PUBLICATION UPDATE

Route to: ☐ ____ ☐ ____ ☐ ____ ☐ ____
☐ ____ ☐ ____ ☐ ____ ☐ ____

Guide to Anti-Money Laundering and BSA Compliance

Publication 4760 Release 32 June 2023

HIGHLIGHTS

Chapter Revisions

- Chapter 1 Customer Identification and BSA Compliance Programs and Requirements
- Chapter 2 Suspicious Activity Reporting Requirements

Chapter 1 includes a summary of the enforcement action against Sterling Bank and Trust, FSB, for failing to implement and maintain an effective Bank Secrecy Act/anti-money laundering program.

- *See* § 1.05[2][a].

Chapter 2 addresses the February 27, 2023, Financial Crimes Enforcement Network (FinCEN) alert issued to financial institutions about the nationwide surge in check fraud schemes targeting the U.S. mail. FinCEN identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to mail theft-related check fraud.

- *See* § 2.14[9][o].

Chapter 2 also includes a detailed listing of money laundering and terrorist financing red flags.

- *See* § 2.16 Exhibit 2.5.

Matthew Bender provides continuing customer support for all its products:

- **Editorial assistance—please consult the "Questions About This Publication" directory printed on the copyright page;**
- **Customer Service—missing pages, shipments, billing or other customer service matters, +1.800.833.9844.**
- **Outside the United States and Canada, +1.937.247.0293, or fax (+1.800.828.8341) or email (international@bender.com);**
- **Toll-free ordering (+1.800.223.1940) or visit www.lexisnexis.com/BrowseUs.**

www.lexis.com

Publication 4760, Release 32, June 2023

FILING INSTRUCTIONS

Guide to Anti-Money Laundering and BSA Compliance

Publication 4760 Release 32 June 2023

Check As Done

- ☐ 1. Check the Title page in the front of your present Volume 1. It should indicate that your set is filed through Release Number 31. If the set is current, proceed with the filing of this release. If your set is not filed through Release Number 31, DO NOT file this release. Please call Customer Services at 1-800-833-9844 for assistance in bringing your set up to date.
- ☐ 2. This Release Number 32 contains only White Revision pages.
- ☐ 3. Circulate the "Publication Update" among those individuals interested in the contents of this release.

Check As Done	*Remove Old Pages Numbered*	*Insert New Pages Numbered*

For faster and easier filing, all references are to right-hand pages only.

VOLUME 1

Revision		
☐	Title page.	Title page
☐	1-1	1-1 thru 1-2.1
☐	1-19 thru 1-22.2(9)	1-19 thru 1-22.2(9)
☐	2-1 thru 2-9.	2-1 thru 2-9
☐	2-50.9	2-50.9 thru 2-50.11
☐	2-73 thru 2-75	2-73 thru 2-81

FILE IN THE FRONT OF THE FIRST VOLUME
OF YOUR SET

To order missing pages log on to our self service center, www.lexisnexis.com/printcdsc or call Customer Services at 1 (800) 833-9844 and have the following information ready:

(1) the publication title;
(2) specific volume, chapter and page numbers; and
(3) your name, phone number, and Matthew Bender account number.

Please recycle removed pages.

MISSING FILING INSTRUCTIONS?
FIND THEM AT www.lexisnexis.com/printcdsc

Use the search tool provided to find and download missing filing instructions, or sign on to the Print & CD Service Center to order missing pages or replacement materials. Visit us soon to see what else the Print & CD Service Center can do for you!

www.lexis.com

Publication 4760, Release 32, June 2023

Guide to Anti-Money Laundering and BSA Compliance

High-Risk Areas
Suspicious Activities
OFAC
USA PATRIOT Act

Jeffrey Torp

A Sheshunoff® Publication

Filed Through:
RELEASE NO. 32 JUNE 2023

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Alise Bruton at 937-610-5182
Email: ..... alise.bruton@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-76987-817-1 (print)

Cite this publication as:

Cite as: Jeffrey Torp, Guide to Anti-Money Laundering and BSA Compliance § [sec. no.] (LexisNexis Sheshunoff)

Example: Jeffrey Torp, Guide to Anti-Money Laundering and BSA Compliance § 1.01 (LexisNexis Sheshunoff)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(Rel. 32-6/2023 Pub.4760)

Chapter 1

Customer Identification and BSA Compliance Programs and Requirements

SYNOPSIS

[c] ***Enforcement Approach***

(Text continued on page 1-3)

are complete, they should be approved by the holding company or lead financial institution. Increasingly, organizations use software or programming solutions to assist in the implementation of the BSA/AML compliance program; these solutions typically include, but are not limited to, monitoring, identifying, and reporting suspicious activity.

§ 1.05 COMMON PROBLEMS IN BSA PROGRAMS

[1] In General

While compliance with the requirements of the BSA has always been a part of the regulatory examination process, BSA compliance now receives more scrutiny that ever. As a result, financial institutions that have had BSA programs go without criticism for years are now finding that some areas of the programs are deficient. One of the best summaries of these findings comes from the Office of the Comptroller of the Currency (OCC) in its Advisory Letter 2000-3. While this only relates the OCC's experience with its examination of national banks, these findings are equally applicable to all financial institutions, since there is nothing unique about national banks that would cause them to be any better or worse than other institutions in the area of BSA compliance.

As a result of in-depth BSA/anti-money laundering examinations, the OCC identified a number of common BSA compliance deficiencies. In general, it was found that institutions had good currency transaction reporting (CTR) programs but lacked adequate systems and controls to ensure timely suspicious activity reporting. It was also found that some financial institutions failed to adequately:

- Document and evaluate new, high-risk accounts for money laundering;
- Establish controls and review procedures for high-risk services;
- Monitor high-risk accounts for money laundering, including transactions that far exceeded the normal range of activity for such accounts;
- Conduct adequate independent testing of high-risk accounts for the possibility of money laundering;
- Train employees to detect suspicious activity in high-risk areas like pouch and wire transfer transactions, particularly to/from known drug source or money-laundering havens; and
- Review CTR filing patterns for suspicious activity.

As a result, a number of suspicious activity reports were not filed in a timely manner. Therefore, financial institutions should make sure that these areas are addressed in their BSA programs.

[2] Recent Enforcement Actions Against Financial Institutions

[a] *Sterling Bank and Trust, FSB—Failure to Implement and Maintain Effective AML Program*

In September 2022, the OCC issued a consent order for payment of a $6,000,000 civil money penalty to Sterling Bank and Trust, FSB. One of the issues involved was the bank making mortgage loans based on fraudulent applications. In addition, during the relevant period, the bank failed to implement an adequate system of BSA/AML internal controls and failed to file SARs in a timely manner.

[b] *CommunityBank of Texas—Failure to Implement and Maintain Effective AML Program*

In December 2021, FinCEN and the OCC assessed an $8 million civil money penalty on CommunityBank of Texas, N.A. (CBOT) for willful violations of the BSA and its implementing regulations.

Specifically, CBOT admitted that it willfully failed to implement and maintain an effective AML program that was reasonably designed to guard against money laundering. CBOT also admitted that it willfully failed to report hundreds of suspicious transactions to FinCEN involving illegal financial activity by its customers and processed by, at, or through the bank even after the bank became aware that certain customers were subjects of criminal investigations. The violations occurred from at least 2015 through 2019 and caused millions of dollars in suspicious transactions to go unreported to FinCEN in a timely and accurate manner, including transactions connected to tax evasion, illegal gambling, money laundering, and other financial crimes.

"CommunityBank of Texas willfully disregarded its lawful obligations to implement and maintain an effective AML program and to identify and report suspicious transactions to FinCEN," said FinCEN's Acting Director

Himamauli Das. "The failures of CommunityBank of Texas enabled criminal activity by depriving regulators and law enforcement of critical financial intelligence. Today's action should serve as a reminder to banks of all sizes that FinCEN and our regulatory partners will work closely together to ensure that banks comply with the Bank Secrecy Act and its implementing regulations in order to combat money laundering and promote national security."

As a result of its own investigation, the OCC assessed a civil penalty of $1 million for related violations. As many of the facts and circumstances underlying the OCC's civil penalty also form the basis of FinCEN's consent order, FinCEN agreed to credit the $1 million civil penalty imposed by the OCC. Taken together, CBOT will pay a total of $8 million to the U.S. Treasury as a penalty for its violations, with $7 million representing FinCEN's penalty and $1 million representing the OCC's penalty.

[c] *Capital One, NA (CONA)—Inadequate Compliance With Requirements of the BSA*

On January 15, 2021, FinCEN assessed a $390 million penalty for various BSA violations. Specifically, FinCEN determined that the bank violated certain of its BSA obligations for its Check Cashing Group (CCG) from about 2008 until about 2014, by willfully failing to establish and maintain an effective anti-money laundering program and willfully failed to accurately and timely file SARs on suspicious transactions associated with the CCG. (*Willfully* means with either reckless disregard or willful blindness.) FinCEN also determined that the bank negligently failed to timely file CTRs for the CCG.

In December 2006, Capital One Financial Corporation (COFC), the holding company for CONA, acquired North Fork Bank (NFB), including that bank's New York and New Jersey check cashing customers. NFB was merged into CONA in August 2007, and CONA established the CCG as part of its Middle Market Lending group. CONA operated the CCG until 2014. The CCG customer base included a range of between approximately 90 and 150 New York- and New Jersey-area check cashers that usually operated storefront locations and conducted check cashing as their primary business.

CONA built its retail and commercial bank lines of business primarily by virtue of a series of acquisitions of regional banks, beginning with the acquisition of Hibernia Bank (Hibernia) in November 2005 and the acquisition of NFB in December 2006. Hibernia and NFB began operating under CONA's name in April 2006 and March 2008, respectively. Prior to CONA's acquisitions of and mergers with Hibernia and NFB, federal and state bank regulators identified deficiencies in the AML programs at both banks, including weaknesses in transaction monitoring.

Establishment of AML program. After acquiring and incorporating NFB and Hibernia, CONA internally acknowledged having significant "residual AML risk attributable to inadequate AML internal controls." To address the deficiencies identified by its regulators, CONA hired BSA/AML officers to build out an enterprise-wide AML program befitting CONA's consolidated operations. Over time, these officers produced enterprise-wide AML policies, procedures, and process controls. However, these controls and procedures were inadequate to address the money laundering risk associated with the CCG, were inconsistently and ineffectively implemented for CCG customers, were plagued by a number of technical failures that were not promptly addressed, and gave too much credence to dubious explanations from the business line about CCG banking activity, all of which ultimately resulted in a failure to guard against money laundering and other criminal and suspicious activity.

Customer due diligence and reviews. A bank's management should have a thorough understanding of the money laundering risks of its customer base. Further, as part of its AML processes, a bank should stay apprised of changes within the industry, business models, and customer profiles and patterns that impact the source, nature, or purpose of a customer's transactional activity; understand red flag indicators; and act on information learned through the AML process.

A bank should combine all of its knowledge about its customers' industries, legitimate business models, individual occupations and activity, and money laundering indicators to assess money laundering risks and apply appropriate risk ratings. Those risk ratings can then aid a bank in assessing the appropriate basis for due diligence and ongoing transaction monitoring for its customers.

In mid-2008, CONA connected certain CCG customer information to its enterprise-wide automated AML monitoring system, which rated customers based on their overall risk for money laundering. CONA used a risk scoring system based on points it assigned for various factors. Based on the risk of the industry and geographic location, CCG customers automatically received a baseline number of points placing them in the highest risk

category. One such review conducted in 2010 identified 6,000 bank customers at highest risk for money laundering. Most CCG customers ranked in the top 100 of these highest risk customers, including C&F Inc. (C&F), a Domenick Pucillo (Pucillo) check cashing entity that was the highest risk among the CCG at number 21 for the entire bank. CONA used the customer scores for different purposes, including semiannual high-risk customer reviews, which was CONA's greatest frequency for regular AML reviews. While these semiannual high-risk customer reviews did focus on identifying if the customer had negative news on them, assessing account activity, comparing the historic dollar volume to the current dollar volume to assess the reasonableness of the CCG customer's transaction activity, and sampling checks within the CCG account, they failed to fully enable CONA to understand the nature and legitimacy of their customers' activity and patterns therein.

Specifically, CONA developed and relied on a macro that aggregated debits and credits for the CCG customer under review and then compared the macro information with a sample of historic transactional dollar volume to determine if the customer's activity was consistent or if it had a statistically significant deviation in transaction volume. As long as the activity appeared to be related to the business model—such as a check casher depositing checks—or had a ready explanation for deviations outside the consistent volume marker, the activity was deemed reasonable, and the initial high-risk alert was closed without further action. Although CCG accounts were reviewed again after initial reviews, often these further reviews were perfunctory, relying too heavily on the results of the macros and comparisons to past activity, without taking additional investigative steps or incorporating additional knowledge about the customers. As a consequence, CONA failed to detect red flags or follow up appropriately on potential indications of suspicious activity. In other words, CONA improperly used consistency as the primary benchmark for reasonableness, overlooking the nature or apparent lawful purpose of their customer's underlying activity and patterns.

AML compliance determinations. CONA's process for investigating suspicious transactions for the CCG was weak and resulted in the failure to fully investigate and report suspicious conduct. For example, from at least January 2009 through December 2013, AML analysts repeatedly identified suspicious activity—variously described as a medical fraud ring, excessive corporate check cashing, high dollar checks, and structured third-party checks—within at least 30 CCG customers' accounts.

However, as part of its ordinary AML process, AML management routinely instructed analysts to contact CONA's relationship manager for the CCG business line to obtain additional information and guidance regarding CCG related transactions. In turn, the business line often suggested vague and implausible explanations for the CCG activity, such as:

- "CTRs filed as necessary"
- "Making payroll"
- "Hurricane Sandy work"
- "Known to customer"
- "A high number of customers in February because of tax refunds being cashed at the stores"
- "Uptick in Corporate Check Cashing"
- "Fewer days in the month"
- "Aggressively looking to manage down excess currency"

At times, CONA's AML analysts accepted such justifications from the CCG business line at face value, which limited their ability to perform effective AML scrutiny and file robust SARs.

As a consequence, CONA failed to fully investigate much of this activity or report it to FinCEN as suspicious.

Unfiled SARs and CTRs. In addition to the above AML program failures, the AML failures that resulted in the willful failures to timely and accurately file SARs and the negligent failure to file CTRs, and the failure by CONA to timely identify such failures, also establish the AML program violations.

As a consequence of its AML program failures, CONA failed to accurately and timely file SARs on its CCG customers. Indeed, CONA filed no SARs on its CCG customer activity until October 2009, and thereafter CONA often failed to detect and report suspicious activity by the check cashers themselves, even as it detected and reported

activity by the check casher's customers. During the relevant period CONA failed to file SARs even when it had direct knowledge of certain CCG customers' indictments and guilty pleas for criminal activity associated with their check cashing operations flowing through the bank's accounts.

[d] *The Bancorp Bank, Wilmington, Delaware—Noncompliance With a BSA/AML-Related Consent Order*

On December 18, 2019, the FDIC issued a consent order to The Bancorp Bank, Wilmington, Delaware, to pay a civil money penalty of $7.5 million for noncompliance with a June 5, 2014, consent order involving, among other things, inadequate monitoring for suspicious activities and failing to file suspicious activity reports when required.

[e] *California Pacific Bank—Noncompliance With a BSA/AML-Related Consent Order*

On October 17, 2019, the FDIC assessed a $225,000 civil money penalty against California Pacific Bank for BSA/AML violations. In particular, the FDIC said that the bank violated the terms of a 2016 order that required the bank to cease and desist from certain practices and to comply with eight provisions related to compliance with the BSA and its regulations and the establishment of an effective BSA/AML compliance program. The FDIC conducted a visitation of the bank beginning on February 26, 2018, and determined that the bank was operating in violations of five provisions of the 2016 order. In an examination of the bank beginning on July 30, 2018, the FDIC concluded that the bank continued to be in violation of those five provisions.

[f] *Capital One, N.A., and Capital One Bank (USA), N.A.—Inadequate BSA/AML Program*

On October 23, 2018 the OCC assessed a $100 million civil money penalty against Capital One, N.A., and Capital One Bank (USA), N.A. for deficiencies in the bank's BSA/AML program.

The deficiencies included weaknesses in its compliance program and related controls; deficiencies in its risk assessment, remote deposit capture and correspondent banking processes; and failing to file suspicious activity reports. In assessing this civil money penalty, the agency found that the bank failed to achieve timely compliance with the OCC's 2015 order, as required.

Specifically, the 2015 consent order addressed the following conduct:

- The bank failed to adopt and implement a compliance program that adequately covered the required BSA/AML program elements due to an inadequate system of internal controls and ineffective independent testing, and the bank failed to file all necessary SARs related to suspicious customer activity;
- Some of the critical deficiencies in the elements of the bank's BSA/AML compliance program included the following:
  - — The bank lacked an enterprise-wide BSA/AML risk assessment;
  - — The bank had systemic deficiencies in its transaction monitoring systems, risk management, and quality assurance programs for its remote deposit capture services;
  - — The bank had systemic deficiencies in its customer due diligence processes and failed to have customer due diligence and enhanced due diligence policies and processes specific to correspondent banking; and
  - — The bank lacked a process by which BSA/AML control decisions are escalated to risk management.
- The bank failed to identify significant volumes of suspicious activity and file the required SARs concerning suspicious customer activities.
- Subsequent to the issuance of the 2015 consent order, the bank failed to file additional SARs and initiated wire transfer transactions which contained inadequate or incomplete information.

[g] *Bank of China NY Branch—Deficiencies in BSA/AML Compliance Program and SAR Filings; Deficiencies in OFAC Compliance*

On April 24, 2018 the OCC issued a consent order for a $12.5 million civil money penalty to Bank of China, New York branch, a federal branch of Bank of China Limited, Beijing, for deficiencies in the branch's BSA/AML compliance program, that resulted in violations of 12 C.F.R. § 21.21 (BSA/AML compliance program), and 12 C.F.R. § 21.11 (suspicious activity report filings), and deficiencies in the branch's compliance with the requirements of the Office of Foreign Asset Control (OFAC).

The Comptroller found the following:

(1) The branch violated 12 C.F.R. § 21.21 and 12 C.F.R. § 21.11. Specifically, the branch failed to adopt and implement a compliance program that adequately covered the required BSA/AML program elements, and the requirements of OFAC, and the branch failed to timely file SARs related to suspicious customer activity.

(2) Some of the critical deficiencies in the elements of the branch's BSA/AML compliance program included the following:

(a) The branch had an inadequate system of internal controls, ineffective independent testing, a weak BSA officer function, and insufficient training.

(b) The branch had systemic deficiencies in its transaction monitoring systems, which resulted in monitoring gaps. These systemic deficiencies resulted in alert and investigation backlogs and led to a failure to file SARs in a timely manner.

(c) The branch had systemic deficiencies in its CDD, enhanced due diligence (EDD), and customer risk rating processes.

(3) The branch failed to file the necessary SARs concerning suspicious customer activity in a timely manner.

[h] *U.S. Bancorp—Inadequate Compliance With U.S. Economic Sanctions, and BSA and AML Requirements*

On February 15, 2018, the Federal Reserve Board ordered Minneapolis-based U.S. Bancorp to improve risk management and oversight of its banking subsidiaries' compliance with U.S. economic sanctions, and Bank Secrecy Act and anti-money-laundering requirements. The Board also required U.S. Bancorp to ensure that firm personnel make timely and complete disclosures to regulatory authorities and imposed a $15 million penalty.

In a separate action, the U.S. Department of Justice announced the execution of a deferred prosecution agreement with U.S. Bancorp for violations of the Bank Secrecy Act that occurred at its national bank subsidiary. The deferred prosecution agreement provides for a $528 million forfeiture by U.S. Bancorp. In addition, the Office of the Comptroller of the Currency and the Financial Crimes Enforcement Network announced penalties of $75 million and $185 million respectively against U.S. Bancorp's national bank subsidiary for violations of the Bank Secrecy Act.

U.S. Bank willfully violated the BSA's program and reporting requirements from 2011 to 2015. As described below, U.S. Bank failed to (a) establish and implement an adequate AML program from 2011 to 2014; (b) report suspicious activity from 2011 to 2014, and; (c) adequately report currency transactions from 2014 to 2015. Rather than maintaining effective, risk-based policies, as required by the BSA, U.S. Bank devoted an inadequate amount of resources to its AML program from 2011 to 2014. First, the bank capped the number of alerts its automated transaction monitoring system would generate for investigation. Testing indicated that these caps caused the bank to fail to investigate and report large numbers of suspicious transactions. Nonetheless, instead of removing the alert caps, the bank terminated the testing that demonstrated the caps' deficiencies.

Similarly, from May 2009 until June 2014, U.S. Bank allowed noncustomers to conduct currency transfers at its branches through a large money transmitter. Although the bank knew that it had an obligation under the BSA to monitor those transfers for suspicious activity, it failed to include them in its automated transaction monitoring system.

The bank also employed inadequate procedures to identify and address high-risk customers that caused it to fail to effectively analyze and report the transactions of such customers. The willfully deficient practices described above caused U.S. Bank to fail to file thousands of SARs. A look-back analysis covering only a portion of the time-period during which these deficiencies persisted caused U.S. Bank to belatedly file more than 2,000 SARs on transactions worth more than $700 million. Some of these late-filed SARs identified transactions worth hundreds of thousands of dollars that potentially related to troubling criminal conduct.

Finally, from July 2014 until May 2015, U.S. Bank filed thousands of CTRs that provided materially inaccurate information to FinCEN. Specifically, the CTRs failed to provide the names of the MSBs that were the ultimate beneficiaries of the transactions. The bank knew that the MSBs were the beneficiaries of the transactions, as it entered the MSBs' TINs in the CTRs. Nevertheless, the bank repeatedly entered the wrong beneficiary name in the CTRs,

thus significantly undermining the utility of the CTRs for law enforcement purposes. The bank allowed this problem to persist for nearly a year, resulting in thousands of materially inaccurate CTRs.

[i] ***Rabobank NA—BSA and AML Failures***

On February 7, 2018, Rabobank National Association (Rabobank), a Roseville, California subsidiary of the Netherlands-based Coöperatieve Rabobank U.A., appeared before U.S. Magistrate Judge Jill L. Burkhardt and pleaded guilty to a felony conspiracy charge for impairing, impeding and obstructing its primary regulator, the OCC, by concealing deficiencies in its AML program and for obstructing the OCC's examination of Rabobank. Rabobank will forfeit $368,701,259 as a result of allowing illicit funds to be processed through the bank without adequate BSA or AML review.

Rabobank pleaded guilty to conspiracy to defraud the United States and to corruptly obstruct an examination of a financial institution. In pleading guilty, Rabobank admitted to conspiring with several former executives to defraud the United States by unlawfully impeding the OCC's ability to regulate the bank, and to obstruct an examination by the OCC of its operations throughout California, including its Calexico and Tecate bank branches. Rabobank admitted that its deficient AML program allowed hundreds of millions of dollars in untraceable cash, sourced from Mexico and elsewhere, to be deposited into its rural bank branches in Imperial County, and transferred via wire transfers, checks, and cash transactions, without proper notification to federal regulators as required by law. Knowing these failures, during the OCC's 2012 examination of Rabobank's BSA/AML compliance program, Rabobank executives actively sought to hide and minimize the deficiencies in its AML program in an effort to deceive the regulators as to its true state in hopes of avoiding regulatory sanctions that had previously been imposed on Rabobank in 2006 and 2008 for nearly identical failures.

"When Rabobank learned that substantial numbers of its customers' transactions were indicative of international narcotics trafficking, organized crime, and money laundering activities, it chose to look the other way and to cover up deficiencies in its anti-money laundering program," said Acting Assistant Attorney General Cronan. "Worse still, Rabobank took steps to obstruct an examination by its regulator into those same deficiencies. The integrity of our financial system depends on prompt reporting by banks and other financial institutions of suspicious, potentially criminal transactions, and on these entities' truthfulness and transparency with their regulators. Rabobank's guilty plea today and forfeiture of more than $360 million is a warning to financial institutions that there are significant consequences for banks that engage in obstructive conduct in an effort to hide their anti-money laundering program failures from their regulators."

"Rabobank had an obligation to shine light on suspected drug traffickers, money launderers and organized crime," said U.S. Attorney Braverman. "Instead, this bank deliberately allowed hundreds of millions of dollars of suspicious cash transactions and wire transfers to flow through its branches and took measures to hide this activity from regulators. We will vigorously protect the integrity of the banking system, and we will not allow the financial institutions in our communities to play any role in facilitating international money laundering or financing transnational criminal organizations."

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

The BSA requires financial institutions to implement and maintain an AML compliance program reasonably designed, among other things: (i) to detect suspicious activity indicative of money laundering and other crimes and (ii) to assure and monitor compliance with the BSA's recordkeeping and reporting requirements, including to report to the U.S. Department of the Treasury any suspicious transactions (through filing SARs) indicative of a possible violation of the law. In its plea agreement, Rabobank admitted knowing that between 2009 and 2012 its BSA/AML program failed in significant ways. Some of these BSA/AML program failures resulted from policies and procedures at Rabobank that precluded and suppressed investigations into suspicious transactions that occurred at its branches, by its accountholders, or by individuals conducting transactions on behalf of its accountholders that had various indications of being involved in, derived from, or promoting illegal conduct.

According to court documents, Rabobank received regular alerts of transactions by "High-Risk" customers, or through accounts deemed to be "High-Risk," and that had been the subject of prior SARs filed by Rabobank. These high-risk customers and accounts included those controlled and managed by Mexican businesses, nonresident aliens, and U.S.-based accountholders who transacted hundreds of millions of dollars in untraceable cash, sourced from Mexico and elsewhere, into and through Rabobank accounts.

According to court documents, Rabobank also created and implemented policies and procedures to prevent adequate investigations into these suspicious transactions, customers, and accounts. Among those policies and procedures was Rabobank's "Verified List"—a policy that effectively resulted in Rabobank executing an end-run the BSA/AML and SAR requirements. In particular, Rabobank instructed its employees that if a customer was on the "Verified List," no further review of that customer's transactions was necessary—even if the transactions generated an internal alert, or the customer's activity had changed dramatically from when it was "verified." Rabobank's BSA/AML staff were further instructed to aggressively increase the number of bank accounts on the Verified List, as evidenced by the fact that in 2009, Rabobank had less than 10 "verified" customers, but by 2012, as a result of its defective BSA/AML policies and procedures, it had more than 1,000 "verified" customers.

Additionally, Rabobank admitted failing to monitor and conduct adequate investigations into these transactions and submit SARs to FinCEN, as required by the BSA. Rabobank's border branches, including those located in Calexico and Tecate in Imperial County, California, were heavily dependent on cash deposits from Mexico. Rabobank knew that millions of dollars in cash deposits at these branches were likely tied to illicit conduct. In particular, the Calexico branch, located about two blocks from the U.S.-Mexico border, was the "highest performing" branch in the Imperial Valley region due to the cash deposits from Mexico. Throughout the relevant time period, Rabobank continued this practice of soliciting cash-intensive customers from Mexico and elsewhere, all the while employing the foregoing inadequate BSA/AML policies and procedures to address the obvious, known "High Risks" associated with these accounts, transactions, and transactors.

When the OCC began conducting its periodic examination of Rabobank in 2012, Rabobank, acting through three of its executives, agreed to, among other things, knowingly obstructing the OCC's examination. Rabobank responded to the OCC's February 2013 initial report of examination with false and misleading information about the state of Rabobank's BSA/AML program. Rabobank also made false and misleading statements to the OCC regarding the existence of reports developed by a third-party consultant, which detailed the deficiencies and resulting ineffectiveness of Rabobank's BSA/AML program.

To further conceal the inadequate nature of its BSA/AML program and to avoid "others contradicting our findings" and statements to the OCC, Rabobank demoted or terminated two RNA employees who were raising questions about the adequacy of Rabobank's BSA/AML program.

[j] *Mega International Commercial Bank—Failure to Maintain an Effective Program to Comply with BSA/AML Laws*

On January 17, 2018, the Federal Reserve Board announced a $29 million penalty against the U.S. operations of Mega International Commercial Bank Co., Ltd., of Taipei, Taiwan, for anti-money laundering violations and required the firm to improve its anti-money laundering oversight and controls. The Board took action because the firm's U.S. banking operations did not maintain an effective program to comply with the Bank Secrecy Act and anti-money laundering laws.

[k] *Citibank—Failure to Comply with Agency's Consent Order Related to BSA/AML Deficiencies*

On December 27, 2017, the OCC assessed a $70 million civil money penalty against Citibank, N.A., for failing to comply with the OCC's 2012 consent order related to BSA and AML deficiencies.

In its 2012 order, the OCC cited the bank for BSA violations, deficiencies in its compliance program, failing to file suspicious activity reports, and weaknesses in controls related to correspondent banking. In assessing this civil money penalty, the agency found that the bank has not achieved compliance with the OCC's 2012 order, failing to complete corrective actions to address BSA/AML compliance issues as required by the order.

[l] *Lone Star National Bank—Lack of BSA/AML Due Diligence*

On November 01, 2017, FinCEN announced the assessment of a $2 million civil money penalty against Lone Star National Bank (Lone Star) for willfully violating the BSA. Lone Star failed to comply with section 312 of the USA PATRIOT Act, which imposes specific due diligence obligations with respect to correspondent banking.

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

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

[m] *Deutsche Bank—Failure to Maintain an Effective Program to Comply With BSA and AML Laws*

On May 30, 2017, the Federal Reserve Board announced a $41 million penalty and consent cease and desist order against the U.S. operations of Deutsche Bank AG for anti-money laundering deficiencies.

The actions were taken by the Board to address unsafe and unsound practices at the firm's domestic banking operations. The Board identified failures by Deutsche Bank's U.S. banking operations to maintain an effective program to comply with the Bank Secrecy Act and anti-money laundering laws.

The consent order requires Deutsche Bank to improve its senior management oversight and controls related to compliance by the U.S. banking operations with anti-money laundering laws.

Deficiencies in Deutsche Bank's transaction monitoring capabilities prevented it from properly assessing BSA/AML risk for billions of dollars in potentially suspicious transactions processed between 2011 and 2015 for certain Deutsche Bank affiliates in Europe for which the affiliates failed to provide sufficiently accurate and complete information.

[n] *Merchants Bank of California—Inadequate Monitoring for BSA Compliance*

On February 27, 2017, FinCEN announced the assessment of a $7 million civil money penalty (CMP) against Merchants Bank of California of Carson, California, for willful violations of several provisions of the BSA. The OCC, the primary federal regulator of Merchants, identified deficiencies in the bank's practices that resulted in violations of previous consent orders entered into by Merchants, as well as other violations. The OCC simultaneously assessed a $1 million CMP against Merchants for these violations.

Merchants failed to (a) establish and implement an adequate AML program, (b) conduct required due diligence on its foreign correspondent accounts, and (c) detect and report suspicious activity. Merchants' failures allowed billions of dollars to flow through the U.S. financial system without effective monitoring to adequately detect and report suspicious activity. Many of these transactions were conducted on behalf of MSBs that were owned or managed by bank insiders who encouraged staff to process these transactions without question or face potential dismissal or retaliation. Bank insiders directly interfered with the BSA staff's attempts to investigate suspicious activity related to these insider-owned accounts.

"The banking of money services businesses is important to the global financial system, and we believe that banks can mitigate the risks associated with such businesses, just as they do with other customers," said FinCEN Acting Director Jamal El-Hindi. "But here we had an institution run by insiders essentially to provide banking services to MSBs that the insiders owned, combined with directions from Bank leadership to staff to ignore BSA requirements with respect to those MSB customers and others. It is certainly not an acceptable way to bank MSBs."

Merchants specialized in providing banking services for check-cashers and money transmitters. However, it provided those services without adequately assessing the money laundering risks and without designing an effective AML program. Merchants also provided its high-risk customers with remote deposit capture services without adequate procedures for monitoring their use.

Merchants failed to provide the necessary level of authority, independence, and responsibility to its BSA officer to ensure compliance with the BSA as required, and compliance staff was not empowered with sufficient authority to implement the bank's AML program. Merchants' leadership impeded BSA analysts and other employees from investigating activity on transactions associated with accounts that were affiliated with bank executives, and the activity in these accounts went unreported for many years. Merchants' interest in revenue compromised efforts to effectively manage and mitigate its deficiencies and risks.

In addition, Merchants banked customers located in several jurisdictions considered to be high-risk but did not identify these customers as foreign correspondent customers and therefore did not implement the required customer due diligence program. In a three-month period, Merchants processed a combined $192 million in high-risk wire transfers through some of these accounts.

[o] *Gibraltar Private Bank—Willful AML Compliance Violations*

In February 2016, FinCEN and the OCC assessed a $4 million CMP against Gibraltar Private Bank and Trust Company of Coral Gables, Florida, for willfully violating federal AML laws. Since first warned of its deficiencies in 2010, Gibraltar's compliance failures persisted until its primary regulator, the OCC, placed Gibraltar under a Consent Order in 2014. The OCC also issued a $2.5 million CMP against the bank.

Gibraltar's substantial AML program deficiencies led to its failure to monitor and detect suspicious activity despite red flags. These deficiencies ultimately caused Gibraltar to fail to timely file at least 120 SARs involving nearly $558 million in transactions occurring during 2009 to 2013. These deficiencies also unreasonably delayed Gibraltar's SAR reporting regarding accounts related to a $1.2 billion Ponzi scheme led by Florida attorney Scott Rothstein. Timely filed SARs play an important role in law enforcement's detection of criminal activity.

"We may never know how that scheme might have been disrupted had Gibraltar more rigorously complied with its obligations under the law. This bank's failure to implement and maintain an effective AML program exposed its customers, its banking peers, and our financial system to significant abuse," said FinCEN Director Jennifer Shasky Calvery.

Gibraltar's transaction monitoring system contained incomplete and inaccurate account opening information and customer risk profiles, which hindered its compliance staff from adequately spotting unusual account activity. Gibraltar also failed to sufficiently address an automated monitoring system that generated an unmanageable number of alerts, including large numbers of false positives, which caused significant delays in Gibraltar's review. Gibraltar also failed to properly train its compliance staff and failed to develop and implement an adequate customer identification program.

FinCEN coordinated its enforcement action with an action by the OCC. The assessment will be deemed satisfied by an immediate payment of $1.5 million to the U.S. Department of the Treasury and by paying $2.5 million in accordance with the penalty imposed by the OCC.

[p] *Bank of Mingo—Serious BSA Violations and Actions by a Branch Manager That Assisted Criminal Activity*

In June 2015, FinCEN and the FDIC assessed a $4.5 million civil money penalty against Bank of Mingo of Williamson, West Virginia (Mingo), for willfully violating the BSA. Mingo had severe and systemic failures in many aspects of its AML program. As a result of these failures, Mingo processed millions of dollars in structured and suspicious cash transactions through the institution.

Mingo serviced high-risk customers without effectively monitoring their accounts for suspicious activity. In one example, Mingo was aware of a high volume of unusual cash transactions conducted by a corporate customer, yet failed to file the requisite CTRs or SARs. That customer conducted over $9 million worth of structured transactions through Mingo's Williamson Branch. The manager of that branch, who is also the former Mayor of Williamson, was convicted in April 2014 of knowingly making a false statement to federal law enforcement agents during an investigation of that scheme to evade BSA reporting requirements.

"This bank's failure to implement and maintain an effective AML program exposed our financial system to significant abuse," said FinCEN Director Jennifer Shasky Calvery. "And, when a bank insider actively promotes a culture of noncompliance, the risks are greatly increased."

From 2008 through 2013, Mingo had significant deficiencies in all aspects of its AML program, including its internal controls, independent testing, training of personnel, and designation of a BSA officer with sufficient resources to adequately oversee its BSA compliance program. Mingo failed to properly assess the money laundering risk associated with its customers. Consequently, Mingo failed to properly designate many customers and their accounts as high risk and failed to adequately monitor and detect the unusual currency transactions or suspicious activities in which these customers engaged.

[q] *First National Community Bank of Dunmore—Failing to Report Suspicious Activity Tied to Judicial Corruption*

In February 2015, FinCEN and the OCC assessed a $1.5 million civil money penalty against the First National Community Bank of Dunmore, Pennsylvania (FNCB) for willfully violating the BSA. The bank admitted that it failed to file suspicious activity reports on transactions involving illicit proceeds from a judicial corruption scheme—spanning over five years—for which Michael Conahan and Mark Ciavarella, both former Pennsylvania judges, were ultimately convicted. Conahan and Ciavarella misused their positions as judges to profit from, among other things, sending thousands of juveniles to detention facilities in which they had a financial interest. Conahan was on FNCB's board of directors and controlled accounts at the bank through which he processed the proceeds of his illegal activity. Despite several red flags indicating suspicious activity, FNCB did not file a single suspicious activity report related to these accounts until after Conahan's first guilty plea in 2009.

"The criminal case affected the lives of thousands of children and parents," noted FinCEN Director Jennifer Shasky Calvery. "Banks have a duty to spot suspicious activity and to report it. Law enforcement relies on this valuable information. FNCB's failure to file timely suspicious activity reports may have deprived law enforcement of information valuable for tracking millions of dollars in related corrupt funds."

Conahan disguised his illegal proceeds through his FNCB accounts. The unreported suspicious transactions that flowed through Conahan's and other FNCB accounts displayed red flags that should have alerted FNCB to potential illicit activity and caused it to file suspicious activity reports. These red flags included:

(1) A 2007 law enforcement subpoena for information related to Conahan and other individuals and entities—although the bank responded to the subpoena, it did not conduct any further analysis or risk rate the accounts as required;

(2) Activity occurring as early as 2005 involving many large, round-dollar transactions often occurring on a single day; and

(3) An abnormal volume of activity compared to account balances. During this time, the bank failed to file suspicious activity reports on any of the accounts despite the numerous red flags.

[r] *North Dade Community Development Federal Credit Union—Failures in Managing High-Risk International Financial Activity*

In November 2014, FinCEN assessed a $300,000 civil money penalty against North Dade Community Development Federal Credit Union in Miami Gardens, Florida for significant BSA violations. North Dade's AML failures exposed the United States financial system to significant opportunities for money laundering and terrorist financing from known high-risk jurisdictions.

The credit union consented to the assessment and admitted that it willfully violated BSA program, reporting, and recordkeeping requirements. Included within these lapses, the credit union failed to comply with Section 314(a) of the USA PATRIOT Act, a program requiring financial institutions to search their records to locate accounts and transactions of persons that may be involved in terrorism or money laundering.

North Dade, a small credit union with $4 million in assets and only five employees, contracted with a third-party vendor and MSB to provide services and subaccounts to 56 MSBs located in high-risk jurisdictions far outside its field of membership, including locations in Central America, the Middle East, and Mexico. The revenue generated from

these accounts constituted 90 percent of North Dade's annual revenue. In 2013 alone, the total transaction volume through North Dade by MSBs included $1.01 billion in outgoing wires and $984 million in remotely captured deposits.

"When a small institution opens its doors to the world, takes on greater risks than it can manage, and puts profits before AML controls, bad actors are bound to take advantage," said FinCEN Director Jennifer Shasky Calvery. "This case raises pretty obvious questions that no one seems to have asked. Why would MSBs located all over the world choose a small Florida credit union to conduct close to $2 billion in transactions? Credit unions pride themselves on close and low-risk relationships with known neighborhood customers. However, North Dade welcomed customers far beyond its field of membership, without adequate policies and procedures to ensure AML compliance."

Director Shasky Calvery also expressed concern about North Dade's failure to comply with FinCEN's 314(a) program. "It is of great concern that North Dade failed to even review the 314(a) requests it received. These are time sensitive requests that, by their very nature, are intended to further criminal investigations into significant money laundering and terrorist financing activities."

From 2009 through 2014, North Dade had significant deficiencies in all aspects of its AML program, including its internal controls, independent testing, training, and failure to designate an appropriate BSA compliance officer. North Dade also had a systemic failure in meeting its 314(a) obligations. North Dade did not provide any meaningful risk assessment for its size and type of business and blindly relied on a third-party vendor to conduct due diligence for all 56 MSBs, which held subaccounts at North Dade. Without itself knowing or understanding its customers or risks, North Dade was unable to adequately monitor, detect, or report significant suspicious transactions and other activities taking place through the credit union, including those related to money laundering and drug trafficking. When the credit union did file suspicious activity reports, the reports were often late and insufficient.

[s] *Bethex Federal Credit Union—Failures in Managing High-Risk International Financial Activity*

Bethex Federal Credit Union was a federally chartered, low-income designated, community development credit union. In December 2015, the NCUA liquidated Bethex, determining that the credit union was insolvent with no prospects of returning to viable operations on its own. FinCEN's penalty is a claim against any assets that remain after the completion of Bethex's liquidation.

Since 2002, Bethex's AML program maintained internal controls specific for low- to moderate-income clientele within its designated field of membership in New York City. In 2011, Bethex began providing banking services to many wholesale, commercial MSBs. Many of these MSBs were located in high-risk jurisdictions outside New York and engaged in high-risk activity, including wiring millions of dollars per month to countries at risk for money laundering. When Bethex began to service these MSBs, it did not take steps to update its AML programs. As a result, Bethex was unable to adequately monitor, detect, and report suspicious activity or mitigate the associated risks, leaving the credit union particularly vulnerable to money laundering.

Among other violations, Bethex failed to timely detect and report suspicious activity to FinCEN and did not file any SARs from 2008 through 2011. In 2013, as a result of a mandated review of previous transactions, it late-filed 28 SARs. The majority of the suspicious activity involved high-volume, large amount transfers outside of Bethex's expected customer base by MSBs capable of exploiting Bethex's AML weaknesses. Most of the SARs were inadequate and contained short, vague narratives encompassing a broad summary of multiple and unrelated instances of suspicious activity. For example, one SAR covered over $906 million in total aggregate of suspicious transactions, but provided little information useful to law enforcement investigators.

[t] *January 7, 2014, JPMorgan/Chase Admits Violation of the BSA for Failed Madoff Oversight; Fined $461 Million by FinCEN*

FinCEN fined J.P. Morgan Chase Bank, N.A. $461 million for willfully violating the BSA by failing to report suspicious transactions arising out of Bernard L. Madoff's decades-long, multi-billion dollar fraudulent investment scheme. In consenting to the assessment of a civil money penalty, JPMorgan admitted to the facts set forth by FinCEN and that its conduct violated the Bank Secrecy Act.

"When JPMorgan suspected Mr. Madoff's fraud, it focused on its own investment exposure and saved itself approximately $250 million," noted FinCEN Director Jennifer Shasky Calvery. "If it had given the same attention to its anti-money laundering responsibilities, it could have saved itself $2 billion, and potentially saved thousands of other fraud victims untold misery and loss."

From the 1970s until he was arrested in December 2008, Bernard L. Madoff committed a massive securities fraud scheme against investors that resulted in more than $20 billion in losses to thousands of victims. JPMorgan, its predecessors and affiliates, had a long relationship with Bernard L. Madoff Investment Securities LLC (BLM), including holding the primary bank accounts in the United States used by BLM to facilitate its fraudulent investment scheme. In addition, from 2006 to 2008, JPMorgan also made its own investments in BLM's so-called "feeder funds."

In 2007, JPMorgan had concerns that BLM could be engaged in fraud that culminated in the identification of several red flags by 2008. These red flags included:

(1) BLM's investment performance appeared too good to be true;

(2) BLM's trading techniques and investment activity lacked expected transparency;

(3) BLM used a small, unknown auditor; and

(4) BLM repeatedly refused to provide full information to JPMorgan as part of its due diligence reviews.

In the Fall of 2008, JPMorgan took steps to protect its own business interests yet failed to notify FinCEN of the same suspicious, potentially fraudulent, activities and failed to file any SAR with FinCEN as required by the BSA.

In October 2008, JPMorgan filed a SAR-equivalent with FinCEN's counterpart in the United Kingdom, the Serious Organised Crime Agency, identifying their concerns about potential fraud. JPMorgan did not file a SAR with FinCEN until after Mr. Madoff's arrest in December 2008. During the intervening time, JPMorgan redeemed approximately $275 million of its own investments from the BLM feeder funds, which in turn drew the funds out of BLM's JPMorgan accounts in the United States. Mr. Madoff also drained billions of dollars out of BLM's JPMorgan accounts during this time period. When Mr. Madoff was arrested on December 11, 2008, JPMorgan booked a loss of approximately $40 million, substantially less than it would have lost but for its transactions in the Fall of 2008.

FinCEN worked in coordination with the U.S. Attorney's Office for the Southern District of New York (SDNY) and the OCC. FinCEN has determined that the penalty in its matter will be $461 million, based on the suspicious transactions that flowed through Mr. Madoff's primary account at JPMorgan during 2008. The OCC will collect a $350 million fine. SDNY will collect $1.7 billion through asset forfeiture and has stated that the funds collected will be contributed to the recovery fund for Mr. Madoff's victims. To ensure the maximum amount of money for the victims, FinCEN deemed its penalty satisfied by JPMorgan's payment to SDNY. In total, JPMorgan has agreed to a combined collection amount of $2.05 billion.

[u] ***September 23, 2013, FinCEN Fines TD Bank for Failing to Report Nearly $1 Billion in Suspicious Transactions Related to Florida Ponzi Scheme***

FinCEN assessed a $37.5 million civil money penalty against TD Bank, N.A. for failure to file suspicious activity reports related to the massive Ponzi scheme orchestrated by Florida attorney Scott Rothstein. The Office of the Comptroller of the Currency also announced the assessment of a concurrent $37.5 million penalty against the bank for related violations. Additionally, the Securities and Exchange Commission has assessed a separate $15 million penalty against the bank for related securities violations.

From April 2008 through September 2009, the bank willfully violated the Bank Secrecy Act's reporting requirements by failing to detect and adequately report suspicious activities in a timely manner. During that period, Rothstein orchestrated a major Ponzi scheme by fraudulently inducing victims to invest in purported settlements involving whistleblower and sexual harassment lawsuits. Thousands of transactions flowed through his multiple law firm accounts at TD Bank which included transactions related to Rothstein's Ponzi scheme. While the Rothstein law firm's accounts alerted in TD Bank's anti-money laundering surveillance software for suspicious activity, TD Bank employees failed to recognize the suspicious activity and file SARs in a timely manner. On January 27, 2010, Rothstein pleaded guilty to a racketeering conspiracy in the United States District Court for the Southern District of Florida and is currently serving a 50-year prison sentence.

In 2011, the bank conducted a review of the Rothstein transactions. Based on the results of the review it filed five late suspicious activity reports, totaling an estimated $900 million in aggregate suspicious transaction activity occurring between April 2008 and October 2009. A lack of adequate training for both the anti-money laundering and business staff contributed to the failure to recognize this suspicious activity.

"In the face of repeated alerts on Mr. Rothstein's accounts by the Bank's anti-money laundering surveillance software over an 18 month period, the Bank did not do enough to prevent the pain and financial suffering of innocent

investors," FinCEN Director Jennifer Shasky Calvery stated. "Financial institutions must do a better job of protecting our financial system and citizens from such harm. It is not acceptable to have a poorly resourced and trained staff overseeing such a critical function."

[v] *September 24, 2013, FinCEN Penalizes New Jersey Community Bank for Risky Dealings with Foreign Money Exchanges*

FinCEN assessed a $4.1 million civil money penalty against Saddle River Valley Bank in Saddle River, New Jersey. FinCEN has determined that the bank violated several provisions of the BSA from 2009 through May 2011. The Bank has consented to the assessment.

Working with the OCC and the U.S. Attorney's Office for the District of New Jersey, FinCEN concluded that the bank willfully violated aspects of the BSA's program, recordkeeping, and reporting requirements by lacking an effective AML program reasonably designed to manage the risks of money laundering and other illicit activity, failing to conduct adequate due diligence on foreign correspondent accounts, and failing to detect and adequately report in a timely manner suspicious activities in the accounts of foreign money exchange houses, also known as casas de cambio. The bank executed $1.5 billion worth of inadequately monitored transactions on behalf of Mexican and Dominican casas de cambio despite publicly available information, such as a FinCEN advisory, that provided ample notice of the heightened risks of dealing with these institutions.

"It's pretty remarkable that a small community bank in suburban New Jersey was attracting more than a billion dollars in transactions with customers in Mexico and the Dominican Republic, and nobody thought it was too good to be true," FinCEN Director Jennifer Shasky Calvery said. "Banks of all sizes, in any part of the country, may be tempted by such lucrative ventures. However, banks must use common sense in evaluating customer risk or seemingly lucrative business could become quite the opposite."

FinCEN's penalty is concurrent with a $4.1 million civil money penalty assessed by the OCC and will be satisfied by one payment of $4.1 million to the U.S. Department of the Treasury. In addition, the U.S. Attorney's Office for the District of New Jersey will collect $4.1 million from the bank through civil asset forfeiture. The bank ceased operations in 2012 and the combined collection amount of $8.2 million represents the majority of its remaining assets.

[w] *HSBC—Lack of Effective AML Program; Failure to Conduct Due Diligence on Certain Foreign Correspondent Accounts; Failure to Detect and Adequately Report Evidence of Money Laundering and Other Illicit Activity*

On December 11, 2012, the U.S. Department of the Treasury reached settlements amounting to $875 million with HSBC Holdings plc (together with its affiliates, HSBC). The Treasury Department's collective settlement, reached by FinCEN, the OCC, and the Office of Foreign Assets Control (OFAC). In total, more than $1.9 billion were assessed in penalties for HSBC's conduct in violation of the BSA and U.S. sanctions.

The bank's breakdowns in AML compliance were particularly egregious because these failures allowed hundreds of millions of dollars from Mexican drug trafficking organizations to flow through accounts in the United States. Despite HSBC's extensive global operations and the substantial resources it had available to manage transnational risk, it failed to help secure the United States financial borders and left dangerous gaps that international drug dealers and other criminals readily abused. The penalties reflect the damage to the integrity of the U.S. financial system inflicted by HSBC, and the federal government's intolerance of behavior and business practices that disregard BSA requirements and U.S. sanctions regimes.

"These settlements implicate willful and dangerous practices by one of the world's biggest banks," said Under Secretary for Terrorism and Financial Intelligence David S. Cohen. "HSBC absolutely knew the risks of the business it pursued, yet it ignored specific, obvious warnings. Its failures allowed hundreds of millions of dollars in drug money to pass through its unattended gates."

The OCC and FinCEN announced separate assessments of $500 million CMP against HSBC Bank USA N.A. (HBUS), McLean, Virginia for BSA violations. The OCC CMP is being levied for failure to comply fully with a remedial order addressing these violations, issued by the OCC in 2010. Both of these penalties will be deemed satisfied by a single payment of $500 million to the Treasury Department. OFAC also reached an additional $375 million agreement with HSBC to settle potential liability for apparent violations of U.S. sanctions that will be deemed satisfied by payment of an equal amount to the Department of Justice for the same pattern of conduct.

Since at least mid-2006, the bank lacked an effective risk-based AML program reasonably designed to manage risks of money laundering or other illicit activity, given the bank's products, services, transaction volume, scope of business activities, geographic reach, and customers. The bank's prolonged systemic failures to comply with BSA suspicious activity reporting requirements resulted in the failure to detect and adequately report evidence of money laundering and other illicit activity.

HBUS's ineffective AML program exposed the U.S. financial system to severe criminal abuse. From 2002 until 2009, despite obvious information to the contrary, the bank rated Mexico as having "standard" money laundering risk, the lowest of the bank's four possible country risk ratings. As a result of ratings like this, hundreds of billions of dollars in wire transactions from Mexico were excluded from the bank's internal AML reviews. Additionally, from 2006 through 2009, the bank did not monitor bulk cash transactions conducted with its Mexican and other foreign affiliates and took delivery of more than $15 billion in cash. In 2006, FinCEN alerted all U.S. financial institutions about money laundering risks associated with United States/Mexico cross-border cash and warned that cash from illegal drug trafficking was being smuggled into Mexico, placed into financial institutions, and then returned to the United States.

Similarly, the bank maintained correspondent accounts for affiliates around the world and did not collect or maintain, as the BSA requires, any customer due diligence information regarding these relationships. As a consequence, many foreign financial institutions and their customers effectively gained unmonitored access to the U.S. financial system without appropriate safeguards against illicit financial activity.

These AML compliance failures meant that the bank did not and could not reliably detect and report suspicious activity and therefore deprived law enforcement and regulators of critical information used to combat money laundering, terrorist finance, transnational organized crime, and other domestic and global financial threats.

OFAC's settlement resolves an investigation into HSBC's apparent violations of the Iranian Transactions Regulations (ITR), 31 C.F.R. part 560; the Burmese Sanctions Regulations (BSR), 31 C.F.R. part 537; the Sudanese Sanctions Regulations (SSR), 31 C.F.R. part 538; the Cuban Assets Control Regulations (CACR), 31 C.F.R. part 515; and the Libyan Sanctions Regulations (LSR), 31 C.F.R. part 550 (which were in effect until 2004).

For a number of years, up to and including 2007, HSBC affiliates in Europe, the Middle East, and Asia processed transactions through U.S. financial institutions that involved countries, entities, or individuals subject to U.S. sanctions. HSBC Group's London head office and Dubai branch engaged in payment practices that interfered with the implementation of U.S. economic sanctions by financial institutions in the United States, including HBUS. Payment practices included the use of Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment messages in a manner that obscured references implicating U.S. sanctions, removal of information from SWIFT messages, and forwarding of payment messages to U.S. financial institutions that falsely referenced an HSBC affiliate as the ordering institution. As a result, payments totaling approximately $430 million were routed through U.S. banks for or on behalf of sanctioned parties in apparent violation of U.S. sanctions.

The Financial Crimes Enforcement Network has determined that HBUS willfully violated the Bank Secrecy Act since at least mid-2006 by:

(1) lacking an effective anti-money laundering program reasonably designed to manage risks of money laundering and other illicit activity, in violation of Title 31, United States Code, Section 5318(h) and 31 C.F.R. § 1020.210;

(2) failing to conduct due diligence on certain foreign correspondent accounts, in violation of Title 31, United States Code, Section 5318(i) and 31 C.F.R. § 1010.610; and

(3) failing to detect and adequately report evidence of money laundering and other illicit activity, in violation of Title 31, United States Code, Section 5318(g) and 31 C.F.R. § 1020.320.

– Violation of the Requirement to Implement an Adequate Anti-Money Laundering Program

HBUS violated the Bank Secrecy Act's anti-money laundering program requirements by:

(i) conducting business without adequate internal controls,

(ii) failing to conduct adequate independent testing for compliance, and

(iii) failing to staff its Bank Secrecy Act compliance program with a reasonably sufficient number of qualified personnel.

(i) HBUS failed to provide for an adequate system of internal controls to ensure ongoing compliance.

HBUS provided a full range of consumer and commercial products and services to individuals, corporations, financial institutions, non-profit organizations, and governments in the United States and abroad, including in jurisdictions with weak anti-money laundering and counter-terrorist financing ("AML/CFT") controls. HBUS did not effectively conduct enterprise-wide, risk-based assessments of potential money laundering risks, given its products, clients, and geographic reach, and HBUS failed to adequately identify potential money laundering vulnerabilities. The Bank's failure to adequately assess risk negatively impacted the effectiveness of its transaction monitoring, which already suffered from additional systemic weaknesses.

Product Risk. Some of the Bank's products and services involved significant anti-money laundering risks, including but not limited to: correspondent accounts, embassy banking, wire transfers, automated clearinghouse ("ACH") transfers, banknotes, lockboxes, clearing of bulk traveler's checks, bearer share accounts, pre-paid cards, foreign exchange, cash letters, international pouch activity, and remote deposit capture. HBUS failed to take appropriate steps to adequately assess the AML/CFT risks posed with respect to many of its products and services.

For instance, the Bank failed to manage money laundering risks associated with its pouch services and did not provide for appropriate controls and monitoring to address the underlying risks posed by this transaction activity. In one example, until November 2008, the Bank cleared traveler's checks received from a foreign respondent bank without monitoring systems in place that were reasonably designed to detect, investigate, and report evidence of money laundering. Several individuals purchased sequentially numbered traveler's checks at a Russian bank in transactions totaling more than $290 million over several years. These traveler's checks were signed in a uniform illegible scrawl and made payable to approximately 30 different customers of a Japanese bank. The Japanese bank was a HBUS correspondent customer and for several years regularly delivered multi-hundred-thousand-dollar batches of these sequentially numbered traveler's checks to HBUS via pouch. During the relevant period of time, HBUS knew or should have known that uniformly signed, sequentially numbered traveler's checks in such high volume are a money laundering "red flag."

Customer Risk. The Bank's written policies, procedures, and controls did not effectively risk rate customers. The Bank's risk rating methodologies were not designed to evaluate customers based on specific customer information and balanced consideration of all relevant factors, including country/jurisdictional risk, products and services provided, expected transaction volume, and nature of customer profiles. Failure to consistently gather reasonably accurate and complete customer documentation undermined the Bank's ability to conduct customer risk assessments. These deficiencies prevented the Bank from performing adequate analysis of the risks associated with particular customers and from determining whether transactions lacked an apparent business or lawful purpose or fell within the particular customer's normal and expected range of conduct.

For example, Group affiliate HSBC Mexico S.A. Banco ("HBMX") was an HBUS respondent bank. The account that HBMX maintained with HBUS accepted bulk deposits of U.S. currency and processed wire transfers. HBMX operated in Mexico, a country that was the subject of publicly available cautionary information about drug trafficking and money laundering vulnerabilities. HBMX's branch in the Cayman Islands operated under a Cayman Islands Monetary Authority license limiting authority to do business to non-residents of the Cayman Islands. Potentially high-risk Mexican casas de cambio and other money transmitter and dollar-exchange businesses were HBMX customers. Despite these risks, until 2009, HBUS treated HBMX as a "standard"

(Text continued on page 1-22.3)

Chapter 2

Suspicious Activity Reporting Requirements

Synopsis

§ 2.01 COMPLIANCE CHECKLISTS

The following checklist is a list of actions, related to suspicious activities, that are encouraged by the regulatory agencies to help ensure an adequate system for the monitoring and reporting of suspicious activities, even though they may not be specifically required by regulation.

	Suspicious Activity Reporting	Yes	No	N/A
1.	Based on a review of Suspicious Activity Reports (SARs), do any accounts or functional areas of the bank require further investigation?			
2.	If so, are there any weaknesses in these areas that require strengthening to address suspicious activities that are taking place?			
3.	Should any additional SARs be filed for any suspicious activity noted during the review?			
4.	Based on a review of various reports for any transactions that appeared suspicious and met the reporting threshold, was a Suspicious Activity Report filed? OCC (national banks): 12 CFR 21.11; OCC (federal savings associations): 12 CFR 180; Federal Reserve (state member banks): 12 CFR 208.62; FDIC (state nonmember banks and savings banks): 12 CFR 353.3; FDIC (state savings associations): 12 CFR 390.355; NCUA (credit unions): 12 CFR 748.1(c)			
5.	Based on a review of correspondent accounts for any transactions that appeared suspicious and met the reporting threshold, was a Suspicious Activity Report filed? OCC (national banks): 12 CFR 21.11; OCC (federal savings associations): 12 CFR 180; Federal Reserve (state member banks): 12 CFR 208.62; FDIC (state nonmember banks and savings banks): 12 CFR 353.3; FDIC (state savings associations): 12 CFR 390.355; NCUA (credit unions): 12 CFR 748.1(c)			
6.	Based on a review of a sample of SARs that were filed:			
	• Was the SAR filed within 30 calendar days after determining a SAR was required (or within 60 days if needed to attempt to identify a suspect)? OCC (national banks): 12 CFR 21.11(b); OCC (federal savings associations): 12 CFR 180(b); Federal Reserve (state member banks): 12 CFR 208.62(b); FDIC (state nonmember banks and savings banks): 12 CFR 353.3(b); FDIC (state savings associations): 12 CFR 390.355(b); NCUA (credit unions): 12 CFR 748.1(c)			
	• Does the institution retain a copy of the SAR and any supporting documentation for five years? OCC (national banks): 12 CFR 21.11(e); OCC (federal savings associations): 12 CFR 180(e); Federal Reserve (state member banks): 12 CFR 208.62(e); FDIC (state nonmember banks and savings banks): 12 CFR 353.3(e); FDIC (state savings associations): 12 CFR 390.355(e); NCUA (credit unions): 12 CFR 748.1(c)			
	• Did management of the institution promptly notify its Board of Directors, or a committee of the board, that the SAR was filed? OCC (national banks): 12 CFR 21.11(f); OCC (federal savings associations): 12 CFR 180(f); Federal Reserve (state member banks): 12 CFR 208.62(f); FDIC (state nonmember banks and savings banks): 12 CFR 353.3(f); FDIC (state savings associations): 12 CFR 390.355(f); NCUA (credit unions): 12 CFR 748.1(c)			
	• Did the institution keep the filing of the SAR confidential? OCC (national banks): 12 CFR 21.11(e); OCC (federal savings associations): 12 CFR 180(g); Federal Reserve (state member banks): 12 CFR 208.62(g); FDIC (state nonmember banks and savings banks): 12 CFR 353.3(g); FDIC (state savings associations): 12 CFR 390.355(g); NCUA (credit unions): 12 CFR 748.1(c)			

Comments:

Suspicious Activity Reports	Yes	No	N/A
1. Does the institution have an individual responsible for preparing and filing Suspicious Activity Reports (SARs)?			
2. Does the institution conduct employee training regarding Suspicious Activity Reports?			
3. Does the institution have a process for ensuring that transaction amounts are consistent with the type and nature of the business or occupation of the customer?			
4. Does the institution have a process for reviewing accounts that are exempted from Currency Transaction Report (CTR) reporting for unusual or suspicious activity?			
5. Does the institution have a process for establishing expected activity levels (for example, historical transaction pattern or input from client or bank officer), including who has the authority to change profiles?			
6. Does the institution have a process for reconciling activity levels of higher-risk accounts against expected activity to ensure that activity levels are reasonable?			
7. Does the institution have a system for reviewing exception reports and determining what parameters are used to filter exceptions?			
8. Does the institution have a process for requesting timely and adequate explanations of activity generated by monitoring reports?			
9. Does the institution have a system for ensuring exception reports are responded to in a timely manner, and are utilized and maintained by appropriate parties to assist in detecting patterns of unusual activity?			
10. Does the institution have a system (automated or manual) to detect structured transactions (both cash in and cash out) that are under the $10,000 reporting threshold?			
11. Does the institution review a listing of the CTRs that have been filed to determine if the institution or any branches had significant changes in the volume or nature of CTRs filed?			
12. Does the institution review the Suspicious Activity Reports related to money laundering it has filed to determine if the institution or any branches had significant changes in the volume or nature of SARs filed, and does it investigate the reasons for any change?			
13. Does the institution review cash shipment reports to determine if there are any unusual trends in the volume or composition of cash shipments?			
14. Does the institution have procedures for documentation of decisions not to file a SAR?			
Comments:			

Information Sharing with Law Enforcement (Section 314(a) of the USA PATRIOT Act)	Yes	No	N/A
1. Does the institution have adequate policies and procedures for receiving and responding to requests from the Financial Crimes Enforcement Network (FinCEN)?			
2. Has the financial institution designated one person to be the point of contact at the institution regarding information requests and any other contact information requested by FinCEN? 31 CFR 1010.520(b)(2)(iii)			
3. If any of the contact information has changed, did the financial institution promptly notify FinCEN of the changes? 31 CFR 1010.520(b)(2)(iii)			
4. For any requests received from FinCEN for information under the rule, did the institution "expeditiously" (or within the time period required in the request) search the required records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FinCEN's request? 31 CFR 1010.520(b)(2)(i)			
5. In response to the request, unless otherwise provided in the request itself, did the institution search its records for: 31 CFR 1010.520(b)(2)(i)			

	• Any current account maintained for a named suspect;				
	• Any account maintained for a named suspect during the preceding *12 months*; and				
	• Any transaction conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmittor or the recipient, during the preceding *six months* that is contained in the wire transfer log, the log of purchase/sales of monetary instruments, and any other transaction records that can be searched electronically?				
6.	If, as a result of the searches, the financial institution did find an account or transaction with any of the individuals or entities, did the institution report the following information to FinCEN, within the time frame specified in the request: 31 CFR 1010.520(b)(2)(ii)				
	• The name of the individual, entity, or organization;				
	• The number of each account, or in the case of a transaction, the date and type of each transaction; and				
	• Any social security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each account was opened or each transaction was conducted?				
7.	Did the institution use the information only for the purpose of: 31 CFR 1010.520(b)(2)(iv)				
	• Reporting to FinCEN as required by the rule;				
	• Determining whether to establish or maintain an account, or to engage in a transaction; or				
	• Assisting the financial institution in complying with any requirement of the rule?				
8.	Review the financial institution's documentation (including account analysis) to evaluate how the financial institution determined whether or not a SAR was warranted.				
9.	If the financial institution uses a third-party vendor to perform or facilitate searches, is there is an agreement and/or procedures to ensure confidentiality?				
Comments:					

Information Sharing Among Financial Institutions (Section 314(b) of the USA PATRIOT Act)	**Yes**	**No**	**N/A**
NOTE: Participation in this information sharing is voluntary, and the following procedures should be performed only if the institution intends to share information with other institutions or associations regarding potential money laundering or terrorist activities.			
1. Does the institution have adequate policies and procedures for receiving and responding to FinCEN requests?			
2. Before engaging in the sharing of information with other financial institutions or associations, did the institution file the required notice with FinCEN (or a certification with FinCEN under the interim rules)? 31 CFR 1010.540(b)(2)			
3. Does the institution submit a new certification each year? 31 CFR 1010.540(b)(2)			
4. Does the institution only share information under the rule regarding individuals, entities, organizations, and countries for purposes of detecting, identifying, or reporting activities that the financial institution or association suspects may involve possible money laundering or terrorist activities? 31 CFR 1010.540(b)(1)			
5. Before sharing information under the rule, does the institution take reasonable steps to verify that the other financial institution or association has also submitted the required notice to FinCEN? 31 CFR 1010.540(b)(3)			
6. With respect to any information received as a result of sharing information under the rule, did the institution use the information for no other purpose other than: 31 CFR 1010.540(b)(4)(i)			
• Identifying and, where appropriate, reporting on money laundering or terrorist activities;			

	• Determining whether to establish or maintain an account, or to engage in a transaction; or			
	• Assisting the financial institution in complying with any requirement of the Bank Secrecy Act (BSA) rules?			
7.	Does the institution only share information regarding individuals, entities, organizations, and countries for purposes of detecting, identifying, or reporting activities that the financial institution or association suspects may involve possible money laundering or terrorist activities? 31 CFR 1010.540(b)(1)			
8.	Does the institution maintain adequate procedures to protect the security and confidentiality of the information? 31 CFR 1010.540(b)(4)(ii)			
9.	If, as a result of information sharing under the rule, the institution suspected that someone is or may be involved in terrorist activity, was the information reported on a SAR and/or otherwise as required? 31 CFR 1010.540(c)			
10.	Review the financial institution's documentation (including account analysis) to evaluate how the financial institution determined whether or not a SAR was warranted.			

Comments:

Because money is the basis for criminal activity or, in the case of terrorism, is an integral part of the activity, the United States government has made it a priority to pursue the funds that are generated by or used in these activities. Since financial institutions occupy a critical position in the U. S. financial system, the government not only requires financial institutions to report information, it *requires them to be proactive* in looking for transactions that may be part of a criminal activity.

In particular, this responsibility takes the form of the Suspicious Activity Report (SAR). This report is required under 31 USC 5318(g) as part of the Bank Secrecy Act (BSA). All of the banking regulatory agencies and the National Credit Union Administration (NCUA) have adopted identical regulations to implement this requirement. The regulations can be found at:

- Office of the Comptroller of the Currency (OCC) (national banks): 12 CFR 21.11
- OCC (federal savings associations): 12 CFR 163.180
- Federal Reserve (state member banks): 12 CFR 208.62
- Federal Deposit Insurance Corporation (FDIC) (state nonmember banks and savings banks): 12 CFR 353
- FDIC (state savings associations): 12 CFR 390.355
- NCUA (credit unions): 12 CFR 748.1(c)

All SARs must be filed electronically. The electronic SAR form and its embedded instructions are accessed at the Financial Crimes Enforcement Network (FinCEN) web site, www.fincen.gov, under the BSA E-Filing tab. A sample of the electronic form is available as Exhibit 2.1.

The law and regulations make it clear that an effective BSA compliance program includes controls and measures to identify and report suspicious transactions in a timely manner. A financial institution must apply due diligence to be able to make an informed decision about the suspicious nature of a particular transaction and whether to file a suspicious SAR.

§ 2.02 WHEN A SAR IS REQUIRED

[1] In General

The SAR is the primary method by which financial institutions are to report suspected criminal activity. However, it is not the only means. There are, of course, instances requiring more immediate attention, such as when a reportable violation is occurring, the financial institution must immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities.

One area that has become extremely important is terrorism. To facilitate the reporting of suspected terrorist activities, the FinCEN established a Financial Institutions Hotline, (866) 556-3974, for financial institutions to voluntarily report to law enforcement suspicious transactions that may relate to terrorist activity against the United States. This hotline is operational seven days a week, 24 hours a day.

However, financial institutions need to be aware that contacting law enforcement directly, whether about terrorism or anything else, does not eliminate the need to file a SAR. A SAR must be filed when required, even if law enforcement was contacted by telephone.

The agencies' SAR regulations mandate that a SAR must be filed for:

- Insider abuse involving any amount.
- Violations of federal law aggregating $5,000 or more when a suspect can be identified.
- Violations of federal law aggregating $25,000 or more regardless of a potential suspect.
- Transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA if the institution knows, suspects, or has reason to suspect that the transaction:
  - — May involve funds from illegal activities or is intended or conducted to hide or disguise illicit funds or assets as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under federal law;
  - — Is designed to evade any of the BSA regulations; or
  - — Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

[2] Money Laundering and Terrorist Financing Red Flags

Money laundering and terrorist financing are two areas of suspicious activity of most importance to the federal government. Therefore, the regulatory agencies have published a list of "red flags" of activities that may be suspicious for these two areas. This list is contained in Appendix F to the agencies' *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual* and is reproduced as Exhibit 2.5.

[3] Suspicious Activity Without a Loss to the Institution

One issue that arises is the SAR filing implications when an institution discovered suspicious activity without suffering a financial loss. FinCEN reminds institutions that although the SAR form has a field to indicate the amount of loss (if applicable), whether an institution suffers a loss is irrelevant to the determination of whether or not suspicious activity has occurred. For example, when cash deposits exceeding applicable thresholds are structured to avoid reporting requirements, the institution most likely will not suffer a loss, but it is required nonetheless to report such activity.

[4] Suspicious Activity at a Location Other Than the Institution

Financial institutions are required to file SARs on suspicious activity even when a portion of the activity occurs outside of the United States or the funds involved in the activity originated from outside the United States. Although foreign-located operations of U.S. organizations are not required to file SARs, an organization may wish, for example, to file a SAR with regard to suspicious activity that occurs outside of the United States when that activity is so egregious that it can potentially cause harm to the entire organization. It is, of course, expected that foreign-located operations of U.S. organizations that identify suspicious activity will report such activity consistent with local reporting requirements in the foreign jurisdiction where the operation is located.

Institutions also frequently are unsure about how to complete a SAR when the suspicious activity occurred at a location other than the financial institution or any of its branches. By requiring the reporting of transactions "conducted or attempted by, at, or through" an institution, FinCEN recognizes that reportable activity does not necessarily happen at an institution's physical location. For example, a bank debit or credit card may be stolen and then used at retail locations to purchase goods or services, but never used at the institution. Such transactions would correctly be characterized as "conducted through" the bank, and assuming appropriate thresholds were met, would require reporting.

When suspicious activity occurs at a location other than the institution, the institution should not put the actual location of the activity in the SAR fields normally used to indicate where activity occurred. Instead, because these fields often are used by law enforcement to determine where supporting documentation is maintained, an institution should list the location of its supporting documentation and records as the address in this field. In the SAR narrative, the institution should indicate that this address is not the location of the activity, but rather where the records are being kept. Any available information about the actual location of the suspicious activity, including (for the example above) the names of the retail businesses, addresses, and contact information, should also be included in the narrative. The SAR should be completed in this manner for any type of reportable suspicious activity occurring somewhere other than the financial institution. For all other transactions that occurred at the financial institution, normal filing procedures should be followed.

[5] Exceptions

There are a few instances where the filing of a SAR is not required, even though they otherwise meet the SAR reporting thresholds. Under the rules, a financial institution need not file a SAR in the case of:

- A robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities; or
- For lost, missing, counterfeit, or stolen securities if the institution files a report under the reporting requirements of 17 CFR 240.17f-1.

§ 2.03 SAR FILINGS AND BSA ENFORCEMENT

[1] In General

An institution's failure to file SARs with respect to transactions the regulatory agencies believe to be suspicious has become a major focus of BSA examinations. In OCC Bulletin 2004-50, the OCC laid out its criteria for citing violations of the SAR filing requirements, which are similar to those of the other agencies.

The OCC stated that it will cite a violation of the SAR regulation if a bank's failure to file a SAR (or SARs) is:

- Accompanied by evidence of bad faith,
- Represents a significant or egregious situation,
- Involves a pattern or practice, or
- Otherwise evidences a systemic breakdown.

The OCC recognizes that the decision to file a SAR is an inherently subjective judgment, and a bank should not be cited for a violation if and when it fails to file a SAR in an isolated circumstance, unless the failure is significant or accompanied by evidence of bad faith, provided that the bank otherwise has adequate systems and controls in place. Before citing a violation, examiners will consider the:

- Severity of violations,
- Time span of violations,
- Frequency or isolated nature of violations, and
- Related findings on prior examinations.

When violations are cited or deficiencies are noted, examiners will consider whether the bank's BSA compliance program is also a problem and will determine whether civil money penalties and/or a referral to FinCEN is appropriate.

On a related note, one of the concerns with respect to SAR filing violations has been that examiners may be using peer group SAR filing numbers to determine if a financial institution is filing "enough" SARs.

[2] In Response to These Concerns

The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal

(Text continued on page 2-11)

[iv] *SAR Narrative*

FinCEN also requests that filers further detail how the suspicious activity relates to environmental crimes. Filers should provide any available details concerning how the illicit product, plant, or waste was solicited, acquired, stored, transported, financed, and paid for. Filers also should provide all available details (such as names, identifiers, and contact information—including internet protocol (IP) and email addresses and phone numbers) regarding:

- Any actual purchasers or sellers of the illicit product, plant, waste or waste disposal services, and their intermediaries or agents
- Volume and dollar amount of the transactions involving an entity that is—or may be functioning as—a supplier of illicit products, plants, waste or waste services
- Any beneficial owner(s) of involved entities (such as shell companies)

In the case of illicit waste, filers should provide all available details and specific descriptions of the waste product and any known details about its origin, transport, and destination. If known, filers should provide information about the place(s) where the reported individuals or entities are operating.

[o] *FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting U.S. Mail*

On February 27, 2023, FinCEN issued an alert to financial institutions on the nationwide surge in check fraud schemes targeting the U.S. mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and is one of the AML/CFT National Priorities. In coordination with the United States Postal Inspection Service (USPIS), FinCEN identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to mail theft-related check fraud.

"FinCEN is proud to partner with the United States Postal Inspection Service in producing this important and timely alert on mail theft-related check fraud designed to assist financial institutions in reversing this disturbing trend," said Acting Director Himamauli Das. "Their vigilance and timely reporting will help law enforcement identify illicit actors who steal mail with the goal of defrauding innocent American taxpayers and businesses."

Criminals have been increasingly targeting the U.S. mail and United States Postal Service mail carriers since the COVID-19 pandemic to commit check fraud. Criminals typically steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Following the initial theft and fraudulent negotiation of the stolen checks, criminals may continue to exploit their victims by using the personal identifiable information found in the stolen mail for future fraud schemes, such as credit card fraud or credit account fraud.

BSA reporting for check fraud has increased significantly in the last three years. In 2021, financial institutions filed over 350,000 SARs to report potential check fraud, a 23 percent increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double from the previous year's number of filings.

In addition to filing a SAR, as applicable, when suspecting this type of fraud, financial institutions should refer their customers who may be victims of mail theft-related check fraud to the USPIS at 1-877-876-2455 or https://www.uspis.gov/report.

[10] Grand Jury Subpoenas and Suspicious Activity Reporting

Grand juries issue subpoenas in furtherance of conducting investigations of subjects and targets of their proceedings, and therefore the receipt of such a subpoena does not, by itself, require the filing of a SAR. However, receipt of a grand jury subpoena or other law enforcement inquiry is pertinent information relevant to a financial institution's overall assessment of risk and the risk profile for the relevant customer and account. Generally, a financial institution should assess and review all relevant information it has about a customer that is the subject of a grand jury subpoena or other law enforcement inquiries, in accordance with its risk-based AML program. For example, the receipt of a grand jury subpoena should cause a financial institution to review relevant account activity and transactions.

The financial institution should determine whether SAR filing is necessary based on its assessment of all information available and applicable regulatory requirements. If a financial institution files a SAR on a customer or

transaction following the receipt of a grand jury subpoena or other law enforcement inquiry, the SAR should focus on the facts and circumstances that support a finding of suspicious activity rather than the subpoena or inquiry itself. [See Question #2 to the agencies' SAR FAQs January 19, 2021.]

Receipt of a grand jury subpoena does not alter the standards for filing a SAR. Financial institutions should only file a SAR for transactions conducted or attempted by, at, or through the financial institution involving or aggregating at least $5,000 when the financial institution knows, suspects, or has reason to suspect that:

- The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities;
- The transaction is designed to evade any requirements under the BSA;
- The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institute knows of no reasonable explanation for the transaction after examining all the available facts; or
- The transaction involves use of the financial institution to facilitate criminal activity.

The failure to adequately describe the factors making the reported transaction or activity suspicious in the narrative of a suspicious activity report lessens its usefulness to law enforcement. Therefore, if a financial institution does prepare a SAR following the service of a grand jury subpoena, it should provide detailed information about the facts and circumstances of the detected suspicious activity, rather than the mere fact that a grand jury subpoena has been received.

Finally, grand juries are confidential proceedings conducted by state and federal prosecutors to determine whether enough evidence exists to formally accuse the subjects of criminal charges. A financial institution that receives a grand jury subpoena in connection with an investigation relating to a possible crime against any financial institution or supervisory agency, or certain other crimes, is prohibited from directly or indirectly notifying any person named in the subpoena about the existence or contents of the subpoena, or information that the financial institution has furnished to the grand jury in response to the subpoena.

§ 2.15 SHARING OF INFORMATION TO DETER MONEY LAUNDERING

[1] In General

Section 314 of the USA PATRIOT Act requires the Department of the Treasury to issue regulations to encourage cooperation among financial institutions, financial regulators, and law enforcement officials for the purpose of sharing information regarding individuals, entities, and organizations "engaged in or reasonably suspected, based on credible evidence, of engaging in" terrorist acts or money laundering activities.

Specifically, the information sharing provisions of section 314 of the USA PATRIOT Act address two types of information sharing:

- Section 314(a) addresses the sharing of information between law enforcement, the regulatory agencies, and financial institutions regarding suspected money laundering and terrorist-related activities.
- Section 314(b) addresses the sharing of information among financial institutions themselves, regarding suspected money laundering and terrorist-related activities.

The rules for section 314 are located in the Bank Secrecy Act regulations, 31 CFR 1010. Specifically, Subpart H consists of the following:

- 1010.505—Definitions
- 1010.520—Information sharing with federal law enforcement agencies
- 1010.540—Voluntary information sharing among financial institutions

[2] Information Sharing Among Financial Institutions (Section 314(b))

The Department of the Treasury has adopted final rules that govern information sharing related to potential money laundering or terrorist activity to replace the interim rules that were previously in effect.

The rules for the sharing of information among financial institutions are contained in 31 CFR 1010.540 of the Bank Secrecy Act regulations. The benefit of the rules is that if you share information under the rule, you are protected from liability for any customer information you provide as part of the process.

Under section 1010.540(a)(1) of the rule, the "financial institutions" that are allowed to share information are those that are required to have an anti-money laundering plan. Currently, this includes the following:

- Banks
- Thrifts
- Credit unions
- Securities broker-dealers
- Futures commission merchants
- Casinos
- Money service businesses
- Mutual funds
- Operators of credit card systems

In addition, these financial institutions are allowed to share information with "associations of financial institutions" as well as these financial institutions. Under section 1010.540(a)(2), an "association of financial institutions" is a group or organization the membership of which is comprised entirely of the types of financial institutions listed above. One example of these associations would be a network of automated teller machines, where all of the participants are financial institutions. If the organization has members that are not one of these types of financial institutions, then they are not included in the information sharing rules.

(Text continued on page 2-51)

t	**Terrorist Financing**	18 USC 2339(a) and 18 USC 2339(b)—Harboring and Concealing Terrorists	Persons or entities who provide material support or resources to various enumerated terrorist acts, including concealing or disguising the nature, location, source or ownership of the material support or resources. Also, persons or entities providing material support or resources to designated foreign terrorist organizations, or attempting or conspiring to do so. The statute explicitly provides for extraterritorial jurisdiction, meaning it can be applied to actions occurring outside the United States.
u	**Identity Theft**	18 USC Section 1028—Identity Theft	A person who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under applicable state or local law. See Issue 2, page 14 of The SAR Activity Review for further details about identity theft at the following hyperlink: http://www.fincen.gov/sarreview2issue4web.pdf

Exhibit 2.5 Money Laundering and Terrorist Financing Red Flags

From Appendix F of the FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual

The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and examiners recognize possible money laundering and terrorist financing schemes. FinCEN issues advisories containing examples of "red flags" to inform and assist banks in reporting instances of suspected money laundering, terrorist financing, and fraud. In order to assist law enforcement in its efforts to target these activities, FinCEN requests that banks check the appropriate box(es) in the Suspicious Activity Information section and include certain key terms in the narrative section of the SAR. The advisories and guidance can be found on FinCEN's website. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity That May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A customer provides an individual taxpayer identification number after having previously used a Social Security number.
- A customer uses different taxpayer identification numbers with variations of his or her name.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer's home or business telephone is disconnected.
- The customer's background differs from that which would be expected on the basis of his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer is a trust, shell company, or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner's identity.

Efforts to Avoid Reporting or Recordkeeping Requirement

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as noncooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $10,000, to evade CTR filing requirements.

Funds Transfers

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Funds transfer activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the customer's operations.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

Automated Clearing House Transactions

- Large-value, automated clearing house (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.
- TPSPs have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.
- Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.
- Unusually high level of transactions initiated over the Internet or by telephone.
- NACHA—The Electronic Payments Association (NACHA) information requests indicate potential concerns with the bank's usage of the ACH system.

Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
- A large volume of cashier's checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the accountholder's business would not appear to justify such activity.
- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.
- Goods or services purchased by the business do not match the customer's stated line of business.
- Payments for goods or services are made by checks, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

Lending Activity

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.
- Loans that lack a legitimate business purpose, provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

Changes in Bank-to-Bank Transactions

- The size and frequency of currency deposits increases rapidly with no corresponding increase in noncurrency deposits.
- A bank is unable to track the true accountholder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank's location.
- Changes in currency-shipment patterns between correspondent banks are significant.

Cross-Border Financial Institution Transactions

- U.S. bank increases sales or exchanges of large denomination U.S. bank notes to Mexican financial institution(s).
- Large volumes of small denomination U.S. banknotes being sent from Mexican casas de cambio to their U.S. accounts via armored transport or sold directly to U.S. banks. These sales or exchanges may involve jurisdictions outside of Mexico.
- Casas de cambio direct the remittance of funds via multiple funds transfers to jurisdictions outside of Mexico that bear no apparent business relationship with the casas de cambio. Funds transfer recipients may include individuals, businesses, and other entities in free trade zones.
- Casas de cambio deposit numerous third-party items, including sequentially numbered monetary instruments, to their accounts at U.S. banks.

- Casas de cambio direct the remittance of funds transfers from their accounts at Mexican financial institutions to accounts at U.S. banks. These funds transfers follow the deposit of currency and third-party items by the casas de cambio into their Mexican financial institution.

Bulk Currency Shipments

- An increase in the sale of large denomination U.S. bank notes to foreign financial institutions by U.S. banks.
- Large volumes of small denomination U.S. bank notes being sent from foreign nonbank financial institutions to their accounts in the United States via armored transport, or sold directly to U.S. banks.
- Multiple wire transfers initiated by foreign nonbank financial institutions that direct U.S. banks to remit funds to other jurisdictions that bear no apparent business relationship with that foreign nonbank financial institution. Recipients may include individuals, businesses, and other entities in free trade zones and other locations.
- The exchange of small denomination U.S. bank notes for large denomination U.S. bank notes that may be sent to foreign countries.
- Deposits by foreign nonbank financial institutions to their accounts at U.S. banks that include third-party items, including sequentially numbered monetary instruments.
- Deposits of currency and third-party items by foreign nonbank financial institutions to their accounts at foreign financial institutions and thereafter direct wire transfers to the foreign nonbank financial institution's accounts at U.S. banks.

Trade Finance

- Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- Customers conducting business in higher-risk jurisdictions.
- Customers shipping items through higher-risk jurisdictions, including transit through noncooperative countries.
- Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties should prompt additional OFAC review.

Privately Owned Automated Teller Machines

- Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.
- Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armored car contracts, lending arrangements, or other appropriate documentation.

Insurance

- A customer purchases products with termination features without concern for the product's investment performance.
- A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
- A customer purchases a product that appears outside the customer's normal range of financial wealth or estate planning needs.
- A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.
- A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.
- A customer uses multiple currency equivalents (e.g., cashier's checks and money orders) from different banks and money services businesses to make insurance policy or annuity payments.

Shell Company Activity

- A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).
- Payments to or from the company have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- Transacting businesses share the same address, provide only a registered agent's address, or have other address inconsistencies.
- Unusually large number and variety of beneficiaries are receiving funds transfers from one company.
- Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers.
- A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Purpose of the shell company is unknown or unclear.

Embassy, Foreign Consulate, and Foreign Mission Accounts

- Official embassy business is conducted through personal accounts.
- Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.
- Accounts are funded through substantial currency transactions.
- Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

Employees

- Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.
- Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- Employee is reluctant to take a vacation.
- Employee overrides a hold placed on an account identified as suspicious so that transactions can occur in the account.

Other Unusual or Suspicious Customer Activity

- Customer frequently exchanges small-dollar denominations for large-dollar denominations.
- Customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- Customer purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold.
- Customer purchases a number of open-end prepaid cards for large amounts. Purchases of prepaid cards are not commensurate with normal business activities.
- Customer receives large and frequent deposits from online payments systems yet has no apparent online or auction business.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- Customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area, despite the availability of such services at an institution closer to them.
- Customer repeatedly uses a bank or branch location that is geographically distant from the customer's home or office without sufficient business purpose.
- Customer exhibits unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, several individuals arrive together, enter frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.
- Unusual use of trust funds in business transactions or other financial activity.
- Customer uses a personal account for business purposes.
- Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.
- Customer makes multiple and frequent currency deposits to various accounts that are purportedly unrelated.

- Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.
- Customer makes high-value transactions not commensurate with the customer's known incomes.

Potentially Suspicious Activity That May Indicate Terrorist Financing

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance "Guidance for Financial Institutions in Detecting Terrorist Financing" provided by the FATF. FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

Activity Inconsistent With the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from higher-risk locations open accounts.

- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

Exhibit 2.6 Environmental Crimes and Descriptions

Crime	Description
Wildlife Trafficking	Wildlife trafficking, also known as the illegal wildlife trade (IWT), involves the illicit trade of protected animals, animal parts, and derivatives thereof, including procurement, transport, and distribution, in violation of international or domestic law, and money laundering related to this activity. The United Nations estimates that in excess of 7,000 different species are illegally trafficked. This activity is increasingly carried out by transnational criminal organizations (TCOs) and both encourages and entrenches corruption. In 2021, the U.S. Department of State identified 28 countries of focus for wildlife trafficking, including six countries of particular concern for related corruption—Cambodia, Cameroon, Democratic Republic of Congo, Laos, Madagascar, and Nigeria. Further, wildlife trafficking bolsters illicit trade routes, threatens critical biodiversity, damages fragile ecosystems, and can lead to the spread of zoonotic diseases. Proceeds from wildlife trafficking are estimated by international organizations to be between $7 and $23 billion per year and account for a quarter of all wildlife trade. IWT uses many of the same routes and methods used by drug traffickers and others engaged in illicit trade and can vary depending on the species. Common smuggling techniques include concealing items in personal bags and falsely identifying goods as legal wildlife or other products. IWT trade ranges from a single live animal to multiton commercial shipments, with the latter becoming increasingly common. IWT can be facilitated by a myriad of funding mechanisms, including, but not limited to, cash, bank transfers (wires and automated clearing house), transfers through informal values transfer systems, transfers through money services businesses, transfers conducted using online or mobile payment processors, and transactions using convertible virtual currencies (CVCs). Traffickers are increasingly turning to social media platforms to advertise, sell, and otherwise engage in IWT, including facilitating payments and the movement of money. The involvement of the United States in IWT includes serving as a source, transit, destination, and money laundering location.
Illegal Logging	Illegal logging and associated trade (ILAT) is generally defined as the harvesting, processing, transporting, buying and selling of timber in violation of national and international laws. ILAT encompasses cutting down protected tree species, cutting down trees on protected land, and logging beyond legal limits. These crimes are often associated with TCOs, corruption, forged documents, misused logging permits, tax evasion, and falsified customs declarations, and result in illicit proceeds estimated by international organizations to be between $51 and $152 billion a year. This activity can have "significant negative impact on land use and tenure, human habitation and sustainable livelihoods and cause climate, land, and asset degradation." Some experts estimate that the "ecosystem service value" lost from illegal logging is $1 trillion or more annually based on what the illegally logged trees would have provided, including the value of absorbing carbon to offset rising carbon dioxide levels. Illegal logging concentrations have been noted in primary rainforests in Central America and South America, central and southern Africa, southeast Asia, and Eastern Europe, accounting for up to 90% of tropical deforestation in some countries. The timber is transported from and through these regions to East Asia, North America, and Western Europe and typically sold in legal markets where the illegal origin of the product is difficult to ascertain. Because this illicit trade is commingled with legal trade, it may involve corporate structures, the use of shell companies in various jurisdictions, and the movement of proceeds in the international financial system. With respect to consumption, China, India, Japan, the United States and certain countries in the European Union are considered the biggest consumers of illegal logging, with China often serving as a processing center for illicit timber from Africa, Asia, and beyond.

Illegal Fishing	Illegal fishing refers to fishing activities conducted in contravention of applicable laws and regulations at the local, regional, and international levels. These crimes are often associated with other illegal activity, including TCOs, corruption, money laundering, human trafficking, piracy, drug trafficking, and forgery, and are estimated by international organizations to result in annual illicit proceeds between $11 and $24 billion. Illegal fishing poses a direct threat to healthy ocean ecosystems, as well as the economic and food security of entire nations. Illegal fishing occurs all over the world with a variety of species. Specific information about the scope of illegal fishing is not readily available as efforts in this area, including those of the U.S. government, are commonly grouped with unregulated and under-regulated fishing, referred to collectively as illegal, unreported, and unregulated fishing or "IUU." With that important caveat, it is instructive to consider available IUU statistics to begin to understand the scope and nature of illegal fishing. It is estimated that, internationally, one in five fish caught originated from IUU. In 2019, the United States alone imported an estimated $2.4 billion in seafood products derived from IUU, including swimming crab, wild-caught warm water shrimp, yellowfin tuna, and squid. The countries involved in the biggest imports of IUU to the United States include China, Russia, Mexico, Vietnam, and Indonesia. According to the U.S. Coast Guard, IUU "has replaced piracy as the leading global maritime security threat" that if unabated will lead to the "deterioration of fragile coastal States and increased tension among foreign-fishing Nations, threatening geo-political stability around the world."
Illegal Mining	Illegal mining involves extraction of various metals, stones, and materials, including gold, silver, iron, coal, diamonds, emeralds, and rare earths, in violation of the law, including by failing to secure legal permits, land rights, licenses, and environmental safeguards. The activity is often associated with other crimes or criminal groups such as TCOs, corruption, fraud, human trafficking, and money laundering. Proceeds from illegal mining are estimated by international organizations to be between $12 and $48 billion per year and the activity results in significant deforestation, loss of biodiversity, environmental damages, and threats to human health. The extraction occurs around the world, by small and large-scale mining, and increasingly involves TCO activity. In addition, this trade is often commingled with legal trade and may involve corporate structures and shell companies in various jurisdictions. Illegal mining is unique in that it provides illicit actors both a source of proceeds as well as a means to launder proceeds from other crimes. Most of the proceeds of this activity are thought to end up in the international financial system. The Federal Bureau of Investigation has found that TCOs are using "often-witting United States businesses to exploit U.S. regulations and export illegally extracted gold to the United States to launder billions of illicit proceeds from criminal operations in Latin America."
Waste and Hazardous Substances Trafficking	Waste trafficking refers to intentional disposal of various kinds of waste, including, electronics, plastic, and industrial byproducts and runoff in a manner inconsistent with waste disposal laws. It can occur during several stages of waste management, specifically collection, transportation, sorting, recycling, and disposal. Hazardous substance trafficking may also involve waste trafficking or trade in regulated substances that are illegal in the United States, such as banned pesticides. The Environmental Protection Agency has identified the illegal disposal of hazardous waste, the export of hazardous waste without the permission of the receiving country, illegal discharge of pollutants into the water, and the disposal of regulated chemicals, like asbestos, inconsistent with laws and regulations, as typical examples of their investigations related to waste management. International organizations estimate that waste trafficking generates $10–12 billion annually.