee where opioids were prescribed without legitimate medical purpose.[88] The medical labs were supposedly testing the pain management clinic patients for opioid addiction, but submitted fraudulent bills to Medicaid and Medicare and split at least $21 million with the doctors prescribing the opioids. DOJ alleged the kickbacks paid by the labs to the doctors were disguised as consulting fees and paid to a shell company set up as a marketing research firm.[89]
- In October 2017, fifteen people were charged in Florida for their roles in an international fraud and money laundering organization from 2008 to 2017.[90] The organization used money mules to register shell companies and open bank accounts in those companies' names throughout south Florida. The accounts were used to receive illicit proceeds from romance, inheritance, and lottery scams committed across the United States. After

[87] M. Kendall Day, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Testimony before the Senate Committee on Banking, Housing, and Urban Affairs, January 17, 2018.
[88] DOJ, Press Release, January 19, 2018, available at https://www.justice.gov/opa/pr/two-top-leaders-italy-and-five-us-residents-indicted-racketeering-health-care-fraud-and-drug.
[89] United States v. Sylvia Hofstetter et al, 3:15-CR-27 (Second Superseding Indictment), available at https://www.justice.gov/opa/page/file/981896/download.
[90] DOJ, Press Release, October 26, 2017, available at https://www.justice.gov/usao-sdfl/pr/fifteen-individuals-charged-multi-million-dollar-international-money-laundering-and.

receiving the money in the shell company accounts, the money mules would wire the proceeds to accounts overseas.

- In September 2017, in New York, Alejandro Javier Rodriguez-Jimenez plead guilty to money laundering charges associated with his leadership of an international money laundering organization working on behalf of drug cartels in Mexico and Central America.[91] Rodriguez-Jimenez used front companies in Nevada and Mexico, and the companies' bank accounts, to launder more than $250 million in drug proceeds internationally. Rodriguez-Jimenez maintained stash houses in New York, Philadelphia, Atlanta, Chicago, and Las Vegas where drug cash was received, deposited into the businesses' bank accounts as legitimate earnings, and then wired under guise of business payments to accounts in Mexico, Hong Kong, Italy and elsewhere.
- In June 2017, a nationwide round-up of alleged perpetrators of healthcare fraud included four defendants in Florida who allegedly used shell companies to launder the proceeds of their fraud. DOJ alleges more than $8 million in false Medicare claims were submitted for home health services that were never provided. Payments were made by Medicare to a bank account held in the name of the alleged home health services company, then transferred to other accounts held by shell companies disguised as relevant business services providers, and ultimately withdrawn as cash.[92]
- In 2017, the DOJ filed a civil complaint seeking the forfeiture and recovery of approximately $144 million in assets that were allegedly the proceeds of foreign corruption offenses that were paid out to shell companies and laundered in and through the United States.[93] Nigerian businessmen allegedly paid bribes to a former Nigerian official to steer oil contracts to companies they owned. The proceeds of the contracts were allegedly paid into accounts held by shell companies, with the money ultimately used to buy a $50 million condominium in New York City and an $80 million yacht.

6. Complicit Merchants, Professionals, and Financial Services Employees

According to the FBI, criminal organizations seek out professionals as potential accomplices if they are in a position to facilitate money laundering.[94] The FBI's Money Laundering, Forfeiture and Bank Fraud Unit (MLF), HSI's Illicit Finance and Proceeds of Crime Unit (IFCPU), and DOJ have increased their focus on these professional money laundering facilitators, including individuals in the financial sector, accountants, real estate agents, and lawyers. Also of concern are merchants who knowingly fail to report receiving cash in amounts of more than $10,000 from a customer in one or related transactions.[95] According to DOJ, the biggest challenge to the prosecution of intermediaries is showing that professionals or individuals who are enlisted by criminals to do certain tasks had the knowledge that they were dealing with tainted money or bad

[91] DOJ, Press Release, September 11, 2017, available at https://www.justice.gov/usao-sdny/pr/leader-international-narcotics-money-laundering-business-pleads-guilty-manhattan.
[92] DOJ, Press Release, July 13, 2017, available at https://www.justice.gov/usao-sdfl/pr/seventy-seven-charged-southern-district-florida-part-largest-health-care-fraud-action; https://www.justice.gov/opa/page/file/981136/download.
[93] DOJ, Press Release, July 14, 2017, available at https://www.justice.gov/opa/pr/department-justice-seeks-recover-over-100-million-obtained-corruption-nigerian-oil-industry.
[94] FBI, Press Release, October 24, 2016, available at https://www.fbi.gov/news/stories/combating-the-growing-money-laundering-threat.
[95] 26 U.S.C. § 6050I and 31 U.S.C. § 5331.

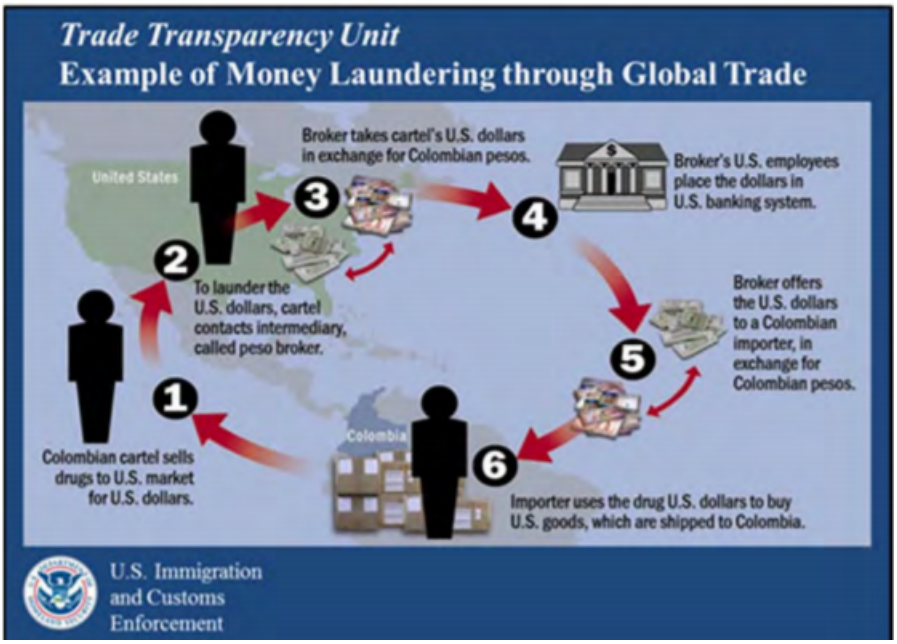
actors, or that they should have known the same in light of the facts and circumstances. Additionally, insufficient criminal liability for intermediaries who conceal the beneficial ownership of legal entities would help bring complicit professionals to justice for conduct that may not be readily provable as money laundering.

A. Merchants

In a typical TBML scheme, known as the Black Market Peso Exchange (BMPE), South American drug traffickers sell their U.S. drug proceeds (denominated in U.S. dollars) at a discount to Colombian money brokers, who in turn sell the currency at below market rates to South American businesses which need it to purchase U.S. goods. Even though the money brokers sell the U.S. dollars to South American merchants, the brokers will typically make the payment on their behalf to the U.S. exporters. Money brokers seek out U.S. merchants willing to accept drug cash without filing a Form 8300 (Report of Cash Payments Over $10,000 Received in a Trade or Business). A U.S. exporter may be unaware he is facilitating money laundering if the money broker is able to get the drug cash into a bank account, depositing it, for example, into a shell or front company account, and uses a check or bank wire to pay the merchant. However, when a U.S. merchant receives a check or wire from a third party unrelated to the South American business ordering the merchandise, it is an indication the transaction may be part of the BMPE.

The BMPE example of TBML demonstrates how professional money launderers can break the link between the predicate crime, drug trafficking, and related money laundering, making it difficult to associate drug traffickers with the money laundering activity. Law enforcement believes there has been an increase in TBML due to improved compliance by financial institutions in the United States with cash reporting requirements and AML laws more generally.[96]

[96] FinCEN Advisory on Colombian Black Market Peso Exchange, available at https://www.fincen.gov/sites/default/files/advisory/advisu9.pdf.



SOURCE: HSI, TRADE TRANSPARENCY UNIT

With the increasing role of China as a supplier of synthetic opioids and related precursors, DEA has noted the development of an Asian version of the BMPE with goods being exported to China by U.S. front companies as payment for drugs.[97] Chinese money brokers are also on the rise, helping drug traffickers in the United States launder their illicit proceeds and simultaneously helping individuals in China circumvent China's capital controls. China prohibits its citizens from exchanging more than $50,000 USD for yuan per year.[98] Money brokers help individuals in China evade the limit by selling them cash acquired from drug dealers in the United States.[99] The money brokers use the yuan they receive in China to buy Chinese goods for export. The goods are sold to merchants in Latin America. The Latin American merchants provide payment in local currency, which the money brokers use to pay the drug cartels for their U.S. drug money.

Case examples:

- In 2018, in Florida, four Peruvians were indicted for their alleged role in a multi-billion-dollar TBML scheme.[100] Previously, in 2017, three others had pleaded guilty in a related case.[101] That investigation found that millions of dollars of U.S. drug proceeds were smuggled to Peru by Peruvian drug traffickers. The traffickers used the cash to buy gold that had been illegally mined in Peru, and then they sold the gold to complicit U.S. refineries. The money laundering cycle was completed when the refineries paid for the gold by sending bank wires that outwardly appeared to be legitimate payments for wholesale gold purchases.

[97] https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.
[98] http://www.safe.gov.cn.
[99] https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.
[100] https://www.justice.gov/usao-sdfl/pr/four-peruvian-members-multi-billion-dollar-international-gold-money-laundering-scheme.
[101] *United States v. Barrage*, Affidavit, ECF No. 1, Case No. 17-cr-20215-RNS (S.D. Fla. Mar. 21, 2017).

- In December 2017, in Los Angeles, Pacific Eurotex Corp., a textile company, and its owners – Morad "Ben" Neman and Hersel Neman – pleaded guilty to using the business to receive bulk cash that they knew or believed to be the proceeds of narcotics trafficking and part of a BMPE scheme.[102] The Nemans received approximately $370,000 in cash delivered on four separate occasions as payment for goods shipped to Mexico, Guatemala, and other countries in Latin America. The brothers structured 384 cash deposits to their business accounts. The HSI-led investigation, dubbed Operation Fashion Police, and several related investigations involving federal, state, and local law enforcement agencies, netted tens of millions in bulk cash stashed at warehouses in the Los Angeles area.[103]
- In January 2016, in El Paso, the owner of ERENE, Inc., an El Paso-based business which primarily sells shoes, was convicted on charges associated with an estimated $100 million BMPE scheme. The company smuggled shoes into Mexico from El Paso in exchange for U.S. dollars paid by Mexican merchants. The shoes were smuggled into the country because ERENE had contracted with suppliers as a retailer not a wholesaler and it wanted to avoid paying customs duties. The scheme was uncovered by HSI scrutinizing US/Mexican trade data with Mexico's Financial Intelligence Unit.[104]
- In September 2015, in New York, three alleged money brokers based in China were indicted for their role in an international money laundering organization that allegedly laundered more than $5 billion in U.S. drug proceeds for drug cartels based in Mexico and Colombia.[105] Prosecutors allege that from January 2004 until their arrest in 2015, the men leading the "Guangzhou Enterprise" managed a BMPE scheme in which U.S. drug dollars were acquired in exchange for Colombia pesos. The dollars were used to acquire Chinese goods, many of which prosecutors say were counterfeit products, for export to Colombia in exchange for pesos.

In response to law enforcement concern about TBML, FinCEN issued a GTO on October 2, 2014, imposing additional reporting and recordkeeping obligations on certain and businesses located within the Los Angeles Fashion District.[106] For the exporters targeted by the GTO, the threshold for filing a Form 8300 was lowered from $10,000 to $3,000. FinCEN followed on April 21, 2015 with a GTO imposing the same additional reporting and recordkeeping requirements on about 700 Miami businesses.[107]

---

[102] https://www.justice.gov/usao-cdca/pr/la-fashion-district-company-and-two-owners-plead-guilty-federal-charges-stemming-money.
[103] https://www.ice.gov/news/releases/large-scale-law-enforcement-effort-targets-downtown-los-angeles-businesses-linked.
[104] https://www.justice.gov/usao-wdtx/pr/el-paso-businessowner-sentenced-federal-prison-role-money-laundering-scheme-associated and https://www.justice.gov/usao-wdtx/pr/el-paso-business-and-businessowner-charged-connection-alleged-fraud-and-trade-based.
[105] https://www.justice.gov/usao-edny/pr/three-members-international-organization-money-launderers-largest-drug-cartels-arrested. In 2016, one of the co-conspirators was successfully extradited from Colombia: https://www.justice.gov/usao-edny/pr/member-alleged-international-organization-money-launderers-largest-drug-cartels.
[106] https://www.fincen.gov/sites/default/files/news_release/20141002.pdf.
[107] https://www.fincen.gov/news/news-releases/fincen-targets-money-laundering-infrastructure-geographic-targeting-order-miami.

The Los Angeles GTO helped to uncover 2,000 businesses that law enforcement investigations revealed were accepting bulk cash without filing the required Form 8300. The Pacific Eurotex Corp case cited above was one of many cases that resulted from a 2017 law enforcement raid of companies suspected of laundering drug money in the Los Angeles Fashion District.[108] During and after the GTOs were implemented FinCEN detected an increase in the use of non-cash payment methods, such as cashiers' checks and foreign bank drafts. Law enforcement also noticed an increase in exporters receiving wire transfers instead of cash to settle transactions. At the time of the Miami and Los Angeles GTOs, wire transfers were not included among the covered payment instruments.[109]

B. Attorneys

Prosecutors have increased their focus on attorneys suspected of being complicit in money laundering, particularly those suspected of laundering funds for drug traffickers. According to HSI, one method attorneys employ to facilitate money laundering is to misuse their Interest on Lawyers Trust Account (IOLTA).[110] These are accounts that lawyers establish at banks to hold or transfer funds on behalf of various clients. The interest earned on an IOLTA is ceded to the state bar association or another entity to pay for pro bono representation or other public interest purposes. These accounts present money laundering risks because they are not subject to mandatory reporting requirements which can allow cash deposits and withdrawals over $10,000 to go undetected, and because the accounts are used to pool the funds of multiple clients the bank holding an IOLTA has no direct relationship with or knowledge of the ultimate beneficial owner of the account. Complicit attorneys might allow illicit proceeds to be deposited in their IOLTAs and then launder the funds through the purchase of real estate or investments, or by transferring the money out of the United States. Attorneys may also be unwitting participants in money laundering schemes, through the use of IOLTAs or by helping clients establish legal entities, open bank accounts, and engage in other "transactional" activities.

Case examples:

- In February 2018, in Virginia, Raymond Juiwen Ho, an attorney who has been disbarred, was sentenced for conspiring to launder more than $2 million derived from a business email compromise scheme. Ho participated in a conspiracy in which co-conspirators sent emails from compromised or imitation accounts that duped victims into transferring money to accounts controlled by Ho, including IOLTAs.[111]
- In 2016, in Florida, Texas attorney Perry Cortese and two others pled guilty to conspiracy to commit money laundering and mail and wire fraud. Many of the fraud victims were law firms that had been solicited online to perform legal work. The firms were provided with counterfeit cashiers' checks and directed to wire money to shell companies that were controlled by the defendants. The defendants also employed hackers who compromised

[108] https://www.justice.gov/usao-cdca/pr/la-fashion-district-company-and-two-owners-plead-guilty-federal-charges-stemming-money

[109] Prior to August 2017, the definition of currency in the GTO and Form 8300 regulations only included cashier's checks, bank drafts, and several other paper-based payment methods, and excluded wire transfers until a legislative amendment added wire transfers in August 2017.

[110] See, *e.g.*, https://www.ice.gov/sites/default/files/documents/Report/2017/CSReport-13-4.pdf;

[111] https://www.justice.gov/usao-edva/pr/former-attorney-sentenced-prison-money-laundering

personal and business e-mail accounts to obtain information that would allow the defendants to order wire transfers from the victims' brokerage and business accounts to shell company accounts controlled by the defendants.[112]

- In 2015, in Minneapolis, lawyer Robert David Boedigheimer was sentenced for using his law firm to launder drug proceeds for his brother-in-law.[113] Boedigheimer created a no-show job with a salary for his brother-in-law, funded by drug proceeds laundered through the law firm's accounts. In return, Boedigheimer received loans from his brother-in-law funded by drug proceeds.
- In December 2014 Portland, Maine attorney Gary Prolman was sentenced for laundering drug proceeds.[114] Prolman laundered about $177,500 of a client's marijuana proceeds by structuring cash deposits and buying cashier's checks. Prolman invested a portion of the proceeds in his sports agency business on behalf of the client and used the cashier's checks to buy real estate for the client using his own name on the deed as the owner.

C. *Real Estate Professionals*

Real estate can be an effective vehicle for money laundering when criminals use a shell company or nominee as the owner of record, as it allows them to keep the true ownership and control out of property records. Criminals can also reduce scrutiny in the purchase process if they avoid a mortgage loan and pay the full price of the property in cash. However, more than three quarters of all existing home sales in 2017 in the United States involved a mortgage.[115] Mortgage lenders, both banks and non-banks, have certain AML obligations, mitigating the potential money laundering risk. However, there are cases in which borrowers, as part of a money laundering scheme, committed bank fraud by falsifying loan documents to secure a mortgage or refinance a property, and then paid the loan off with illicit proceeds. There have also been cases in which industry insiders have committed and facilitated mortgage fraud.[116]

According to the National Association of Realtors, 87% of buyers purchased their home through a real estate agent or broker—a share that has steadily increased from 69 percent in 2001.[117] Real estate agents can assist with a transaction, but they do not receive the funds to complete the sale of a home other than when the seller's real estate agent accepts earnest money (a minimal deposit of funds to demonstrate the buyer's interest).[118] However, because of their market knowledge, real estate agents are in a position to help commit fraud and facilitate money laundering, whether knowingly or unwittingly.

---

[112] https://www.justice.gov/usao-mdfl/pr/texas-attorney-sentenced-25-years-prison-international-money-laundering-conspiracy; https://www.justice.gov/usao-mdfl/pr/jury-finds-texas-lawyer-and-others-guilty-international-money-laundering-and-fraud

[113] https://www.justice.gov/usao-mn/pr/suspended-attorney-sentenced-five-years-prison-using-law-firm-launder-drug-money.

[114] https://www.justice.gov/usao-me/pr/saco-attorney-pleads-guilty-177500-money-laundering-conspiracy

[115] https://www.nar.realtor/newsroom/existing-home-sales-soar-56-percent-in-november-to-strongest-pace-in-over-a-decade.

[116] https://www.fbi.gov/investigate/white-collar-crime/mortgage-fraud.

[117] https://www.nar.realtor/research-and-statistics/quick-real-estate-statistics

[118] Earnest money is placed into a trust account with either the real estate broker or title company. A real estate agent receiving or paying out amounts of more than $10,000 in cash or monetary instruments must report the transaction to FinCEN by filing a Form 8300.

Other real estate professionals, such as attorneys, title/escrow agents, and mortgage brokers, are also well-placed to facilitate criminal schemes. Although the process of settlement differs by state, based on legal requirements or local practice, there is no customer due diligence obligation generally imposed on the array of professionals who help individuals or legal entities buy real estate in the United States. There are no obligations imposed on the person, often the closing agent, who receives funds from the purchaser and disburses them to lien holders or the seller, other than the requirement to file a Form 8300 should they receive cash or monetary instruments above the $10,000 threshold. Furthermore, the salient question for AML purposes is not who the titleholder of record will be, or even who the beneficial owner of that titleholder is, but whose dollars are being used to acquire the property. In other words, law enforcement is most interested in who stands to benefit from the placement of those funds in the U.S. market. Such an inquiry about the source of funds in an all cash real estate transaction is not made by real estate professionals in the normal course of business, particularly those whose economic interests align with a smooth transaction and a good reputation among potential foreign investors.

Law enforcement agencies report that legal entities, such as limited liability companies (LLC), are frequently used to acquire real properties with funds of criminal origin. Sometimes, the deed indicates that one LLC holds title, but at the real estate closing, the funds which finalize the purchase are wired in from a seemingly unrelated source, frequently another legal entity, through a foreign bank or perhaps an attorney IOLTA or escrow account.

Case examples:

- In 2017, in San Francisco, real estate agent Robert Jacobsen pleaded guilty to wire fraud and money laundering charges. Jacobsen created a shell company with a name similar to the company that held the mortgage on sellers' homes. He then hired an attorney to sue his phony company claiming that the mortgages were invalid. Controlling both sides of the lawsuits, Jacobsen was able to get the deeds of trust invalidated by federal or state courts. When Jacobsen sold the properties, he kept most of the proceeds, laundering the money through multiple bank accounts in the United States and in Belize, and buying property and a yacht.[119]
- In 2016, in Oakland, California, real estate agent Anthony Keslinke was sentenced after pleading guilty to conspiracy to commit bank fraud and money laundering.[120] The real estate agent used straw buyers to purchase real estate through "short sales," and falsified documents to aid in the purchases. He ultimately used his own funds to purchase the properties at prices steeply reduced due to Keslinke's fraud. The properties were purchased in the names of the straw buyers, and often resold for a significant profit. The real estate agent also accepted $550,000 from an undercover agent posing as a drug dealer and attempted to launder the money by wiring the funds from his business bank accounts.

[119] https://www.justice.gov/usao-ndca/pr/east-bay-real-estate-agent-pleads-guilty-wire-fraud-and-money-laundering-connection
[120] https://www.justice.gov/usao-ndca/pr/danville-real-estate-agent-sentenced-four-years-prison-bank-fraud-and-money-laundering

- In 2016, in Texas, fifteen people were charged in connection with drug trafficking and money laundering.[121] One of the alleged drug traffickers was also accused of wire fraud affecting a financial institution for making false statements in connection with the repeated refinancing of a mortgage loan on a property valued at over $1 million. The alleged drug trafficker falsely represented to the bank that he had a non-taxable annual cash flow income of more than $500,000.
- In 2013, in Texas, real estate agent Freddy Centeno was sentenced to prison for laundering money for a convicted drug trafficker. The real estate agent admitted helping to launder drug profits through the purchase of residential and commercial properties. He arranged the transactions to conceal the ownership of the property.[122]

Property purchases without a mortgage present a significant money laundering risk. In such circumstances, the purchaser does not undergo the scrutiny of the loan application and underwriting process; moreover, the payment in these "all-cash" transactions is typically a wire transfer or cashier's check for the full purchase price, potentially obscuring both the true purchaser and the source of funds. To gather more information on the money laundering risk associated with these purchases, in 2016, 2017, and 2018 FinCEN issued, renewed, and expanded GTOs requiring U.S. title insurance companies in major metropolitan areas to report beneficial ownership information on legal entities that purchase high-value residential real estate without a bank loan.[123] To date, FinCEN has found that approximately thirty percent of the real estate transactions reported under the GTOs involved a beneficial owner or purchaser representative who had previously been the subject of a SAR, signaling that persons purchasing or facilitating the purchase of real estate without financing may present a heightened money laundering risk[124] To gain further insight into all-cash purchases, Treasury is studying such purchases in all amounts—beyond high-end residential properties—as cases suggest that criminals purchase real estate at all price levels for personal and investment use.

D. Financial Services Employees

Criminals seek out insiders at financial institutions to help them launder their illicit proceeds. Individuals who own, manage, or otherwise work for financial services providers present a significant money laundering risk if they abuse their professional position for criminal purposes including money laundering. These professionals may undermine an institution's AML compliance program or culture by, among other things, not conducting customer due diligence, not complying with recordkeeping or reporting requirements, or otherwise facilitating or turning a blind eye to suspicious activity. Case examples demonstrate that such insiders are found in many types of regulated financial services providers. Furthermore, criminals have, in some

[121] https://www.justice.gov/usao-wdtx/pr/federal-and-state-authorities-arrest-15-individuals-federal-drug-trafficking-and-money
[122] https://archives.fbi.gov/archives/sanantonio/press-releases/2013/real-estate-agent-headed-to-prison-for-money-laundering
[123] https://www.fincen.gov/sites/default/files/shared/Real%20Estate%20GTO%20Order%20-%208.22.17%20Final%20for%20execution%20-%20Generic.pdf; https://www.fincen.gov/sites/default/files/shared/FAQs%20on%20Phase%204%20Real%20Estate%20GTO%208.22.2017%20FINAL.pdf.
[124] https://www.fincen.gov/sites/default/files/advisory/2017-08-22/Risk%20in%20Real%20Estate%20Advisory_FINAL%20508%20Tuesday%20%28002%29.pdf.

instances, purchased or obtained control of foreign and domestic institutions to further their criminal schemes. These compromised financial institutions, whether foreign or domestic, present risks to U.S. financial institutions and the U.S. financial system, as they can disguise the movement of funds into and out of the United States by criminal actors.

Bankers

- In October 2017, in New York, the former chairman and CEO of the Helping Other People Excel Federal Credit Union in Lakewood, New Jersey was sentenced to prison for accepting $150,000 in bribes in order to cede control of the credit union to operators of an illegal money transmitter.[125] Also sentenced were the operators of the unlicensed money transmitter, Coin.mx, an internet-based Bitcoin exchange. The Coin.mx operators bribed the credit union chairman to allow them to take over the financial institution in order to secure reliable access to the automated clearing house network to process transactions. Coin.mx had previously attempted to open and maintain accounts at banks by misrepresenting the nature of the business and miscoding customer's credit and debit card transactions. Tens of millions of dollars of electronic financial transactions were processed through the credit union without adequate controls.
- In June 2017, in New York, a former Swiss banker, pled guilty to participating in a money laundering conspiracy in connection with facilitating the payment of millions of dollars of bribes to various high-ranking soccer officials.[126] The banker furthered the bribery conspiracy by, among other things, opening a bank account in the name of a shell company on behalf of one recipient and assisting in paying more than $25 million in bribes into the account. The banker was compensated more than $1 million for his work facilitating the bribe payments.
- In June 2017, the FRB permanently bared two former employees of Regions Bank, based in Birmingham, Alabama, from the banking industry after both pled guilty to conspiracy to commit money laundering, and conspiracy to commit bank bribery and wire fraud affecting a financial institution.[127]
- In March 2017, in California, a former Wells Fargo branch manager was convicted of money laundering and false bank entry charges in connection with a fraud scheme.[128] The scheme involved making fraudulent offers to trademark applicants for registration and monitoring services. The former branch manager laundered the funds by instructing staff to open bogus accounts to process fraudulent withdrawals, wire transfers, and cashiers' checks. The manager offered payments and promotions to staff to induce them to conduct the fraudulent transactions. More than $1 million was laundered through the accounts, with the former branch manager receiving a percentage of the laundered proceeds.

[125] https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-sentenced-more-5-years-prison-leading-multimillion
[126] https://www.justice.gov/opa/pr/former-swiss-banker-pleads-guilty-money-laundering-charge-connection-soccer-bribery-scheme
[127] https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170607a.htm
[128] https://www.justice.gov/opa/pr/former-wells-fargo-branch-manager-convicted-laundering-proceeds-trademark-scam.

- In 2016, in Georgia, a bank teller was sentenced to nearly three years in prison for cashing fraudulently obtained income tax refund checks.[129] The teller's co-conspirators filed fraudulent income tax returns using stolen identities and directed other co-conspirators to bring the fraudulently obtained refund checks to the teller to cash. The teller cashed approximately 330 fraudulently obtained checks worth more than $600,000, in exchange for a fee.

MSB Operators

- In June 2017, in Georgia, 11 people were charged with laundering more than $40 million in drug proceeds on behalf of Mexican TCOs through money remitters.[130] Managers and employees of Atlanta-area money remitters helped launderers send the illicit proceeds to Mexico by structuring transactions and falsifying sender information. Several of the defendants allegedly served as the BSA/AML compliance officers for the remitters.
- In 2016, in Pennsylvania, the former owners of Tropical Express, a money transmitting business, were sentenced to prison for conspiring to structure financial transactions. The two defendants structured approximately $340,000 of drug trafficking proceeds and transmitted the funds by wire to the Dominican Republic.[131]
- In July 2017, in Florida, as part of a health care fraud enforcement action, a man pled guilty to operating as an unlicensed money transmitter. He was charged with cashing checks totaling $100,000, the proceeds of which were used to pay kickbacks to Medicare beneficiaries engaged in a fraudulent home health services scheme.[132]

Broker-dealers

- In 2016, in New York, the former director of compliance at Trident Partners Ltd., a registered broker-dealer, pleaded guilty to wire fraud in connection with a scheme to misappropriate investor funds.[133] The director, who was also the firm's AML officer, was also charged with money laundering related to the scheme, which involved fraudulently soliciting overseas investors and then stealing their money.
- In 2017, Scottsdale Capital Advisors Corporation ("SCAC") was found to have violated FINRA rules related to the sale of unregistered securities. The investigation into SCAC centered on the deposit and sale of unregistered securities by nominee corporations that were customers of the firm's offshore affiliate. Due to the omnibus nature of the account for SCAC's affiliate, and the nominee corporation structure of its affiliate's customers, the true beneficial ownership of the shares being deposited and sold was not transparent to

[129] https://www.justice.gov/opa/pr/georgia-bank-teller-sentenced-prison-cashing-fraudulently-obtained-income-tax-refund-checks.
[130] https://www.justice.gov/usao-ndga/pr/eleven-individuals-charged-following-investigation-targeting-drug-money-laundering; see also https://www.ice.gov/news/releases/11-indicted-laundering-40-million-atlanta-area-drug-proceeds.
[131] https://www.justice.gov/usao-mdpa/pr/former-owners-money-transmitter-business-sentenced-conspiring-structure-financial
[132] https://www.justice.gov/usao-sdfl/pr/seventy-seven-charged-southern-district-florida-part-largest-health-care-fraud-action
[133] https://www.justice.gov/usao-edny/pr/former-chief-compliance-officer-long-island-brokerage-firm-indicted-fraud-and-money; *United States v. Quigley*, Judgement, 2:15-CR-00258-001 (JMA) (E.D.N.Y. Nov. 7, 2016)

SCAC and the firm failed to take reasonable steps to ensure that the securities being sold were registered. As a result, SCAC was fined $1.5 million and its owner permanently barred from the securities industry, and other members of SCAC's management team were also individually sanctioned.

Precious Metals

In March 2018, in Texas, U.S. gold refinery Elemetal LLC, pled guilty to failure to maintain an adequate AML program.[134] According to court records, the international gold trade is commonly used for laundering illegally mined gold, narcotics, and other criminal proceeds. Criminals trade illegal gold through shell companies using false or incomplete documents. The gold is smuggled through third-party countries and then sold to refineries in the United States in an effort to hide the true source of the gold from foreign and United States law enforcement. Recognizing the high risk of gold-based money laundering, federal law requires precious metals dealers to establish AML programs under the BSA. Court records indicate Elemental accepted gold without requesting or obtaining adequate or in some instances any, identification of the persons supplying the gold or information regarding the source of the gold. Publicly available information indicated Elemental's customers and suppliers were supplying criminally derived gold. Three employees in Miami pled guilty to conspiracy to commit money laundering in a related case (U.S. v. Barrage, et al., Case No. 17- 20215-CR-SCOLA). The Elemental case was an OCDETF investigation with agents from HSI, FBI, DEA, and IRS.

7. Compliance Deficiencies

Compliance deficiencies at regulated financial institutions continue to be a money laundering vulnerability. But given the size of the financial services industry, it is may be inevitable despite diligent oversight that there will be compliance deficiencies. There are more than 11,000 depository institutions (5,593 FDIC insured banks,[135] and 5,573 federally insured credit unions[136]), more than 24,000 MSBs registered with FinCEN[137], almost 4,000 active broker-dealers registered with the SEC, and approximately 1,000 casinos.[138]

The consequence of lax compliance can be very significant depending on the institution and the circumstances. According to the FDIC, the assets within the banking industry are concentrated today in a small number of large, complex banks and other financial institutions that have highly diverse business strategies and complex legal and business structures that make it difficult for the management of these companies to fully understand and manage their risks.[139] The U.S. financial system is vulnerable to compliance deficiencies at both domestic and foreign financial institutions that operate in the U.S.

[134] https://www.justice.gov/usao-sdfl/pr/us-gold-refinery-pleads-guilty-charge-failure-maintain-adequate-anti-money-laundering
[135] https://research.fdic.gov/bankfind/
[136] https://www.ncua.gov/analysis/Pages/industry/industry-at-a-glance-december-2017.pdf
[137] https://www.fincen.gov/msb-registrant-search
[138] https://www.americangaming.org/sites/default/files/research_files/2017%20State%20of%20the%20States.pdf
[139] https://www.fdic.gov/about/strategic/strategic/bankingindustry.html

According to the OCC[140] BSA/AML/OFAC compliance risk management is an area of emphasis as some banks have not adopted appropriate risk management systems to keep pace with evolving risks, resource constraints, changes in business models, and regulatory changes. New U.S. economic and trade sanctions, as well as additional requirements in existing sanctions programs based on dynamic foreign policy and national security goals, may increase compliance and operational risks for banks as they attempt to address the resulting change management issues.

State and federal supervisors strive to identify and resolve AML/CFT compliance deficiencies early and privately recommend improvements and remedial actions to prevent lapses from becoming more serious and requiring a public enforcement action, or an eventual Department of Justice criminal referral. According to the federal banking agencies, the vast majority of BSA/AML compliance deficiencies they identify are resolved through the supervisory process without the need for an enforcement action.[141] However, that is not always possible.

Case examples:

- In January 2018, the OCC assessed a $70 million penalty against Citibank, N.A., for failing to comply with the agency's 2012 consent order related to BSA/AML deficiencies.[142] In the 2012 order, the OCC cited the bank for, among other things, failing to file SARs and weaknesses in controls related to correspondent banking. The OCC found that Citibank had failed to complete the required corrective actions.
- In October 2017, FinCEN imposed a civil money penalty of $2 million on Lone Star National Bank of Pharr, Texas for willfully violating the BSA from 2010 through 2014.[143] FinCEN's action followed the April 2015 OCC $1 million penalty assessed against the bank for failing to comply with the agency's 2012 consent order related to BSA/AML deficiencies.[144] In the 2012 order, the OCC cited the bank for deficiencies with its internal controls, independent audit, suspicious activity reporting, and foreign correspondent banking program. The OCC found that Lone Star had failed to complete the required corrective actions. The OCC had been citing the bank for BSA/AML deficiencies since 2010.
- In February 2017, the OCC assessed a $1 million penalty against Merchants Bank of California, NA, for failing to comply with the agency's 2010 and 2014 consent orders related to BSA/AML deficiencies.[145] Also in February 2017 FinCEN imposed a civil penalty of $7 million on Merchants Bank for failing to establish and implement an

[140] https://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2018.pdf.
[141] https://www.treasury.gov/press-center/press-releases/Documents/Foreign%20Correspondent%20Banking%20Fact%20Sheet.pdf.
[142] https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-3.html.
[143] https://www.fincen.gov/sites/default/files/enforcement_action/2017-11-01/Lone%20Star.ASSESSMENT%20OF%20CIVIL%20MONEY%20PENALTY%20-%20Final%2011.01_0.pdf.
[144] https://www.occ.gov/static/enforcement-actions/ea2015-028.pdf
[145] https://www.occ.gov/static/enforcement-actions/ea2017-013.pdf

adequate AML program.[146] Merchants Bank allowed billions of dollars to flow through the U.S. financial system without effective monitoring or suspicious activity reporting for higher-risk customers that included as many as 165 check-cashing customers and 44 money transmitters. Many of these transactions were conducted on behalf of MSBs that were owned or managed by bank insiders who encouraged staff to process these transactions without question or face retaliation.

- In January 2017, the New York Department of Financial Services (DFS) fined Deutsche Bank $425 million for extensive compliance failures that resulted in $10 billion being transferred out of Russia via mirror trading involving the bank's Moscow, London, and New York offices.[147] According to DFS, the scheme involved certain companies issuing orders to Deutsche Bank's Moscow equities desk to purchase Russian blue chip stocks. The trades were paid for in rubles. Later, sometimes on the same day, a related party would sell the same Russian stock at the same price through Deutsche Bank's London branch. The selling counterparty, which was typically registered in an offshore territory, would be paid for its shares in U.S. dollars. According to DFS, none of the trades demonstrated any legitimate economic rationale, but they had the effect of exchanging (or potentially laundering) rubles held in Russia for dollars held elsewhere.
- In March 2016, FinCEN penalized Thriftway Food Mart and its owner and compliance officer for willful and repeated violations of the BSA.[148] Thriftway conducted approximately $1 million in check cashing volume and money order sales per month. A 2013 IRS Small Business/Self-Employed Division examination found that 95 percent of the CTRs filed by Thriftway were incomplete or inaccurate and one-third were filed late.
- In August 2016, the former operator of the Normandie Casino in California was ordered by a federal court to pay a $1 million criminal fine and to forfeit nearly $1.4 million after pleading guilty to BSA violations, including not filing CTRs on certain customers.[149] In order to attract high-roller gamblers, the casino's president and chief operating officer explicitly agreed not to identify those customers in CTRs. The casino instead named the promoter who had brought in the high rollers or structured the transactions to avoid filing a CTR.
- In December 2016, FINRA fined Citi International Financial Services, LLC $5,750,000 for compliance failures associated with securities transactions that facilitated the conversion of foreign currency into and out of U.S. currency. Citi International Financial Services permitted foreign customers to purchase shares of stock on a local stock exchange in local currency, but then package the foreign securities into American Depository Receipts for sale on U.S. markets to generate U.S. dollar proceeds without adequate AML risk management. The scenario also involved the packaging of U.S. securities for sale on foreign markets to generate proceeds in foreign currencies. Over a two year period, these transactions had an aggregate value of $380 million.
- In September 2016, FINRA fined Raymond James Associates, Inc. and Raymond James Financial Services, Inc., $8 million and $9 million, respectively, for failing to dedicate

[146] https://www.fincen.gov/sites/default/files/enforcement_action/2017-02-27/Merchants%20Bank%20of%20California%20Assessment%20of%20CMP%2002.24.2017.v2.pdf
[147] http://www.dfs.ny.gov/about/press/pr1701301.htm.
[148] https://www.fincen.gov/sites/default/files/enforcement_action/Thriftway_Assessment.pdf
[149] https://www.justice.gov/usao-cdca/pr/normandie-casino-operator-agrees-plead-guilty-federal-felony-charges-violating-anti.

resources to the firms' AML compliance programs commensurate with the firms' growth. The firms allowed red flags of potentially suspicious activity to go undetected or inadequately investigated. FINRA had previously fined Raymond James Financial Services, Inc. $400,000 in 2012 for failing to detect and report suspicious transactions in the accounts of a customer who was operating a Ponzi scheme.

- In June 2016 FINRA censured Avila Capital Markets, Inc. and fined the firm $350,000 for executing transactions for customers in high risk jurisdictions for money laundering without tailoring its AML program to its foreign customer base or its Venezuelan bond business, which constituted the majority of the firms' revenue. During a three year period, the firm facilitated the sale of over $2.5 billion in Venezuelan bonds. Despite public pronouncements identifying Venezuela as posing a high money laundering and terrorist financing risk, the firm neither established nor implemented a program reasonably designed to cause the detection and reporting of suspicious transactions associated with these bonds. In addition to the fine and censure, the firm was required to engage an independent consultant to review its policies, systems and procedures.

8. Criminal Violations

The most severe AML compliance deficiencies can result in criminal prosecution. These enforcement actions differ from supervisory enforcement actions, which seek to remedy BSA compliance deficiencies that have not risen to the criminal level. These cases of egregious or willful criminality are often—but not always—resolved by DOJ with a deferred prosecution agreement (DPA) or a non-prosecution agreement (NPA).

DPAs and NPAs can involve, among other things, an admission of wrongdoing by the institution; the imposition of fines, penalties, or forfeitures; the installation of an independent monitor; and a requirement to implement specific remedial actions to improve compliance within a designated timeframe. Strategic considerations—such as the ability to affect compliance improvements in the financial institution's worldwide operations or the decision not to jeopardize the institution's U.S. banking license—may make a DPA or NPA an attractive alternative to an immediate criminal charge, the possibility of which persists for the term of the agreement in the event of a breach.

Between 2015 and 2017, DOJ entered into two new BSA-related DPAs against banks; one new NPA against a bank; one new DPA against an MSB; and one DPA against a bank employee. During this period, DOJ also monitored conduct and remedial measures by financial institutions that had previously entered into AML and sanctions-related agreements. In 2018, DPAs that would have otherwise expired were extended: one with a bank and another with an MSB.

- In May 2017, Banamex USA (BUSA), a subsidiary of Citigroup Inc., entered into an NPA admitting to criminal violations, including the willful failure to maintain an effective AML compliance program and willful failure to file SARs.[150] From 2007 through at least 2012, the bank's monitoring system generated more than 18,000 alerts involving more than $142 million in potentially suspicious remittance transactions, but

[150] DOJ, Press Release, https://www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations.

BUSA conducted fewer than ten investigations and filed only nine SARs as a result of these alerts. The bank failed to file SARs on suspicious remittance transactions to Mexico that fit typologies consistent with human smuggling, fraud, and drug trafficking.[151] BUSA also admitted that it should have improved its monitoring of MSB remittances but failed to do so. In July 2015, the FDIC and California Department of Business Oversight had ordered BUSA to pay a $140 million civil money penalty to resolve separate BSA regulatory investigations.[152] In February 2017, the FDIC also announced enforcement actions against four former senior BUSA executives relating to BSA violations.

- In January 2017, the Western Union Company (WU), a global MSB, entered into a DPA in which it admitted to criminal violations, including willfully failing to maintain an effective AML program and aiding and abetting wire fraud.[153] Between 2004 and 2012, Western Union violated the BSA and anti-fraud statutes by processing hundreds of millions of dollars of illicit transactions, some involving complicit WU agents. The illegal activity included payments associated with international consumer fraud schemes and structured transactions to China related to human smuggling. In connection with the DPA, WU agreed to forfeit $586 million, the largest forfeiture ever imposed on a MSB. Concurrently, FinCEN assessed a civil penalty of $184 million.[154]
- In June 2015, Bank of Mingo in West Virginia entered into a DPA for its failure to develop, implement, and maintain an effective AML program. The bank was charged with failing to implement internal controls that would have resulted in the bank obtaining "know-your-customer" information, failing to prevent customers from structuring cash transactions to avoid CTR requirements, and failing to file SARs about certain dubious conduct, such as the structuring of cash transactions. The bank agreed to forfeit $2.2 million, representing the amount involved in illegally structured currency transactions.[155] Concurrently, FinCEN[156] and the FDIC[157] assessed civil penalties.
- In February 2018, Rabobank, the California subsidiary of the Netherlands-based Coöperatieve Rabobank U.A., pleaded guilty to conspiracy to defraud the United States and to corruptly obstruct an examination of a financial institution.[158] Rabobank also agreed to forfeit almost $369 million for allowing illicit funds to be processed through the bank without adequate AML controls. In its plea, Rabobank admitted to conspiring with several former executives to defraud the United States by unlawfully impeding the OCC's ability to regulate the bank and to obstruct an examination by the OCC of its operations throughout California. Rabobank admitted that its deficient AML program allowed hundreds of millions of dollars in untraceable cash, sourced from Mexico and elsewhere, to be deposited into its bank branches on the southwest border and transferred

[151] DOJ, Press Release, https://www.justice.gov/opa/press-release/file/967871/download
[152] FDIC, Press Release, https://www.fdic.gov/news/news/press/2015/pr15061.html
[153] https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million
[154] https://www.fincen.gov/news/news-releases/fincen-fines-western-union-financial-services-inc-past-violations-anti-money
[155] https://www.justice.gov/usao-sdwv/pr/us-attorney-booth-goodwin-announces-charge-against-bank-mingo.
[156] https://www.fincen.gov/news/news-releases/fincen-penalizes-west-virginia-bank-serious-bsa-violations-and-actions-branch
[157] https://www.fdic.gov/news/news/press/2015/pr15049.html
[158] https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million.

via wire transfers, checks, and cash transactions, without proper notification to federal regulators as required by law. Rabobank executives then sought to hide and minimize the deficiencies in its AML program during a 2012 OCC exam in order to deceive the regulators and avoid additional regulatory sanctions that had previously been imposed on Rabobank for nearly identical failures. A former Rabobank vice president entered into a DPA with the DOJ in December 2017 for his role in aiding and abetting Rabobank's failure to maintain an adequate AML program. The OCC assessed a $50 million civil money penalty against the bank.[159]

[159] https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-15.html

CONCLUSION

Anonymity in transactions and funds transfers is the main risk that facilitates money laundering. It is most evident in the use of U.S. currency for illicit retail transactions, such as drug trafficking, human smuggling and trafficking, and various activities associated with organized crime. There is also the movement of currency in bulk to drug suppliers in Mexico and Colombia. Even when illicit drugs are sold online, there are case examples of payment in currency sent through the mail. In some examples of fraud, such as healthcare fraud and business e-mail compromise, criminals complete the crime using an electronic funds transfer through the banking system, but then begin the money laundering process by withdrawing cash in order to break the paper trail and disguise the source of the funds.

To the extent that virtual currencies are able to provide the same level of anonymity as physical cash, they create an even greater risk because virtual currencies can be transmitted and used globally. In addition to providing another means to pay for contraband or illicit services, virtual currencies also are now being used in the layering stage of money laundering to disguise the origin of illicit proceeds.

The risk of the misuse of cash and even virtual currency is mitigated in the United States by transaction recordkeeping and reporting requirements that create obligations for certain financial institutions. Even businesses and individuals have cash reporting obligations in certain circumstances. But these obligations are only effective to the extent they are followed. The vast majority of financial Institutions' BSA/AML compliance programs are successful in effectively managing money laundering risks; however, given the size of the U.S. financial system and scope of the economy, it is not completely surprising that are examples of complicity and lax compliance which undermine existing safeguards.

The reason trade exists as a money laundering vehicle facilitating TBML is because there are merchants who are either knowingly complicit in accepting illicit cash in exchange for trade goods, and fail to report the transaction as required, or they are willfully blind in accepting payment by check or wire from money brokers acting on behalf of the merchants ordering goods for import. Lawyers, accountants, company registration agents, and real estate agents also may be complicit or willfully blind when they create shell companies, open bank accounts, and conduct transactions, including property purchases. All of which have the effect of allowing criminals, including corrupt foreign political figures, to launder their illicit proceeds.

Complicit insiders and compliance deficiencies at financial institutions pose a particularly significant money laundering risk because of the potential consequences. The case examples presented illustrate that a financial institution with a grossly inadequate BSA/AML compliance program can have the same effect, allowing millions of dollars in suspicious transactions to occur without adequate screening or reporting.

Case examples demonstrate that professional money launderers continually seek out banks and MSBs with either weak controls or corruptible staff to gain access to the financial system. Even ordinary citizens recruited online are being enticed into knowingly becoming money mules and helping criminals launder illicit proceeds.

Money laundering schemes have relied on the use of shell companies and other legal entities formed to conceal the identity of the individuals who own or control the illicit money, particularly when the money moves across borders. New requirements to identify the beneficial owner of legal entities at account opening should mitigate this money laundering risk.
As long as crime is committed for economic gain and vulnerabilities present opportunities, money laundering will adapt, evolve, and persist. The illicit use of virtual currencies, scope of global money laundering network operations, and recruitment of sometimes unwitting money mules to facilitate the laundering process demonstrate how money laundering is adapting and evolving. U.S. law enforcement and regulatory agencies work together to stay abreast of money laundering methods and maintain close relationships with foreign counterparts to share information and bolster opportunities for cooperation.