National Money Laundering Risk Assessment

2015

The fight against money laundering and terrorist financing is a pillar of U.S. national security and a strong financial system. It is an undertaking that requires the coordinated and dedicated efforts of policy makers, law enforcement, supervisors, and the private sector, particularly financial institutions. It is essential that we work closely together to develop and effectively implement strong laws and regulations to detect, deter, and disrupt illicit finance. Equally important is that we understand and communicate the money laundering and terrorist financing threats, vulnerabilities, and risks facing our country.

In this spirit, the Department of the Treasury is proud to publish the National Money Laundering Risk Assessment and National Terrorist Financing Risk Assessment. These reports – based on an analysis of more than 5,000 law enforcement cases, financial reporting by U.S. financial institutions and reports from across government and the private sector – represent an unprecedented review of the key money laundering and terrorist financing risks to the United States. The purpose of these assessments is to help the public and private sectors understand the money laundering and terrorist financing methods used in the United States, the risks that these activities pose to our financial system and national security, and the effectiveness of our current efforts to combat these methods. Our goal is to more effectively target and prevent these activities.

These assessments should be used by industry and other stakeholders to help inform a risk-based approach to identify, assess, and manage risks in compliance with their obligations under the Bank Secrecy Act and sanctions laws. It is the view of the Treasury Department that financial institutions that establish and maintain appropriate risk-based anti-money laundering programs will be well positioned to effectively manage accounts, prevent illicit transactions, and avoid enforcement action. The assessments published today should be used as one additional tool in evaluating risk, but should not be read in isolation. Additionally, these assessments can help financial institutions determine how best to efficiently allocate resources to combat money laundering and terrorist financing.

The United States has a large, complex, and open financial system – making it a destination for legitimate trade and investment, but also a target for illicit activity and actors. Our anti-money laundering and countering the financing of terrorism framework is sophisticated and well-designed to address these threats, while maintaining an attractive business environment. Our law enforcement and supervisory authorities are well equipped to investigate and take enforcement actions when our financial system is abused by illicit actors. In addition, the U.S. financial sector is a key partner in our efforts to combat illicit finance – our financial institutions devote considerable time and resources to identifying and assessing risks and in taking steps to mitigate those risks.

We hope these reports will be a centerpiece of the robust public and private sector efforts that are underway to mitigate the illicit finance risks facing the United States as we work together to make the U.S. financial sector the safest and most secure in the world.

Adam J. Szubin
Acting Under Secretary, Terrorism and Financial Intelligence

Table of Contents

EXECUTIVE SUMMARY 1
Threats 2
Vulnerabilities 3
Risks 4

INTRODUCTION 5
Participants 6
Sources 7
Methodology 9

SECTION I. THREATS: PREDICATE CRIMES 10
A. Fraud 11
B. Drug Trafficking 14
C. Human Smuggling 17
D. Organized Crime 17
E. Public Corruption 20

SECTION II. VULNERABILITIES AND RISKS: MONEY LAUNDERING METHODS 22
A. Cash 23
B. Banking 35
C. Money Services Businesses 54
D. Casinos 74
E. Securities 78

CONCLUSION 85

Executive Summary

EXECUTIVE SUMMARY

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

Threats

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

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

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

Drug trafficking is a cash business generating an estimated $64 billion annually from U.S. sales. Mexico is the primary source of supply for some drugs and a transit point for others. Although there are no reliable estimates of how much money Mexican drug trafficking organizations earn overall (estimates range from $6 billion to $39 billion), for cocaine, Mexican suppliers are estimated to earn about 14 cents

[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 separate the proceeds from the crime through a series of transactions; and (3) integration, where the illicit funds re-enter the economy disguised as legitimate funds.

of every dollar spent by retail buyers in the United States. It is the thousands of low level drug dealers and distributors throughout the country who receive most of the drug proceeds.

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

International organized crime groups target U.S. interests both domestically and abroad. The criminal activity associated with these groups includes alien smuggling, drug trafficking, extortion, financial fraud, illegal gambling, kidnapping, loan sharking, prostitution, racketeering, and money laundering. Some groups engage in white-collar crimes and co-mingle illegal activities with legitimate business ventures.

Vulnerabilities

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

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

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

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

To move funds into an account at a bank or broker-dealer, case examples show criminals may use an individual, serving as a nominee, to open the account and shield the identities of the criminals who own

and control the funds. Alternatively, the account may be opened in the name of a business that was created to hide the beneficial owner who controls the funds.

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

Risks

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

- Widespread use of cash, making it difficult for authorities to differentiate between licit and illicit use and movement of bank notes;
- Structured transactions below applicable thresholds to avoid reporting and recordkeeping obligations;
- Individuals and entities that disguise the nature, purpose, ownership, and control of accounts;
- Occasional AML compliance deficiencies, which are an inevitable consequence of a financial system with hundreds of thousands of locations for financial services;
- Complicit violators within financial institutions; and
- Complicit merchants, particularly wholesalers who facilitate TBML, and financial services providers.

The case examples cited throughout the NMLRA show that criminals use every feasible money laundering method available to them, exploiting opportunities wherever they find them. This means that in practice, different money laundering methods are used simultaneously or sequentially, or are alternated in response to actions taken by law enforcement and financial supervisors. The continuously shifting and opportunistic focus of money launderers makes it difficult and potentially misleading to attempt to rank order financial services or sectors on the basis of money laundering risk.

[2] *See* U.S. Terrorist Financing Risk Assessment 2015.

INTRODUCTION

INTRODUCTION

The 2015 National Money Laundering Risk Assessment (NMLRA) identifies the money laundering risks that are of priority concern to the United States. The purpose of the NMLRA is to help the public and private sectors recognize and understand the money laundering methods used in the United States, the effectiveness of current efforts to address the threats and vulnerabilities that create money laundering opportunities, and the residual risk to the financial system and national security.

The NMLRA updates and expands the National Money Laundering Threat Assessment (MLTA) of 2005[3] by:

- Consolidating information from agency-specific, Congressional, and White House sources published since 2006;
- Identifying case examples and trends from approximately 5,000 money laundering-related federal prosecutions (2006-2011);
- Drawing from the work of the interagency Task Force on the U.S. Anti-Money Laundering Framework and the Securities and Derivatives Markets Working Group, which have identified illicit financing threats, trends, and risks in the United States; and
- Identifying priority money laundering risks.

Participants

The NMLRA was drafted by the Department of the Treasury's Office of Terrorist Financing and Financial Crimes (TFFC). In preparing the NMLRA, TFFC consulted with the following offices and agencies:

- Department of the Treasury
    - Terrorism and Financing Intelligence
        - Financial Crimes Enforcement Network (FinCEN)
        - Office of Foreign Assets Control (OFAC)
        - Office of Intelligence and Analysis (OIA)
        - Treasury Executive Office of Asset Forfeiture (TEOAF)
    - Internal Revenue Service (IRS)
        - Criminal Investigations (CI)
        - Small Business/Self-employed (SBSE)
- Department of Justice (DOJ)
    - Executive Office for United States Attorneys (EOUSA)
    - Asset Forfeiture and Money Laundering Section (AFMLS)

[3] U.S. Money Laundering Threat Assessment, U.S. Money Laundering Threat Assessment Working Group, 2005.

  - Drug Enforcement Administration (DEA)
  - Federal Bureau of Investigation (FBI)
- Department of Homeland Security (DHS)
  - Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI)
  - United States Secret Service (USSS)
- Department of Health and Human Services (HHS)
- United States Postal Service (USPS)
- Staff of the Federal functional regulators (FFR)[4]

Sources

The NMLRA is compiled from agency-specific, interagency, and Congressional advisories, analysis, guidance, reports, and testimony published since 2006, new domestic research and analysis, and relevant private sector and international studies. Private sector input was incorporated through analysis conducted by the Financial Crimes Enforcement Network (FinCEN) of Bank Secrecy Act reporting, including suspicious activity reports (SARs) and currency transaction reports (CTRs).

The Department of the Treasury, with the support of EOUSA, conducted an unprecedented analysis of some 5,000 federal indictments and other charging documents alleging money laundering and related charges in cases from 2006 to 2011.[5] The criminal charging documents reviewed cited at least one of the following money laundering-related charges:

- Title 18 of the U.S. Code, Section 1956, which prohibits conducting a financial transaction with the proceeds of any of a number of specified unlawful activities (SUAs) with the specific intent to promote an SUA; conceal or disguise the source, origin, nature, ownership, or control of the proceeds; evade reporting requirements; or evade taxes. The SUAs for 18 U.S.C. § 1956 and 18 U.S.C. § 1957 are identified at 18 U.S.C. § 1956(c)(7). This statute also criminalizes the international movement of criminal proceeds with the specific intent to conceal or disguise the source, origin, nature, ownership, or control of the proceeds or to evade reporting requirements. Even the international movement of clean money is illegal if the movement is conducted with the specific intent of promoting illegal activity.
- Title 18 of the U.S. Code, Section 1957, which makes it a crime to conduct a monetary transaction of more than $10,000 knowing those funds were proceeds of an SUA.

[4]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, 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 and the Chicago Mercantile Exchange Group, Inc.

[5] Many states also have laws against money laundering. *See* Appendix A for list of state money laundering laws.

- Title 18 of the U.S. Code, Section 1960, which prohibits operating a money transmitting business without obtaining a state license, if one is required; without registering with the Financial Crimes Enforcement Network; or, regardless of the business's license or registration status, transmitting or transporting funds derived from a criminal offense or intended to be used to promote or support unlawful activity.
- Title 31 of the U.S. Code, Section 5313, which 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.
- Title 31 of the U.S. Code, Section 5316, requires an individual to file a Currency or Monetary Instruments Report (CMIR) with FinCEN whenever the individual brings into or takes out of the country more than $10,000 in monetary instruments, including currency, traveler's checks, and all bearer negotiable financial instruments. Willful failure to file a CMIR is criminalized under Title 31 of the U.S. Code, Section 5322.
- Title 31 of the U.S. Code, Section 5324, prohibits anyone from intentionally structuring transactions in amounts less than $10,000 specifically to evade the CTR, CMIR, or Form 8300 filing requirements and prohibits anyone from filing a CTR, CMIR, or Form 8300 that contains a material omission or misstatement.
- Title 31 of the U.S. Code, Section 5331, which requires a nonfinancial trade or business to file a Form 8300 with FinCEN for each cash transaction or two or more related cash transactions in a day that aggregate to more than $10,000. Willful failure to file a Form 8300 is criminalized under Title 31 of the U.S. Code, Section 5322.
- Title 31 of the U.S. Code, Section 5332, which makes it a crime to conceal and transport more than $10,000 in currency or other monetary instruments into or out of the United States with the intent to evade the CMIR requirement.

These statutes encompass a broad range of money laundering activity. It should be noted, however, that not all prosecutions for financial crimes include a money laundering or related charge, so the indictments and other court documents reviewed are not necessarily representative of all financial crime prosecutions. Additionally, the criminal charging documents were not intended to support this type of research as criminal charging documents need not catalog every criminal act or detail. Despite the flaws inherent in this type of study, the data provide a revealing glimpse into the state of illicit finance in the United States. The case examples cited in the NMLRA illustrate current money laundering risks. The cases reveal a number of ultimately failed schemes to launder money.

Methodology

The terminology and methodology of the NMLRA are based on the guidance of the FATF,[6] which presents a process for conducting a risk assessment at the national level. This approach uses the following key concepts:

- **Threats**: These are the predicate crimes that are associated with money laundering. In some cases, specific crimes are associated with specific money laundering methods. Understanding the threat environment is essential to understanding the vulnerabilities that create money laundering opportunities, and to understanding the residual risks.
- **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, or reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity.
- **Consequence**: Not all money laundering methods have equal consequences. The methods that allow for the most amount of money to be laundered most effectively or most quickly present the greatest potential consequences.
- **Risk**: Risk is a function of threat, vulnerability, and consequence. It represents a summary judgment.

The NMLRA uses all available information to identify as objectively as possible the priority money laundering risks to the United States.[7] The fact-finding and assessment process involved:

- Identifying the nature and volume of predicate financial crime in the United States to determine the source of domestic illicit proceeds;
- Tallying the money laundering methods identified through civil and criminal investigations and criminal prosecutions;
- Assessing the deterrent effect of domestic regulation, supervision, and enforcement on potential money laundering methods; and
- Using the foregoing research and analysis to identify residual money laundering risks in the United States.

The NMLRA begins with an overview of the predicate crimes associated with money laundering that are the threats present in the United States. Following this overview, a chapter is devoted to each of the financial sectors identified as money laundering conduits in law enforcement investigations and prosecutions, supervisory examinations, and reporting to FinCEN. Each chapter identifies the relevant preventive measures, money laundering vulnerabilities with case examples, and the residual risks.

[6] FATF Guidance, National Money Laundering and Terrorist Financing Risk Assessment, February 2013.
[7] The NMLRA considers the threat, vulnerabilities, consequences, and risks posed to the United States as a whole, as opposed to the risks relevant to a financial institution. Each financial institution should conduct its own risk assessment based on vulnerabilities and other relevant factors specific to that financial institution.

Threats: Predicate Crimes

SECTION I. THREATS: PREDICATE CRIMES

The United Nations Office on Drugs and Crime (UNODC) estimated proceeds from all forms of financial crime in the United States, excluding tax evasion, was $300 billion in 2010, or about two percent of the U.S. economy.[8] This is comparable to U.S. estimates. UNODC estimates illicit drug sales were $64 billion[9], which the DEA believes is a reasonable current estimate, putting the proceeds for all other forms of financial crime in the United States at $236 billion, most of which is attributable to fraud.

A. Fraud

The dollar volume of fraud dwarfs other illicit proceeds-generating crimes in the United States. Unlike drug trafficking, fraud proceeds rarely start off as a cash purchase. The transactions typically occur through normal, regulated financial channels and are intended to appear as legitimate.[10] Criminals will, however, use check cashers, money transmitters, automated teller machines (ATMs), and normal withdrawals or transfers from bank or brokerage accounts to cash out fraud proceeds.

A number of crimes today involve misuse of computers and illicit computer access via the Internet. According to DOJ, "One study earlier this year found that the United States is number one in data breaches world-wide — accounting for about 76 percent of all incidents in 2014. Another study last summer estimated the annual cost of cybercrime at no less than $400 billion."[11] Law enforcement has been encountering criminal misuse of computers since the early 1980s, the dawn of the computer age.[12] The Computer Fraud and Abuse Act (CFAA) brought existing law up to date in 1986 in order to address the unauthorized access and use of computers and computer networks. Since then, the CFAA has been amended at least eight times as computer crimes have grown in sophistication. Cyber criminals today can attack the U.S. from overseas, beyond the immediate reach of American law enforcement. To respond, U.S. authorities work closely with foreign counterparts and use a combination of civil and criminal tools. Cybercrime can exploit new payment technologies for money laundering, but may also rely on low technology options.

1. Healthcare Fraud

According to the FBI, the National Health Care Anti-Fraud Association estimates that 3 to 5 percent of total health care expenses are fraudulent.[13] Healthcare fraud accounts for the largest dollar volume of

[8] United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting From Drug Trafficking and other Transnational Organized Crimes, October 2011.
[9] Estimates vary. RAND Corporation estimated $100 billion in the study, "What America's Users Spend on Illegal Drugs: 2000-2010," prepared for ONDCP, Office of Research, February 2014. Available at http://www.whitehouse.gov/sites/default/files/ondcp/policy-and-research/wausid_results_report.pdf
[10] FinCEN published guidance for financial institutions on potential indicators of healthcare fraud in the SAR Activity Review, Issue 20, October 2009.
[11] Caldwell, Leslie R., Assistant Attorney General, Remarks at the Criminal Division's Cybersecurity Industry Roundtable, Washington, D.C., April 29, 2015.
[12] DOJ, *Prosecuting Intellectual Property Crimes* (Office of Legal Education 2013).
[13] FBI, DOJ, FY 2014 Authorization and Budget Request to Congress, April 2013. That would put healthcare fraud between $84 billion and $140 billion based on the Centers for Medicare and Medicaid Services tally of $2.8 trillion in healthcare spending in 2012. Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html

fraud losses to the federal government, approximately $80 billion annually.[14] Healthcare fraud also victimizes private sector insurance companies.[15] The FBI estimates insurance fraud to be a separate $30 billion dollar a year enterprise.[16] Payments are often obtained illegally by check and cashed through check cashing services, some of which are complicit in the fraud. Medical identity theft, in addition to victimizing the payer, can also take advantage of unsuspecting patients and medical professionals. Often the information is "stolen by employees at medical facilities, and resold on the black market."[17] In May 2009, the DOJ and HHS created the Health Care Fraud Prevention and Enforcement Action Team (HEAT).[18] HEAT's work led to a 75 percent increase in individuals charged with criminal healthcare fraud from 2008 to 2011.[19] In FY 2013, the Justice Department opened 1,013 new criminal health care fraud investigations.

2. Identity Theft

According to DOJ, Bureau of Justice Statistics, direct and indirect losses from identity theft totaled $24.7 billion in 2012. Among identity theft victims, existing bank (37%) or credit card accounts (40%) were the most common types of misused information.[20] Identity theft refers to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception. A stolen payment card or hacked bank or brokerage account may be referred to as access device fraud, bank fraud, credit card fraud, cyber fraud, and/or identity theft. Cybercriminals who steal personal data may exploit it themselves or sell it. Typical sales of stolen identity information involve funds transfers through money transmitters and are often under the $3,000 federal recordkeeping threshold.[21] When transferring funds out of a hacked bank account, cybercriminals may hire intermediaries ("money mules") who receive the fraudulent funds transfers often without knowing the transactions are illegal.[22] The money mules are instructed to take a percentage of the funds they receive as their compensation and forward the rest via a licensed money transmitter, often to a recipient outside the United States. Recent cases demonstrate cybercriminals can avoid using money mules by transferring funds from hacked accounts to prepaid debit cards, and cashing out at an ATM.

[14] FBI, Health Care Fraud. Available at http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud
[15] Available at http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud
[16] Available at http://www.fbi.gov/news/stories/2012/january/insurance_013112
[17] Medical Identity Theft, Coalition Against Financial Fraud. Available at http://www.insurancefraud.org/scam-alerts-medical-id-theft.htm#.UyXbF6hdWSo
[18] Peter F. Neronha, United States Attorney District of Rhode Island, "Efforts to Prevent, Investigate, and Prosecute Medicare and Medicaid Fraud," Testimony before the U.S. Senate Committee on Judiciary Committee, Subcommittee on Crime and Terrorism, March 26, 2012.
[19] HHS, Medicare Fraud Strike Force Charges 91 Individuals for Approximately $430 Million in False Billing, October 4, 2012. Available at http://www.hhs.gov/news/press/2012pres/10/20121004a.html
[20] Erika Harrell, Ph.D. and Lynn Langton, Ph.D., DOJ, Office of Justice Programs, Bureau of Justice Statistic, Victims of Identity Theft, 2012. Available at http://www.bjs.gov/content/pub/pdf/vit12.pdf
[21] *See* https://www.ftc.gov/news-events/press-releases/2009/10/moneygram-pay-18-million-settle-ftc-charges-it-allowed-its-money
[22] *See* http://www.fbi.gov/newyork/press-releases/2010/nyfo093010.htm

3. Tax Fraud

The IRS found $6.5 billion in attempted fraudulent tax refunds in 2010, and the Treasury Inspector General for Tax Administration (TIGTA) found potentially $5.2 billion more.[23] Tax fraud linked to identity theft increased to more than 1.1 million cases in 2011, up from 51,700 in 2008.[24] Identity thieves who obtain a legitimate taxpayer's name and Social Security number can file a fraudulent claim for a tax refund early in the filing season before the legitimate taxpayer files. Income tax refunds can be paid by paper check or electronically either via direct deposit to a bank account or to a prepaid debit card. Criminals can open prepaid debit card accounts online using stolen identity information, and then cash out a fraudulent tax refund at an ATM. To help financial institutions identify and report suspicious transactions associated with potential tax refund fraud, FinCEN issued an Advisory on February 26, 2013, identifying red flag indicators associated with potentially fraudulent tax refund direct deposit transactions.[25]

4. Mortgage Fraud

Mortgage fraud results in an estimated $4 billion to $6 billion in annual losses in the United States.[26] Mortgage fraud schemes contain some material misstatement, misrepresentation, or omission that is relied on by an underwriter or lender to fund, purchase, or insure a loan.[27] Mortgage fraud can be used to generate illicit profits or to qualify for housing. On August 16, 2012, FinCEN issued an advisory highlighting common fraud schemes and potential red flags related to mortgage loan fraud so that financial institutions may better assist law enforcement when filing suspicious transactions.[28] Drug traffickers and others who rely on an illicit cash income use mortgage fraud to acquire property. Between 2005 and 2013 pending FBI mortgage fraud investigations almost tripled to 1,954, with close to 70 percent involving losses of more than $1 million.[29] The FBI currently has 84 task forces or working groups investigating complex financial crimes including mortgage fraud.

5. Retail and Consumer Fraud

As payment alternatives have increased and the Internet has expanded sales options, the role of third party payment processors (TPPPs) has grown. TPPPs are bank customers that provide payment-processing services to merchants and other business entities. TPPPs work for merchants to facilitate non-cash payments, and some facilitate fraud. One indication of a problem is an unusually high rate of reversed transactions because of consumer complaints. The industry average return rate for automated clearing house transactions is less than 1.5 percent, and less than 0.5 percent for checks, but some processors and

[23] Treasury Inspector General for Tax Administration, There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft, July 19, 2012, Reference Number: 2012-42-080. Available at http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html
[24] *Id*.
[25] FinCEN, Advisory, Tax Refund Fraud and Related Identity Theft, FIN-2013-A001, February 26, 2013.
[26] National Associate of Realtors®. Available at http://www.realtor.org/rmoquiz2.nsf/mortgagefraud?openform
[27] Available at http://www.fbi.gov/about-us/investigate/white_collar/mortgage-fraud/mortgagefraudwarning.pdf
[28] FinCEN, Advisory, Suspicious Activity Related to Mortgage Loan Fraud, FIN-2012-A009, August 16, 2012.
[29] Robert S. Mueller III, Director, FBI, Testimony before the Senate Judiciary Committee, December 14, 2011; FBI, Just the Facts, Mortgage Fraud Statistics. Available at http://www.fbi.gov/about-us/investigate/white_collar/mortgage-fraud.

merchants have return rates of up to 85 percent.[30] The FDIC and the OCC have issued guidance regarding the risks associated with banking TPPPs.[31] FinCEN issued an Advisory on the risk associated with TPPPs on October 22, 2012.[32]

6. Securities Fraud

The term securities fraud covers a wide range of illegal activities including, among others, affinity fraud, high yield investment programs, microcap fraud, Ponzi schemes, pre-initial public offering investment scams, pyramid schemes, insider trading, market manipulation, and pump and dump schemes.[33] Securities accounts can be used to originate illicit proceeds through the implementation of these fraudulent securities trading practices. Securities fraud is the most common predicate crime for criminal money laundering cases involving transactions through broker-dealers. The proceeds of drug trafficking and other crimes sometimes find their way into brokerage accounts at the layering stage more than at the placement stage.[34] Most identified cases of illicit activity in the securities markets relate to some form of fraud, including securities fraud, identity theft, or embezzlement. In 2013, the SEC filed 686 enforcement actions, which resulted in more than $3.4 billion in disgorgement of illicit profits and penalties combined.[35]

B. Drug Trafficking

Although drug use in America has declined by one-third since its peak in the late 1970s,[36] recent data show a mixed picture. According to the 2012 National Survey on Drug Use and Health, the number of people using marijuana, the most popular illegal drug in America, increased by 30 percent between 2007 and 2012.[37] During the same period, the survey shows heroin use almost doubled, cocaine use fell by a third, and use of methamphetamines dropped by 40 percent.

In 2011, the National Drug Intelligence Center (NDIC) found that Mexican-based drug trafficking organizations (DTOs) "dominate the supply, trafficking, and wholesale distribution of most illicit drugs in the United States. Various other [DTOs] operate throughout the country, but none impacts the U.S. drug trade as significantly as Mexican-based traffickers. Reasons for Mexican organizations' dominance include their control of smuggling routes across the U.S. southwest border and their capacity to produce, transport, and/or distribute cocaine, heroin, marijuana, and methamphetamine."[38] Other DTOs and gangs

[30] Michael J. Bresnick, Financial Fraud Enforcement Task Force Executive Director, Remarks at the Exchequer Club of Washington, D.C., March 20, 2013.
[31] FDIC, Guidance on Payment Processor Relationships, FDIC FIL-127-2008, November 7, 2008 (revised July 2014); Risk Management Guidance: Payment Processors, OCC Bulletin 2008-12, April 24, 2008.
[32] FinCEN, Advisory, Risk Associated with Third-Party Payment Processors, FIN-2012-A010, October 22, 2012.
[33] *See* SEC, Investing Basics. Available at http://investor.gov/investing-basics/avoiding-fraud/types-fraud
[34] *See* USA v. Oladimeji Seun A Yelotan, (S.D. Miss., July 8, 2014)(1:14-cr-00033-HSO-JMR); Zions First National Bank, Civil Money Penalty, FinCEN, Feb. 10, 2011.
[35] *Fiscal Year 2013 Agency Financial Report*, U.S. Securities and Exchange Commission, at p. 17. Available at http://www.sec.gov/about/secpar/secafr2013.pdf; *Fiscal Year 2014 Agency Financial Report*, U.S. Securities and Exchange Commission, at p. 19. Available at http://www.sec.gov/about/secpar/secafr2014.pdf
[36] R. Gil Kerlikowske, Director, National Drug Control Policy, Remarks before the 51st Regular Session of Inter-American Drug Abuse Control Commission, Washington, DC, May 9, 2012.
[37] HHS, Results from the 2012 National Survey on Drug Use and Health: Summary of National Findings.
[38] NDIC, DOJ, National Drug Threat Assessment 2011.

based in Columbia and the Caribbean are involved in transporting and distributing drugs to and in the United States.[39]

Federal law enforcement agencies focus their investigative resources on the leadership of the major drug trafficking and money laundering organizations, which tend to be headquartered outside the United States. State and local law enforcement agencies focus more on street level drug dealers, who may be members of gangs affiliated with Latin American drug DTOs.[40] FBI estimates that 1.4 million people belong to 33,000 violent street gangs, motorcycle gangs, and prison gangs in the United States.[41] Gangs are engaged in robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. According to the 2011 National Gang Threat Assessment, prepared by the National Gang Intelligence Center, "[m]any US-based gangs have established strong working relationships with Central America and Mexico-based DTOs to perpetuate the smuggling of drugs across the US-Mexico and US-Canada borders."[42]

1. Marijuana

Although authorities agree marijuana is the most popular illegal drug in the United States, there is little additional information available.[43] In 2010 NDIC reported, "the amount of marijuana available in the United States—including marijuana produced both domestically and internationally—is unknown."[44] The Office of National Drug Control Policy concurs: "The extant methodology for estimating the amount of marijuana available to the United States lacks credibility."[45] State ballot initiatives were passed in 2012 legalizing marijuana in the states of Colorado and Washington, and more than a dozen other states have passed decriminalization measures.

2. Heroin

The number of people starting to use heroin has been steadily rising since 2007, which may reflect a shift away from abuse of prescription pain relievers to a similar, easier to obtain, and cheaper alternative.[46] Despite its recent surge in popularity, heroin remains one of the least used illegal drugs in the United States with around one percent of the population having tried it.[47] The U.S. heroin market is supplied entirely from foreign sources, with more than half of the supply coming from Mexico.[48] The increase in Mexican heroin production since 2006 coincides with a decrease in production in Colombia.[49] U.S. retail expenditure on heroin is estimated to be $12 billion.[50]

---

[39] *See* ONDCP overview of the Carribbean. Available at https://www.whitehouse.gov/ondcp/caribbean
[40] In addition to the federal statutes prohibiting money laundering (18 U.S.C. § 1956 and 18 U.S.C. § 1957), there are also prohibitions in some states allowing for state-level prosecutions for money laundering. See Appendix 1 for a list of state statutes prohibiting money laundering.
[41] *See* FBI overview of Gangs. Available at http://www.fbi.gov/about-us/investigate/vc_majorthefts/gangs
[42] National Gang Intelligence Center, FBI, National Gang Threat Assessment – Emerging Trends, 2011. Available at http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment
[43] HHS, Results from the 2012 National Survey on Drug Use and Health: Summary of National Findings.
[44] NDIC, National Drug Threat Assessment 2010.
[45] Drug Availability Estimates in the United States, ONDCP, 2012.
[46] National Institute on Drug Abuse, Letter from the Director. Available at http://www.drugabuse.gov/publications/research-reports/heroin/letter-director
[47] DEA FY 2012 Performance Budget.
[48] Drug Availability Estimates in the United States, ONDCP, June 2012.
[49] United Nations Office on Drugs and Crime, World Drug Report 2013.
[50] What America's Users Spend on Illegal Drugs, ONDCP, 2012.

3. Cocaine

The United States remains the single largest national cocaine market in the world, but this market has been in decline for 30 years because of law enforcement successes domestically and in Colombia, violence between DTOs, and a gradual decline in demand.[51] As much as 70 percent of the revenue generated by cocaine is earned by mid-level wholesalers and retail dealers.[52]

4. Methamphetamine

Methamphetamine is the most widely abused, domestically produced synthetic drug in the United States. According to DEA, Mexican DTOs produce at least 80 percent of the methamphetamine consumed in the United States.[53] However, domestic production is increasing.[54]

5. Synthetic/Designer Drugs

Synthetic or designer drugs are unregulated psychoactive substances designed to mimic the effects of controlled substances. Their use is proliferating.[55] Among students in the United States, use of designer drugs is already more widespread than the use of all other illicit drugs except marijuana. The vast majority of this new generation of designer drugs are developed and manufactured in foreign clandestine laboratories and then smuggled into the United States in bulk form or as finished product.[56]

Organized Crime Drug Enforcement Task Forces

The Department of Justice's Organized Crime Drug Enforcement Task Forces (OCDETF) coordinates federal law enforcement efforts against the largest national and international drug trafficking and money laundering organizations. Consistent with the President's National Drug Control Strategy, OCDETF attacks all elements of the most significant drug trafficking organizations affecting the United States including money laundering and firearms trafficking that support the drug trade. OCDETF coordinates the annual formulation of the Consolidated Priority Organization Target (CPOT) List, a multi-agency-nominated target list of the command and control elements of the most prolific international drug trafficking and money laundering organizations. Twenty-eight of the current 67 CPOT targets are based in Mexico. OCDETF also requires its participants to identify and nominate major Regional Priority Organization Targets (RPOTs) as part of the annual Regional Strategic Plan. As of the end of FY 2013, 94 percent of all active OCDETF investigations were multi-district, multi-state, multi-regional or international in scope.

Beginning in FY 2010, 100 percent of OCDETF investigations have had an active financial component. In FY 2013, 11 percent of OCDETF defendants were charged with financial violations and 74 percent of indictments resulting from OCDETF investigations included asset forfeiture. From FY 2010 to FY 2013 OCDETF investigations were responsible for the seizure of over $2.65 billion.

Source: Organized Crime Drug Enforcement Task Forces, Department of Justice, FY2015 Interagency Crime and Drug Enforcement Congressional Budget Submission

[51] United Nations Office on Drugs and Crime, World Drug Report 2013.
[52] United Nations Office on Drugs and Crime, Globalization of Crime, 2010.
[53] DEA, FY 2013 Performance Budget Congressional Submission.
[54] NDIC, Central Valley California High Intensity Drug Trafficking Area Drug Market Analysis 2010.
[55] United Nations Office on Drugs and Crime, World Drug Report 2013.
[56] Joseph T. Rannazzisi, DEA, Testimony before the U.S. Senate Caucus on International Narcotics Control, September 25, 2013.

Designer drugs, because they are not controlled substances, are sold openly on the shelves at gas stations, convenience stores, and via the Internet. At retail establishments they are sold with disclaimers such as "not for human consumption," in products masquerading as incense, potpourri, bath salts, plant food, glass/window and jewelry cleaner, badger repellant, and snail/slug repellant.[57]

DEA is leading an ongoing multinational law enforcement investigation, dubbed Project Synergy, which targets designer drug manufacturing and distribution networks. As of May 2014, 150 individuals have been arrested and more than $20 million in cash and assets has been seized. The investigation has uncovered a "massive flow of drug-related proceeds to countries in the Middle East, including Yemen, Jordan, Syria, and Lebanon, as well as other countries."[58]

C. Human Smuggling

Alien smugglers pay fees to DTOs to operate in the areas controlled by the DTOs, according to DHS, Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI).[59] Countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) use smugglers located in Mexico to cross the United States/Mexico border. The DTOs dictate when and where the smugglers will cross the border. In other respects the DTOs and human smugglers operate independently. Most illegal aliens entering the United States from Mexico are Mexican, and more than 90 percent of illegal Mexican migrants are assisted by professional smugglers.[60] Payment is typically made using money transmitters or bank deposits. FinCEN issued an advisory in September 2014 alerting financial institutions to red flag indicators of potentially illicit financial activity linked to human smuggling and human trafficking.[61]

D. Organized Crime

Organized criminal groups from all over the world are present in the United States and target the United States from abroad. These organizations include the Italian La Cosa Nostra (Mafia), as well as groups from Africa, Asia, Eurasia, and the Middle East.[62] Criminal activity associated with organized crime includes extortion, illegal gambling, kidnapping, loan sharking, murder, prostitution, and racketeering. These groups also smuggle aliens; traffic in drugs; commit financial fraud and counterfeiting; and launder money. Some organized criminal groups cooperate across ethnic and racial lines, engage in white-collar crimes, and co-mingle illegal activities with legitimate business ventures. According to the President's Strategy to Combat Transnational Organized Crime,[63] developing countries where the rule of law is weak

[57] *Id.*
[58] DEA News: Huge Synthetic Drug Takedown, news release, May 7, 2014. Available at http://www.dea.gov/divisions/hq/2014/hq050714.shtml
[59] Matthew Allen, Phoenix Special Agent in Charge, U.S. Immigration and Customs Enforcement Homeland Security Investigations, testimony before the House Committee on Homeland Security, Subcommittee on Border and Maritime Security, May 21, 2012.
[60] United Nations Office on Drugs and Crime, The Globalization of Crime, 2010.
[61] FinCEN, Advisory, Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking–Financial Red Flags, FIN-2014-A008, September 11, 2014.
[62] *See* FBI overview of Organized Crime. Available at http://www.fbi.gov/about-us/investigate/organizedcrime/overview
[63] White House, Strategy to Combat Transnational Organized Crime, July 2011. Available at https://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf

can be particularly susceptible to criminal influences. That Strategy cites a World Bank estimate of about $1 trillion spent annually on bribery of public officials, causing an array of economic distortions and damage to legitimate economic activity.

The International Organized Crime Intelligence and Operations Center (IOC-2) is the centerpiece of DOJ's transnational organized crime program. The role of the IOC-2 is to marshal the resources and information of nine U.S. law enforcement agencies, as well as federal prosecutors, to combat those transnational organized crime groups posing the greatest threat to the United States, including but not limited to those criminal organizations named on the Top International Criminal Organizations Target (TICOT) List.

1. La Cosa Nostra

La Cosa Nostra has operated in the United States for more than 100 years, becoming entrenched in almost all aspects of business, particularly in New York. While this organization will intermingle illicit proceeds with legitimate business profits, the FBI notes that one of the difficulties in tracing Mafia proceeds is the group's preference for cash (bank notes). Payouts related to fraud, extortion, and other criminal activities are generally made in cash. Mafia members will store up to several million dollars in cash rather than place the money in a bank.

In 2011 the FBI led the largest Mafia investigation in the Bureau's history, resulting in approximately 130 arrests, predominantly in New York.[64] Charges included murder, drug trafficking, arson, loan sharking, illegal gambling, witness tampering, labor racketeering, and extortion. According to the FBI New York field office, the Mafia extortion racket, or so-called "mob tax," alone generates millions of dollars annually.[65]

2. African Criminal Enterprises

African criminal enterprises have been identified in major metropolitan areas across the United States selling illegal drugs and perpetrating various fraud schemes.[66] The political, social, and economic conditions in African countries like Nigeria, Ghana, and Liberia have helped some enterprises expand globally. Nigerian criminal enterprises are among the most aggressive and expansionist of the international criminal groups. The Nigerian groups are infamous for their financial frauds, which cost the United States an estimated $1 billion to $2 billion annually. Schemes are diverse, targeting individuals, businesses, and government offices. Examples include:

- Advance fee (or 419) fraud which typically involves a person claiming to have access to a large amount of money that they are willing to share in return for help transferring or depositing the funds. The victim is asked for money to pay initial fees. After the money is transferred, the benefactor disappears.

[64] FBI, Mafia Takedown, news release, January 20, 2011. Available at http://www.fbi.gov/news/stories/2011/january/mafia_012011
[65] Statement by FBI New York Field Office Assistant Director in Charge Janice K. Fedarcyk, January 20, 2011.
[66] *See* FBI overview of African organized crime. Available at http://www.fbi.gov/about-us/investigate/organizedcrime/african

- Online dating scams, which involve taking advantage of individuals who are led to believe a serious relationship is developing. The victim may be asked for money to pay for travel in order to meet, or for a health emergency. Once the money is transferred the paramour disappears. Alternatively, the victim may be asked to perform some activity that helps to support another criminal scheme.
- Check cashing/funds transfer fraud, which involves a person outside the United States asking for help transferring funds. The victim, who may be contacted as a result of posting a resume online, may receive money orders, checks, or funds transfers, and is asked to take a percentage and transfer the funds offshore. The funds received are typically fraudulent or stolen.

Some element of each of these illicit activities was present in a 2014 indictment in Mississippi in which more than a dozen members of a Nigerian criminal organization were charged with fraud, account takeovers, and money laundering.[67] The group operated via the Internet, primarily from South Africa but with alleged co-conspirators in the United States and Canada. The group allegedly bought stolen credit card numbers, bank and brokerage account data, and personal identifying information online. They used the information to open new accounts, transferring value from the hacked accounts to banks accounts opened with stolen account information and altered or forged foreign passports. The group also used the stolen funds to buy consumer electronics, or transferred the money to prepaid cards. The group allegedly recruited additional victims and unknowing accomplices by sending mass e-mails to U.S. participants at online dating sites and other online community web sites. Some victims were sent counterfeit checks and asked to deposit them into their bank accounts and transfer the proceeds to recipients in Africa. Others were asked to receive shipment of fraudulently acquired merchandise and reship the goods to Africa.

3. Eurasian Organized Crime

According to law enforcement, Russian and Eurasian organized crime groups leverage close political ties abroad to protect their interests and facilitate access to the international financial system.[68] Eurasian organized crime groups are a particular concern because of their systemic use of sophisticated schemes to move and conceal their criminal proceeds using U.S. banking institutions and U.S. incorporated shell companies. FinCEN, citing SARs, reported in 2006 on the apparent abuse by Russian criminal groups of U.S. shell companies[69] used to open bank accounts outside the United States:

> "A review of SAR data on both a macro and micro scale indicates that suspected shell companies incorporated or organized in the United States have moved billions of dollars globally from accounts at banks in foreign countries, particularly those of the former Soviet Union, and predominantly the Russian Federation and Latvia. Most of these companies are LLCs and corporations … Many of the U.S.-based suspected shell companies were observed to maintain banking relationships with Eastern European financial institutions, particularly in Russia and Latvia."

[67] USA v. Oladimeji Seun A Yelotan, (S.D. Miss., July 8, 2014)(1:14-cr-00033-HSO-JMR).
[68] White House, Strategy to Combat Transnational Organized Crime, July 2011.
[69] Available at http://www.fincen.gov/news_room/rp/files/LLCAssessment_FINAL.pdf; See below for a discussion of the misuse of shell companies, particularly to access the banking system.

In 2013, in New York, 34 alleged members and associates of two related Russian-American organized crime groups were indicted for a range of offenses including the operation of at least two international bookmaking organizations that catered to wealthy individuals in the United States, Russia, and the Ukraine.[70] One enterprise is alleged to have moved tens of millions of dollars in illicit gambling proceeds from the former Soviet Union through shell companies in Cyprus into various investments and shell companies in the United States.[71] The other enterprise allegedly laundered the proceeds of a gambling operation through U.S. bank accounts and a Bronx plumbing company in which the organization acquired a 50 percent ownership interest as payment of a gambling debt.

In 2011, in Los Angeles, 90 people were charged in two indictments targeting the Eurasian street gang known as Armenian Power.[72] One indictment accused defendants of participating in sophisticated bank fraud schemes, identity theft, debit card skimming, and manufacturing counterfeit checks. The gang's membership is made up of individuals from Armenia and other countries of the former Soviet bloc. According to the FBI, Armenian Power uses bank wires and couriers carrying cash, gold, and diamonds to send illicit proceeds to Armenia.

4. Middle Eastern Criminal Enterprises

The FBI notes that although there is a nexus between terrorist financing and financial crime supporting Islamist extremist groups, there are also Middle Eastern criminal groups operating to make money through illegal activities.[73] These Middle Eastern groups typically are loosely organized theft or financial fraud rings and have been active in the United States since the 1970s.

E. Public Corruption

Public Corruption within in the United States involves the corruption of local, state, and federal government officials. Many taxpayer dollars are wasted or lost as a result of corrupt acts by public officials.[74] In 2013, 315 federal officials were convicted of public corruption offenses, including a former Congressman who was convicted of 17 felony offenses including money laundering. [75] Most corruption cases are handled by the local United States Attorney's Office in the district where the crime occurred. DOJ's Public Integrity Section oversees the federal effort to combat corruption through the prosecution of elected and appointed public officials at all levels of government. In addition, the United States is often a desirable destination for the proceeds of foreign official corruption, which undermines democratic institutions and threatens national security.[76] The Asset Forfeiture/Money Laundering Section of DOJ has

[70] U.S. Attorney for the SDNY, Manhattan U.S. Attorney Charges 34 Members and Associates of Two Russian-American Organized Crime Enterprises with Operating International Sportsbooks That Laundered More Than $100 Million, news release, April 16, 2013.
[71] USA v. Alimzhan Tokhtakhounov, (S.D.N.Y., Apr. 12, 2013) (13 CRIM 268).
[72] Department of Justice, Armenian Power Gang Leaders Convicted for Their Role in Racketeering Conspiracy, news release, April 17, 2014.
[73] *See* FBI overview of Middle Eastern Criminal Enterprises. Available at http://www.fbi.gov/about-us/investigate/organizedcrime/mideast
[74] FBI, FY 2015 Authorization and Budget Request to Congress, March 2014.
[75] DOJ, Report to the Congress on the Activities and Operations of the Public Integrity Section for 2013. Nationwide federal prosecutions of public corruption in 2013 included 1,134 charged, 1,037 convicted, and 499 awaiting trial. Available at http://www.justice.gov/criminal/pin/docs/2013-Annual-Report.pdf
[76] White House, Strategy to Combat Transnational Organized Crime, July 2011.

a dedicated kleptocracy team that focuses on recovering the proceeds of foreign official corruption. Domestic and foreign official corruption are separate threats and are distinguishable from the bribery of foreign officials by U.S. companies, which is addressed by the U.S. Foreign Corrupt Practices Act (FCPA).[77]

[77] *See* DOJ overview of FCPA. Available at http://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf

Vulnerabilities and Risks: Money Laundering Methods

SECTION II. VULNERABILITIES AND RISKS: MONEY LAUNDERING METHODS

In the context of this risk assessment, vulnerability refers to the money laundering methods that make it possible to use the proceeds of financial crimes (the threats). Different threats exploit different vulnerabilities. Risk is a function of threat, vulnerability, and consequence and represents a summary judgment.

A. Cash

Cash (bank notes) is an essential component of the U.S. and global economies, and of money laundering. There was approximately $1.36 trillion of U.S. banknotes in circulation as of March 11, 2015,[78] and much of that currency circulates globally. To mitigate the risks associated with the deposit or use of large sums of potentially illicit anonymous cash, the Bank Secrecy Act (BSA)[79] established AML customer identification, recordkeeping, and reporting obligations for financial institutions, which reduce the potential for criminals to place illicit proceeds into the financial system or to use illicit proceeds anonymously. Financial institutions are required to verify a customer's identity and retain records of certain information prior to issuing or selling bank checks and drafts, cashier's checks, money orders, and traveler's checks when purchased with cash (bank notes) in amounts between $3,000 and $10,000 inclusive.[80] For cash transactions above $10,000, whether a single transaction or a series of related transactions with a customer in a single business day, financial institutions are required to file a Currency Transaction Report (CTR) with FinCEN.[81] Other businesses must report cash transactions of more than $10,000 to the IRS and FinCEN (Form 8300[82]), subject to certain exceptions.[83] Purchases of monetary instruments and wire transfers under $3,000 do not require a transaction record or customer identification. Retail transactions under $10,000 in cash or monetary instruments do not have to be reported to the IRS or FinCEN.

1. Vulnerabilities

Drug proceeds start and often remain as cash, while proceeds from fraud rarely start out as cash but may end up as cash after laundering, or during the layering stage in an effort to break the audit trail. At each stage in the drug trafficking supply chain, from South America to Mexico, from Mexico to the United States, and within the United States, illicit drug purchases are typically paid for with cash.[84] Street dealers use the cash they earn from retail transactions to purchase their next drug supply from midlevel

[78] Available at http://www.federalreserve.gov/faqs/currency_12773.htm
[79] The Currency and Foreign Transactions Reporting Act of 1970 (commonly referred to as the "Bank Secrecy Act") requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. The USA PATRIOT Act of 2001 amended the BSA. *See* 31 U.S.C. § 5311-5330 and 31 C.F.R. Chapter X. Available at http://www.fincen.gov/statutes_regs/bsa/
[80] 31 C.F.R. § 1010.415.
[81] 31 C.F.R. § 1010.311.
[82] 31 C.F.R. § 1010.330.
[83] *Id*.
[84] Exceptions are illegal online pharmacies and web sites selling illegal drugs, which accept electronic payments. *See* Online Pharmacy Guide for Acquirers June 2014, Visa Inc.; *see also* http://www.fincen.gov/law_enforcement/ss/html/Issue13-story4.html;

wholesalers who in turn purchase their next drug supply from top level wholesalers. The DTOs will allow trusted top level wholesalers to receive drug shipments worth millions of dollars on consignment, with payment made in cash after the drugs are sold.[85]

The largest portion of each dollar spent on illegal drugs goes to the lower rungs of distributors and street sellers.[86] One estimate of how a consumer's dollar spent on cocaine is allocated has the Andean growers' share at about 1.5 percent, the processors' share at 1 percent, the Colombian and Mexican transporters' share at 13 percent, the Mexican and U.S. wholesalers' share at 15 percent, and the Mexican and U.S. mid-level to final retailers' share at about 70 percent.[87] It is difficult to estimate accurately how much money the Mexican DTOs earn from the drug trade overall. Estimates range from a low of $6 billion to a high of $39 billion.[88] The wide disparity is due to varying estimation models and differing assumptions about consumption, purity, and price.

The cash earned by retail dealers is typically held and spent as cash. A drug trafficker attempting to use more than $10,000 in cash (bank notes) in a transaction with a merchant may attempt to break up the purchase into a series of smaller payments (referred to as structuring) in an attempt to avoid the merchant reporting the transaction to FinCEN and the IRS. Alternatively, a drug trafficker may seek a complicit merchant who will accept the cash and agree not to report the transaction. There have been a number of cases of complicit merchants working with drug traffickers to launder cash (see Table 1).

Drug trafficking is probably the most significant source of illicit cash, but it is not the only source:

- In 2008, Newark, N.J., police detective was indicted for money laundering for her part in helping a heroin dealer and operator of an illegal gambling ring launder his illicit proceeds. The proceeds from illicit gambling, estimated by DEA to be as much as $10,000 a day, generated almost as much cash as the weekly revenues from heroin distribution. The woman wrote checks to pay for the air conditioning system in the heroin dealer's luxury home in return for illicit cash.[89]
- In 2006, in Michigan, 15 people were indicted on charges of illegal gambling and money laundering.[90] According to the indictment, debt collectors for the gambling ring used a used car business as a front to receive and launder millions of dollars in illicit gambling debt payments. In addition to accepting cash and checks at the car dealership, and depositing the funds in the business's bank account, the dealership also took car titles as payment from losing bettors and sold the cars on the lot.

[85] USA v. Arturo Beltran-Leyva, et al., (N.D. Ill., 2009). Available at http://www.justice.gov/usao/iln/pr/chicago/2009/pr0820_01b.pdf
[86] *See* Cameron H. Holmes, Mexico Threat Assessment: Strategy and Countermeasures, Southwest Border Anti-Money Laundering Alliance, August 2012, Page 10.
[87] *Id*. Figures add to more than 100 because of rounding.
[88] NDIC estimated DTOs earn $18b to $39b in the 2008 National Drug Threat Assessment. RAND Corporation put the figure at approximately $6 billion in Reducing Drug Trafficking Revenues and Violence in Mexico, Beau Kilmer, Jonathan P. Caulkins, Brittany M. Bond, Peter H. Reuter, 2010.
[89] DEA, Suspended Newark Police Detective Convicted at Trial for Laundering Gambling and Drug Proceeds, news release, October 30, 2008.
[90] USA v. Peter Dominic Tocco, et al., (E.D. Mich., Mar. 3, 2006)(2:06-cr-20122-AC-VMM).

- In 2006, in Ohio, two men were indicted for their involvement in operating illegal pain clinics at which patients received prescriptions for narcotics.[91] The clinics operated for only weeks or months at most before closing and being reestablished elsewhere on an ongoing basis. Patients could allegedly obtain a medical prescription for Lorcet and Xanax if they brought an x-ray and could pay cash. Payments ranged between $150 and $250 per patient per visit. The cash was split at the end of each day between the employees, including a licensed physician. The physician allegedly made structured cash deposits to local bank accounts and then made structured withdrawals in the form of cashier's checks, which were used to buy a car and a boat, and to make deposits to a brokerage account.

Table 1. Examples of Money Laundering Using Drug Cash

Boats, Cars, and Motorcycles

- In 2012, a Texas auto dealer was convicted for intentionally selling luxury cars to individuals for cash derived from illegal activities. No IRS Form 8300 was filed to report the large cash transactions. The dealer registered the cars in the names of nominees, and recorded the transactions as leases so that the dealership would retain ownership if the cars were seized by law enforcement. (USA v. Richard Alan Arledge, (E.D. Tex., Dec. 6, 2010) (4:09-cr-00089-RAS-DDB).
- In 2009, in Ohio, a used car dealer was charged with laundering drug proceeds for known Cleveland area drug dealers, accepting cash for high-end used cars and structuring the deals to avoid IRS reporting requirements. The dealer sold three cars for approximately $51,000.00 in cash to undercover FBI agents posing as drug dealers. (USA vs. Vincent Pisano, (N.D. Ohio, Feb. 3, 2009) (1:09-cr-00034).
- In 2008, in Virginia, an auto dealer was charged with money laundering for allegedly facilitating the cash purchase of boats, cars, and motorcycles for individuals alleged to be involved in a variety of illicit activities including drug trafficking and illegal gambling. The defendant allegedly used checks drawn on his auto dealership's bank account to buy motorcycles, cars, and boats, which he then resold for cash. The accused allegedly structured the deposit of the cash he received into his personal and business accounts. (USA vs. Shirland L. Fitzgerald, et. al., (W.D. Va., Sept. 10, 2008) (4:08-cr-00001-JLK).

Bribes, Horses, and Farm Expenses

- In 2012, in Texas, several individuals associated with the Los Zetas drug trafficking organization, were indicted for laundering drug proceeds through the purchase, breeding, training, and racing of quarter horses outside of Dallas. Cash payments of $200,000 a month on average went to boarding, breeding, and training the horses, and on at least one occasion between $200,000 and $300,000 in cash was paid to an owner in Oklahoma to purchase a horse. (continued on next page)

[91] USA v. Nick Capurro and William H. Jewell, Jr., (S.D. Ohio, Sept. 20, 2006)(1:06-cr-00112-SAS).

Examples of Money Laundering Using Drug Cash, Continued

Bribes, Horses, and Farm Expenses, continued

- Among the routine expenses, allegedly, was paying bribes in Mexico. The bank notes that were old and dilapidated, or had markings on them, were allegedly used for bribes. (FBI Affidavit in Support of Search Warrant, filed June 11, 2012, 3:12-MJ-255).

Jewelry

- In 2014, a Pennsylvania jeweler pleaded guilty to failing to file an IRS form 8300 following the receipt of approximately $12,500 in currency as payment for a watch. The transaction allegedly involved the proceeds of drug trafficking. (DOJ, Pittsburgh Jewelry Store Owner Failed to File IRS Report of $10,000+ Transaction, news release, January 15, 2014).
- In 2009, a New Jersey couple was charged with cocaine trafficking and money laundering in relation to an alleged distribution network that stretched from Canada to Georgia. Total cash expenditures by the couple over seven years were estimated to be more than $5 million with approximately $2 million spent on jewelry. (Monmouth County Prosecutor's Office, news release, Leader of a Narcotics Trafficking and Money Laundering Network Indicted Along with 15 Others as Part of a Racketeering Scheme, January 27, 2009).
- In 2006, a Georgia man was indicted for money laundering for allegedly agreeing to sell jewelry for cash that was represented to be drug proceeds. The Atlanta jeweler allegedly accepted more than $50,000 in cash without reporting the transaction to FinCEN and the IRS. (USA vs. Toros Seher, et. al., (N.D. GA., Aug. 23, 2006)(1:06-cr-00322-TCB-CCH).

Real estate

- In 2013, a New York man was convicted of conspiracy to distribute a large amount of cocaine. The man allegedly paid $467,000 in cash to build and furnish a house, which his grandmother allowed to be put in her name. (IRS-CI, Examples of Narcotics-Related Investigations - Fiscal Year 2013, http://www.irs.gov/uac/Examples-of-Narcotics-Related-Investigations-Fiscal-Year-2013)
- In 2012, in Mississippi, seven people were charged in two indictments with marijuana trafficking and money laundering. According to one indictment two defendants spent almost $1.5 million in cash over two years on home improvements at several properties, vehicles, and other items. To avoid using more than $10,000 in cash at any one time, the pair used a combination of cash, cashier's checks, and money orders to make some of the purchases. (3:12-cr-00014-DPJ-LRA)(S.D. Miss., Feb. 23, 2012).
- In 2006, a Tennessee real estate broker was indicted for falsifying loan documents and transaction records to facilitate a home sale to a cocaine dealer. The broker received $415,000 in cash to purchase the property. The broker allegedly structured bank deposits, prepared a fraudulent mortgage application, and arranged for a straw buyer. (1:06-cr-00029 filed April 11, 2006).

a. Bulk Cash Smuggling

Bulk cash smuggling is the process of physically moving hidden amounts of cash and monetary instruments in excess of $10,000 into or out of the United States without filing a Report of International Transportation of Currency or Monetary Instruments (CMIR) with U.S. Customs and Border Protection.[92] Some of the cash collected domestically to pay Mexican DTOs for drugs is channeled from distribution cells across the United States to cities and towns along the southwest border, and from there is smuggled into Mexico.[93] Bulk cash smuggling remains the primary method Mexican DTOs use to move illicit proceeds across the southwest border into Mexico.[94] The following case example is typical:

- In 2008, in Wyoming, eight people were indicted in a large scale methamphetamine distribution and money laundering ring.[95] According to the indictment, the drug was smuggled into the United States from Mexico for distribution in Arizona, Utah and Wyoming. The drug was acquired on consignment, meaning that payment to the sellers in Mexico was made after the drug was sold in the United States. Proceeds were sent to Arizona via cash and money transmitters for aggregation, with the cash subsequently smuggled into Mexico to pay the methamphetamine sellers.

Drug proceeds owed to a particular DTO enter Mexico in the geographic area where the DTO controls the smuggling routes. Arizona, for example, borders the Mexican state of Sonora where the Sinaloa Cartel is dominant. Arizona serves as a consolidation and staging point for drug proceeds going to the Sinaloa Cartel. In FY 2011, more than half of all currency and monetary instruments seized along the southwest border in connection with ICE HSI narcotics investigations were seized in Arizona.[96]

Based on a survey sample of cash seizures at official points of entry along the southwest border, ICE HSI reports cash seizures consist primarily of $20 bills, which the DTOs use to pay employees and for operational expenses. Excess $20 bills and other small denomination notes have usually been exchanged for $100 bills at *centros cambiarios* (money exchangers) in Mexico, and potentially through other financial services providers, and are used to pay drug suppliers or stored for future use.[97]

[92] Each person (including a bank) who physically transports, mails, or ships currency or monetary instruments in excess of $10,000 at one time out of or into the United States (and each person who causes such transportation, mailing, or shipment) must file a Report of International Transportation of Currency or Monetary Instruments (FinCEN Form 105).
[93] A Line in the Sand: Countering Crime, Violence and Terror at the Southwest Boarder, Majority Report of the House Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management, November 2012.
[94] *Id*.
[95] USA v. Vidal Carrillo-Ontiveros, et al., (D. Wyo., Sept., 19, 2007)(2:07-cr-00237-WFD).
[96] Mathew C. Allen, Special Agent in Charge, Homeland Security Investigations, Phoenix, Arizona, U.S. Immigration and Customs Enforcement, Department of Homeland Security, testimony before the Subcommittee on Border and Maritime Security of the House Committee on Homeland Security, May 21, 2012.
[97] USA – Mexico, Bi-National Criminal Proceeds Study, Department of Homeland Security; The Physical Flow of Dollars in the Mexican Financial System (June 2010).

Much of the cash that goes to the Mexican DTOs remains as cash. No more than half and potentially much less of the cash is placed in a financial institution at the direction of a DTO.[98] DEA points out that the seizure of $205 million in U.S. $100 banknotes in March 2007 from a Mexico City residence is an example of an alleged supplier of precursor chemicals to Mexican DTOs stockpiling cash.[99]

U.S. currency not used, or sold to money brokers, in the United States, and not used or stored in Mexico, is sent to Argentina, Brazil, Colombia, Guatemala, Honduras, or Panama for laundering or to pay narcotics suppliers.

Mexican regulations, which took effect in 2010, limiting U.S. bank note deposits by individual account holders at financial institutions to $4,000 per month, and U.S. currency exchanges by non-account holders to $1,500 per month, may have been a factor in DTOs moving more currency to other countries (see Table 2).[100] Banks had been allowed to accept up to $14,000 in currency per month from businesses operating in the U.S. border region or in defined tourist areas. The restrictions also apply to brokerage houses and casas de cambio. In 2014 the restrictions were revised and allowed Mexican financial institutions to opt into a regime that lifted the deposit restrictions for businesses operating for at least three years, as long as the customers provide their banks with financial statements and tax returns for the last three years, and can justify conducting transactions involving U.S. bank notes in amounts above the $14,000 threshold. Businesses unable or unwilling to comply continue to be subject to the original limits.

Bulk Cash Smuggling Center

U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) National Bulk Cash Smuggling Center (BCSC) in Williston, Vermont provides operational support to federal, state, and local law enforcement bulk cash interdictions and investigations. Since its inception in August 2009, the BCSC has initiated 824 investigations, which have resulted in 648 criminal arrests, 431 indictments, and 319 convictions.

HSI's Operation Firewall is a partnership with U. S. Customs and Border Protection to disrupt the smuggling of bulk cash en route to the border, at the border, and internationally. Operation Firewall targets the full array of methods used to smuggle bulk cash, including commercial and private passenger vehicles, commercial airline shipments and passengers, and pedestrians crossing U.S. borders with Mexico and Canada. Since its inception in 2005 through March 2012, Operation Firewall has resulted in more than 6,613 seizures totaling more than $611 million, and the arrests of 1,416 individuals. These efforts include 469 international seizures totaling more than $267 million and 302 international arrests.

Source: ICE HSI, National Bulk Cash Smuggling Center, Williston, Vermont

[98] *Id.*
[99] Affidavit in Support of Complaint and Arrest Warrant for Zhenli Ye Gon, (D.D.C., June 15, 2007) (1:07-cr-00181-EGS).
[100] Key Locations and Vulnerabilities Related to Money Laundering Methods Used by Transnational Criminal Organizations to Transport, Launder, and Store Illicit Proceeds, ICE HSI – Office of Intelligence, August, 15, 2013.

Table 2

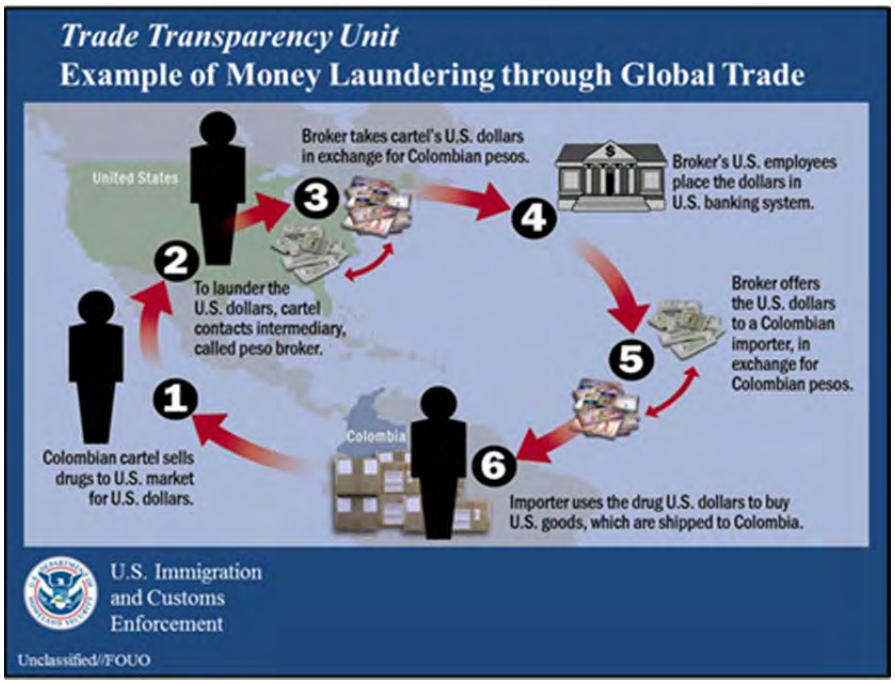
U.S. Dollar Cash Deposit Restrictions in Mexico				
Individuals			**Businesses**	
Bank Customer	**Non-bank Customer**		Border/Tourist Areas	Rest of Country
	Mexican Nationals	Foreigners		
$4,000/month	$300/day or $1,500/month	$1,500/month	$14,000/month or unlimited if additional information provided	Prohibited, or unlimited if additional information provided

b. Trade-based Money Laundering

Trade-based money laundering (TBML) is the process of disguising the origin of criminal proceeds through the import or export of merchandise and trade-related financial transactions. TBML refers to a variety of schemes that can involve moving illicit merchandise, falsifying the value of merchandise, and misrepresenting trade-related financial transactions with the purpose of disguising the origin of criminal proceeds and integrating the funds into the financial system. TBML is one of the more complex methods of money laundering to investigate, particularly because it involves complicit merchants.

TBML can have a more destructive impact on legitimate commerce than other money laundering schemes. According to ICE HSI, transnational criminal organizations may dump imported goods purchased with illicit proceeds at a discount into a market just to expedite the money laundering process. The below-market pricing is a cost of doing business for the money launderer, but it puts legitimate businesses at a competitive disadvantage. This activity can create a barrier to entrepreneurship, crowding out legitimate economic activity. TBML also robs governments of tax revenue due to the sale of underpriced goods, and reduced duties collected on undervalued imports and fraudulent cargo manifests. The funds laundered through TBML schemes are estimated to be in the billions of dollars annually.[101]

[101] ICE HSI, Trade Transparency Unit overview of TBML. Available at http://www.ice.gov/trade-transparency



According to DEA [102], much of the bulk U.S. currency that comes into Panama from Mexico goes to the Colon Free Trade Zone to pay for goods destined for Colombia. [103] DEA explains that this exchange of cash from Mexican DTOs, typically through a money broker, to legitimate merchants exporting goods to Colombia is an example of TBML. This example, involving the exchange of U.S. drug dollars for Colombian pesos to pay Colombian DTOs, is referred to as the Black Market Peso Exchange (BMPE).[104] Mexican drug traffickers now are satisfying their debts to their Colombian cocaine suppliers by delivering drug cash to Colombian money brokers' agents in the United States. The cash is either placed into the U.S. financial system, smuggled out of the United States, or delivered to U.S. businesses in payment for goods shipped to Colombian importers. The importers in Colombia pay the money brokers in Colombian pesos, which the money brokers use to satisfy the Mexican drug traffickers' debt to the Colombian cocaine suppliers.

In recent years, Colombian money brokers have emerged as full service money laundering intermediaries, arranging for the pick-up in the United States of cash due to Colombian DTOs and making the money available in foreign currencies or accounts in Colombia and elsewhere. This connection between Mexican DTOs and Colombian money brokers has reduced the cost and risk to both Mexican and Colombian DTOs. The Mexican DTO's custody of drug dollars in the United States and associated money laundering concerns end when the money broker picks up the cash. As discussed in a 2010 case, "in practice, the BMPE process often involves more than one peso broker: in many instances, one broker has the direct relationship with the narcotics trafficker in Colombia and bears ultimate responsibility for the laundering of the drug money; a second broker has the criminal associates in the United States and elsewhere outside of Colombia who can collect and accumulate the narcotics proceeds; and a third broker has the contacts with Colombian individuals and companies who want to sell pesos for dollars to import goods into Colombia while avoiding United States and Colombian currency exchange and income reporting requirements."[105] According to U.S. law enforcement, one of the apparent consequences of the restrictions

[102] DEA, Office of Financial Operations, A Perspective on Mexican Bulk Cash Movement and Money Laundering Trends, February 2012.
[103] *Id*.
[104] The black market peso exchange is a large-scale money laundering system used to launder proceeds of narcotic sales in the United States by Latin American drug cartels by facilitating swaps of dollars in the U.S. for pesos through the sale of dollars to Latin America businessmen seeking to buy U.S. goods to export.
[105] USA v. Paolo Gomez and Jairo Herman Torres, (S.D.N.Y., Jan. 11, 2010)(1:09-cr-00611-MGC).

on the deposit of U.S. dollars in Mexico is the emergence of Mexican money brokers who acquire drug dollars in the United States to sell to Mexican importers, paralleling the role of Colombian money brokers (see Table 3).[106] In one case, the Mexican money broker identified potential importers in Mexico for U.S. goods and then required a U.S. wholesaler to accept payment in cash for the orders. The money broker, acting as intermediary, would not identify the customers, requiring the U.S. wholesaler to accept the cash or reject the sale.[107] This arrangement not only creates a trade-related market in the United States for drug cash, but more importantly it entices legitimate merchants to take on the role of money launderer on behalf of Mexican drug traffickers and Colombian money brokers.

Table 3 ***Case Examples of Cash Used in Trade-based Money Laundering***

- In 2014, in Florida, a Ft. Lauderdale jeweler pleaded guilty to money laundering in a case that involved allegations of TBML. The jeweler accepted drug cash, primarily $20 bills, from a Mexican DTO, and in exchange would send the corresponding value, minus a commission, via wire transfers to Mexico. The jeweler deposited the drug cash in the business's bank account as if it had been received over the counter from retail customers, and maintained false invoices in its records to justify the wires as payments for gold although no gold was received.[1] In a separate scheme, the jeweler undervalued legitimate gold shipments from Guatemala to evade the tax due. The tax evasion scheme was detected by ICE HSI by comparing the declared value of the gold with its actual market value. The scheme was charged as smuggling and money laundering.
- In 2013, a California wholesale distributor of silk flowers and other goods was indicted on charges alleging the Los Angeles company accepted drug cash in payment for goods it shipped to Mexico. The company also allegedly structured the deposit of additional cash into its bank account for the purpose of making BMPE-related payments to other U.S. merchants, as directed by a Mexican peso broker. USA v. Peace & Rich Import Inc., et al., (C.D. Cal., Feb. 13, 2013) (2:13-cr-00107-JAK).
- In 2012, in California, a Mexican businessman pleaded guilty in federal court to conspiring with the owners of a Los Angeles toy wholesaler, Woody Toys, to launder drug dollars. The toy company accepted drug cash in payment for toys shipped to Mexican merchants, and subsequently made structured bank deposits with the drug cash. (U.S. Attorney for the Central District of California, Mexican Toy Dealer Pleads Guilty in Drug Money Laundering Case, news release, August 1, 2012)

[106] DEA, Office of Financial Operations, A Perspective on Mexican Bulk Cash Movement and Money Laundering Trends, February 2012.
[107] USA v. Peace & Rich Import Inc., Chaur Hwan Lin and Antonio Pareja, (C.D. Cal., Feb. 13, 2013) (2:13-cr-00107-JAK).

Table 3 ***Case Examples of Cash Used in Trade-based Money Laundering Cont.***

- In 2010, in Georgia, the owner of an Atlanta car dealership was convicted of money laundering in connection with a TBML scheme that involved repatriating the proceeds of U.S. heroin sales to Nigeria. Proceeds of heroin sales in Detroit were sent to the auto dealer in Atlanta who used the money, sent as cash and money orders, to buy cars. The auto dealer did not file a Form 8300 to report the transactions. Some of the cars were shipped to Nigeria to pay the heroin suppliers. Other cars were sold to launder the drug proceeds and raise additional revenue. The auto dealer raised additional revenue by hiding in each vehicle shipped from the United States undeclared consumer goods for resale in Africa. In addition, the auto dealer also operated an unlicensed money transmitting business and used a portion of the proceeds from his legitimate African auto sales to pay out remittances in Nigeria without having to transfer funds through the financial system.
- In 2012, in California, the owners of Angel Toy Company were sentenced in association with a BMPE scheme similar to the 2013 case above, in which the toy manufacturer agreed to accept drug cash in payment for toys shipped to Colombia and then structured the deposit of the cash into the company's bank account. (U.S. Attorney for the Central District of California , Owners of Los Angeles Toy Company Sentenced to Federal Prison for Role in International Scheme to Launder Money for Drug Traffickers, news release, January 31, 2012)
- In 2011, in New York, Vikram Datta, the owner of multiple retail perfume stores located on the United States-Mexico border, was convicted of charges related to exporting perfume to Mexico in exchange for payment in drug dollars. After drugs were sold in the U.S., the proceeds were smuggled to Mexico where the cash was sold to Mexican money exchange businesses for Mexican pesos. The exchange businesses later transported the U.S. drug dollars back into the United States and used them to purchase perfume from retailers in Laredo, Texas, that would then ship the perfume to purchasers in Mexico. From January 2009 through January 2011, more than $25 million in U.S. currency was deposited in bank accounts controlled by Datta. (IRS-CI, Businessman Sentenced for Laundering Millions of Dollars for a Mexican Narcotics Trafficking Organization, http://www.irs.gov/uac/Examples-of-Money-Laundering-Investigations-Fiscal-Year-2012)

c. Licit and Illicit Cash Often Indistinguishable

According to the Federal Reserve, of the U.S. currency in circulation, approximately three-quarters is in the form of $100 bank notes and about three-quarters of those U.S. $100 bills are held outside the United States.[108] Although there was estimated to be a general decline in the share of $100 bank notes held abroad between the late 1990s and 2007, the financial crisis in 2008 reversed that trend as more citizens globally acquired U.S. dollars, particularly $100 banknotes.

A 10-year study of U.S. currency held abroad, conducted jointly by the U.S. Treasury, Federal Reserve, and U.S. Secret Service, found that foreigners hold U.S. currency because it is anonymous, portable, and liquid, reasons relevant to both law abiding citizens and criminals.[109] The following reasons, cited by the joint study, for holding and using U.S. banknotes abroad can complicate U.S. law enforcement efforts to trace the illicit movement of cash outside the United States:

- In times and places where the political or economic situation is uncertain, U.S. currency is held for security against inflation and general calamity
- Expatriate workers throughout the world often carry or send portions of their earnings to their home countries as U.S. currency; and between visits home workers may hold U.S. banknotes
- Travelers to other parts of the world carry U.S. currency because it is easier to exchange for local currency than the traveler's home currency
- Cross-border trade in many areas is conducted largely in U.S. currency
- Informal, or unlicensed, sectors in many economies are highly dollarized

The joint study estimates that Russia and other countries in Eurasia and other parts of Europe account for about 40 percent of international holdings of U.S. currency. About 25 percent of U.S. bank notes held outside the United States are held in Latin America, 20 percent are in Africa and the Middle East, and about 15 percent are in Asia. Many Latin American countries have made exclusive or significant use of U.S. currency in their history, including Argentina, the Dominican Republic, Mexico, Panama, Peru, and Uruguay.[110] Panama, Ecuador, and El Salvador currently have dollarized economies.

Federal Reserve researchers found that "currency movements are difficult to measure for some of the same reasons that currency is popular: It can be easily concealed and readily carried across borders, even in large quantities."[111] Many cash couriers are believed to cross daily from the United States to Mexico at official points of entry smuggling small amounts of currency (usually $5,000–$10,000) on behalf of

[108] Ruth Judson, Crisis and Calm: Demand for U.S. Currency at Home and Abroad from the Fall of the Berlin Wall to 2011, Board of Governors of the Federal Reserve System, November 2012.
[109] U.S. Treasury (2006), The Use and Counterfeiting of U.S. Currency Abroad, Part III, Washington, DC: U.S. Department of the Treasury.
[110] IMF, Dollarization Declines in Latin America, Finance & Development, March 2010, Volume 47, Number 1. Available at https://www.imf.org/external/pubs/ft/fandd/2010/03/dataspot.htm
[111] Richard D. Porter and Ruth A. Judson, The Location of U.S. Currency: How Much Is Abroad?, Federal Reserve Bulletin, October 1996.

Mexican DTOs.[112] There are also many opportunities for smuggling between official points of entry along the almost 2,000 mile U.S./Mexico border and the 5,225-mile U.S./Canada border. Most bulk cash seizures occur at airports, which may be due to the additional time U.S. Customs and Border Protection officers have to inspect luggage and conduct one-on-one interviews with passengers compared to the situation along the U.S. land borders.[113]

Another complicating factor in identifying illicit cash and illicit actors is the role of speculators who buy and sell bank notes hoping to make money on the difference between the black market exchange rate and the legitimate market exchange rate.[114] Speculators buy dollars from money brokers selling drug cash and then sell it at the market rate or use the cash, and in the process inadvertently help to launder drug proceeds and confuse law enforcement. When speculators declare cash when crossing the US/Mexico border or when their financial institutions file CTRs or SARs regarding large cash deposits, law enforcement is left to figure out whether these individuals are opportunists or real money launderers.

2. Risks

Cash (bank notes) is an effective money laundering vehicle. It is anonymous, widely used, and everyday spending with illicit cash is difficult to trace and impossible to confiscate once it is spent. Using large quantities of cash, however, can be conspicuous, cumbersome, and dangerous for criminals. Cash reporting and record keeping requirements mitigate this risk. The role of complicit retailers and wholesalers willing to accept cash in amounts exceeding $10,000 without reporting the transactions to the IRS or FinCEN is a problem that law enforcement is assessing and monitoring. The ongoing challenge for policy makers is to balance continued progress against the illicit use of cash with the need to accommodate legitimate cash transactions, as well as widespread legitimate demand for U.S. currency globally.

[112] USA – Mexico, Bi-National Criminal Proceeds Study, Department of Homeland Security; The Physical Flow of Dollars in the Mexican Financial System (June 2010).
[113] *Id*.
[114] *Id*.

B. Banking

Most Americans use a bank for financial services.[115] As of 2011, fewer than 10 percent of American adults lived in a household without a bank account.[116] The U.S. banking system consists of approximately 13,000 depository institutions that operate within a variety of diverse business models, of which half are banks (commercial banks, community banks, industrial loan companies, and savings associations). The other half are credit unions, which are not-for-profit organizations that hold just less than 10 percent of total domestic deposits. In comparison, just six banks hold more than 40 percent of total domestic deposits.[117] Although all financial institutions are exposed to potential illicit activity, the large proportion of dollar-denominated transactions that clear daily through these six banks put them at highest risk. Americans that do not have access to, or choose not to use, traditional banking services may obtain financial services using money services businesses (MSBs).[118] But MSBs, in turn, must have access to the banking system in order to settle accounts among agents and other financial institutions. Banks may also hold accounts with other banks, including both U.S. and foreign banks, in order to facilitate domestic as well as cross-border transactions and other financial services.

Banks offer a wide range of products and services that are intended to increase customer convenience and access to funds. While most customers use these products and services as intended, criminals are continually seeking opportunities to misuse them for illicit purposes. This misuse by criminals tests the internal controls established by banks to manage the risks associated with the use of these products and services. One of the key challenges facing banks is adequately adapting their controls on a timely basis to close vulnerabilities exploited by criminals.

1. Vulnerabilities

The global dominance of the U.S. dollar generates trillions of dollars of daily transaction volume through U.S. banks, creating significant exposure to potential money laundering activity. The Federal Reserve System's real-time gross settlement system, Fedwire, which is used to clear and settle payments with immediate finality, processed an average of $3.5 trillion in daily funds transfers in 2014.[119] The Clearing House Interbank Payment System (CHIPS)[120] is the largest private-sector U.S.-dollar funds-transfer system in the world, clearing and settling an average of $1.5 trillion in cross-border and domestic payments daily. CHIPS estimates that it is responsible for processing more than 95 percent of U.S. dollar-denominated cross-border transactions, and nearly half of all domestic wire transactions.[121] The average value of a transaction on Fedwire and CHIPS is in the millions of dollars. The automated clearinghouse

[115] FDIC, National Survey of Unbanked and Underbanked Households, 2013; Under the BSA, as implemented by 31 C.F.R. § 1010.100, the term "bank" includes each agent, agency, branch or office within the U.S. of commercial banks, savings and loan associations, thrift institutions, credit unions, and foreign banks. The term "bank" is used throughout this document generically to refer to these financial institutions.
[116] FDIC, National Survey of Unbanked and Underbanked Households, 2011.
[117] Those banks are: Bank of America (12.7%), Wells Fargo & Company (10%), JPMorgan Chase & Co (9.7%), Citigroup Inc. (4.4%), U.S. Bancorp (2.5%), and PNC Financial Services Group (2.3%). Source: FDIC Summary of Deposits and OTS Branch Office Survey, 2012.
[118] MSBs include check cashers, currency exchangers, and sellers of money orders, prepaid access, and travelers checks.
[119] http://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm
[120] http://www.chips.org/home.php
[121] *Id*.

network (ACH), through which U.S. banks transfer electronic payments that are not settled in real time, processes more than $10 trillion in transactions annually. This exposure to a daily flow of trillions of dollars in transaction volume from large value to small value payment systems requires banks to maintain robust safeguards to minimize the potential for illicit activity. Like any other financial industry, deficient compliance practices and complicit insiders are vulnerabilities, but the stakes are higher for banks given the volume and value of transactions that U.S. banks engage in daily.

Preserving the integrity of the U.S. financial system requires that banks effectively monitor and control the money laundering risks to which they are exposed. To this end, banks are required to establish a written AML program reasonably designed to prevent their financial institutions from being used to facilitate money laundering and the financing of terrorist activities.[122] The introduction of illicit proceeds into the financial system is the first and critical step in the money laundering process and banks are most vulnerable to being used for this purpose by criminals. Once illicit proceeds are placed into the financial system, the continued use of banks to move those funds both domestically and internationally can further obscure their criminal origins and facilitate their integration into the system. Therefore, establishing and maintaining an effective customer identification program (CIP) is a key control.

Banks are put in a vulnerable position when individuals and entities attempt to disguise the nature, purpose, or ownership of their accounts. This can occur through:

- Structuring and misuse of currency deposits (interstate funnel accounts)
- Misuse of correspondent banking services
- Misuse of new payment technologies
- Nominees and misuse of legal entities
- Money Brokers and Trade-based money laundering
- Misuse of third party payment processors

Banks put themselves in a vulnerable position when they fail to maintain effective compliance programs. Even in circumstances in which banks have effective compliance programs, a complicit employee can make a bank vulnerable to illicit activity.

a. Misuse of Banking Products and Services

Structuring and Misuse of Currency Deposits (Interstate Funnel Accounts)

Structuring is a common technique used to avoid a cash transaction threshold at which a financial institution applies recordkeeping and/or reporting obligations. Case examples demonstrate that customers will structure deposits and withdrawals to keep cash transactions below $10,000 to avoid the CTR reporting threshold:

[122] *See* 31 C.F.R 1020.210.

- In 2013, an Albuquerque fire fighter was convicted of drug trafficking and money laundering. He admitted to structuring 37 cash deposits and withdrawals to launder drug proceeds.[123] He had been charged with 14 co-defendants with distributing cocaine, methamphetamine, and marijuana in the state.
- In 2013, a Las Vegas attorney was sentenced for structuring cash deposits as part of a tax evasion scheme. The attorney was charged with making or assisting in 15 structured deposits totaling $138,700 for the purpose of evading bank reporting requirements.[124]
- In 2012, the owner and employees of a grocery store in Dayton, OH, were charged with laundering the proceeds of fraud committed against the Supplemental Nutrition Assistance Program (SNAP), formerly the Food Stamp Program. The defendants allegedly claimed reimbursement for more than $3.8 million in benefits they had accepted and in return, provided SNAP beneficiaries with cash, weapons, ammunition, and other nonfood items not allowed under the program. Upon receiving the SNAP reimbursements to the grocery store's bank account, the defendants allegedly made structured cash withdrawals to avoid the bank filing a CTR.[125]
- In 2009, a New York City police officer was charged in connection with a drug trafficking and money laundering investigation. The officer allegedly structured multiple cash deposits of between $1,000 and $7,900 into seven bank accounts. The money was earned from the officer's husband's heroin trafficking ring.[126]

A variation on routine structuring is the misuse of currency deposits or interstate funnel accounts, a term coined by ICE HSI, which involves using an account at a bank with branches nationwide to make structured deposits in one or more geographic locations and then structured withdrawals in the state where the account was opened. This money laundering technique provides a method for criminal organizations to move illicit proceeds rapidly across the United States, and, among other things, avoid overland transport of cash or the use of mail and express mail services. Funnel accounts are distinguishable from concentration accounts used legitimately by businesses, including banks, with considerable daily cash flow activity from multiple locations that require quick processing and settlement of transactions.[127] According to ICE HSI, the typical interstate funnel account is held by a nominee in one state and receives regular cash deposits at branch locations in other states. The time lapse between the deposits and the cash withdrawals ranges from minutes to a few days. The individual deposits and withdrawals are typically under $10,000, and the accounts have limited credits besides the cash deposits (i.e. no payroll or other deposit activity). Nominees are typically paid a fee for each account they open, and they turn over all access to the accounts.[128]

[123] FBI, Former Albuquerque Fireman Sentenced to 30 Months in Federal Prison for Structuring Drug Trafficking Proceeds, news release, August 21, 2013.
[124] IRS-CI, Examples of Money Laundering Investigations - Fiscal Year 2013.
[125] USA v. Al-Idu Al-Gaheem, et al., (S.D. Ohio, Mar. 20, 2012)(3:12-cr-00037-TSB).
[126] USA v. Yaniris Balbuena, (S.D.N.Y., Feb. 12, 2009).
[127] Federal Financial Institution Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual, at page 262-63 [hereinafter FFIEC BSA/AML Exam Manual]. Available at https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014.pdf
[128] ICE HIS, Corner Stone Report, Vol XI: No. 1 , Winter 2014.

The technique is known to be used to funnel drug proceeds to the southwest border region in preparation for smuggling the cash into Mexico. According to ICE HSI, this money transfer method was first associated with human smuggling organizations. This method is believed to be a reaction to increased scrutiny of remittance transactions by MSBs following greater focus by Arizona law enforcement on the use of MSBs to transfer payments to guides responsible for bringing illegal immigrants into the United States.[129] It is also a reaction to increased interdiction efforts on bulk cash movement along interstate highways as called for in the Office of National Drug Control Policy, National Southwest Border Counternarcotics Strategy.[130] The sustained campaign by state and federal law enforcement over the last decade against the use of money transmitters to pay human smugglers, and the movement of drug proceeds to the southwest border, apparently has prompted a shift to interstate funnel accounts, using the banking system rather than money transmitter networks to move illicit funds domestically:[131]

- In 2014, DHS, responding to the rise in illegal migration into south Texas, launched Operation Coyote, which involved channeling resources into the Rio Grande Valley to focus on criminal human smuggling and DTOs. In less than a month the campaign resulted in the seizure of more than $625,000 in illicit profits from 288 bank accounts held by human smuggling and DTOs.[132] To date, Operation Coyote has resulted in the seizure of more than $ 1 million dollars from 488 bank accounts in suspected illicit proceeds. As of August 2014, 363 smugglers and their associates have been arrested.
- In 2012, an HSI investigation in Arizona resulted in the arrest of 48 members of four different criminal organizations for alien smuggling, money laundering, and immigration violations, and the seizure of over $200,000. The subsequent investigation revealed evidence that the human smuggling fees were being paid to the organization through interstate funnel accounts.

Recent case examples demonstrate that the funnel account method is now widely used among drug traffickers:

- In 2013, in West Virginia, a Florida man was convicted of drug trafficking and money laundering for mailing packages containing oxycodone pills from Tampa to traffickers in West Virginia. The traffickers paid for the drugs by making cash deposits in West Virginia to bank accounts the supplier controlled in Florida.[133]
- In 2013, in Texas, nine alleged members of the Mexican Gulf Cartel DTO were charged with money laundering. From 2008 to 2012 distributors of illegal drugs in Florida allegedly paid for the narcotics by making structured deposits to bank accounts at local branches of a national bank.

[129] Leigh H. Winchell, Homeland Security Investigations, U.S. Immigration and Customs Enforcement, Department of Homeland Security, testimony before the Senate Governmental Affairs Permanent Subcommittee on Investigations, July 17, 2012.
[130] Available at http://www.whitehouse.gov//sites/default/files/ondcp/policy-and-research/southwest_border_strategy_2013.pdf
[131] *See* http://www.dhs.gov/news/2012/05/21/written-testimony-us-immigration-and-customs-enforcement-house-homeland-security; http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A008.pdf
[132] DHS, Secretary Johnson Announces 192 Criminal Arrests in Ongoing ICE Operation to Crack Down on Human Smuggling to the Rio Grande Valley, news release, July 22, 2014.
[133] DOJ, Man Who Illegally Mailed Nearly 20,000 Oxycodone Pills to West Virginia Sentenced to 14 Years in Prison, October 17, 2013.

The drug suppliers in Brownsville, Texas made structured withdrawals. The cash was then allegedly distributed to couriers who carried it across the Texas border into Mexico.[134]

- In 2013, in California, 13 people were charged with drug trafficking and structuring deposits and withdrawals through interstate funnel accounts at branches of four national banks.[135] The group allegedly obtained prescriptions for oxycodone, hydrocodone, and medical marijuana from a doctor in California.[136] The drugs were sold online and distributed through the mail or by physical delivery. Buyers paid more than $3.5 million by structuring cash deposits into the alleged dealers' accounts at bank branches around the United States. The defendants allegedly made structured cash withdrawals from their accounts in California.
- In 2011, in South Carolina, two men were prosecuted for drug trafficking and money laundering allegedly bought marijuana from suppliers in Arizona, California, and Georgia, and paid by making cash deposits into the suppliers' accounts via bank branch locations in South Carolina.[137]

To alert financial institutions to funnel accounts, FinCEN published an Advisory in 2011[138] describing funnel account activity, and followed it with another Advisory in 2012 providing additional guidance and red flags associated with funnel account activity coming from Mexico.[139] FinCEN reinforced the 2011 and 2012 advisories in 2014 when it issued another advisory alerting financial institutions of the link between funnel accounts and TBML.[140] In this latest variation, FinCEN reported that instead of withdrawing the structured cash that has been funneled into an account from various deposit points, an intermediary uses wire transfers or checks to pay suppliers for goods that are then shipped to foreign countries for sale.

Correspondent Banking

Correspondent banking is the provision of banking services between two unrelated financial institutions, whether domestic or international. Correspondent banking relationships are essential to the function of the U.S. and international financial system, facilitating everything from remittances, development, trade finance, and economic development.

Foreign correspondent banking relationships allow financial institutions worldwide to facilitate cross-border transactions in their currency of choice. They also enable financial institutions to conduct business and provide services to clients in foreign countries without the expense and burden of establishing a foreign presence. However, because of the complexity of correspondent account relationships, multiple intermediary financial institutions may be involved in a single funds transfer transaction.

---

[134] ICE, 9 members of Gulf Cartel money laundering cell arrested, 1 fugitive remains. News release, October 28, 2013. Available at http://www.ice.gov/news/releases/1310/131028brownsville.htm
[135] USA v. Chanrath Yim Yath, Memorandum of Plea Agreement, (E.D. Cal., Mar. 21, 2014)(1:13-cr-00136-AWI-BAM).
[136] 13 Indicted in Multimillion Dollar Interstate Drug Trafficking Conspiracy, news release, United States Attorney Benjamin B. Wagner, Eastern District of California, April 18, 2013.
[137] Case 4:11-cr-02165-RBH, criminal complaint filed Aug. 29, 2011.
[138] FinCEN Advisory, Information on Narcotics and Bulk Currency Corridors, FIN-2011-A009, April 21, 2011.
[139] FinCEN Advisory, Update on U.S. Currency Restrictions in Mexico, FIN-2012-A006, July 18, 2012.
[140] FinCEN Advisory, Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, FIN-2014-A005, May 28, 2014.

FinCEN has estimated there are approximately 300 banks in the United States that provide correspondent banking services to foreign financial institutions.[141] When these U.S. banks receive funds or instructions for a funds transfer from a foreign correspondent bank, they likely do not have a relationship with the originator of the payment. For this reason, conducting appropriate due diligence on the foreign correspondent bank is critical to managing the vulnerability associated with this product.[142] The complexity and volume of transactions that flow through U.S. correspondent accounts, coupled with the varying (often limited) recordkeeping requirements of funds transfer systems in different countries, increase the likelihood that some correspondent accounts can be exploited to facilitate the flow of illicit proceeds into or through the U.S. financial system.

Remote Deposit Capture

As cross-border wire transfers have come under increased scrutiny, DTOs have found paper checks, money orders, traveler's checks, and cashier's checks to be an alternative. Money launderers can transfer large dollar amounts outside the United States by writing checks or buying money orders, traveler's checks, and cashier's checks and depositing them in accounts at foreign financial institutions. Sending those paper items back to the United States for clearing used to be a time-consuming process. Now, however, banks can scan the items and send a digital file via remote deposit capture (RDC). RDC is used to make depositing checks faster and more convenient. When properly managed, RDC can reduce processing costs, support new and existing products by financial institutions, and accelerate the availability of customers' funds.[143] However, the more efficient processing of millions of checks a day can make it difficult to aggregate related payments or scrutinize individual items for evidence of money laundering in a timely manner. In 2009 the Federal Financial Institution Examination Council (FFIEC) issued an advisory noting RDC exposes banks to additional risks than those inherent in traditional check processing systems.[144]

- In 2011, FinCEN and the OCC cited Zions First National Bank, Utah, for violating BSA requirements to establish and implement an effective AML program with respect to its foreign correspondent customers' account relationships; timely filing of SARs; and compliance with the foreign correspondent account regulations. The bank had 54 foreign correspondent relationships, including 19 foreign money transmitters. With the implementation of RDC, the value of checks sent from correspondent financial institutions to Zions went from hundreds of millions to billions of dollars between 2005 and 2007.[145]

Prepaid Debit Cards

Prepaid debit cards (also referred to as prepaid access devices or stored value cards) operate within either an open or closed loop system. Open loop cards (also referred to as general purpose cards) carry the brand of a payment network (i.e. American Express, Discover, MasterCard, or Visa) and are accepted by merchants and at ATMs that connect to the affiliated global payment network. In the United States most

[141] FinCEN, Implications and Benefits of Cross-Border Funds Transmittal Reporting, January 2009.
[142] *See* Wolfsberg AML Principles for Correspondent Banking. The Clearing House, Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking;
[143] Financial Regulators Release Guidance on Risk Management of Remote Deposit Capture (January 14, 2009). Available at http://www.ffiec.gov/press/pr011409.htm
[144] *See* http://www.occ.gov/news-issuances/bulletins/2009/bulletin-2009-4a.pdf
[145] Zions First National Bank, Civil Money Penalty, FinCEN, February 10, 2011.

payment networks require that their branded prepaid cards be issued by a bank that is a member of that payment network.[146] Closed loop cards generally can only be used to buy goods or services from the merchant issuing the card or a select group of merchants or service providers that participate in the network. Closed loop cards may also be used for public transportation, transactions on a specific university campus, or purchases at a specific chain of stores.

To add value to open loop or general purpose cards, card program managers usually require that the cardholder register by providing customer identification information. Banks that issue prepaid cards are expected to establish appropriate internal controls around their prepaid programs to ensure that these products are not used to facilitate illicit activity. Banks are expected to establish and implement appropriate policies for monitoring, identifying, and reporting suspicious activity related to prepaid card programs.[147]

When used for illicit purposes, branded general purpose reloadable prepaid debit cards have been associated with cashing out the proceeds of fraud and being used as an alternative to cash in much the same way that money orders, travelers' checks, and nonbank wires are used.

- In 2013, in Alabama, a woman and her son-in-law were convicted of an identity theft/tax refund fraud scheme in which the woman, who worked for a debt collection company, stole identity information and provided it to her son-in-law to use to file fraudulent tax refund claims. The pair directed the IRS to pay the refunds on prepaid debit cards.[148]
- In 2012, in Oregon, a woman pleaded guilty to tax evasion and fraud for claiming a $2.1 million refund on her state tax return, which the Oregon Department of Revenue allowed to be paid on a single Visa prepaid debit card. The refund payment went through three levels of approval.[149]
- In 2012, in Wisconsin, a man pleaded guilty to drug trafficking and money laundering. He used the proceeds from selling cocaine and marijuana to buy and add value to prepaid debit cards, which he then used to buy goods and services.[150]
- In 2008, in California, an indictment charging nine defendants with drug trafficking and money laundering cites the use of prepaid debit cards among the methods used to launder the drug proceeds. The group allegedly used the illicit proceeds to structure cash deposits to bank accounts, buy money orders, send wire transfers to foreign banks, and buy prepaid debit cards.[151]
- In 2007, in New York, 12 men were indicted for illegal gambling and money laundering in connection with a Costa Rica-based gambling website and call center, referred to as a "wire room," which set odds and managed bets on behalf of U.S.-based sports bookies.[152] The Costa Rican wire room charged the bookies a fee for each bet that was taken. The U.S.-based bookies

[146] FFIEC BSA/AML Exam Manual at page 227.
[147] *Id*., at pages 230-32.
[148] DOJ, news release, Debt Collection Employee and Son-in-Law Sent to Prison for Identity Theft Tax Scheme, November 4, 2013.
[149] Harry Esteve, The inside story of Oregon's $2.1 million tax fraud case, The Oregonian, September 29, 2012. Available at http://www.oregonlive.com/politics/index.ssf/2012/09/the_inside_story_of_oregons_21.html
[150] DOJ, news release, Western District of Wisconsin, February 2, 2012.
[151] USA v. Gustavio Osorio Rios, et al., (C.D. Cal., Sept. 5, 2008)(2:08-cr-01057-VBF).
[152] USA v. Carmen Cicalese, et al., (S.D.N.Y., Dec. 11, 2007)(1:07-cr-01125-GBD).

paid the fee by cash, prepaid debit cards, and wire transfers. On one occasion, the wire room used a Pakistan-based hawala to move money collected from bookies in the United States.[153]

- In 2007, in Oregon, a man was convicted of Social Security number fraud and money laundering. He used fraudulent Turkish and Bulgarian passports and U.S. visas to obtain Social Security cards in false identities. Using the false identities he applied for and received credit cards, which he used to acquire prepaid debit cards and then abandoned the credit card debt.[154]

b. Misuse of Customer Relationships

Nominees and Misuse of Legal Entities

Using a bank account held in someone else's name, or in the name of a business, to hold, send, or receive illicit proceeds, is a sophisticated method to circumvent a bank's account opening procedures. As noted above, funnel accounts are typically held by a nominee. The following case examples identify other scenarios in which a bank's procedures are circumvented:

- In 2012, in California, a San Diego real estate agent was sentenced to prison for helping drug traffickers purchase property.[155] The real estate agent admitted he facilitated false loan applications in the name of nominee purchasers, verification documents, and financial documents. The real estate agent admitted falsifying the purchaser's income, employment history and the source of down payments for the properties.
- In 2011, in California, four people were indicted in Los Angeles for illegally distributing a generic liquid cough suppressant (promethazine with codeine) that is a commonly abused controlled substance.[156] According to court documents, the leader of the group owned Los Angeles area pharmacies and bought the cough syrup from wholesale distributors. The cough syrup was smuggled to Houston, Texas, where it was sold for approximately $10 million. The proceeds were sent back to Los Angeles as cash and money orders. Nominees were hired to open personal bank accounts and business accounts, and to make structured deposits of the cash and money orders.

[153] United States Attorney for the Southern District of New York, Twelve Charged in Multimillion Dollars Internet Gambling Operation, news release, January 7, 2007.
[154] USA v. Behcet Alkis, (D. Or., Feb. 27, 2007)(CR07-66-KI).
[155] IRS-CI, Examples of Money Laundering Investigations - Fiscal Year 2012.
[156] USA v. Lucita Uy, et al., (C.D. Cal., May 11, 2011)(2:11-cr-00426-ODW).

There are several types of businesses that can be misused in order to circumvent banks' procedures. These include the use of front companies, shell companies, and shelf companies. Front companies[157] are functioning businesses that combine illicit proceeds with earnings from legitimate operations, obscuring the source, ownership, and control of the illegal funds. When a company is used as a front to deposit, move, or use illicit proceeds it can be difficult for the bank holding the account to know that the company's banking activity includes money laundering.

A shell company is registered with the state as a legal entity, but has no physical operations or assets. Shell companies can serve legitimate purposes; for example, holding property rights or financial assets. Most companies technically begin as shell companies until they are put to operational use. Shell companies can also be used to conceal the source, ownership, and control of illegal proceeds.[158]

A shelf company is a legal entity that is state-registered, but has not been used for any purpose. It was created and put on the "shelf," awaiting a buyer who does not want to go through the process of creating a new legal entity. The fact that a shelf company, when acquired, is not a newly registered legal entity can help to obscure the origin and nature of the business, and the age of the company may add an air of legitimacy. Some shelf companies also come with a history of financial records. It may then serve the function of a shell company.

Financial Institution Takeover

In 2011 in New Jersey an organized crime investigation led by the Federal Bureau of Investigation culminated in indictments against 13 people, including attorneys and certified public accountants (CPAs), for illegally taking over and looting a publicly-held Texas mortgage company. The organized crime figures used intimidation to force out the existing officers and directors and used the company's assets to acquire shell companies they owned at inflated prices, fund bogus consulting contracts, and pay for personal expenditures including mortgages. Complicit attorneys and CPAs used complex structures involving trusts and shell companies to hide the ownership of the companies acquired by the hijacked mortgage company. They also filed false documents with regulators, including the Securities and Exchange Commission, and prepared false tax returns and other documents for the principals in the scheme to facilitate legitimate loans and mortgages that were paid with funds looted from the Texas company.

Source: USA v. Nicodemo Scarfo, et al ,Case 1:11-cr-00740-RBK filed October 26, 2011 in the District of New Jersey

When a legal entity is registered with state authorities there is no requirement in any state to provide beneficial ownership information (i.e. the natural person or persons who own or control the company). Banks are required to identify the beneficial owner of an account in limited circumstances.[159] There are ample case examples of individuals who own or control a legal entity hiding behind nominees who serve as officers and directors, and as signatories for bank accounts.

[157] Jennifer Shasky Calvery, DOJ, Testimony before the House Subcommittee on Crime, Terrorism, and Homeland Security, February 8, 2012.
[158] *Id*.
[159] 31 C.F.R. §§ 1010.610 and 1010.620

- In 2013, in South Carolina, two men were sentenced for money laundering and smuggling more than $3 million worth of cigarettes from South Carolina to New York. The men used a retail tobacco store they owned in South Carolina as a front company to purchase cigarettes in the low tax state of South Carolina that were to be sold illegally in New York, a higher tax state. The men deposited the revenue from the illegal cigarette sales into the tobacco store's bank account. [160]
- In 2007, in Colorado, defendants who were charged with drug trafficking allegedly opened bank accounts, made structured cash deposits to the accounts, and used nominees to facilitate large purchases. According to the indictment, the defendants regularly brought cocaine into the United States from Mexico for distribution in Colorado, Texas, Georgia and elsewhere, earning more than $15 million. The defendants used straw buyers in Denver to acquire cars and applied for home loans listing a co-conspirator's business as their employer on the mortgage applications.[161]
- In 2007, in Michigan, a man who allegedly led a heroin distribution conspiracy laundered the proceeds through a car wash business. The defendant allegedly over-reported business earnings for tax purposes to create the appearance of legitimate wealth, and used the false tax returns as proof of income when applying for mortgages and buying homes.[162]
- In 2006, in Idaho, more than a dozen people, including an attorney, an accountant, and a mortgage broker, were prosecuted for their role in a nationwide drug trafficking organization that had been operating for 30 years. According to the indictment: "The defendants and their associates would create and use nominees and nominee entities including 'shell' or 'shelf' corporations, trusts, foundations, partnerships and other businesses and personal entities, in a variety of forms and names, in order to provide legitimate fronts for their income." According to the indictment, legal entities were used to open bank and brokerage accounts, and hold title to property and cars.[163]

Foreign Money Transmitters

Mexico is making significant progress in supervising and enforcing AML/CFT obligations on casas de cambio (CDC), which are Mexican money transmitters, resulting in shifts in the ways in which drug traffickers handle cash.[164] In April 2006, FinCEN issued an advisory to U.S. financial institutions to alert them to the smuggling of bulk U.S. currency into Mexico,[165] which often was brought back to the United States and deposited in U.S. correspondent accounts held by Mexican banks and CDCs. In response to this detected activity, supervisors and law enforcement in the U.S. and Mexico took action to mitigate the abuse of the financial system. On the U.S. side of the border there have been a number of enforcement actions in recent years brought against U.S. banks because of inadequate monitoring and management of correspondent relationships with Mexican financial institutions:

[160] DOJ, South Carolina, news release, Two Plead Guilty to Conspiracy to Launder Funds, January 30, 2013. Available at https://www.atf.gov/press/releases/2013/04/041213-char-two-men-sentenced-in-cigarette-trafficking-operation.html
[161] USA v. Samuel Everett Orozco, et al., (D. Colo., Dec. 19, 2007)(1:07-cr-00275).
[162] USA v. Hijji Jarrett, et al.,(W.D. Mich., Oct. 18, 2006) (1:06-cr-00210).
[163] USA v. Kent Allen Jones, et al., (D. Idaho, Sept. 13, 2006)(1:06-cr-00126).
[164] *See* discussion below on regulations and supervision in Mexico.
[165] FinCEN, Advisory, Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States, FIN-2006-A003, April 28, 2006.

- In 2013, in New Jersey, Saddle River Valley Bank (SRVB) agreed to pay an $8.2 million penalty to resolve civil claims brought by DOJ, FinCEN, and the OCC regarding SRVB's failure to maintain an effective AML program. According to DOJ, the bank processed at least $1.5 billion in transactions on behalf of four CDC accountholders, three in Mexico and one in the Dominican Republic. The same Mexican CDCs also held accounts at Wachovia Bank in Florida that were used for illicit activity.[166]

- In 2012, in New York, HSBC entered into a deferred prosecution agreement (DPA) in response to failing to maintain an effective AML program and violations of the International Emergency Economic Powers Act, and the Trading with the Enemy Act. The charges followed an investigation by ICE HSI into hundreds of thousands of dollars of daily U.S. currency deposits into HSBC Mexico accounts held by CDCs and subsequent TBML-linked wire transfers from HSBC-US. According to DOJ, from 2006 to 2010, HSBC-US failed to adequately monitor more than $670 billion in wire transfers and $9.4 billion in purchases of U.S. bank notes from HSBC Mexico. DOJ also states HSBC Mexico's lax AML controls caused it to be the preferred financial institution for Mexican DTOs and money launderers during this period.[167]

- In 2011, in Florida, Ocean Bank entered into a DPA in response to a charge of willfully failing to establish an adequate AML program. The charge followed a criminal investigation into drug money laundering involving at least $11 million of structured currency deposits, unusual deposits of money orders and cashier's checks, and remittances from Mexican casas de cambio.[168] The Bank failed to recognize and mitigate risks and report transaction activity often associated with money laundering involving direct foreign account relationships in high-risk jurisdictions.[169]

- In 2010, in Florida, Wachovia Bank, N.A. entered into a DPA in response to a charge of willfully failing to establish an adequate AML program. The charge followed an investigation by DEA and IRS-CI into $13 million of wire transfers initiated by CDCs from correspondent accounts at Wachovia to pay for aircraft subsequently used to transport illegal drugs to the United States.[170]

- In 2007, in California, Union Bank of California (UBOC) entered into a DPA in response to a charge of willfully failing to establish an adequate AML program. The charge followed an investigation by DEA of U.S. drug proceeds into CDCs and from there to correspondent accounts held by the CDCs at UBOC. Deposits at UBOC were made using cash, third party checks, travelers' checks, sequential money orders, and wires from Mexican banks.[171]

The following are among the money laundering methods Mexican DTOs used to move illicit proceeds into and through the banks in the case examples cited above:

[166] USA v. $4,100,000 In U.S. Currency, Settlement Agreement, September 23, 2013.
[167] USA v. HSBC Bank USA, N.A. and HSBC Holdings PLC., Deferred Prosecution Agreement, 1:12-cr-00763-ILG, December 11, 2012.
[168] USA v. Ocean Bank, Deferred Prosecution Agreement, 1:11-cr-20553-JEM, August 16, 2011.
[169] *See also* http://www.fincen.gov/news_room/nr/html/20110822.html
[170] USA v. Wachovia Bank N.A., Deferred Prosecution Agreement, 10-20165-CR-Lenard, March 16, 2010; *See also* OCC, In the Matter of Wachovia Bank, National Association, Consent Order for a Civil Money Penalty, #2010-036, March 10, 2010. The OCC found found that Wachovia N.A. "failed to implement adequate policies, procedures, or monitoring controls governing the repatriation of nearly $14 billion of USD bulk cash for high risk casa de cambio ("CDC") and other foreign correspondent customers."
[171] USA v. Union Bank of California, Deferred Prosecution Agreement, 3:07-CR02566-W, September 18, 2007.

- Drug cash was handed off in the United States to complicit U.S. front companies that intermingled licit and illicit cash, making combined deposits to accounts held at the banks.
- Drug cash was smuggled into Mexico and placed with centros cambiarios and CDCs (some owned by or complicit with the DTOs), which then deposited some of the cash with Mexican banks and wired the money to U.S. accounts. The bank notes were then shipped back to the United States via bulk cash repatriation services provided by U.S. banks to their correspondents.
- Some of the drug proceeds smuggled into Mexico were used to purchase money orders, travelers checks, and third party checks drawn on U.S. banks to diversify the monetary instruments that were later brought back to the United States for deposit into accounts held by CDCs at U.S. banks.
- Wires were sent from the CDC accounts at both Mexican and U.S. banks in support of TBML schemes.[172]

Following the 2010 restrictions in Mexico, there was a significant decline in the purchase of dollars by Mexican financial institutions. According to DEA, that drop was also due to enforcement actions taken by U.S. and Mexican law enforcement agencies and the fact that most major U.S. banks stopped acquiring U.S. bank notes from Mexican correspondents.[173] As a result, there has been a sharp reduction in the number of CDCs operating in Mexico. In 2007 there were 24 registered CDCs.[174] Today there are eight. Other exchange houses in Mexico currently include more than 1,000 centros cambiarios, which are retail foreign exchange dealers. Centros cambiarios were not directly affected by the 2010 Mexican dollar restrictions, and they are able to accept $10,000 per customer per day. However, the U.S. dollar limits imposed on Mexican banks and CDCs has affected the amount of currency centros cambiarios can sell to banks and CDCs. Consequently, the centros cambiarios must balance their dollar and pesos surpluses by distributing currency among their branch networks, selling currency within the legal limits to banks and CDCs, or selling bulk cash dollars to U.S. MSBs. The Mexican supervisor (CNBV) is working to ensure centros cambiarios in Mexico are registered and supervised.

Despite the 2010 U.S. currency restrictions in Mexico and decline in U.S. bank note purchases by Mexican financial institutions, DEA reports there has not been an appreciable impact on the volume of drug trafficking or money laundering, because money laundering methods have changed.[175] Mexican DTOs have used front companies and individuals to receive wires and act as nominees to place U.S. currency into the Mexican banking system.[176] And couriers, nominee account holders, and front companies are doing the same in the United States.

[172] Mexican casas de cambio, unlike money services businesses in the United States, may act as brokers for financial transactions. For example, a casa de cambio as part of its routine business may direct payment to a U.S. manufacturer for export of commodities to Mexico.
[173] DEA, Office of Financial Operations, A Perspective on Mexican Bulk Cash Movement and Money Laundering Trends, February 2012.
[174] NDIC, National Drug Threat Assessment, 2008.
[175] DEA, Office of Financial Operations, A Perspective on Mexican Bulk Cash Movement and Money Laundering Trends, February 2012.
[176] DEA estimates that the amount of currency decreased with the 2010 regulations and anticipates that the amount of currency will increase with recent changes in regulations.

An alternative scheme in response to the challenges to get U.S. drug dollars into the financial system in Mexico is the use of armored cars to transport the currency back to the United States. In 2013, in Florida, two men were indicted on money laundering charges in relation to a scheme that allegedly involved the transport via armored car of drug cash from Mexico to the United States for deposit in a U.S. bank.[177] In 2014, in response to concerns about the lack of transparency in the movement of cash by armored car services and other common carriers of currency across the U.S./Mexico border, FinCEN issued guidance clarifying the circumstances under which the narrow exemption to the CMIR filing requirements apply[178] and a ruling that determined that certain armored car activity would be considered as MSB activity.[179]

Money Brokers and TBML

A recent trend, attributable to the demise of Mexican CDCs and perhaps also the Mexican restrictions on U.S. dollar deposits, is the rise of illicit money brokers. DEA reports Mexican DTOs sell U.S. dollars and other currencies, including euros earned from European drug sales, to illicit money brokers who operate in the United States and elsewhere. These foreign exchange dealers have combined their legal and illegal business.

Mexican money brokers move cash overtly as a routine part of their business. Much of the money smuggled into Mexico and then brought back into the United States for deposit is believed to be reported, as required, to U.S. Customs and Border Protection on CMIR forms upon entry into the United States. However, discrepancies between reporting on CMIRs and subsequent CTR filings by U.S. banks, when the cash is deposited, indicate that cash brought from Mexico is being comingled with additional cash already in the United States before being deposited. One method money launderers use to create the impression that large currency deposits consist of legitimate funds is to show financial institution employees a completed CMIR form. But the CMIR, whether or not legitimate, is irrelevant to whether a transaction should be considered suspicious.[180]

In May 2014, FinCEN issued an advisory[181] regarding TBML, updating a February 2010 advisory, providing red flag indicators drawn from analysis of SARs and law enforcement input.[182]

Third Party Payment Processors

Third party payment processors (TPPPs) facilitate retail transactions allowing brick-and-mortar and web-based merchants to accept a variety of payment methods. As such, legitimate TPPPs provide an important service to merchants. TPPPs may establish customer relationships with banks or contract with the bank to access its payment networks, including check clearing systems and the automated clearing house (ACH) to send and receive payments. To mitigate the risk of money laundering and fraud associated with these

[177] USA v. Martin Diaz and Enrique Guerra, affidavit, (S.D. Fl., Mar 6, 2013)(1:13-mj-02306-RLD).
[178] *See* FinCEN, CMIR Guidance for Common Carriers of Currency, Including Armored Car Services, FIN-2014-G002, August 1, 2014.
[179] *See* FinCEN, Ruling, Administrative Ruling on the Application of FinCEN Regulations to Currency Transporters, Including Armored Car Services, and Exceptive Relief, FIN-2014-R010, September 24, 2014.
[180] FinCEN, Update on U.S. Currency Restrictions in Mexico, Advisory, FIN-2012-A006, July 18, 2012.
[181] FinCEN, Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, FIN-2014-A005, May 2014.
[182] FinCEN, Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering, FIN-2010-A001, February 18, 2010.

customers, banks are expected to implement appropriate controls to ensure that they identify and understand the nature and source of the transactions processed.[183]

Unscrupulous TPPPs have been associated with money laundering, identity theft, and fraud schemes, including telemarketing fraud.[184] According to DOJ, telemarking fraud alone costs Americans about $40 billion each year and disproportionately victimizes the elderly.[185] The Federal banking agencies[186] (FBAs) and FinCEN have issued advisories and guidance since 2005 regarding the risks associated with TPPPs.[187] The following are case examples of fraud and money laundering through TPPPs:

- In 2012, in New York, a man was convicted of bank fraud in connection with processing payments for illegal online poker sites. The FBI investigation that led to the prosecution revealed the man, who was one of several payment processors charged, used accounts at three banks, misleading the banks as to the nature of the transactions. The man also approached three failing banks offering to invest millions of dollars in each in exchange for being allowed to process online poker transactions.[188] Among the banks involved was SunFirst Bank, Utah, which entered into a Consent Order with the Federal Deposit Insurance Corporation (FDIC) in 2010 ordering the bank to stop providing payment processing for any third party payment processor without written approval from the FDIC.[189] The bank failed in 2012.
- In 2012, in Pennsylvania, First Bank of Delaware settled civil claims brought by DOJ, which alleged the bank allowed a number of fraudulent businesses and payment processors to debit consumer accounts knowing or turning a blind eye to the fact the consumer authorization for the withdrawals had been obtained by fraud. The bank was assessed a $15 million penalty for BSA and related violations.[190]
- In 2009, in New York, a man was charged with bank fraud and money laundering in connection with processing payments for illegal online gambling sites. The FBI investigation that led to the prosecution revealed the man opened accounts at U.S. banks in the names of legal entities, misrepresenting the nature of the businesses and the purpose of the transactions. The accounts were used to transfer funds to and from U.S. customers to accounts in Cyprus held by online gambling sites.[191]

[183] FFIEC BSA/AML Exam Manual at page 236-37.
[184] FinCEN, Advisory, Risk Associated with Third-Party Payment Processors, FIN-2012-A010, Oct. 22, 2012.
[185] Department of Justice, Eastern District of Pennsylvania, news release, Wachovia Issues More Than $150 million in Checks to Victims of Payment Processing Center Scam, Dec. 11, 2008.
[186] Board of Governors of the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, and the Office of the Comptroller of the Currency.
[187] OCC Policy Analysis Paper #6, ACH Payments: Changing Users and Changing Uses, Oct.2005; OCC, OCC, Bulletin 2006-39, Sept. 1, 2006; FFIEC BSA/AML Exam Manual; FDIC, Guidance on Payment Processor Relationships, FDIC FIL-127-2008, November 7, 2008 (revised July 2014); FinCEN, Advisory, Risk Associated with Third-Party Payment Processors, FIN-2012-A010, Oct. 22, 2012.
[188] DOJ, Southern District of New York, news release, Payment Processor for Internet Poker Companies Sentenced in Manhattan Federal Court, October 3, 2012.
[189] FDIC Consent Order, FDIC-10-845b, November 9, 2010.
[190] DOJ, Eastern District of Pennsylvania, news release, Department of Justice Announces $15 million Settlement with Local Bank Accused of Consumer Fraud, November 19, 2012.
[191] USA v. Douglas Rennick, (S.D.N.Y., Aug. 5, 2009)(1:09-cr-00752-SHS). Available at http://www.fbi.gov/newyork/press-releases/2009/nyfo080609.htm

- In 2008, Wachovia Bank entered into a settlement agreement with the OCC and a DPA with the DOJ in 2010 that directed the bank to pay more than $150 million to the more than 740,000 consumers harmed by the bank's relationships with fraudulent telemarketers and an unscrupulous TPPP.[192] The telemarketers obtained victims' bank account information over the phone by offering a range of dubious products and services, and then passed the account information to the TPPP, which generated a remotely-created check. Using accounts at Wachovia Bank, the TPPP processed the unsigned bank drafts for payment. The TPPP knew the telemarketers had obtained the account information through fraud, and the OCC concluded the bank had engaged in unsafe or unsound practices.

c. Compliance Deficiencies

Strong BSA/AML compliance programs[193] are essential to mitigate the vulnerabilities noted above. Banks may be vulnerable to money laundering when they fail to keep pace with how criminals exploit new products and services, or when AML programs are insufficient.[194] A number of recent BSA/AML enforcement actions involving large complex banking organizations have highlighted the need for effective internal controls and corporate governance.[195]

- *JPMC Bank, N.A., Columbus, Ohio (JPMC)* – In January 2013, the OCC entered into a C&D order with JPMC Bank, N.A., and two of its affiliates, to address deficiencies involving internal controls, independent testing, customer due diligence, risk assessment, and SAR processes (monitoring, investigating and decision-making). Additionally, the bank did not have enterprise-wide policies and procedures to ensure that, on a risk basis, customer transactions at foreign branch locations can be assessed, aggregated, and monitored. Concurrent with the OCC's enforcement action, the Board of Governors of the Federal Reserve System issued a cease and desist order upon consent with the bank's parent company, JPMorgan Chase & Co. that focused on requiring improvements in enterprise-wide risk management programs.

Additionally, high-risk services or products including foreign correspondent banking, cross-border funds transfers, bulk cash repatriation, and remote deposit capture can be high-risk areas that some banks have not managed effectively.

- *Citibank, N.A., Sioux Falls, South Dakota* (Citibank) – In April 2012, the OCC entered into a C&D order with Citibank, N.A., to address BSA deficiencies involving internal controls, customer due diligence, audit, monitoring of its RDC and international cash letter instrument

[192] *See* http://www.occ.gov/news-issuances/news-releases/2008/nr-occ-2008-48.html
[193] Depository institutions are required by regulation to establish and maintain compliance programs that consist of four components: (1) a system of internal controls to ensure ongoing compliance; (2) independent testing of BSA/AML compliance; (3) designation of and individual or individuals responsible for managing BSA compliance; and (4) training for appropriate personnel.
[194] Office of the Controller of the Currency, Semi Annual Risk Perspective, Spring 2013.
[195] *See, e.g.,* In the Matter of JPMorgan Chase Bank, N.A., Columbus Ohio, OCC 2013-002 AA-EC-13-04, Art. IV, p.8 (Jan. 14, 2013); In the Matter of Citibank, N.A., Sioux Falls, South Dakota, OCC 2012-52 AA-EC-12-18, Art. IV, p.7. (Apr. 4, 2012)); In the Matter of HSBC Bank USA, N.A., Mclean, VA, OCC 2010-199 AA-EC-10-98, Art. VI, p.10 (Sept. 24, 2010); In the Matter of Wachovia Bank, National Association, Charlotte, N.C., OCC 2010-37 AA-EC-10-17, Art. II, p.5. (Mar. 12, 2010).

processing in connection with foreign correspondent banking, and suspicious activity reporting relating to that monitoring. These findings resulted in violations by the bank of statutory and regulatory requirements to maintain an adequate BSA compliance program, file SARs, and conduct appropriate due diligence on foreign correspondent accounts.

- On October 16, 2013, the FRB announced the execution of an enforcement action against Commerzbank AG's New York branch. Commerzbank AG and its New York branch agreed to jointly develop a written plan to enhance management's oversight of the New York branch's compliance with BSA/AML requirements; retain an independent consultant to review the branch's compliance with BSA/AML requirements; enhance the branch's BSA/AML compliance program, customer due diligence program, and suspicious activity monitoring program; and conduct a transaction review to determine whether suspicious activity was properly identified. The enforcement action followed a previous enforcement action against the branch in 2012 for similar deficiencies in the branch's bulk cash transaction business line.
- First Bank of Delaware, 2012 – The FDIC, concurrently with DOJ and FinCEN, assessed a $15 million CMP which was satisfied by one $15 million payment to the U.S. Treasury. The FDIC concluded that the bank's BSA compliance program was deficient in all four elements: internal controls, independent testing, designation of individual to coordinate and monitor compliance, and training for appropriate personnel. The bank had not effectively implemented policies and procedures to mitigate potential money laundering risks, given its high-risk products and clients, and failed to detect and report suspicious activity.
- In 2010, Pamrapo Savings Bank of New Jersey pleaded guilty to failing to file CTRs and SARs related to approximately $35 million in illegal and suspicious financial transactions. The bank admitted that it willfully violated the BSA to avoid the expense of compliance, and admitted it made false and misleading statements to bank regulators.[196]

FBAs have the authority to hold corporate directors personally responsible for inadequate BSA compliance:

- In 2013, the OCC issued Civil Money Penalties and personal Cease and Desist Orders against three former board members and two former board chairs for actions that contributed to violations of the BSA at Security National Bank of North Lauderdale, Florida.[197] In 2010 the OCC had issued a Consent Order directing the bank to correct a number of BSA deficiencies.[198] The bank failed in May 2012.

[196] DOJ, Pamrapo Savings Bank of New Jersey Pleads Guilty to Conspiracy to Commit Bank Secrecy Act Violations and Forfeits $5 Million, news release, March 29, 2010. Available at http://www.justice.gov/opa/pr/2010/March/10-crm-335.html

[197] Harold Connell (OCC docket number AA-EC-12-94, January 2, 2013), Robert Dietz (OCC docket number AA-EC-12-95, January 2, 2013), Timothy Kenney (OCC docket number AA-EC-11-12-96, January 2, 2013), Manual Fernandez (OCC docket number AA-EC-12-98, January 2, 2013), Harper Floyd (OCC docket number AA-EC-12-99, January 2, 2013).

[198] OCC docket number AA-EC-10-36, May 19, 2010.

- In 2011, the OCC assessed a Civil Money Penalty against Pacific National Bank of Florida for failure to implement an effective AML program and report suspicious transactions.[199] Four board members including the bank's chairman and the chief executive were also fined for the compliance lapse.[200]

Unfortunately, even when a bank has a strong AML program, a single complicit employee can circumvent appropriate policies and procedures to facilitate criminal activity. In 2013, in California, one of dozens of people charged with using stolen identities to commit bank and tax fraud was a bank employee who allegedly used her position to open bank accounts to receive fraudulent tax refunds and launder the proceeds.[201]

In August 2014, FinCEN issued an advisory to financial institutions, including banks, calling attention to recent AML enforcement actions and emphasizing the culture of an organization is critical to its compliance.[202] FinCEN advised financial institutions that they can strengthen their organization's BSA compliance by ensuring that:

- Its leadership actively supports and understands compliance efforts;
- Efforts to manage and mitigate BSA/AML deficiencies and risks are not compromised by revenue interests;
- Relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts;
- The institution devotes adequate resources to its compliance function;
- The compliance program is effective by, among other things, ensuring that it is tested by an independent and competent party; and
- Its leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used.

2. Risks

Banks, particularly the largest banks in the United States, are at the center of the global financial system and as such are at greatest risk for criminal abuse. Recent AML enforcement actions are indications that misuse of banking products and services and customer relationships continues to be present in the United States at banks with BSA/AML program deficiencies.

[199] OCC docket number AA-EC-10-127, March 22, 2011.
[200] Jose Baloyra (OCC docket number AA-EC-11-06, April 14, 2011), Andrès Baquerizo (OCC docket number AA-EC-11-07, April 14, 2011), Ralph Fernandez (OCC docket number AA-EC-11-08, April 14, 2011) , Eduardo Gross (OCC docket number AA-EC-11-09, April 14, 2011), and Joaquin Urquiola (OCC docket number AA-EC-11-10, April 14, 2011).
[201] More Than 50 People Indicted in Massive Fraud Ring Thousands of Stolen Identities Used to Get Millions in Bogus Tax Refunds, news release, U.S. Attorney's Office, Southern District of California, September 26, 2013.
[202] FinCEN, Advisory, U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007, August 11, 2014.

While structuring is a common money laundering method in the United States, banks file thousands of SARs annually citing structuring and law enforcement utilizes these SARs to identify criminal activity and identify individuals. This suggests that, generally, structuring does not go undetected.

Identifying suspicious activity depends in part on the adequacy of a bank's customer due diligence policies and procedures. Not knowing who owns or controls an account (i.e., the beneficial owner) can make it difficult for a bank to understand how an account is being used and whether the activity is legitimate. There is no current federal obligation to identify the beneficial owner of an account except in very specific circumstances (i.e., correspondent banking relationships and private banking for non-U.S. clients).[203]

The use of businesses and other legal entities to commingle licit and illicit funds tests a bank's ability to accurately identify sources of funds to determine if transaction activity is suspicious. Even when a bank is able to do so, a business mixing licit and illicit proceeds can frustrate a prosecutor's use of the money laundering charge that prohibits the spending of more than $10,000 of illicit proceeds (18 U.S.C. 1957).[204] In both the Fifth and Ninth Circuits, courts have held that when a defendant transfers over $10,000 from a commingled account, the defendant is entitled to a presumption that the first money moved out of the account is legitimate. This "criminal proceeds — last out" standard often prevents the government from pursuing section 1957 charges where illegal proceeds are moved through a commingled account.

As the preceding section demonstrates, once a money launderer comes under law enforcement, regulatory, or supervisory focus, they shift their methods, often alternating among existing money laundering methods. They may also seek opportunities to abuse new technology and payment services. As such, it is likely that vulnerabilities will continue to be exploited and the necessity for banks to manage the resulting risk will continue. Recognizing evolving vulnerabilities in the banking system, the FFIEC states in its examination manual that "FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. Examiners should focus on evaluating a bank's policies, procedures, and processes to identify, evaluate, and report suspicious activity."[205]

Section 312 of the USA PATRIOT Act requires U.S. financial institutions to perform due diligence and, where appropriate, enhanced due diligence, with regard to correspondent accounts established or maintained for foreign financial institutions.[206] The regulation recognizes the vulnerability created by the misuse of foreign correspondent banking relationships to facilitate the placement of illicit funds into the U.S. financial system. A U.S. banking association discussing this vulnerability concluded that "once a person is able to inject funds into the payment system that are the product of a criminal act, are intended to finance a criminal act, or are tied to a party subject to U.S. sanctions, it is very difficult, and in many cases impossible, to identify those funds as they move from bank to bank. If banks sending payments through the system are engaged in deceptive practices, it can be almost impossible for correspondent banks to detect. Government cooperation in setting and enforcing international standards for anti-money

[203] *See* 31 C.F.R. §§ 1010.610 and 1010.620.
[204] Jennifer Shasky Calvery, DOJ, Testimony before the House Subcommittee on Crime, Terrorism, and Homeland Security, February 8, 2012.
[205] FFIEC BSA/AML Exam Manual, Suspicious Activity Reporting – Overview (2014).
[206] 31 C.F.R. §§ 1010.610 and 1010.620.

laundering and transparency in the financial system is essential if banks' efforts to detect and report potential money laundering are to be effective."[207]

In addition, poorly regulated and supervised foreign financial institutions put U.S. banks at risk and frustrate law enforcement efforts. According to DEA, law enforcement generally has access to the information it needs to identify and investigate significant money laundering cases in the United States. However, the same transparency is not always present in other countries.[208] ICE HSI notes that their investigators continue to encounter challenges in accessing foreign financial transaction data.[209]

With few exceptions, U.S. regulation, supervision, and enforcement are effective and adequate. Between 2006 to 2012, out of the approximately 13,000 depository institutions in the United States only approximately 1 percent were subjected to formal enforcement actions requiring them to improve their programs, and over the last three years the issuance of enforcement actions has decreased significantly.

[207] The Clearing House, Clearing House Association, L.L.C., Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking, September 2014.
[208] *See* DEA overview of Money Laundering. Available at http://www.justice.gov/dea/ops/money.shtml
[209] Key Locations and Vulnerabilities Related to Money Laundering Methods Used by Transnational Criminal Organizations to Transport, Launder, and Store Illicit Proceeds, ICE HSI – Office of Intelligence, August, 15, 2013.

C. Money Services Businesses

More than 90 percent of households in the United States have an account with a depository financial institution yet many people, particularly immigrants, prefer to use MSBs for financial services because of convenience, cost, familiarity, or tradition. More than a quarter of American households use non-bank financial institutions such as MSBs, to do everything from paying their bills and cashing checks to supporting their family members abroad. An MSB is defined by regulation[210] to be any person, wherever located, doing business wholly or substantially in the United States, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities[211]:

- Money transmitter
- Check casher
- Issuer or seller of money orders
- Issuer or seller of traveler's checks
- Dealer in foreign exchange
- Provider or seller of prepaid access

All principal MSBs, except for the United States Postal Service, are required to register with FinCEN[212] and to establish a written AML program reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[213] Additionally, the BSA requires MSBs to file CTRs[214] and SARs,[215] and maintain certain records. The MSB recordkeeping requirements ($3,000 for money orders and traveler's checks) are specific to purchases of cashier's checks, money orders and traveler's checks;[216] dealers in foreign exchange;[217] and money transmitters.[218] In addition, many states have licensing criteria for certain types of MSBs such as money transmitters and check cashers.

Size of the MSB Principal and Agent Populations

There were 41,788 MSBs registered with FinCEN as of April 10, 2015.[219] In 2011, FinCEN surveyed the approximately 25,000 MSBs that reported on their registration form that they had agents.[220] One hundred

[210] 31 C.F.R. § 1010.100(ff).
[211] Banks, foreign banks, persons registered with and functionally regulated and examined by the Securities and Exchange Commission, the Commodities Futures Trading Commission, or its foreign equivalents, and natural persons that engage in infrequent, not for profit or gain activity similar to MSB activity, are not encompassed by the MSB definition.
[212] *See* 31 C.F.R. § 1022.380.
[213] *See* 31 C.F.R. § 1022.210.
[214] *See* 31 C.F.R. § 1010.311.
[215] *See* 31 C.F.R. § 1022.320. Check cashers are not covered by the SAR requirement. *See* 31 C.F.R. § 1022.320(a)(1), (5).
[216] *See* 31 C.F.R. § 1010.415.
[217] *See* 31 C.F.R. § 1022.410.
[218] *See* 31 C.F.R. § 1010.410(e)–(f).
[219] *See* FinCEN, MSB Registrant Search Web page for the most recent registration total. Available at http://www.fincen.gov/financial_institutions/msb/msbstateselector.html
[220] FinCEN, The SAR Activity Review, Issue 21, May 2012.

and seventy companies responded to the survey, reporting more than 230,000 agents.[221] The number of agents reported per MSB principal ranged from under ten to tens of thousands. Table 5 illustrates the number of principals that reported having agents and the corresponding number of agents reported.

Table 5

Number of Principals	***Number of Agents Reported per Principal***
3	20,000 or more
0	15,000 – 19,999
2	10,000 – 14,999
2	5,000 – 9,999
18	1,000 – 4,999
7	500-999
25	100-499
21	50-99
54	10-49
65	Less than 10

The highest volume of MSB agents was reported in California, Texas, New York, and Florida, which are the most populous states. There was also a high volume of agents reported in Georgia and North Carolina. Principals were asked to identify which MSB activities their agents conduct on behalf of the principal. Table 6 shows the totals reported for each category of agent activity listed.

Table 6

Category of MSB Activity Reported	***Number of Agents Reported***
Money Transmitter	178,944
Seller of Money Orders	95,975
Issuer of Money Orders	1,289
Dealer in Foreign Exchange	435
Check Casher	275
Seller of Traveler's Checks	29
Issuer of Traveler's Checks	16

Note: Totals are approximate and based on totals reported, as not every principal checked a box for every agent

[221] An agent is a separate business entity from the principal that the principal authorizes, through a written agreement or otherwise, to sell its instruments or, in the case of funds transmission, to sell its send and receive transfer services.

C1. Money Transmitters

Money transmitters are defined as any person that accepts currency, funds, or other value that substitutes for currency from one person and transmits currency, funds, or other value that substitutes for currency to another person or location, by any means.[222] The definition is agnostic with respect to technology or business process. All service providers that meet the definition of a money transmitter are subject to the applicable regulations, including exchangers and administrators of virtual currency.[223]

Historically, consumers have chosen to send remittances[224] abroad largely through money transmitters such as Western Union and MoneyGram.[225] The federal recordkeeping requirement for money transmitters, and certain other MSBs, allows funds transfers below $3,000 without requiring the verification and recording of the customer's identification or sending certain information about the transmitter and the transaction with the payment.[226]

Individuals in the United States send approximately $37 billion annually to households abroad.[227] The average remittance from the United States to Latin America was estimated in 2011 to be only $290 with the average to Mexico only $400.[228] In addition to the approximately one million legal immigrants who become lawful permanent residents in the United States each year[229], there are an estimated 11.4 million illegal immigrants in the U.S.; most are from Mexico.[230] More than half of the immigrants in the country are believed to live in California, New York, Florida, and Texas.

Section 359 of the USA PATRIOT Act expanded the definition of financial institution to include any person who engages as a business in an informal value transfer system (IVTS) or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside the

[222] A money transmitting service includes accepting currency or funds denominated in the currency of any country and transmitting the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal Reserve bank or other facility of the Board of Governors of the Federal Reserve System, or an electronic funds transfer network (31 U.S.C. § 5330 (d)(2).
[223] FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,
March 18, 2013. Available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
[224] Definitions of remittance transfer vary, based on the method and purpose of the transfer. For this report, a remittance transfer is defined as a transfer of funds from a consumer in the United States to a consumer or business in a foreign country. This definition is based on the definition in section 919(g)(2) of the Electronic Fund Transfer Act, as amended by section 1073(a) of the Dodd-Frank Act.
[225] Board of Governors of the Federal Reserve System, Report to the Congress on the Use of the ACH System and Other Payment Mechanisms for Remittance Transfers to Foreign Countries, April 2013.
[226] 31 C.F.R. § 1010.410 (e) and (f).
[227] This is the figure for "personal transfers" from the Bureau of Economic Analysis (BEA), Table 5.1, line 9 of the U.S. International Transaction Accounts. The BEA defines personal transfers, or remittances, as transfers from U.S. resident immigrants to foreign residents. According to the Board of Governors of the Federal Reserve System, the BEA's definition of an international remittance differs from the definition in the Dodd-Frank Act. In particular, the BEA's definition excludes remittance transfers sent to businesses, and it is not limited to remittances sent in electronic form.
[228] Manuel Orozco, Future Trends in Remittances to Latin America and the Caribbean, Table 7, InterAmerican Dialogue, May 2012. Orozco notes the average remittance figures were reported by transfer companies to him.
[229] Randall Monger and James Yankay, U.S. Lawful Permanent Residents: 2013, Annual Flow Report, Department of Homeland Security, Office of Immigration Statistics, May 2014.
[230] Brian Baker and Nancy Rytina, Estimates of the Unauthorized Immigrant Population Residing in the United States: 2012, DHS, Office of Immigration Statistics, March 2013.

conventional financial institution system.[231] Depending on the ethnic group, IVTS are called by a variety of names including, for example, "hawala" (Middle East, Afghanistan, Pakistan); "hundi" (India); or "fei ch'ien" (China).[232] FinCEN recognizes IVTS as a form of money transmitter,[233] noting expatriates and immigrants often use IVTS to send money back to their home countries and legitimate companies, traders, and government agencies use IVTS to conduct business in countries with inadequate formal financial systems.[234] IVTS may legally operate in the United States given compliance with applicable state and federal laws, including registration with FinCEN as a money transmitter.

Virtual Currency

Virtual currency is not legal tender but can be transferred from entity to entity, person to person, as a substitute for legal tender and later converted into real currency. In July 2011 FinCEN published a final rule amending, among other things, the definition of money transmitter, adding the language "or other value," so the definition now reads: "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[235] FinCEN issued interpretive guidance in March 2013 clarifying that based on certain activities that constitute money transmission, administrators and exchangers of convertible virtual currency are money transmitters, and are required to comply with the same registration, AML program, recordkeeping, and CTR and SAR reporting obligations that apply to money transmitters.[236]

In 2015, San Francisco-based Ripple Labs Inc., the developer and seller of a virtual currency known as XRP, was cited by FinCEN in the first civil enforcement action against a virtual currency exchanger. FinCEN cited Ripple Labs and a wholly-owned subsidiary with willfully operating as an MSB and selling its virtual currency without registering with FinCEN, failing to implement and maintain an adequate AML program, and failing to report suspicious activity related to several financial transactions. Concurrent with FinCEN's enforcement action, DOJ reached a settlement agreement with Ripple Labs to resolve a criminal investigation into the Bank Secrecy Act violations. FinCEN assessed a $700,000 civil money penalty concurrent with the U.S. Attorney's Office for the Northern District of California's settlement agreement, which included a forfeiture of $450,000.[237]

Centralized virtual currencies have a centralized repository and a single administrator. Liberty Reserve, which FinCEN identified in 2014 as being of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act, is an example of a centralized virtual currency. Decentralized virtual currencies have no central repository and no single administrator. Instead, value is electronically

[231] Section 359 of the USA PATRIOT Act.
[232] FinCEN, Advisory, Informal Value Transfer Systems, Issue 33, March 2003.
[233] 31 U.S.C. § 5330.
[234] FinCEN, Advisory, Informal Value Transfer Systems, Issue 33, March 2003.
[235] 31 C.F.R. § 1010.100(ff)(5)(i)(A
[236] An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency; *See* Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, March 18, 2013.
[237] Available at http://www.fincen.gov/news_room/nr/pdf/20150505.pdf. The $450,000 forfeiture in the DOJ settlement will be credited to partially satisfy FinCEN's $700,000 civil money penalty.

transmitted between parties without an intermediary. Bitcoin is an example of a decentralized virtual currency. Bitcoin is also known as a cryptocurrency, meaning that it relies on cryptographic software protocols to generate the currency and validate transactions.[238]

The development of virtual currencies is an attempt to meet a legitimate market demand. According to a Federal Reserve Bank of Chicago economist, U.S. consumers want payment options that are versatile and that provide immediate finality.[239] No U.S. payment method meets that description, although cash may come closest. Virtual currencies can mimic cash's immediate finality and anonymity and are more versatile than cash for online and cross-border transactions, making virtual currencies vulnerable for illicit transactions.

Decentralized convertible virtual currency such as Bitcoin is still a niche payments product. The total 24-hour transfer volume for the top 10 Bitcoin exchangers was $22,995,398, averaging $249/transaction (as of March 30, 2015).[240]

1. Vulnerabilities

a. Structuring

The following case examples illustrate that money transmission, and other MSB financial services that allow for anonymous transactions below the $3,000 recordkeeping threshold (i.e. money orders and travelers checks), are used for a variety of illicit payments:

- In 2011, in St. Croix, Virgin Islands, seven people were sentenced for money laundering and drug trafficking involving the transfer of drugs from St. Croix to Fairbanks, Alaska and sending the illicit proceeds back.[241] Cocaine and crack cocaine were the drugs that were distributed, usually via Express Mail parcels, and payment was sent back via Western Union wires and money orders. Hundreds of thousands of dollars were sent in amounts averaging less than $2,000 per wire.
- In 2008, in California, four members of a San Diego family were indicted for running a small alien smuggling ring that had allegedly been bringing illegal immigrants into the United States from Mexico since 1996, earning approximately $50,000 a year.[242] According to the indictment, the defendants instructed the sponsors of the illegal immigrants to pay the smuggling fee, which ranged from $1,000 and $3,000 per person, via nonbank wire transfer and to structure the payment across multiple wires.
- In 2008, in Wyoming, 21 people were indicted on charges of distributing methamphetamine in Colorado, Montana, South Dakota, and Wyoming. According to the indictment, payment for the

[238] *See* http://www.fincen.gov/news_room/testimony/html/20131119.html
[239] Bruce J. Summers, Facilitating Consumer Payment Innovation through Changes in Clearing and Settlement, paper presented at the Federal Reserve Bank of Kansas City "Consumer Payment Innovation in the Connected Age" conference, March 29-30, 2012, Kansas City, Mo
[240] *See* Crypto-Currency Market Capitalizations as of April 2015. Available at http://coinmarketcap.com/.
[241] IRS-CI, Examples of Money Laundering Investigations - Fiscal Year 2012.
[242] USA v. Maria Del Carmen Alvarez, et al., (S.D. Cal., Aug. 29, 2008)(3:08-cr-02937-H).

methamphetamine was made in cash, wire transfers through money transmitters, and deposits to alleged dealers' bank accounts.[243]

- In 2007, in Montana, three men were indicted for manufacturing and selling anabolic steroids and laundering the proceeds.[244] The men bought the drugs from a supplier in China and resold them online. According to the indictment and the subsequent guilty plea of one of the defendants[245], retail buyers sent cash, U.S. Postal Service money orders, and Western Union and MoneyGram wires to the sellers. The sellers, in turn, wired payments to suppliers in China. According to court documents, Western Union eventually cut off wire service access to one of the defendants. E-Gold, a virtual currency was also used to pay Chinese suppliers.

b. Compliance Deficiencies

As with any financial service provider, covered entities and employees who choose to disregard AML policies and procedures will undermine an organization's regulatory compliance strategy, as the following case examples demonstrate:

- In 2014, FinCEN imposed a $125,000 civil money penalty against a New Jersey MSB for ignoring repeated warnings from state and federal examiners, and its own independent auditor, to correct deficiencies with its internal controls, independent testing, and training. Prior to a 2011 examination, the MSB has never filed a single SAR.[246]

- In 2014, a FinCEN investigation determined that since November 2007, a Michigan MSB failed to implement any AML program and during its operation, transmitted approximately 1,400 wires per year to Yemen. The MSB agreed to cease operating and agreed to pay a civil money $12,000 penalty.[247]

- In 2012, MoneyGram, the second largest money transmitter in the United States, signed a deferred prosecution agreement with the Department of Justice and agreed to address the problems in its AML program that facilitated fraud.[248] MoneyGram agents knowingly assisted various schemes that involved U.S. consumers wiring more than $100 million to Canada in response to fraudulent claims that they had to pay a fee or a tax before receiving a lottery winning, salary payment, or loan that they were falsely told was due them. According to a complaint filed by the Federal Trade Commission, 79 percent of all MoneyGram wire transfers of $1,000 or more from the United States to Canada over a sample period in 2007 were fraud-induced payments.

- In 2010, Western Union entered into a $94 million settlement agreement with the state of Arizona after having been accused of processing more than $500 million in payments to human smugglers

[243] USA v. Jose Suarez-Negrete, et al., indictment, (D. Wyo., May 14, 2008)(2:08-cr-00105-ABJ).
[244] USA vs. Jimmy Ray Jones, et al., (D. Mont., Oct. 3, 2007)(9:07-cr-00066-DWM).
[245] USA v. Jimmy Ray Jones, Offer of Proof in Support of Guilty Plea, (D. Mont., Jan. 25, 2008)(9:07-cr-00066-DWM).
[246] *See* http://www.fincen.gov/news_room/nr/pdf/20140828.pdf
[247] *See* http://www.fincen.gov/news_room/nr/pdf/20140207.pdf
[248] Moneygram Deferred Prosecution Agreement, Statement of Facts, November 9, 2012. Available at http://www.justice.gov/usao/pam/news/2012/MoneyGram_DPA_11_09_2012.pdf

annually between 2003 and 2007.[249] Before releasing family members smuggled into the United States, the smugglers allegedly demanded that their commissions be sent to them by Western Union. From 2003 to 2008, $176 million in payments were sent from 29 states to recipients in Arizona who received the funds through eight allegedly complicit Western Union agents.

- In 2008, Sigue Corporation, then the third largest money transmitter in the United States with agents primarily serving the U.S.-Mexico corridor, entered into a deferred prosecution agreement with the Department of Justice and consented to the assessment of a civil money penalty by FinCEN due to its failure to maintain an effective AML program.[250] A DEA undercover operation in 22 states identified 59 Sigue agents that had agreed to structure wire transfers of more than $500,000 that was represented to be drug proceeds.
- In 2007, the El Dorado Task Force[251] in New York conducted Operation Pinpoint, a sting operation against money transmitters allegedly facilitating drug money laundering.[252] Twenty-seven money transmitters were prosecuted. The money transmitters had allegedly agreed to transfer drug proceeds to Colombia and to structure the transactions in order to avoid federal recordkeeping and reporting requirements.

c. Unregistered / Unlicensed MSBs

In addition to the thousands of MSB principals registered with FinCEN and their hundreds of thousands of agents, there are also unregistered MSBs and agents operating in the United States illegally. In 2011, depository institutions submitted almost 5,300 SARs citing potential unlicensed MSB activity. Almost half of the SARs (46%) were filed in California, New York, Texas, and Florida and many identified grocery or convenience stores, gas stations, or liquor stores as potentially operating illegally as money transmitters, check cashers, or currency exchangers. Additionally, individuals may misuse their personal or business bank accounts to transmit funds for customers on a commercial scale thus operating as unregistered MSBs. The following are case examples of unregistered or unlicensed MSBs:

- In 2011 FinCEN assessed a $12,500 civil money penalty against a Maine-based unregistered money transmitter for funds transfers between January 2006 and October 2010.[253] In a typical transaction, a customer provided the owner with cash, checks, or money orders, along with instructions to transmit funds to a specified beneficiary, and owner deposited those funds into her U.S. deposit accounts, which she then transferred to Cambodia.
- In 2010 in Michigan two men were charged with criminal conspiracy and operating as unlicensed money transmitters.[254] The men owned and operated a small grocery store where they allegedly charged a commission of 6-7 percent to arrange funds transfers to countries including Somalia,

[249] State of Arizona, ex rel. Attorney General Terry Goddard, Plaintif v. Western Union Financial Services, Inc., Defendant, Settlement Agreement, March 11, 2010.
[250] *See* http://www.justice.gov/opa/documents/sigue-deferred-prosecution-agreement.pdf
[251] The El Dorado Task Force is made up of federal, state, and local intelligence analysts, police, special agents, and prosecutors who target financial crime at all levels in the New York/New Jersey area.
[252] USA v. Liliana Valencia and Maria Irizarry, Affidavit in Support of Arrest and Search Warrants, 1:07-cr-00384-ILG filed in United States District Court in the Southern District of New York on February 2, 2007.
[253] Available at http://www.fincen.gov/news_room/ea/files/ASSESSMENT_SarithMeas_Enforcement_matter_number_2011-10.pdf
[254] USA v. Mohamed Abukar Sufi and Omar Abukar Sufi, (W.D. Mich., Aug. 11, 2010)(1:10-cr-00234-JTN).

Ethiopia, Saudi Arabia, Sudan, Yemen, Uganda, Kenya, and the United Arab Emirates. The men allegedly structured cash deposits into a bank account and then purchased cashier's checks made out to unlicensed money transmitters in Ohio and Michigan who facilitated the funds transfers.

- In 2010 FinCEN assessed a $25,000 civil money penalty against an Oregon-based unregistered money transmitter.[255] From July 2002 through March 2009, the unregistered money transmitter conducted more than 4,200 funds transfers in the United States, amounting to more than $172 million, to and from a number of locations in Europe and Asia. According to the FBI, the man behind this global scheme created five shell corporations—businesses that only existed on paper—in Oregon and began moving money through these bogus companies for his overseas business associates.[256]

Unregistered and unlicensed MSBs can include hawalas and other forms of IVTS. There is no practical or functional distinction between a hawala and any other money transmitter. While it is theoretically possible for informal systems to operate wholly outside of the banking system, it is not often the case. Instead, law enforcement investigations indicate IVTS often use an account at a bank to clear and settle transactions internationally. The following are case examples of unlicensed IVTS:

- In 2007, eight defendants in Maryland from Pakistan and Bangladesh were charged with operating an unlicensed IVTS.[257] This case was a sting operation in which law enforcement used a cooperating witness to request the transfer of cash that was represented to be illicit proceeds. In return for a commission of 5 to 7 percent, the defendants allegedly received the cash in the U.S. and made the corresponding value available in Spain, Australia, and elsewhere.
- In 2006, 22 people in New York were indicted for distributing the drug khat in the United States and laundering the proceeds through a hawala network that was also used to pay suppliers in Europe and Africa.[258] According to the indictment, khat distributors collected approximately $5 million annually, which was laundered through hawalas located in New York, Minnesota, Ohio, and elsewhere in the United States. The hawalas reconciled accounts with counterparts in Europe, Africa, and Dubai, by transferring funds between bank accounts in the United States and bank accounts in Dubai.

FinCEN asked depository institutions in September 2010 to use the abbreviation "IVTS" in the SAR narrative when reporting suspicious activity associated with informal money transmitters.[259] In the 10 months following the request, 527 SARs were filed.[260] The majority of those SARs contained descriptions of suspicious currency exchange activity involving Latin America and Middle East countries, particularly the United Arab Emirates, Yemen, and Iran.

SAR data indicates that unregistered money transmitters may be used to build parallel currency exchange mechanisms to circumvent exchange controls, such as in Venezuela, Argentina, and Mexico. Additional

[255] Available http://www.fincen.gov/news_room/nr/html/20110308.html
[256] *See* http://www.fbi.gov/news/stories/2011/march/money_030811/money_030811
[257] USA v. Abdul Rehman, et al., (D. Md., Sept. 20, 2007).
[258] USA v. Bashi Muse, et al., sealed superseding indictment, (S.D.N.Y, July 26, 2006).
[259] FinCEN, Informal Value Transfer Systems, FinCEN Advisory FIN-2010-A011, September 1, 2010.
[260] FinCEN, The SAR Activity Review: Trends, Tips & Issues, FinCEN, Issue 20, October 2011.

data indicates transactions that originate from exchange houses and trading firms in Latin America and the Middle East are routed through personal and business accounts in the United States to purchase goods and property in the United States.

d. Virtual Currency

Convertible virtual currency administrators and exchangers conducting business in the United States are subject to the same BSA regulations as other money transmitters. However, the rapid evolution of the market, the development of new business models and entry of new virtual currency payments developers and providers—many from a non-financial services environment (e.g., the technology sector), where industry is not as highly regulated as in the financial sector—together with the potential to operate without a domestic presence, is leading to service providers entering the market that do not comply with BSA obligations. The Secret Service observes that criminals are looking for and finding virtual currencies that offer: [261]

- Anonymity for both users and transactions
- The ability to move illicit proceeds from one country to another quickly
- Low volatility, which results in lower exchange risk
- Widespread adoption in the criminal underground
- Trustworthiness

The following virtual currency prosecutions involve service providers that intentionally promoted anonymity and other virtual currency attributes attractive to criminals:

- In 2013, in Oregon, two Portland residents and two Vancouver residents were charged with drug trafficking and money laundering in connection with selling methamphetamine internationally in exchange for Bitcoin through the now defunct online illicit bazaar Silk Road.[262] Silk Road was only accessible through an encrypted underground network, TOR (formerly, The Onion Router),[263] and the majority of electronic communications between buyers and sellers was on the Silk Road website via internal private messaging. All transactions were paid for in Bitcoin. The methamphetamine was allegedly sent to buyers through the United States Postal Service and package delivery services. The Bitcoins received by the alleged drug traffickers were later exchanged online for U.S. currency received as money orders and via PayPal and Western Union wires. The funds were ultimately placed in U.S. bank and prepaid card accounts opened with false identification, and the money then distributed to members of the organization.
- In 2013, in New York, Liberty Reserve, a centralized virtual currency based in Costa Rica, its principal founder, and six others were charged with money laundering and operating as an

[261] Written testimony of USSS Criminal Investigative Division Special Agent in Charge Edward Lowery III for a Senate Committee on Homeland Security and Governmental Affairs hearing titled "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies", November 18, 2013.
[262] USA v. Jason Weld Hagen, et al., (D. Or., Dec. 10, 2013)(3:13-cr-00596-JO).
[263] TOR directs Internet traffic through a free, worldwide, volunteer network consisting of more than four thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis.

unlicensed money transmitter.[264] The defendants were convicted in 2013 and 2014. Before founding Liberty Reserve, its principal had been convicted in the United States for operating "Gold Age," an exchanger for e-Gold, a precious metals-based virtual currency. The Secret Service estimates that Liberty Reserve had more than one million users worldwide, with more than 200,000 in the United States, and processed more than $1.4 billion of transactions annually.[265] Those transactions involved payments associated with credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography.[266] The Secret Service worked closely with IRS-CI and ICE/HSI as part of the Global Illicit Financial Team (GIFT) to conduct the investigation into Liberty Reserve.

- In 2013, in New York, Western Express International, Inc., a virtual currency exchanger for e-Gold and WebMoney, and its president pleaded guilty to money laundering and other charges brought by the Manhattan District Attorney.[267] According to the Secret Service, hackers who sold stolen credit card information online for e-Gold and WebMoney could exchange the virtual currencies for real money through Western Express.[268] Western Express exchanged $15 million in WebMoney and $20 million in e-Gold, which supported the global trafficking of stolen account data.
- In 2008, in Washington, D.C., e-Gold Ltd., the administrator for the centralized virtual currency e-Gold, and its three principal directors and owners, pleaded guilty to criminal charges relating to money laundering and operating an illegal money transmitting business.[269] E-Gold had been indicted in 2007.[270] A valid email address was the only information required to open an e-Gold account. An account could be funded by buying e-Gold, a digital representation of gold bullion, from an exchanger who transferred the virtual currency from the exchanger's account to the buyer's account. Account holders anywhere could conduct anonymous transactions over the Internet by transferring e-Gold from one account to another on the e-Gold web site. E-Gold quickly became the preferred method to pay for stolen financial information and child pornography.[271]

2. Risks

Money transmitters provide an essential service for immigrants and non-immigrants who cannot or choose not to use banks to send money home to family overseas. The money laundering consequence of allowing the typical $200-$400 remittance to be processed without verifying customer identification is low. Money transmitters with effective AML programs help to deter money laundering by filing timely SARs that flag structuring and other suspicious activity. The industry, however, is large, which makes

[264] USA v. Liberty Reserve, S.A., et al., (S.D.N.Y., May 20, 2013)(13 Crim. 368).
[265] Lowery, *supra* note 261.
[266] Jennifer Shasky Calvery, FinCEN, Before the United States Senate Committee on Homeland Security and Government Affairs, November 18, 2013.
[267] Cyrus Vance, Jr, District Attorney New York County, Western Express Cybercriminals Convicted at Trial Sentenced to Significant State Prison Time, news release, August 8, 2013.
[268] Lowery, *supra* note 261.
[269] DOJ, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges, News release 08-635, July 21, 2008.
[270] USA v. e-Gold, Ltd., et al., (D. D.C., Apr. 24, 2007)(CR-07-109).
[271] Lowery, *supra* note 261.

maintaining adequate oversight to ensure BSA compliance a continuing challenge. Virtual currencies operating illegally are a vulnerability for banks and other MSBs, because for virtual currencies to operate in the United States their exchangers have to be able to send and receive payments through the domestic financial system. Unlicensed virtual currency administrators and exchangers, like other unlicensed money transmitters and money launderers, use nominees, front companies, and shell companies to open accounts in order to disguise the true nature and purpose of their transactions. Identifying and prosecuting unlicensed and unregistered money transmitters remains a priority for FinCEN and U.S. law enforcement.

C2. Check Cashers

A check casher is defined by FinCEN as a person that accepts checks or monetary instruments in return for currency or a combination of currency, other monetary instruments, or other instruments in an amount greater than $1,000 for any person on any day in one or more transactions. Check cashers may operate as stand-alone businesses or may be an additional service offered by money transmitter agents or other retailers (e.g., a grocer or liquor store) as an accommodation to its customers. Check cashers must implement an AML Program and file CTRs, but have no SAR filing or recordkeeping obligation.

Approximately 12 million households do not have a checking account and instead rely on check cashers or other financial institutions to cash checks, according to the Brookings Institution.[272] Brookings researchers found that 93 percent of nonbank check- cashing operations are located within one mile of a bank or credit union branch, leading them to conclude that "consumers who use check cashers are making a conscious choice to use these firms instead of banks."[273] However, the use of paper payments in aggregate has been declining rapidly over the last decade in favor of electronic payment options. The 2013 Federal Reserve Payments Study found the number of checks paid in 2012 was less than half the number paid in 2003.[274]

1. Vulnerabilities

The dominant vulnerability is compliance deficiencies, including outright complicity. Some check cashing stores are being used to cash large checks or a series of smaller checks on behalf of professional criminals, particularly those who perpetrate healthcare fraud.[275] Billions of dollars in fraudulently obtained Medicare reimbursement checks are cashed through check cashers that are either knowingly filing CTRs that include false identifying information, or are avoiding filing CTRs altogether. Many of those identified as laundering proceeds of healthcare fraud through check cashing companies have been linked to Eurasian organized crime groups.[276]

[272] Matt Fellowes and Mia Mabanta, Banking on Wealth, Brookings Institution, 2008.
[273] *Id*.
[274] Available at https://frbservices.org/files/communications/pdf/general/2013_fed_res_paymt_study_detailed_rpt.pdf
[275] Jennifer Shasky Calvery, DOJ, Statement for the Record, House Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, February 2012.
[276] *Id*.

Recent indictments illustrate that criminals present checks to check cashers who they know will not ask for proof of the payee's identity and will either not file a CTR or will file false reports.[277]

In 2012, four indictments were unsealed charging check cashers in California, New York, and Pennsylvania with BSA violations.[278] In one of the cases, Belair Payroll Services, a licensed check casher in Queens, New York, cashed checks associated with healthcare fraud.[279] Two Belair customers named in the indictment had allegedly recruited foreign students in the United States on temporary J-1 visas to create shell companies and open bank accounts, which subsequently were used to deposit payments received from a fraudulent healthcare billing scheme. The defendants wrote checks on the shell company accounts to cash out the healthcare fraud proceeds and cashed them at Belair Payroll Services, which allegedly agreed not to file CTRs or to file false CTRs on the cash payments that exceeded $10,000.

Operation Universal Money Fast

Operation Universal Money Fast in 2009 targeted a large, sophisticated fraud against Medicare and private insurance companies in the southeastern United States. The perpetrators of the fraud opened shell companies and phantom clinics across Florida, Georgia, Louisiana, North Carolina, and South Carolina. The clinics were empty store fronts; some were nothing more than a post office box. No patients were ever seen or treated and no doctors worked there, yet tens of millions of dollars in bogus claims related primarily to HIV infusion therapy were submitted to Medicare and private insurers. The criminals used stolen identities and paid for the complicity of some physicians to lend an air of legitimacy to the fraud. To conceal their identities, the criminals registered the bogus businesses in the names of nominee owners. They also opened their own check-cashing store, Universal Money Fast, to launder more than $50 million in benefits paid by Medicare and private insurers.

Source: FBI, Health Care Fraud, accessed at: http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud

According to the indictments involving check cashers, the allegations in the Belair Payroll Processing case are typical. Perpetrators of fraud, particularly healthcare fraud, in which the payment is made by check in response to a false claim, seek out check cashers who agree to cash checks for tens of thousands of dollars without filing a CTR or to make a false report.

- In 2012, a Los Angeles check casher, AAA Cash Advance, and its manager, pleaded guilty to failing to file CTRs and failing to maintain an effective AML program.[280] According to the indictment, AAA cashed checks for more than $10,000, without filing a CTR. The checks were written on the account of a fake healthcare business and on the account of a fictitious doctor. The checks were made out to a variety of fictitious individuals and entities.

[277] Department of Justice news release, Check Cashers in Brooklyn, Philadelphia and Los Angeles Charged for Alleged Violations of Anti-Money Laundering Laws, June 14, 2012. Available at http://www.justice.gov/opa/pr/2012/June/12-crm-757.html
[278] *Id*.
[279] USA v. Belair Payroll Services, Inc., et al., (E.D.N.Y., June 12, 2012)(No. 11-591).
[280] USA v. AAA Cash Advance, Inc. and Dianna Brigitt, (C.D. Cal., June 12, 2012)(CR 12-0599).

- In 2006, a check casher, Pronto Cash of Florida, Inc., and five individuals were charged with operating an unlicensed money transmitter, money laundering, and facilitating the unlawful employment of illegal aliens.[281] The check casher allegedly helped Florida construction companies and subcontractors evade the requirement that workers must be legal residents and that employers must maintain workers compensation insurance. For a fee, the check casher made fraudulent insurance certificates available to contractors and cashed illicit checks that allowed the contractors to pay their illegal employees.

2. Risks

The use of paper checks is declining overall, although the U.S. government continues to use checks, in addition to other payment options, to issue federal payments, including for Medicare and Medicaid reimbursement and income tax refunds. More effective anti-fraud safeguards on the part of the government may reduce the potential for fraudulent payments and potential misuse of check cashers. Check cashers will pose a high risk for money laundering, particularly with respect to fraud against the government, as long as there are check cashers that are lax in their BSA compliance or complicit in criminal activity.[282] Because check cashers are exempt from SAR and recordkeeping requirements, they can purport to be blind to fraudulent activity even as they process inherently suspicious transactions.

C3. Money Orders

Money order sellers are required under the BSA to develop, implement, and maintain an AML program, verify and record customer identification for cash purchases of money orders totaling $3,000 or more, and file CTRs and SARs.

Money orders are offered for a fee by businesses such as Western Union and MoneyGram as well as the United States Postal Service (USPS). USPS is the oldest seller of money orders in the United States and today accounts for approximately 30 percent of the market. But USPS confirms Federal Reserve figures that demonstrate the decline in USPS money order sales (see Figure 1). In 2013, USPS sold 103 million money orders with a value of $21.4 billion. The average value was $208. USPS flagged about 5 percent, or 5.3 million, of the money orders they sold in 2013 as potentially suspicious. After further review just over 100,000 SARs were filed, with each SAR covering approximately 15 money orders. Half of the SARs cited structuring.

[281] USA vs. Pronto Cash of Florida, Inc., et al., indictment, (M.D.FL., Oct. 25, 2006)(6:06-cr-00196-ACC-DAB).
[282] Colorado Check Casher Penalized and Put Under Corrective Measures Due to Extensive and Repeated BSA Violations (March 18, 2015). Available at http://www.fincen.gov/news_room/nr/pdf/20150318.pdf

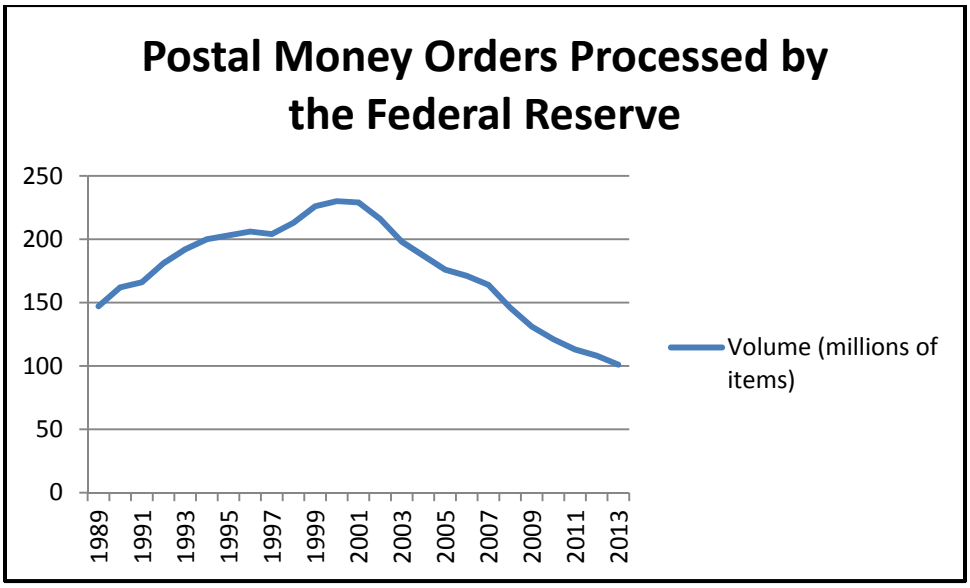


Figure 1 Source: Board of Governors of the Federal Reserve System (http://www.federalreserve.gov/paymentsystems/check_postalmosprocqtr.htm)

1. Vulnerabilities

Unlike wire transfers, money orders are sold with the payee field left blank to be filled in by the payer. The name of the payee is not known to the issuer until that person cashes the money order and the document is cleared and sent to the issuer for settlement. This means money order sellers are unable to screen the name of the payee and, and depending on the amount, the name of the payer may not be verified. As with nonbank wires, the BSA recordkeeping obligation only requires issuers and sellers of money orders to verify and record customer identification when selling money orders for cash above $3,000, which invites structuring, as demonstrated in the following case examples:

- In 2007, in Georgia, a man and woman were indicted for drug trafficking and money laundering, depositing funds into a bank account opened in the name of a shell company created to appear as an investment advisory firm.[283] The couple allegedly distributed cocaine, using a portion of the proceeds to make structured purchases of money orders. Cash and money orders were deposited to the business bank account, which was opened in the name of Spigner Investment Group Inc. The couple bought cars, real estate, and funded investment accounts using funds transfers from the bank account.
- In 2007, in New York, structured money order purchases were part of the Operation Pinpoint drug money laundering investigation in which the owners or employees of 27 money transmitters were arrested on charges of helping to transfer drug proceeds to Colombia.[284] In addition to allegedly structuring wire transfers, the MSBs also structured money order sales. "The storefronts were operating as networks, with one remitter or money order issuer accepting a portion of the

[283] USA v. Steven Spigner and Yojuana Spigner, (N.D. GA., Oct. 23, 2007)(1:07-cr-00355-RWS-GGB).
[284] United States Attorney's Office, Eastern District of New York, Twenty-Seven Individuals Charged in Continuing Probe of Drug Money Laundering in Money Remitter Industry, news release, February 7, 2007.

drug money, and then recommending several other money remitter locations to the money launderer to handle the rest of the drug money. The storefronts shared in the profits made from each customer who brought drug money to a group of stores."[285]

- In 2007, in Washington, D.C., a woman was charged under the organized crime statute[286] for operating a multimillion dollar prostitution ring across several states and laundering the proceeds through money orders, banks, real estate, and securities investments.[287] The defendant, who lived in California, allegedly owned and managed Pamela Martin and Associates, which advertised as an escort service. The business managed the appointments for the employees who allegedly were instructed to keep a portion of the cash they earned and use the rest to buy money orders which were mailed to the defendant. According to the indictment, the defendant deposited the money orders in bank accounts in California and subsequently drew on the accounts to buy real estate and fund several brokerage accounts.
- In 2006, in New Jersey, five people were charged with laundering drug proceeds, using a TBML scheme to move the money from the United States to Colombia.[288] A portion of the U.S. drug proceeds was used to make structured purchases of money orders which were sent by mail to a defendant who deposited them, disguised as legitimate revenue, into the commercial bank account of a computer products and services company. The company subsequently made peso-denominated payments to Colombia—to pay the drug traffickers—under the guise of buying computer parts.

2. Risk

The risks for money orders are similar to those identified above for non-bank wires. Although used legitimately for relatively small value transactions, money orders present a money laundering risk due to the opportunity to conduct anonymous transactions below the federal recordkeeping threshold. The risk is magnified by structuring.

C4. Traveler's Checks

The use of traveler's checks has been in decline since the mid-1990s; today there is less than $4 billion in traveler's checks outstanding (see Figure 2).[289] Traveler's checks are still used for money laundering, but apparently not often, given the limited number of cases. Like money orders and nonbank wire transfers, the purchase of more than $3,000 in traveler's checks with cash obligates the seller to verify and record the purchaser's identity along with the transaction information. Issuers and sellers of travelers checks also are required to develop, implement, and maintain an AML program, and file CTRs and SARs.

[285] *Id*.
[286] 8 U.S.C. § 1962(c), Racketeer Influenced and Corrupt Organizations.
[287] USA v. Deborah Jeane Palfrey, (D. D.C., Mar. 1, 2007)(1:07-cr-00046-JR).
[288] USA v. Jonathan Chu, et al., (D. N.J., 2006)(Case 2:06-cr-00007-WHW).
[289] *See* http://www.federalreserve.gov/Releases/h6/current/default.htm

1. Vulnerabilities

As with money orders and nonbank wires, the $3,000 recordkeeping threshold creates a potentially significant risk for structuring[290] and money laundering. The purchase of traveler's checks, regardless of the recordkeeping threshold, typically involves the buyer providing identifying information. However, FinCEN has noted that SAR reports have indicated that the name and/or address on the purchase agreement have been left blank, or were unverifiable, illegible, or did not match the signature name on the corresponding traveler's checks. [291]

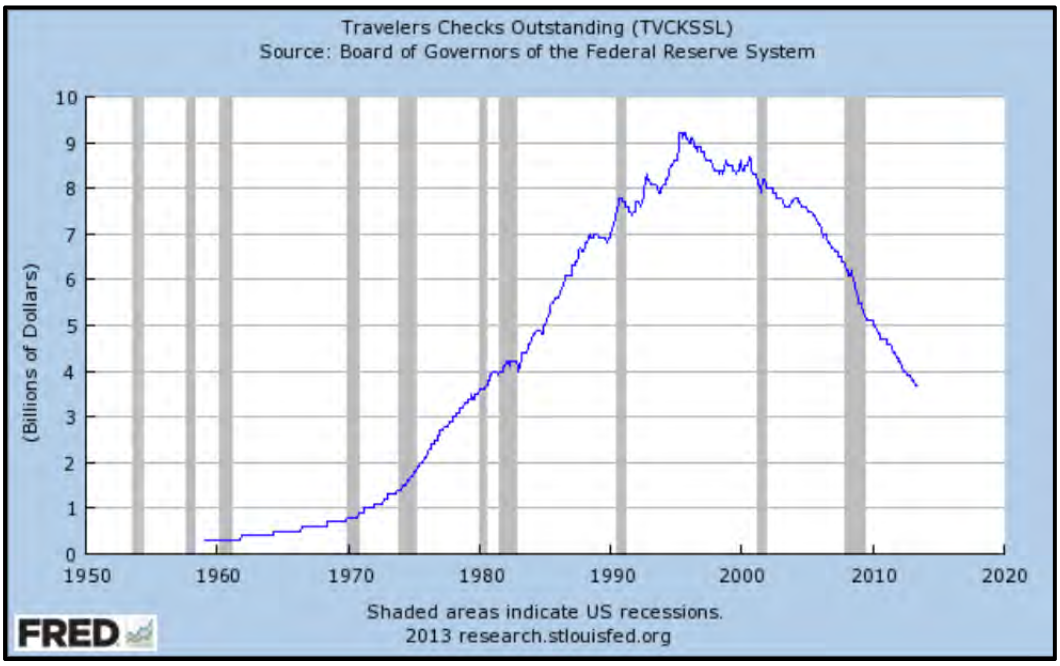


Figure 2

- In 2012, the Senate Permanent Subcommittee on Investigations, in its report on money laundering through HSBC Bank, cited the illegibility of the signature on a series of suspicious U.S.—issued traveler's checks that were cleared through HSBC-US.[292] The Subcommittee report noted that HSBC-US cleared more than $290 million in bulk U.S. dollar traveler's checks in less than four years for a Japanese regional bank, at times clearing $500,000 or more per day. The checks had been bought in Russia and reportedly used to purchase used cars.
- In 2011, in New York, two brothers plead guilty to laundering drug proceeds involving the use of traveler's checks, wires, and bank accounts.[293] The brothers allegedly received almost $100,000 in traveler's checks that had been purchased outside the United States with drug proceeds. The traveler's checks were deposited into personal bank accounts in New Jersey as well as into an

[290] In some cases structuring is not intended to facilitate money laundering, but to facilitate tax evasion or simply to avoid a report being filed with a government agency on the customer's financial activity.
[291] FinCEN, SAR Activity Review, Issue 3, October 2001.
[292] Senate Permanent Subcommittee on Investigations, U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History, July 17, 2012.
[293] USA v. Carlos Aguirre and Julio Aguirre, (S.D.N.Y., July 22, 2011)(1:10-cr-00487-RJS).

account held in the name of a business. The funds were subsequently used to purchase real estate that was held in the name of the business.

- In the 2010 OCC Consent Order against Wachovia, the bank's failure to appropriately monitor traveler's checks is cited. Traveler's checks purchased in Mexico, and suspected of having been acquired with drug proceeds, were deposited in large numbers at Wachovia in the United States. According to court documents in the DOJ prosecution of Wachovia, Mexican "casas de cambio regularly deposited traveler's checks through pouch deposits that contained numerous examples of structuring, sequential serial numbers and endorsement/deposit dates on or near the date of purchase. Other suspicious elements included 'smurf' marks, or unusual markings, and traveler's checks that lacked any legible signature."[294]

2. Risks

Although traveler's checks receive the same regulatory treatment under the BSA as nonbank wires and money orders, there are important differences that affect their potential money laundering risk. The legitimate rationale for using traveler's checks is that the checks are registered to an identified purchaser, so that they can be replaced if lost or stolen. Ostensibly, this feature should lower the money laundering risk. Case examples demonstrate, however, that buyers who intend to use traveler's checks to launder illicit cash can provide inaccurate or illegible identifying information and structure purchases to avoid verification. A feature that increases the money laundering risk of traveler's checks above that of U.S.-issued money orders and nonbank wire transfers is that U.S.-issued traveler's checks can be purchased and used abroad in countries with potentially weaker AML laws than exist in the United States.

C5. Foreign Exchange Dealers

A dealer in foreign exchange (FX), also known as a money broker, is any person that accepts the currency or other monetary instruments, funds, or other instruments denominated in the currency of one or more countries, in exchange for the currency or other monetary instruments, funds, or other instruments denominated in the currency of one or more other countries, in an amount greater than $1,000 for any other person on any day in one or more transactions, whether or not for same day delivery.[295] An FX dealer is required to develop, implement, and maintain a risk-based AML program and file CTRs and SARs. FX dealers also have a comprehensive recordkeeping obligation under the BSA, which recognizes that unlike other MSBs, FX dealers hold accounts. When opening an account an FX dealer must collect, verify, and record customer identification.[296] For transaction-based customers, the threshold for verifying customer identification as part of the recordkeeping requirement is $1,000, rather than the $3,000 threshold that applies to money orders, money transmission, and traveler's check cash sales.

1. Vulnerabilities

The dominant vulnerability is compliance deficiencies, including – in extreme cases – outright complicity. The recordkeeping requirement for FX dealers is unique among MSBs, and reduces the potential money laundering vulnerabilities of licensed FX dealers that comply with the BSA. However,

[294] USA v. Wachovia Bank, N.A., (S.D. FL., Mar. 12, 2010)(CR10-20165).
[295] 31 C.F.R. § 1010.100(ff)(1).
[296] 31 C.F.R. § 1022.410.

FX dealers that facilitate money laundering can potentially integrate legal and illegal transactions. Also, unlicensed FX dealers pose the same risk to banks and other MSBs posed by unlicensed money transmitters who disguise the true nature and purpose of their transactions, as is illustrated in the following case example:

- In 2013, in South Dakota, a man plead guilty to charges of illegally selling Iraqi dinar over the Internet.[297] The man bought the bank notes from a seller who smuggled the currency out of Iraq and sent it to the United States from Jordan. The currency was sent in structured shipments, each under the $10,000 threshold for filing a CMIR. The South Dakota man used several businesses as fronts to buy and sell the currency and deposit the proceeds in South Dakota bank accounts. The man received cashier's checks, money orders, personal checks, and precious metal coins in payment for the foreign currency.

Money brokers who acquire dollars in the United States from Mexican DTOs and facilitate payment in pesos through TBML are FX dealers operating illegally. In 2013, in New York, two indictments named 19 people who allegedly laundered drug proceeds. Twelve of the defendants allegedly were money brokers who operated out of retail shopping malls in Cali, Colombia.[298] The money brokers allegedly coordinated a large network of money movers who collected the drug proceeds in the United States.

The TBML scheme used to exchange U.S. dollars for Colombian pesos, known as the BMPE, has been copied and adapted to local conditions by criminal organizations across the globe, with recent evidence of TBML schemes used to launder the proceeds of illegal trade of pirated goods.[299] The mechanics of the scheme are the same everywhere: illicit proceeds in one currency are used to purchase goods that are sold in exchange for another currency. HSI Office of Intelligence (HSI-Intel), Illicit Finance Unit, researched SARs filed between October 2011 and September 2012 citing TBML and found that 93 countries were identified in the SARs. The top five countries included three from Latin America and one each from Africa and Asia.[300]

2. Risks

The most significant vulnerability associated with FX dealers is the potential for dealers operating illegally to integrate the buying and selling of illicit proceeds into their normal business, seamlessly facilitating money laundering while also conducting legitimate FX transactions.

C6. Prepaid Access

According to the most recent edition of the Federal Reserve System's payments study, in 2009 there were 6 billion prepaid card transactions, valued at more than $140 billion in the United States.[301] The 2013

[297] USA v. David Olmsted, (S.D.S.D., 2013)(5:11-cr-50027-JLV).
[298] United States Attorney for the Eastern District of New York, 16 Members Of An International Money Laundering Scheme Arrested In The United States And Colombia, news release, March 14, 2013.
[299] Jennifer Shasky Calvery, DOJ, Statement for the Record, House Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, February 8, 2012.
[300] ICE HSI, Office of Intelligence, Primary Locations of Trade- Based Money Laundering Activity from 1 October 2011 to 30 September 2012, February 14, 2013.
[301] *See* http://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2012/D-2012-August-Prepaid.pdf

FDIC National Survey of Unbanked and Underbanked Households states that 7.9 percent of all households used a general purpose reloadable prepaid card in the previous 12 months.[302]

In 2011, FinCEN renamed "stored value" as "prepaid access" and developed new regulatory obligations for non-bank prepaid access providers and sellers (see Bank section above for discussion of bank-managed prepaid card programs).[303] Prepaid access refers to any payment method that involves access to funds or the value of funds that (1) have been paid in advance and (2) can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number. Mobile payments, using cell phones as the access device, are a form of prepaid access.

Nonbank providers of prepaid access are required to develop, implement, and maintain a risk-based AML program, file CTRs and SARs, and maintain transaction records on certain products. The recordkeeping requirement also mandates that customer information (including, name, date of birth, address, and identification number) be collected and retained for open loop prepaid access products that allow either:

- Access to more than $1,000;
- International use;
- Transfers between prepaid access products within a prepaid program; or
- Loads from non-depository sources.

The customer identification requirement also applies to closed loop prepaid access products that have $2,000 or more maximum value per device per day**.**

Sellers are not required to register with FinCEN, but must maintain an AML program if they sell certain prepaid access products.[304]

1. Vulnerabilities

For the consumer, prepaid cards look and function much like traditional debit or credit cards, and are marketed to, and used by consumers as an alternative or supplement to traditional bank accounts and monetary instruments. However, prepaid card transactions often involve more parties and sub-parties than is typical of routine debit or credit card transactions.

Branded prepaid debit cards (payments for which are cleared and settled through the four major credit card networks) must be issued by a bank. However, the issuing bank may be issuing the card on its own behalf (a bank-centered prepaid card) or on behalf of a (non-bank) prepaid access provider (MSB-led prepaid access cards). Prepaid access providers must register with FinCEN and are bound by FinCEN's prepaid access rules as a provider of prepaid access. Banks and prepaid access providers often outsource card program management to independent specialty firms. Because of this arrangement, the information created by the sale and use of prepaid cards may be dispersed among several service providers, potentially

[302] Available at https://www.fdic.gov/householdsurvey/2013report.pdf
[303] *See* FinCEN, "Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access" 76 FR 45403 (July 29, 2011); *see also* 31 C.F.R. § 1010.100
[304] Visa, MasterCard, Discover, American Express.

creating obstacles, both to financial institutions' customer due diligence and to criminal investigation and prosecution.

Law enforcement emphasizes that prepaid cards function as monetary instruments, similar to money orders, but are not included in the definition of that term.[305] Only cash and monetary instruments are subject to declaration on the CMIR form when a person transports more than $10,000 into or out of the United States.

Foreign-issued Prepaid Cards

A 2013 study by the Federal Reserve Bank of Atlanta notes that, although FinCEN's regulations and enhanced transparency in the prepaid industry within the United States have made prepaid access less inherently desirable to illicit actors, concerns remain with respect to the ease of transfer and transport of foreign-issued prepaid access products, given the lack of similar regulatory and industry controls outside of the United States.[306] Individuals can obtain foreign-issued branded prepaid cards anonymously over the Internet, or with minimal or no customer identification and record keeping in brick-and-mortar outlets in insufficiently regulated foreign jurisdictions.

While U.S.-issued general purpose reloadable (GPR) cards generally are limited to a few thousand dollars in total load, foreign-issued GPR cards may be much higher in value. In any event, GPR prepaid cards can be reloaded frequently and may be used to purchase high-value goods. Despite voluntary industry efforts to address the money laundering risks of foreign-issued prepaid cards, vulnerabilities remain.[307] Additionally, offshore third party processers that process international prepaid transactions for foreign issued prepaid card issuers may be unregulated, have insufficient AML/CFT controls, or may be wittingly complicit in allowing illicit proceeds to be laundered through the cards. Absent effective AML/CFT controls in issuing and acquiring institutions, foreign-issued prepaid cards may provide a ready way for money launderers to access and use their tainted funds worldwide.

2. Risks

Below the $1,000 threshold, open loop prepaid debit cards, like money orders and wire transfers below $3,000, can be used anonymously (although not for person-to-person transfer, international use, or non-depository reloads). There are case examples that demonstrate criminals use prepaid cards for money laundering. It is not clear, however, whether these cards are each loaded with less than $1,000, which would make the risk low.

[305] *See* 31 U.S.C. § 5312(a)(3)(C).
[306] Douglas King, "Have Anti-Money Laundering Measures Kept Pace with the Rapid Growth of GPR Prepaid Cards?" Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta (January 2013). Available at https://www.frbatlanta.org/documents/rprf/rprf_pubs/130117_wp.pdf
[307] Although U.S. regulations do not currently require branded card networks operating in the United States to establish an AML/CFT program reasonably designed to address the money laundering/terrorist financing risks associated with foreign-issued prepaid cards, particularly those issued in high-risk foreign jurisdictions, U.S. branded card networks report they have voluntarily adopted internal AML/CFT controls in this area.

According to ICE HSI, open and closed loop prepaid access devices are used to move value out of the United States, and not including prepaid debit cards in the definition of monetary instruments creates a risk of cross-border money laundering.

D. Casinos

The American Gaming Association counts more than 1,300 casinos and card rooms across the 42 states that have some form of legal casino gambling. The 246 tribes with gaming operations in 2012 had revenues of approximately $27 billion,[311] accounting for more than 70 percent of the gross gambling revenue[312] at all licensed gaming facilities in the United States.[313] While tribal gaming operations dominate overall U.S. legal gaming revenue, Las Vegas and Atlantic City continue to top the list of casino markets (see Figure 3). Casinos in New Jersey and Nevada file the most casino SARs and are the venues most often cited in criminal prosecutions involving money laundering through casinos. In 2013, casinos and card clubs in the United States filed more than 27,000 SARs, with Nevada and New Jersey filing more than 40 percent.

Top 10 U.S. Casino Markets by Annual Revenue	
Casino Market	**2012 Annual Revenues**
1 Las Vegas Strip, Nev.	$6.207 billion
2 Atlantic City, N.J.	$3.052 billion
3 Chicagoland, Ind./Ill.	$2.243 billion
4 Detroit, Mich.	$1.417 billion
5 Connecticut	$1.230 billion[308]
6 Philadelphia, Pa.	$1.167 billion
7 St. Louis, Mo./Ill.	$1.108 billion
8 Gulf Coast, Miss.[309]	$1.095 billion
9 The Poconos, Pa.[310]	$902.48 million
10 Tunica/Lula, Miss.	$821.95 million

Figure 3 Source: American Gaming Association

A gaming casino is subject to BSA requirements[314] if it has gross annual gaming revenue of more than $1 million and is duly licensed as a casino under the laws of a state, territory, or possession of the United States; or if it is a tribal gaming operation.[315] Casinos and card clubs subject to the BSA are required to develop, implement, and maintain an AML program; file casino CTRs and SARs; and maintain certain transaction records. Casinos do not have a distinct customer identification program obligation.

The AML program requirement for casinos is unique in that it includes an obligation to establish procedures for using all available information to collect customer identification when necessary for

[308] Includes only revenue from slot machines.
[309] Includes casinos in Gulfport, Bay St. Louis, and unincorporated Hancock County, Miss.
[310] Includes casinos in Bethlehem, Mt. Airy, and Wilkes-Barre, Pa.
[311] National Indian Gaming Association, 2013 Annual Report.
[312] Gross gaming revenue is the amount wagered minus the winnings returned to players.
[313] Gross gaming revenue was just over $37 billion in 2012 according to the American Gaming Association (State of the States, 2013).
[314] Casino responsibilities under the BSA include: a written AML compliance program (31 C.F.R. § 1021.210); filing CTRs (31 C.F.R. § 1021.311); filing SARs (31 C.F.R. § 1021.320); and maintaining certain transaction records (31 C.F.R. § 1021.410)
[315] This include tribal gaming operations conducted pursuant to the Indian Gaming Regulatory Act (25 U.S.C. § 2701 et seq.) or other federal, state, or tribal law or arrangement affecting Indian lands, including casinos operating under the assumption or under the view that no such authorization is required for casino operation on Indian lands (*See* 1010.1009(t)(5)(i)).

recordkeeping and reporting purposes and to use the casino's computer systems to aid in assuring compliance. These systems are also expected to be used in identifying transactions or patterns of transactions required to be reported as suspicious, including in relation to a customer's source of funds.[316]

The recordkeeping rule for casinos is more stringent than the obligation for money transmitters. Casinos must collect and retain the customer's name, address, and Social Security number whenever a customer sends or receives an international wire transfer regardless of the amount.[317] Money transmitters have no obligation to collect or retain customer identification information on foreign or domestic funds transfers below $3,000.

1. Vulnerabilities

a. Licit and Illicit Cash Often Indistinguishable

Criminal prosecutions show that illicit proceeds earned from drug trafficking, illegal gambling, and fraud are placed in casinos directly as cash (bank notes), or transferred by wire or check. The IRS-CI Las Vegas field office notes that most often criminals who use casinos to launder illicit proceeds do it through gambling and spending on entertainment.

FinCEN reviewed casino SARs filed from 2004 through June 2011 and found that, as with other financial institutions, structuring was the most commonly reported suspicious activity.[318] The IRS-CI Las Vegas field office notes that the area within Nevada casinos known as the "sports book," where wagers are taken on sporting events, tend to be where casinos in the state see significant dollar structuring. Because Nevada is the only state that allows sports betting, the Nevada sports books are used by illegal out-of-state bookies and Internet-based gambling sites to make wagers that help them balance their odds. Runners and agents working for these out-of-state gambling organizations are the people who are most likely to be structuring in an attempt to avoid being identified. Other gamblers who structure are individuals trying to avoid paying the tax due on winnings.

Although the second-most frequently cited suspicious activity in FinCEN's study was "Other," these SARs most often described customers displaying unusual behavior which IRS-CI interprets as potential cheating or fraud schemes against the casino.

The third-most frequently reported suspicious activity is minimal gaming, characterized by a customer buying chips or depositing funds into an account with the casino and then cashing out after little or no play. This may be indicative of money laundering, especially at casinos that allow a customer to exchange cash for a casino check or wire transfer. Another possible explanation of minimal gaming activity is criminals attempting to exchange counterfeit bills for legitimate currency. According to the Secret Service, an average of $40,000 a week in counterfeit currency is reported by Nevada casinos.

The following are case examples of illicit cash placed in casinos for laundering:

- In 2012, in New York, 25 people were indicted on charges of illegal gambling and money laundering, including using nominees, or runners, to open accounts, place bets, and collect

[316] Remarks of Jennifer Shasky Calvery, FinCEN, 2014 BSA Conference Las Vegas, NV, June 12, 2014.
[317] *See* § 1021.410.
[318] FinCEN, Suspicious Activity Reporting in the Gaming Industry, March 2012.

winnings at a licensed Las Vegas sports book on behalf of out-of-state bettors.[319] The bettors used off-shore gambling web sites to place their wagers. Among those indicted were runners who allegedly collected and distributed illegal gambling proceeds, transporting cash throughout the United States and to and from Panama and Costa Rica.[320] One of the defendants, the director of risk management at a Las Vegas sports book, pleaded guilty to knowingly taking illegal bets from runners.[321]

- In 2011, in New Jersey, a woman was convicted of fraudulently misrepresenting herself as a U.S. government official who, for a fee, could help immigrants achieve permanent legal resident status.[322] She earned hundreds of thousands of dollars, a portion of which, according to the indictment, she wired for deposit to a bank account in Portugal. Among the defendant's expenditures in the United States were trips to Atlantic City casinos where she allegedly spent tens of thousands of dollars in cash.

- In 2011, in Maryland, a man and woman who managed a multimillion dollar heroin ring in the Baltimore area were indicted on drug trafficking and money laundering charges.[323] The heroin was purchased from suppliers in New York and brought to the Baltimore area for retail sale. The couple allegedly used drug cash for gambling in Las Vegas casinos and bought lottery tickets from winners. The couple allegedly conspired with a used car dealer, paying the dealer with drug cash in exchange for checks written on the dealership's bank account.[324] The couple also created two limited liability companies that held title to eight properties.

- In 2011, in New York, a man was indicted for allegedly using casino slot machines to launder illicit proceeds.[325] The defendant, a South Carolina tobacco farmer, allegedly sold tobacco to individuals in New York who sold untaxed cigarettes in Canada. The individuals allegedly also bought marijuana in Canada for sale in the United States. The South Carolina farmer was paid for his tobacco with cash earned from marijuana sales. The transactions took place on an Indian reservation on the U.S./Canadian border. The farmer allegedly routinely visited the Mohawk Bingo Palace on the reservation, putting tens of thousands of dollars in U.S. currency into slot machines and then receiving a casino check for the credit balance.

- In 2010, in Arizona, a man was indicted for operating a fraudulent gambling enterprise in which he allegedly solicited funds based on claims of an insider advantage that would allow him to generate gambling profits for investors.[326] Investors were instructed to wire money to a credit union account in Arizona. The defendant allegedly wired approximately $4 million from the credit union to accounts at Las Vegas casinos where he either used the money to gamble or converted it to cash for his own use.

[319] The People of the State of New York against Vincent Basciano Jr. et al., indictment, case no. 2593/2012 filed in the Supreme Court of the State of New York, County of Queens.
[320] Twenty-Five Individuals Indicted in Multi-Million-Dollar Illegal Nationwide Sports Betting Ring Charged with Enterprise Corruption and Promoting Gambling, news release, FBI, October 25, 2012.
[321] Michael Colbert (E.D.N.Y., Aug. 21, 2013) (criminal information).
[322] USA v. Rosa Blake, (D. N.J., 2009)(2:09-cr-00926-WHW).
[323] USA v. Steven Blackwell et al, (D. MD., Apr. 21, 2011)(1:10-cr-00493-JFM).
[324] Steven Blackwell Pleads Guilty in Multi-Million-Dollar Heroin and Money Laundering Conspiracy, FBI news release, November 23, 2011.
[325] USA v. William David Humphries, (N.D.N.Y., May 11, 2011)(8:11-cr-00088-NAM).
[326] USA v. Anthony Mark Boscarino, (D. Ariz., Aug. 4, 2010) (4:10-cr-01942-CKJ-JJM).

b. Accessing Illicit Offshore Funds

As U.S. casino companies expand internationally, with foreign marketing branches and sister properties, there is the potential for a person to establish a casino account in one country and access the funds through an affiliated casino in another country. The most significant money laundering vulnerability at U.S. casinos is the potential for individuals to access foreign funds of questionable origin through U.S. casinos, and to use the money for gambling and other personal or entertainment expenses, and then withdraw or transfer the remaining funds either in the United States or elsewhere.

- In 2013, the Department of Justice agreed to conclude a criminal investigation against the Las Vegas Sands Corp., which operates the Venetian-Palazzo hotel complex.[327] The Sands agreed to pay to the United States $47.4 million, which is the sum sent to the Venetian-Palazzo casino by or on behalf of Zhenli Ye Gon. In March 2007, approximately $207 million was seized by law enforcement authorities from Ye Gon's residence in Mexico City in what remains the largest seizure of currency by law enforcement. Ye Gon is charged in Mexico with drug trafficking offenses. According to the non-prosecution agreement, casino officials should have identified Ye Gon's transactions as suspicious and filed one or more SARs.

c. Compliance Deficiencies

As with all businesses, casinos are vulnerable to institutional compliance deficiencies and money laundering opportunities created by complicit employees. The following case is an example:

- In 2013, in the Northern Mariana Islands, the Tinian Dynasty Hotel & Casino and two employees were indicted on charges of evading the casino's CTR filing obligation.[328] The indictment resulted from an undercover investigation in which two IRS-CI agents posed as gamblers who used large amounts of U.S. currency at the casino and explained they did not want any BSA reports filed. The defendants allegedly cooperated. In 2014, FinCEN reached an agreement with one of the defendants, George Que, the former VIP Services Manager at the casino, to permanently bar him from working in financial institutions as a result of his willful violations of the BSA and assessed a $5,000 civil money penalty.

2. Risks

Casinos are primarily destinations for recreation and entertainment, not financial services, which may lead some casinos to intentionally or inadvertently put customer service above BSA compliance. An example is the reluctance at some casinos to tell a customer directly that a CTR must be filed for one or a series of transactions aggregating to $10,000 or more, and to ask for the information needed to file the report. Rather than asking the customer for identification, a casino may rely on previous records for the information; or if the information is not available, the casino may file a partially completed CTR and attempt to collect additional information should another CTR have to be filed in the future.

[327] Operator of Venetian Resort In Las Vegas Agrees To Return Over $47 Million After Receiving Money Under Suspicious Circumstances, news release, United States Attorney's Office for the Central District of California, August 27, 2013.
[328] USA v. Hong Kong Entertainment (Overseas) Investments, Ltd. Dba Tinian Dynasty Hotel & Casino, Tim Blyth, and George Que, (N. N. Mar. I., May 9, 2013)(1:13-cr-00002).

Casinos that choose to use an incremental approach, filing a partially completed form and asking for more information the next time a CTR needs to be filed, are not complying with BSA obligations.[329] According to FinCEN, after filing a partial CTR the first time a customer's currency activity exceeds $10,000, some casinos file another partial CTR the next time a CTR is filed if the customer refuses to give the information requested and will only bar the customer from the casino if the customer again refuses the necessary information the third time a CTR has to be filed. FinCEN issued an advisory in 2009 reminding casinos that structuring is illegal.[330]

E. Securities

The U.S. securities industry is made up of individuals and institutions engaged in issuing and trading debt, equity, and derivative securities. The key participants include:

- **Broker-dealers:** The Securities and Exchange Commission (SEC) oversaw approximately 4,500 broker-dealers as of fiscal year 2014.[331] The Financial Industry Regulatory Authority (FINRA) the largest self-regulatory organization for broker-dealers doing business with the public in the United States. As of the end of 2009, FINRA-registered broker-dealers held over 109 million retail and institutional accounts.[332] Broker-dealers are generally subject to the same BSA regulatory obligations as banks: among other things, they must develop, implement, and maintain an AML program that is reasonably designed to achieve compliance with the BSA, including the establishment and implementation of a customer identification program, the maintenance of certain transaction records, and the filing of CTRs and SARs.
- **Investment advisers**: As of April 1, 2015, 11,615 SEC-registered advisers reported more than $66 trillion assets under management. [333] In addition, there are more than 275,000 state-registered investment adviser representatives and more than 15,000 state-registered investment advisers.[334] Investment advisers are not currently covered by AML regulations (except for those applicable to all businesses or persons, such as the Form 8300 Report of Cash Payments Over $10,000 Received in a Trade or Business and Report of Foreign Bank and Financial Accounts filing obligations).
- **Investment companies:** Investment companies (such as mutual funds) are usually required to be registered with the SEC. As of 2013, approximately $15 trillion in assets were invested in mutual funds.[335] Mutual funds generally have the same AML obligations as broker-dealers. Other investment companies, however, are not currently covered by AML regulations, in part because there does not seem to be a need for such coverage. For example, because of certain structural factors associated with closed-end funds and unit investment trusts, those investment companies do not appear to

[329] FinCEN, Frequently Asked Questions: Casino Recordkeeping, Reporting, and Compliance Program Requirements, August 13, 2012.
[330] FinCEN, Structuring by Casino Patrons and Personnel, Advisory, July 1, 2009.
[331] Securities and Exchange Commission, *FY 2016 Congressional Budget Justification, FY 2016 Annual Performance Plan, FY 2014 Annual Performance Report.*
[332] Securities and Exchange Commission, *Study on Investment Advisers and Broker Dealers* (January 2011).
[333] Based on Investment Adviser Registration Depository data as of April 1, 2015.
[334] Securities and Exchange Commission, Study on Investment Advisers and Broker Dealers (January 2011).
[335] Investment Company Institute, *2014 Investment Company Fact Book,* 54th Edition.

present a risk of money laundering that would be effectively addressed by subjecting them to additional regulation.[336]

These securities industry participants, while not prohibited from accepting cash, typically do not accept cash, which reduces the money laundering placement risk. Generally, the money laundering risk in the securities industry arises from the potential misuse of certain account structures, products and services, or transactions. These include, but are not limited to, master/sub and omnibus account structures and services, intermediated relationships, microcap securities, structured products, private placements, direct market access, certain foreign bond transactions, and using brokerage accounts for bank-like activity with few if any securities transactions. As discussed above in Section I.A.6., most identified cases of illicit activity in the securities markets relate to some form of fraud, including securities fraud, identity theft, or embezzlement.

1. Vulnerabilities

a. Master/sub and Omnibus Accounts

The master/sub-account trading model is a vehicle that could be used to further violations of laws and regulations. Although these types of accounts may be used for legitimate business purposes, potential misuse of the account structure raises regulatory concerns with respect to: (i) money laundering, (ii) insider trading, (iii) market manipulation, (iv) account intrusions, (v) information security violations, and (vi) unregistered broker-dealer activity.[337]

Generally, in a master/sub-account arrangement a top-level customer opens an account with a registered broker-dealer (the "master account") that permits the customer to have subordinate accounts for different trading activities ("sub-accounts"). In many, if not most, instances, the customer opening the master account is a limited liability company, limited liability partnership, or similar legal entity or another broker-dealer. The master account will usually be subdivided into sub-accounts for the use of individual traders or groups of traders. In some instances, these sub-accounts are further divided to such an extent that the master account customer and the broker-dealer may not know the actual identity of these underlying traders. This trading model could permit anonymous access to the securities markets, a vulnerability that could be exploited for fraud and other illicit activity.

Certain customers who open a master account and maintain client sub-accounts are not subject to AML regulations, even though they may be in the best position to detect and report suspicious activity related to their own clients. Similar to other omnibus account arrangements, investment advisers commonly maintain accounts with broker-dealers that enable the adviser to execute trades on behalf of a pooled investment vehicle client, such as a hedge fund, that benefits investors in the pooled investment vehicle. In these cases, the investment adviser – and not the broker-dealer – has the direct relationship with the underlying investors and is best able to identify red flags. Investment advisers are not currently subject to AML regulations in the United States.

[336] *See* A Report to Congress, submitted by The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission, and the staff of the Commodity Futures Trading Commission (Dec. 31, 2002), available at http://www.fincen.gov/news_room/rp/files/356report.pdf.
[337] SEC Staff, Master/Sub-accounts, National Exam Risk Alert, Volume 1, Issue 1, September 29, 2011.

- In 2014, the SEC (in a settled action) and FINRA charged Los Angeles-based Wedbush Securities Inc. with AML-related violations associated with the firm's business of providing direct market access to broker-dealers and nonregistered market participants, including foreign firms.[338] In the first instance, Wedbush violated the SEC's market access rule by failing to implement adequate risk controls before providing customers with access to the market. Moreover, Wedbush failed to file required suspicious activity reports related to potentially manipulative trading by its direct market access customers. In addition, FINRA charged that Wedbush failed to establish, maintain and enforce adequate AML policies and procedures, and failed to investigate and report thousands of suspicious transactions potentially intended to manipulate market prices.
- In 2010, the SEC (in a settled action) and FinCEN found that Pinnacle Capital Markets violated its CIP obligations under the BSA. Pinnacle held master omnibus accounts for foreign entities, which in turn were subdivided into sub-accounts for other foreign entities.[339] The SEC found that Pinnacle treated these sub-account holders in the same manner as it did its regular account holders, allowing them to use direct market access software to enter securities trades directly and instantly through their own computers. The SEC concluded that the sub-account holders were Pinnacle's customers for purposes of the CIP rule because the sub-account holders effected securities transactions directly and without the intermediation of the master account holders. Pinnacle had not collected identifying information on the sub-account holders or verified their identities.

b. Foreign Correspondent Relationships

As in the banking context, securities firms that maintain correspondent accounts for foreign financial institutions[340] may be unwitting conduits for illicit activity of the foreign firm's underlying clients.

- In January 2015, the SEC (in a settled action) charged Oppenheimer & Co., Inc., with, among other things, aiding and abetting illegal unregistered broker-dealer activity by a customer, an off-shore broker-dealer. Oppenheimer inadequately monitored the foreign financial institution's transactions and consequently did not detect or investigate numerous suspicious transactions conducted through the account, including prohibited third-party activity and illegal penny stock

[338] SEC Announces Charges Against Wedbush Securities and Two Officials for Market Access Violations, Press Rel. No. 2014-115, June 6, 2014; Wedbush Securities and Two Officials Agree to Settle SEC Case; L.A.-Based Broker-Dealer Admits Wrongdoing and Will Pay Financial Penalty for Market Access Violations, Press Rel. No. 2014-263, Nov. 20, 2014; FINRA Charges Wedbush Securities for Systemic Market Access Violations, Anti-Money Laundering and Supervisory Deficiencies, news release, August 18, 2014.

[339] *See In the Matter of: Pinnacle Capital Markets, LLC,* FinCEN Matter No. 2010-4 (Sept. 1, 2010); *In the Matter of Pinnacle Capital Markets LLC and Michael A. Paciorek*, Exchange Act Release No. 62811 (Sept. 1, 2010) (settled administrative proceeding).

[340] For broker-dealers, correspondent accounts established on behalf of foreign financial institutions include, but are not limited to: (1) accounts to purchase, sell, lend, or otherwise hold securities, including securities repurchase programs; (2) prime brokerage accounts that clear and settle securities transactions for clients; (3) accounts for trading foreign currency; (4) custody accounts for holding securities or other assets in connection with securities transactions as collateral; and (5) over-the-counter derivative contracts. *See FinCEN; Anti-Money Laundering Programs; Special Due Diligence Programs for Certain Foreign Accounts*, 71 FR 496, 499 (Jan. 4, 2006).

trading.[341] Oppenheimer agreed to admit wrongdoing and pay $10 million to settle the SEC's charges. Oppenheimer will pay an additional $10 million to settle a parallel action by FinCEN. These represent the largest AML-related penalties ever assessed against a securities firm.

- In February 2014, FINRA issued its highest fine to date for AML violations, fining Brown Brothers Harriman (BBH), a New York-based investment bank, $8 million, and fined the bank's former AML compliance officer $25,000.[342] According to FINRA, BBH did not have an adequate AML program in place to monitor and detect suspicious penny stock transactions and file appropriate SARs. FINRA found that between 2009 and 2013 BBH facilitated transactions in at least six billion shares of penny stocks, often on behalf of undisclosed customers of foreign banks in known bank secrecy havens. FINRA notes penny stocks pose a high risk for fraud because low-priced securities can be manipulated. BBH's customers generated at least $850 million in profits through their penny stock transactions.
- In 2012, in New York, Mario Ernesto Villanueva Madrid, the former governor of the Mexican state of Quintana Roo, pled guilty to conspiring to launder millions of dollars in bribes through bank and brokerage accounts in the U.S. and other countries, including an account at a U.S. investment bank.[343] According to the U.S. Attorney for the Southern District of New York, Villanueva Madrid received payments of between $400,000 and $500,000 for each shipment of cocaine that the Juarez organization transported through his state. Villanueva Madrid held millions of dollars in an account that had been secretly opened for him at the Mexican bank Banamex in the name of Lehman Brothers Private Client Services. A large portion of the illicit proceeds – over $7 million – was transferred into an account at Lehman Brothers[344] opened for Villanueva Madrid under a fictitious name. Villanueva Madrid's illicit funds at Lehman and in other U.S. accounts, totaling over $19 million, were seized and later forfeited by U.S. authorities.
- Also see the Pinnacle case described above.

c. Misuse of Legal Entities

Microcap companies that are dormant in the over-the-counter market and delinquent in their public filings can be used to harm investors through reverse mergers and pump-and-dump schemes. Additionally, the SEC is addressing the manipulation of microcap shell companies through an initiative known as Operation Shell-Expel in which the SEC identifies dormant companies ripe for abuse. Since it began in 2012, Operation Shell-Expel has resulted in trading suspensions of more than 800 microcap stocks, which

[341] *See* Press Rel. No. 2015-14, SEC Charges Oppenheimer With Securities Law Violations Related to Improper Penny Stock Sales (Jan. 27, 2015). Available at http://www.sec.gov/news/pressrelease/2015-14.html; *see also* http://www.fincen.gov/news_room/nr/pdf/20150127.pdf

[342] FINRA Fines Brown Brothers Harriman a Record $8 Million for Substantial Anti-Money Laundering Compliance Failures, news release, February 5, 2014.

[343] Former Governor Of Mexican State Pleads Guilty In Manhattan Federal Court To Money Laundering Charge In Connection With Narcotics Bribes, news release, United States Attorney's Office for the Southern District of New York, August 2, 2012. Available at http://www.justice.gov/usao/nys/pressreleases/August12/villanuevamadridplea.html

[344] Lehman Brothers was the fourth largest investment bank in the United States before declaring bankruptcy in 2008. Lehman Brothers North America was subsequently acquired by Barclays Investment Banking and Capital Markets.

comprises more than eight percent of the OTC market.[345] According to the FBI, proceeds from securities fraud often go first to offshore banks and into the accounts of foreign shell companies. Then, the money comes back to the United States disguised as corporate dividend payments or interest payments on nonexistent loans and is deposited into the accounts of U.S. shell companies.[346]

- U.S. v. John G. Rizzo (2013): DOJ and the SEC charged John G. Rizzo, the former CEO of iTrackr Systems Inc., of orchestrating a fraudulent scheme to solicit foreign investors in order to evade registration requirements under U.S. securities laws. He raised approximately $2.5 million from these foreign investors who were unwise to the scheme. Rizzo funneled the money raised to his bank account in Belize, and after paying commissions to those who elicited the investments, he used the remainder to pay his personal expenses. Rizzo also purchased a shell company in the British Virgin Islands, unrelated to iTrackr, and used it to evade U.S. income tax. In a parallel action, the U.S. Attorney's Office for the Southern District of California announced criminal charges against Rizzo on August 2, 2013.[347]

With the globalization of markets, the FBI has seen foreign entities using the legal practice of reverse mergers[348] in order to gain access to the markets. Once they have access to the market, fraudsters use market manipulation schemes to make profits and victimize U.S. investors. The FBI adds that criminals now are attempting stock market manipulation via cyber intrusion.[349] Market manipulation fraud via computer intrusion involves criminals hacking into victims' personal online brokerage accounts and using them to purchase shares of a targeted stock to inflate its price. As in traditional pump and dump schemes, once the price of the stock reaches a certain point, the perpetrators dump their own shares and walk away with a profit.[350]

d. Compliance Deficiencies

The SEC and FINRA have brought a number of cases citing regulated firms and/or their employees for failing to implement an adequate AML compliance program including to perform basic customer identification and suspicious activity monitoring and reporting.[351] AML regulatory actions against securities firms often involve the firm's failure to identify and report activity that may indicate the predicate offense of securities fraud committed by a customer.

[345] Available at http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370540714936; http://www.sec.gov/news/pressrelease/2015-44.html
[346] See FBI, Investors Beware Stock Fraud Case Offers Lessons. Available at http://www.fbi.gov/news/stories/2010/january/fraud_012910
[347] SEC v. John G. Rizzo, Civil Action No. 13 CV 1801 MMA (BLM) (S.D. Cal. Aug. 2, 2013). Available at https://www.sec.gov/litigation/litreleases/2013/lr22770.htm
[348] The manipulation schemes often involve the legal technique of reverse merging a private company into a publicly traded shell without having to do an initial public offering. In a reverse merger, investors of a private company acquire a majority of the shares of the public shell company, which is then merged with the purchasing entity. This allows the fraudsters to engage in manipulative trading by driving up the price and volume of stock, and then profiting when the fraudsters dump their shares into the inflated market they themselves created.
[349] FBI, Department of Justice, FY 2014 Authorization and Budget Request to Congress, April 2013.
[350] Available at http://www.fbi.gov/about-us/investigate/white_collar/market-manipulation-fraud
[351] Available at http://www.sec.gov/News/Speech/Detail/Speech/1365171489982#P26_5924

These actions have resulted in significant fines, supervisory bars, and industry bars and suspensions, and emphasize that suspicious activity monitoring and reporting is not only the responsibility of the firm but also individuals at the firm that are directly responsible for filing SARs on the behalf of the firm.[352]

- In January 2014, FINRA fined the Mexican brokerage firm Banorte-Ixe Securities International, Inc. $475,000 for supervisory and AML lapses.[353] Banorte-Ixe Securities maintained offices in New York City and McAllen, Texas and primarily serviced Mexican nationals seeking to invest in U.S. and global securities. FINRA charged Banorte-Ixe Securities with not registering some 200 to 400 "foreign finders" who were working as account representatives in Mexico, referring and working with clients. The company's clientele was made up primarily of high net worth Mexican nationals, some of whom used their accounts to move large sums of money in and out of Mexico while conducting few if any securities transactions. According to FINRA, Banorte-Ixe Securities opened an account for a corporate customer owned, in part, by an individual with reported ties to a Mexican drug cartel, and did not detect, investigate, or report the suspicious rapid movement of $25 million in and out of the account.
- In an April 2013 complaint, FINRA's Department of Enforcement alleged that an AML compliance officer (AMLCO) failed to enforce his firm's AML procedures by failing to respond to red flags of suspicious AML activity. The findings stated that the firm's AML program was also inadequate where the AMLCO permitted his role to become compromised by his role as the representative handling accounts engaging in large volumes of transactions through which low-priced stocks were received into and sold in accounts at the firm. When the clearing firm brought red flags of suspicious customer activity to his attention, the AMLCO ignored the red flags and did not take reasonable steps to investigate, and as necessary, report the activity. He was fined $20,000, suspended from association with any FINRA member in any capacity for 30 days, and suspended from association with any FINRA member in any principal capacity for an additional five months.[354]
- In January 2007, FINRA fined Banc of America Investment Services, Inc. for failing to obtain the names of the beneficial owners of a number of accounts due to concerns from some at the firm that obtaining such information could cause the account holders to move their accounts elsewhere.[355] This occurred despite repeated and ongoing requests from a senior lawyer at the firm, the firm's risk committee, and the firm's clearing firm to obtain the names of the beneficial owners before conducting transactions in the accounts. In addition, FINRA found that the firm's processes were insufficient to ensure that its independent obligations regarding the filing of a SAR were met.

[352] *See* Elizabeth Pagliarini, Release No. 34-63964 (Feb. 24, 2011), Kenneth Brown, FINRA Letter of Acceptance, Waiver and Consent No. 2007007151703 (July 23, 2010), Mark Edward Diemer, FINRA Letter of Acceptance, Waiver and Consent No. 2009016254302 (Oct. 11, 2010), David William Dube, FINRA Letter of Acceptance, Waiver and Consent No. 2008011713801 (Nov. 9, 2010).
[353] FINRA Fines Banorte-Ixe Securities $475,000 for Inadequate Anti-Money Laundering Program and for Failing to Register Foreign Finders, news release, January 28, 2014.
[354] DOE V. Vincent Au, FINRA Order Accepting Offer of Settlement No. 2009016312701, July 18, 2013; *see also* https://www.finra.org/sites/default/files/DisciplinaryAction/p342525.pdf
[355] *See* Banc of America Investment Services, Inc., FINRA Letter of Acceptance, Waiver and Consent No. E062004038601 (Jan. 29, 2007).

- Also see the Wedbush Securities Inc. and Brown Brothers Harriman cases described above.

In early 2015, the SEC's Office of Compliance Inspections and Examinations' (OCIE) announced its exam priorities for 2015, which include examining "clearing and introducing broker-dealers' AML programs, using our analytic capabilities to focus on firms that have not filed SARs or have filed incomplete or late SARs. Additionally, we will conduct examinations of the AML programs of broker-dealers that allow customers to deposit and withdraw cash and/or provide customers direct access to the markets from higher-risk jurisdictions."[356] FINRA also announced that its AML 2015 examination priorities include focusing on the adequacy of firm surveillance systems and processes to identify potentially suspicious transfers to and from brokerage accounts typically associated with bank accounts, and to verify the business purpose of activity conducted through these accounts.[357] In addition, FINRA announced that its examiners will focus on the adequacy of firms' surveillance of customer trading and will evaluate whether firms have systems to monitor for red flags indicative of suspicious customer trading activity.[358]

2. Risks

The securities industry faces many of the same money laundering risks as the banking industry, including placement, layering, and integration risks, although to varying degrees. As noted above, the placement risk is reduced in the securities industry because industry participants, while not prohibited from accepting cash, typically do not accept cash. The layering risk is more of a concern. Once a criminal has funded a securities account with illicit proceeds – typically transferring funds that were originally placed in a bank account – the criminal can invest the money, transfer ownership interests in shares cross-border or use the securities account to move funds globally through checks and wires. Additionally, the lack of beneficial ownership information for certain account structures, such as master/sub or omnibus accounts, limits a broker-dealer's visibility into who actually owns or controls the account, and may create opportunities for money laundering.

[356] http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf
[357] *See* 2015 Regulatory and Examination Priorities Letter, January 6, 2015. Available at http://www.finra.org/sites/default/files/p602239.pdf
[358] *See id.*

Conclusion

CONCLUSION

The NMLRA is based primarily on law enforcement, supervisory, and FinCEN analysis, guidance, reports, and testimony published since 2006 and a review of almost 5,000 recent money laundering-related prosecutions. The terminology and methodology are based on the guidance of the FATF.

An estimated $300 billion is generated through illicit activity annually in the United States, with approximately 20 percent of that associated with illegal drug trafficking. Fraud accounts for most of the illicit proceeds in the United States, and most of that is perpetrated against U.S. government programs. The money laundering methods identified in the NMLRA exploit one or more of the following vulnerabilities:

- Use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds
- Opening bank and brokerage accounts in the names of businesses and nominees to disguise the identity of the individuals who control the accounts
- Deficient compliance with AML regulations
- Merchants and financial institutions wittingly facilitating illicit activity

AML regulation, supervision, enforcement, and compliance in the United States are generally successful in minimizing money laundering risks. Although criminals respond to new payment technologies and law enforcement initiatives and use their own innovation to spur new money laundering methods, the underlying vulnerabilities remain largely the same.

Regulatory recordkeeping and reporting requirements allow for anonymous transactions at merchants and financial institutions in amounts below the specified thresholds, which also create the opportunity for structuring. Allowing low value transactions without requiring customer identification creates a constant money laundering vulnerability, but also facilitates access to the financial system which is an important policy objective. The consequence is that criminals can spend cash freely, without fear of detection, below the specified recordkeeping and reporting thresholds, unless they attempt structuring which many do. Financial institutions are adept at identifying structuring and file hundreds of thousands of SARs annually and many people are prosecuted.

The use of nominees and businesses (including front companies and shell companies) to open accounts at banks and broker-dealers in order to disguise the identity of the individuals who control the accounts is intended to mislead the financial institution. Identifying when a customer is misrepresenting their identity or the purpose of their account poses a constant challenge to financial institutions, and creates a high risk for money laundering. As a practical matter, it is not possible to detect and report all potentially illicit transactions that flow through a financial institution.

Deficient AML compliance and criminal complicity are not systemic vulnerabilities in the United States, but in a $17 trillion economy with hundreds of casinos, thousands of broker-dealers, more than 10,000 banks, tens of thousands of MSB principals, and hundreds of thousands of MSB agents, it is inevitable that there will be a few that become deficient in their BSA compliance – or worse, that they create opportunities for money laundering. As the case examples in the NMLRA demonstrate, a single financial

institution can be responsible for billions of dollars of money laundering. Even at financial institutions with otherwise effective AML controls, a single complicit employee can be responsible for significant criminal activity.

Because financial crime can involve transactions that cross borders, U.S. financial institutions and supervisory and law enforcement authorities depend on foreign counterparts to help minimize money laundering risks. Law enforcement generally has access to the information it needs to investigate money laundering cases in the United States, but cooperation and transparency are not always present in other countries. Criminals moving money into or out of the United States often will route transactions through jurisdictions where they can obscure the financial trail with the help of corrupt officials or weak regulation and enforcement.

The potential for anonymity in financial transactions underlies most of the vulnerabilities in this risk assessment. There is always a concern regarding the potential exploitation of any new product or technology as a vehicle for money laundering. U.S. law enforcement and regulatory agencies are monitoring trends in new payment methods such as virtual currencies.

APPENDIX A: State Money Laundering Laws

Alabama

- **Alabama Code § 20-2-93** All monies traceable to the sale or exchange of illegal controlled substances are forfeitable.
- **Alabama Code § 13A-12-200.8** Makes all monies and negotiable instruments obtained or intended to be used in violation of Division 5, Article 4, Chapter 12 of Title 13A (child porn violations)

Arizona

- **AZ Revised Statute 13-2317** (Money Laundering)-Contains provisions similar to 18 U.S.C. 1956, 18 U.S.C. 1952, and Federal Title 31 reporting requirements.
- **AZ Revised Statute 6-1202**- Contains provisions requiring money transmitters to be licensed similar to 18 U.S.C. 1960. A "business" requires 10 activities regulated by the statute in a calendar year. Failure to file the report is also a violation of 13-2317.

Arkansas

- **Arkansas Title 5, Subtitle 6, Chap 64, SubChap 5** Civil forfeiture of anything of value exchanged for a controlled substance or traceable thereto in violation of this section. There is a rebuttable presumption that any money found in close proximity to a forfeitable controlled substance is itself forfeitable under this section.
- **Arkansas Title 5, Subtitle 4, Chap 42, SubChap 2** (Money Laundering) Contains money laundering prohibitions similar to 18 U.S.C. 1956. The statute also allows a civil action to be brought with the burden of proof as "preponderance of evidence."

California

- **CA Health and Safety Code 11370.6** – Possession of excess of $100k obtained as a result of unlawful sale, transport, etc. of "controlled substance."
- **CA Health and Safety Code 11370.9** – (General Money Laundering) - Contains provisions similar to 18 U.S.C. 1956 and the 18 U.S.C. 1960. It appears to have a $25,000 threshold.

Florida

- **Florida Statute Title XLVII, Chap 932** (Contraband Forfeiture Act) Provides a general forfeiture statute for various types of contraband including illicit bulk currency. The statute, among other things, provides for the forfeiture of any bulk currency that has been used or attempted to be used in commission of a felony or represents the proceeds therefrom. The definitions in Section **932.01** have information regarding what constitutes "contraband."
- **Florida Statute Title XLVI, Chap 896.101** (Florida Money Laundering Act) Provides prohibitions against money laundering similar to 18 U.S.C. 1956 but also with a more general prohibition regarding transportation of illicit currency (that doesn't require border crossing).

- **Florida Statute Title XXXIII, Chap 560.111** (Money Service Businesses) Provides regulation of money service businesses similar to 18 U.S.C. 1960 and makes a violation of 18 U.S.C. 1960 and various other federal and state financial authorities a violation of the Florida statute.

Illinois

- **Illinois Statute 725 ICLS 150** (Drug Asset Forfeiture Procedure Act) Provides civil forfeiture of assets, including currency, that are attributable to the sale of illegal controlled substances and is based on the federal narcotics civil forfeiture act. Provides certain rebuttable presumptions including one in which all money found in close proximity to forfeitable substances is itself subject to forfeit as presumed to be subject to forfeiture.
- **Illinois Statute ILCS 5/29B of 1961** (Money Laundering) Has provisions similar to 18 U.S.C. 1956. Although passed in 1961 it appears to still be good law.
- **Illinois Statute 205 ILCS 657 / 10** (Transmitters of Money Act) Provides prohibitions similar to 18 U.S.C. 1960 requiring a license to engage in money transmission

New Mexico

- **New Mexico Statute 30-51-4** - (Money Laundering Act) – Contains provisions similar to 18 U.S.C. 1956.

New York

- **New York Code Article 13-A, Section 1311** A civil action may be commenced in personam to recover proceeds or instrumentalities of a crime against a criminal defendant or a non-criminal defendant within 5 years of commission of the crime. No criminal conviction is required. Because it is a civil suit the burden of proof is only "preponderance of the evidence."
- **New York Penal Code 470** (Money Laundering) Similar to 18 U.S.C. 1956 which requires defendant to know that property involved in a financial transaction represents proceeds of criminal conduct and then conducts a financial transaction which in fact involves proceeds of specified criminal conduct with intent to conceal the nature, location…or avoid a reporting requirement…
- **New York Penal Code 480** If a person is convicted of a felony then any property constituting proceeds or substitute proceeds of the offense are forfeitable unless disproportionate to the defendant's gains.

Ohio

- **Ohio Revised Code 1315.53** –Has reporting requirements similar to Federal Title 31 reporting requirements.
- **Ohio Revised Code 1315.55** –Contains provisions similar to traditional money laundering and 18 U.S.C. 1952 and 18 U.S.C. 1960 prohibitions).
- **Ohio Revised Code 2981.02** (Property Subject to Forfeiture) – Allows forfeiture of proceeds derived from commission of crime.

Oklahoma

- **O.S. 63-2-503.1a - 63-2-503.1i** (Drug Money Laundering and Wire Transmitter Act)- Contains provisions which are similar to 18 U.S.C. 1956 and 18 U.S.C. 1960 as well as prohibition on acts violating Federal Title 31 reporting requirements.
- **O.S. 21-1268.7** –Contains prohibitions similar to the crimes outlined in the Drug Money Laundering and Wire Transmitter Act but in the context of terrorism.

Tennessee

- **Tennessee Title 39-14-903** (Money Laundering) – contains traditional prohibitions against money laundering similar to 18 U.S.C. 1956.
- **Tennessee Title 45-7-202** (Money Transmitters) - contains requirements for registration of money transmitters similar to 18 U.S.C. 1960. It does not have a prohibition on a business of transporting currency known to be derived from an unlawful source as found in 18 U.S.C. 1960.
- **Tennessee Title 39-11-703** (Forfeiture of criminal proceeds) – provides forfeiture of proceeds traceable to violation of any statute.

Texas

- **Texas Penal Code, Title 7 Section 34.02** (Money Laundering) – Contains provisions encompassing elements from both 18 U.S.C. 1956 and 18 U.S.C. 1960 and 18 U.S.C. 1952 (regarding transporting currency derived from criminal activity).
- **Texas Finance Code Section 151.302** (Money Transmitters) – Similar to 18 U.S.C. 1960 regarding transportation of currency know to be derived from criminal activity.
- **Texas Code of Criminal Procedure Chapter 59, Article 59.02** (Forfeiture of contraband) - Provides forfeiture of proceeds gained from commission of a felony.

APPENDIX B: Public Sector AML Reports Published Since 2006

- Agency-specific reports
  - DEA: A Perspective on Mexican Bulk Cash Movement and Money Laundering Trends
  - DEA: Money Laundering Report
  - FBI: Financial Crimes Report
  - HHS: Health Care Fraud and Abuse Control Program Report
  - High Intensity Drug Trafficking Area (HIDTA) Threat Assessments
  - ICE-HSI: Key Locations and Vulnerabilities Related to Money Laundering Methods Used by Transnational Criminals Organizations to Transport, Launder, and Store Illicit Proceeds
  - IRS-CI: Annual Reports
  - National Drug Intelligence Center: National Bulk Cash Smuggling Threat Assessment
  - Office of the Comptroller of the Currency National Risk Committee Reports
- Interagency studies and strategies:
  - National Drug Threat Assessments
  - National Drug Control Strategies
  - National Gang Threat Assessment
  - National Southwest Border Counternarcotics Strategies
  - National Strategy for Counterterrorism
  - Strategy to Combat Transnational Organized Crime
  - USA/Mexico Bi-national Criminal Proceeds Study
- Congressional reports
  - A Line in the Sand: Countering Crime, Violence and Terror at the Southwest Border
  - The Buck Stops Here: Improving U.S. Anti-Money Laundering Practices
  - U.S. and Mexican Responses to Mexican Drug Trafficking Organizations
  - U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History