United States Government Accountability Office

Report to Congressional Requesters

January 2016

INTERNATIONAL REMITTANCES

Money Laundering Risks and Views on Enhanced Customer Verification and Recordkeeping Requirements

Accessible Version

GAO-16-65

GAO Highlights

Highlights of GAO-16-65, a report to congressional requesters

January 2016

INTERNATIONAL REMITTANCES

Money Laundering Risks and Views on Enhanced Customer Verification and Recordkeeping Requirements

Why GAO Did This Study

The World Bank has estimated remittance outflows will reach $586 billion in 2015. However, some reports have indicated that remittance providers may be vulnerable to money laundering. Remittance providers are generally subject to both federal and state oversight.

GAO was asked to examine the potential illicit uses of remittances and assess whether requiring remittance senders to provide certain types of identification at a threshold below the current $3,000 level would be useful for U.S. AML efforts. This report examines (1) BSA remittance requirements that exist for remittance providers and related challenges that remittance providers face in complying with these requirements; (2) money laundering risks that remittances pose; and (3) stakeholders' views on the extent to which requiring remittance providers to verify identification and collect information at a lower dollar transaction amount than is currently required, or adding a requirement to verify legal immigration status, would assist federal agencies' AML efforts. GAO reviewed laws and regulations, analyzed compliance data, and interviewed stakeholders (Financial Crimes Enforcement Network, regulators, remittance providers, law enforcement, and industry and other associations). GAO also interviewed a nongeneralizable selection of five money transmitters and four depository institutions based on factors such as remittance volume.

GAO is not making recommendations in this report. Agencies provided technical comments, which we incorporated as appropriate.

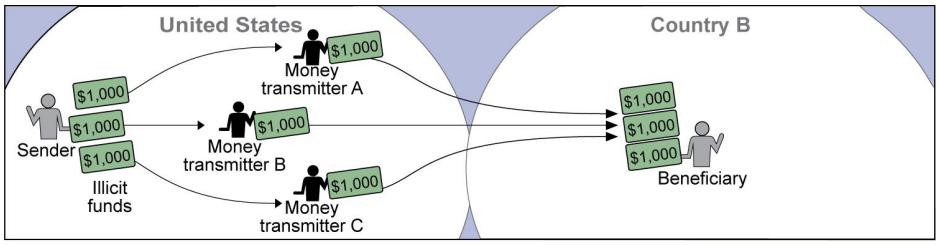
View GAO-16-65. For more information, contact Lawrance L. Evans, Jr. at (202) 512-8678 or evansl@gao.gov.

What GAO Found

Financial institutions, such as money transmitters and depository institutions that provide remittance transfers—funds sent from individuals in one country to a recipient in another country—are subject to anti-money laundering (AML) requirements under the Bank Secrecy Act (BSA). For example, these remittance providers must report suspicious and other transactions, and obtain and record information for each funds transfer of $3,000 or more. Remittance providers GAO spoke with identified challenges related to BSA compliance—including monitoring large amounts of remittance data to identify and prevent illicit activity, and keeping up to date with the changing behavior of criminals. Further, some banks have ended account relationships with money transmitters—which need bank accounts to conduct business. Money transmitters going out of business could lead remittance senders to use informal methods that are less detectable.

Remittances can pose money laundering risks, as funds related to illicit activity may go undetected due to the large volume of transactions or remittance providers' inadequate oversight of the various entities involved. Stakeholders identified money laundering risks associated with customers, geographic location, products, and agents (entities authorized to provide remittances) that may fail to follow BSA requirements. Remittances can be used to launder proceeds from different types of criminal activities, including drug trafficking and human smuggling, through methods such as structuring. For example, as the figure shows, a sender may structure remittances by breaking up a transaction into multiple transactions to avoid the $3,000 funds transfer threshold.

Example of Structuring to Launder Illicit Funds



Source: GAO (analysis); Art Explosion (images). | GAO-16-65

Many stakeholders said that a lower dollar threshold would benefit agencies' AML efforts, but verifying remitters' legal immigration status might not benefit such efforts. Law enforcement officials GAO spoke with said that a centralized database of remittances—one potential result of a proposed rule that would require remittance providers to report certain remittances data at a low dollar threshold—would be useful in assisting AML efforts. Larger remittance providers generally did not object to lowering the funds transfer threshold because they had already self-imposed lower thresholds. But bank regulators and some stakeholders said that a lower threshold could create additional recordkeeping requirements and costs for smaller providers and for customers. Stakeholders generally expressed concern that a requirement to check the legal status of a remittance sender might not assist AML efforts because it could lead senders to use less detectable forms of transmitting money.

Contents

Table

Figures

Abbreviations

ACH	automated clearing house
AML	anti-money laundering
BSA	Bank Secrecy Act
CFPB	Consumer Financial Protection Bureau
DHS	Department of Homeland Security
DOJ	Department of Justice
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FTC	Federal Trade Commission
IRS	Internal Revenue Service
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
Treasury	Department of the Treasury
USPS	United States Postal Service

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 15, 2016

The Honorable David Vitter
United States Senate

The Honorable Tom Price
Chairman
Committee on the Budget
House of Representatives

The World Bank has estimated global remittances for 2015 to be $586 billion with expected growth of 4.1 percent in 2016.[1] These remittance transfers—funds sent from individuals in one country to a recipient in another country—have gained attention over the years, largely because they are an important source of funds for some countries.[2] For many of the receiving countries, remittances are the largest source of foreign currency, often amounting to more than official foreign assistance from governmental international aid organizations and developed countries such as the United States. These transfers are generally considered a stable source of funds for receiving countries. Both nondepository and depository financial institutions provide money transfer services. Nondepository institutions providing such services are generally known as money transmitters. Depository financial institutions—such as banks and credit unions—also provide remittance transfer services. However, some international and U.S. agency reports have indicated that remittance providers may be vulnerable to money laundering and other illicit activities. For example, the Financial Action Task Force—an intergovernmental body developing and promoting policies to combat money laundering and terrorist financing—has identified instances in which entities providing remittance services, like other financial

[1]World Bank Group, "Remittances growth to slow sharply in 2015, as Europe and Russia stay weak; pick up expected next year," (Apr. 13, 2015). We have ongoing work underway that will be reporting on the reliability of remittance estimates in a separate report that we plan to issue in fiscal year 2016.

[2]Definitions of remittances vary based on the transfer method, purpose, and provider—that is, the entity transferring the funds for the sender. For purposes of this report, we define remittances as the transfer of funds from consumers in the United States to persons or businesses in a foreign country.

institutions, may have unintentionally or intentionally participated in money laundering.[3]

The United States has taken steps to regulate remittance providers and prevent money laundering. The Bank Secrecy Act (BSA) is an important tool in federal law enforcement efforts to detect and deter the use of financial institutions (including those that send remittances) for criminal activity, including money laundering and terrorist financing.[4] The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury (Treasury), is responsible for administering the BSA. The BSA and implementing regulations generally require depository and other financial institutions—including money transmitters—to collect and retain various records of customer transactions, verify customers' identities in certain situations, maintain anti-money laundering (AML) programs, and report suspicious and other transactions. For example, financial institutions that provide money transfer services must obtain and retain specific information, such as name and address of the sender, for each transfer of $3,000 or more.[5] For purposes of this report, we refer to the funding level at which requirements are imposed for obtaining identification and other information on remittances as the funds transfer threshold. FinCEN has published an advance notice of proposed rulemaking and a proposed rule related to the funds transfer threshold amount and related identification requirements.[6] Legislation has also been proposed that, if enacted, could affect identification requirements by requiring financial institutions that provide

[3]Financial Action Task Force, *Money Laundering through Money Remittance and Currency Exchange Providers* (June 2010), 7.

[4]Bank Secrecy Act, titles I and II of Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-1959, and 31 U.S.C. § 5311 et seq.).

[5]31 C.F.R. § 1020.410(a) (recordkeeping requirements for banks); 31 C.F.R. § 1010.410(e) (recordkeeping requirements for nondepository financial institutions). For simplification purposes we use the term "funds transfer" for both depository and nondepository institutions in this report. Under the BSA, the term "funds transfer" is used in the context of depository institutions, and the term "transmittal of funds"—which includes funds transfers—is used in the context of nondepository financial institutions. *See* 31 C.F.R. §§ 1010.100(w), (ddd), 1010.410(e), 1020.410(a).

[6]*See* Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds, Advance Notice of Proposed Rulemaking, 71 Fed. Reg. 35,564 (June 21, 2006). The 2006 advance notice of proposed rulemaking was published jointly with the Board of Governors of the Federal Reserve System (Federal Reserve). *See also* Cross-Border Electronic Transmittals of Funds, Notice of Proposed Rulemaking, 75 Fed. Reg. 60,377 (Sept. 30, 2010).

remittance services to request certain identification for remittance transfers at nearly any dollar amount. For example, the Remittance Status Verification Act would require remittance transfer providers to verify the legal status under the U.S. immigration laws of remittance senders and impose a fine on those who are unable to provide proof of their immigration status.[7]

You asked us to examine potential illicit uses of remittance transfers and determine, to the extent possible, whether information that would be collected under the proposed Remittance Status Verification Act would assist federal agencies' AML efforts. This report examines (1) BSA remittance requirements that exist for remittance providers and related challenges that remittance providers face in complying with these requirements; (2) the money laundering risks that remittance transfer methods pose; (3) stakeholders' views on the extent to which requiring money transmitters and depository institutions to verify identification and collect information at a lower dollar transaction amount than is currently required, or adding a requirement to verify legal immigration status, would assist federal agencies' AML efforts.[8]

To examine BSA remittance requirements that exist for remittance providers, we reviewed relevant laws and regulations. We obtained

[7]Remittance Status Verification Act of 2015, S. 79, 114th Cong. (2015). The Remittance Status Verification Act would amend the Electronic Fund Transfer Act, which provides a consumer protection framework for remittance transfers made by senders in the United States to recipients in a foreign country. The Electronic Fund Transfer Act defines a "remittance transfer provider" as "any person or financial institution that provides remittance transfers for a consumer in the normal course of its business, whether or not the consumer holds an account with such person or financial institution." 15 U.S.C. § 1693o-1(g)(3). The Electronic Fund Transfer Act defines a "remittance transfer" as the "electronic transfer of funds requested by a sender located in any state to a designated recipient that is initiated by a remittance transfer provider, whether or not the sender holds an account with the remittance transfer provider," but does not include small value transactions in the amount of $15 or less. 15 U.S.C. § 1693o-1(g)(2); 12 C.F.R. § 1005.30(e).

[8]We obtained stakeholder views on both (1) lowering or eliminating the reporting dollar threshold for collecting and retaining information on funds transfers and (2) imposing a requirement that individuals document immigration status for funds transfers beginning at a near-zero threshold. Because imposing these requirements beginning at a low dollar threshold may result in similar challenges and benefits for law enforcement, stakeholders' views on a lower dollar threshold for required BSA recordkeeping may inform our discussion of the potential effects of the immigrant status documentation requirement. We will be considering the potential effects of imposing a fine on remittance senders unable to show proof of legal immigration status in greater depth in a separate report.

information from providers on their efforts to comply with BSA remittance requirements and the challenges they faced in doing so. We also obtained and analyzed available data on money transmitters' compliance with BSA-related requirements. We assessed the reliability of data by reviewing related documentation of the database from which the data come and also through interviews with agency officials, and found the data to be reliable for purposes of this report. To examine the money laundering risks posed by remittance transfers, we reviewed and summarized reports and documents that federal law enforcement, regulatory agencies, international organizations, and remittance providers maintain on money laundering through remittance transfers. To examine stakeholders' views on the extent to which lowering the funds transfer threshold for complying with recordkeeping requirements or adding a legal immigration status verification requirement would assist agencies' AML efforts, we reviewed an advance notice of proposed rulemaking, a proposed rule, and proposed legislation related to remittance transfers—including public comment letters available on the advance notice. For all objectives, we interviewed officials from FinCEN, federal law enforcement entities, federal and state regulators, industry associations, money transmitters, depository institutions, and policy and consumer advocacy groups. We judgmentally selected a cross-section of money transmitters and depository institutions that included five nondepository money transmitters and four depository institutions based on a number of factors, including the volume of remittances and diversity of countries serviced. Appendix I describes our objectives, scope, and methodology in greater detail.

We conducted this performance audit from October 2014 to December 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Remittance Transfer Methods

Remittance transfers include many types of international transfers including cash-to-cash money transfers, international wire transfers, some prepaid card transfers, and automated clearing house (ACH) transactions.[9] According to a Treasury report on money laundering risks, 90 percent of households in the United States have an account with a depository institution such as a bank, thrift, or credit union.[10] Regardless, many people, particularly immigrants, use money services businesses to send money abroad because of convenience, cost, familiarity, or tradition. Money services businesses, which do not include depository institutions, are persons doing business in one or more of the following capacities, subject to exceptions:[11]

- Dealer in foreign exchange
- Check casher
- Issuer or seller of traveler's checks or money orders
- Provider or seller of prepaid access
- Money transmitter[12]
- United States Postal Service (USPS)[13]

There were about 29,000 registered money services businesses in the United States as of September 2015.[14] They typically work through agents—

[9]The ACH is a system that clears and settles batched electronic transfers for participating depository institutions. International ACH makes up a small but growing portion of remittance transfers.

[10]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

[11]31 C.F.R. § 1010.100(ff).

[12]FinCEN regulations define a money transmitter as a person that provides money transmission services, which means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location by any means. The definition of money transmitter also includes any other person engaged in the transfer of funds. 31 C.F.R. § 1010.100(ff)(5). For purposes of this report, we focus on the money transmitter subset of money services businesses, and thus use the term "money transmitter" rather than "money services business" throughout the report. Money transmitters generally provide funds transfers, including international remittances, which are the focus of this report.

[13]Although USPS is treated as a separate subset of money services businesses from money transmitters under FinCEN regulations, we use the term "money transmitter" as including traditional money transmitters as well as USPS for the purposes of this report because USPS provides some comparable services to those money transmitters provide.

separate business entities generally authorized to, among other things, send and receive money transfers.[15] According to FinCEN 2011 survey data, the most frequent activity agents conducted was money transmitter services—transferring funds from one person to another person or location.

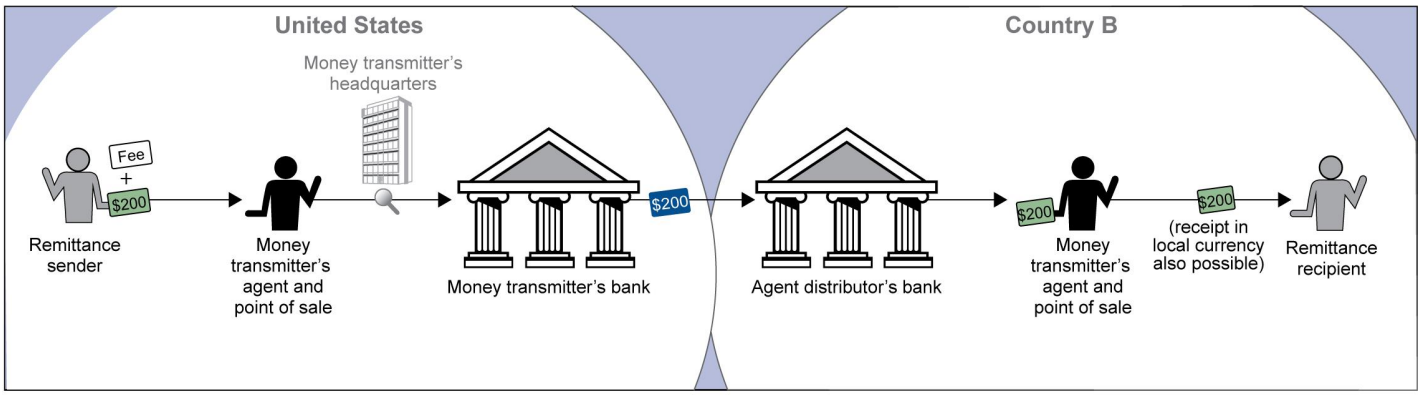
Remittances can be sent through, among others, money transmitters and depository institutions. Historically, consumers have primarily chosen to send remittances through money transmitters. Most remittance transfers are initiated in person at retail outlets that offer these services. Money transmitters generally operate through their own retail store fronts, or through grocery stores, financial services outlets, convenience stores, and other retailers that serve as agents. Depository institutions generally conduct remittances through their local branches. In one type of common money transmitter transaction—known as a cash-to-cash transfer (see fig. 1)—a sender can walk into a money transmitter agent location and provide cash to cover the transfer amounts and fees, and senders generally must provide basic information about themselves and the recipient (typically a name, address, and phone number) at the time of the transfer request. The agent processes the transaction, and the money transmitter's headquarters screens it for BSA compliance. The money can then be transferred to a recipient, usually through a distributor agent in the destination country. The money can be wired through the money transmitter's bank to the distributor agent's bank, or transferred by other means to a specified agent in the recipient's country. The distributor agent pays out cash to the recipient in either U.S. dollars or local currency.[16]

[14]Each money services business is generally required to register with FinCEN, and include in its registration, among other things, a list of its agents. *See* 31 C.F.R. § 1022.380(a).

[15]A money services business enters into a service agreement with the agent. Many of the terms of the agreement are generally stipulated by the state requirements where the money services business is located. Among other features, the agreement typically identifies the rights and obligations of both parties, as well as responsibilities for complying with all state and federal laws. In this report, the term "agent" does not denote a particular legal relationship. It includes legal agents, authorized delegates, or affiliates that act on behalf of a money transmitter in some capacity. Financial Crimes Enforcement Network and Internal Revenue Service, *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses* (December 2008).

[16]Money transmitters often instruct agents to pay out funds before the funds are sent to the foreign location. Money may be disbursed to the recipient in U.S. dollars or local currency depending on the destination, the money transmitter's service offering, and the preference of either the sender or the recipient.

Figure 1: Example of a Money Transmitter Cash-to-Cash Remittance Transfer



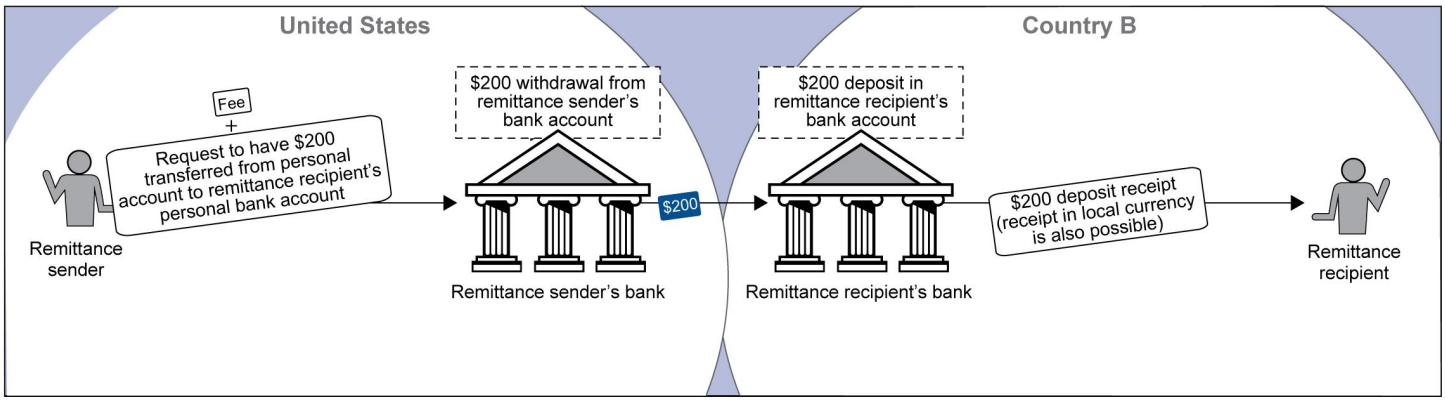
Source: GAO (analysis); Art Explosion (images). | GAO-16-65

Note: Money transmitters often instruct agents to pay out funds to recipients before the funds are sent to the foreign location.

Figure 2 shows a bank-to-bank remittance transfer. The sender requests that money be removed from a bank account and transferred directly to the recipient's bank account. Figure 2 is an example of a simple funds transfer between two customers with only the remittance sender's and remittance recipient's banks involved. As the number of institutions involved increases, the transfer scenarios get more complicated. These more complicated scenarios are more common in the context of remittances, particularly if an originator's institution does not have a branch in the recipient's foreign location. In this case, one financial institution may rely upon established business relationships with additional financial institutions to complete the transaction—known as a correspondent banking relationship.[17]

[17]The financial industry commonly uses many terms to describe these additional financial institutions. These terms include "intermediary" financial institution, "instructing" financial institution, "sender's correspondent," and "receiver's correspondent." For purposes of this study, we use the term "correspondent" to describe these additional financial institutions. Financial Crimes Enforcement Network, *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* (October 2006).

Figure 2: Example of a Bank-to-Bank Remittance Transfer



Source: GAO (analysis); Art Explosion (images). | GAO-16-65

Note: This is an example of a simple funds transfer. More complicated transfers may involve more entities, such as correspondent banks.

According to a 2011 report on remittance transfers from the Consumer Financial Protection Bureau (CFPB), industry participants and researchers report that cash-to-cash transfers made through money transmitters continue to account for the majority of personal transfers, rather than transfers through debits from or direct deposits to accounts held at depository institutions or credit unions.[18] Using state licensing data, CFPB estimated that money transmitters sent from the United States about 150 million international money transfers in 2012, with an estimated $49 billion total market value.[19] In contrast, according to reported depository institution data, depository institutions sent about 13 million international money transfers in calendar year 2014.[20] Although CFPB estimates show that money transmitters are responsible for sending the great majority of the remittance transfers, CFPB believes that the typical size of transfers sent by

[18]Consumer Financial Protection Bureau, *Report on Remittance Transfers* (July 20, 2011).

[19]*See* 79 Fed. Reg. 5302, 5306-07 n.37 (Jan. 31, 2014).

[20]Data for depository institution international money transfers were derived from calendar year 2014 call-report data reported by banks and credit unions on the number of remittance transfers originated.

depository institutions is generally larger than the typical size of transfers sent by a money transmitter. A typical transfer sent by a depository institution may be in the thousands of dollars, while CFPB estimates that the typical size of remittance transfers sent by money transmitters is in the hundreds of dollars.[21] CFPB estimates from 2012 state supervisory data showed that the average transaction size for money transmitter remittances originating in the United States was about $300.[22]

As consumers and money transmitters become more technologically sophisticated, money transmitters have started offering an increasing range of other transfer methods. For example, according to the 2011 CFPB report on remittance transfers, several money transmitters have begun to permit consumers to transfer or receive money through accounts tied to e-mail addresses or mobile phone numbers (often called Internet or mobile phone "wallets"). According to a 2015 World Bank news release, despite its potential to lower costs, the use of mobile technology in cross-border transactions remains limited.[23]

Other Methods of Remittance Transfers

Remittance senders use a variety of other methods and products to send funds, such as prepaid cards sent by USPS; or the physical movement of money outside of the United States—such as using courier services that carry funds across the border.[24] One other method includes international money orders sent through USPS. Remittance senders can mail international money orders to about 30 countries through USPS's international mail services. Recipients can then cash these money orders either at local post offices or banks in destination countries.

Other methods for facilitating remittances include informal value transfer systems. Informal value transfer systems are often used in places where formal financial transactions are unavailable, expensive, or unreliable. A

[21]*See* 79 Fed. Reg. 55,970, 55,972 (Sept. 18, 2014).

[22]*See* 79 Fed. Reg. 5302, 5314 n.85 (Jan. 31, 2014).

[23]World Bank Group, "Remittances growth to slow sharply in 2015, as Europe and Russia stay weak; pick up expected next year," (Apr. 13, 2015).

[24]Each person (including a bank) who physically transports, mails, or ships currency or monetary instruments in excess of $10,000 at one time out of or into the United States (and each person who causes the transfer) must file a Report of International Transportation of Currency or Monetary Instruments (FinCEN Form 105). *See* 31 U.S.C. § 5316.

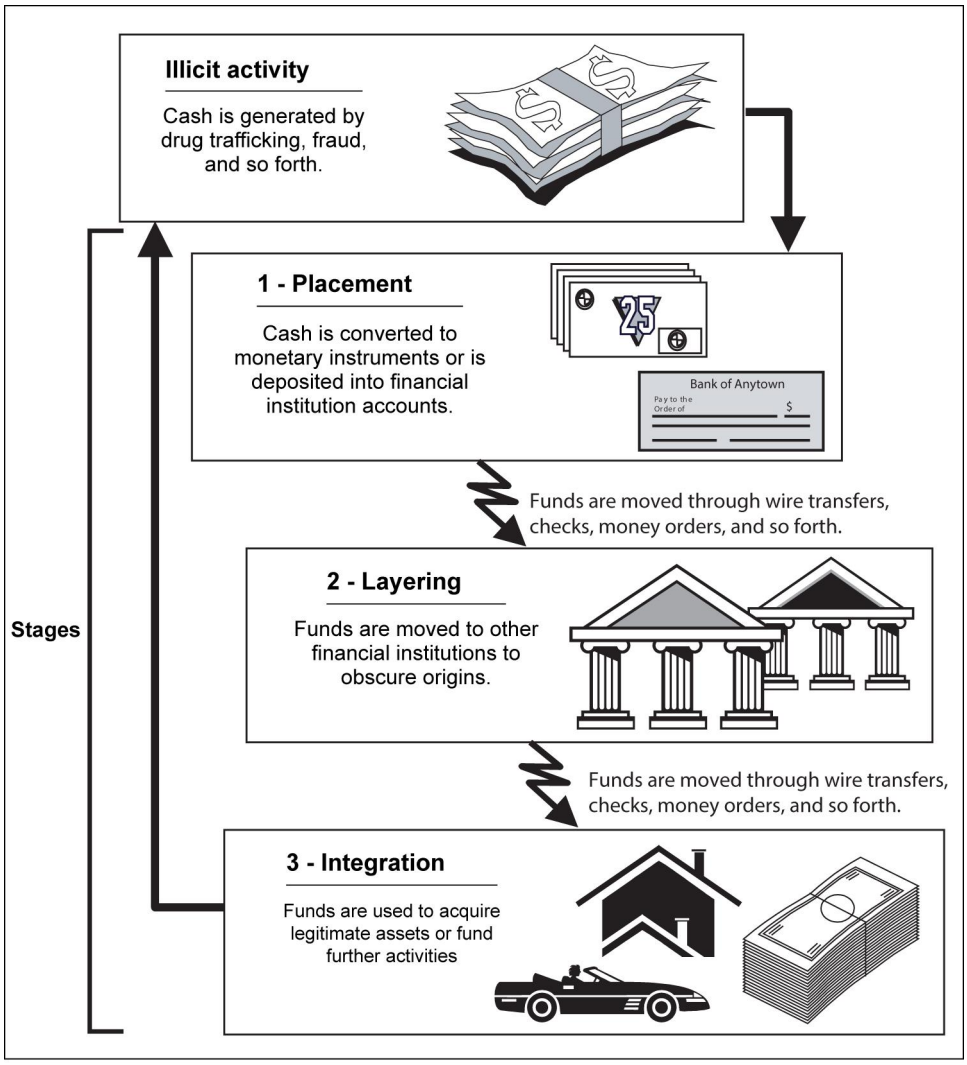
common type of informal value transfer is a hawala. The components of hawala that distinguish it from other remittance systems are trust and the extensive use of connections such as family relationships or regional affiliations.[25] Under the hawala system, a customer hands cash to a person known as a "hawaladar" and requests that an equivalent amount be delivered in local currency to a recipient in a different country. The hawaladar then contacts a hawaladar in the receiving country and asks that the funds be disbursed to the recipient. In most cases, fees are factored into the exchange rate or the amount that is disbursed.

Money Laundering

Money laundering—the process of making illegally gained proceeds appear legal—occurs in three distinct phases, as illustrated in figure 3. According to Treasury, placement occurs when illicitly obtained funds are introduced into the financial system. The funds are then separated from their criminal origins as they pass through several financial transactions in a process called layering. The next phase, integration, occurs when the funds are mixed with legitimately obtained money or used to acquire assets.

[25]Financial Crimes Enforcement Network in cooperation with INTERPOL/FOPAC, *The Hawala Alternative Remittance System and its Role in Money Laundering (January 2000).*

Figure 3: Three Stages of Money Laundering



Source: Financial Crimes Enforcement Network, *FinCEN Related Series: An Assessment of Narcotics Related Money Laundering*, July 1992. | GAO-16-65

Federal and State Oversight of Financial Institutions

Money transmitters and depository institutions are both generally subject to federal and state oversight. In general, money transmitters must register with FinCEN and provide information on structure and ownership.[26] Money transmitters also may be required to obtain licenses from states in which they are incorporated or conducting business. Depository institutions are regulated by state and federal banking regulators according to how they are chartered, and they provide related information when obtaining their charter.[27]

FinCEN often works in conjunction with federal and state regulators to support the examinations of both money transmitters and depository institutions. FinCEN issues regulations under the BSA and supports the examination functions performed by other federal regulators, including the federal banking regulators, the Internal Revenue Service (IRS), the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC).[28] FinCEN also collaborates with federal and state banking regulators and has issued joint guidance and rules with federal regulators. FinCEN relies on the federal banking regulators to examine depository institutions within their respective jurisdictions for BSA compliance. The federal banking regulators require institutions under their supervision to establish and maintain a BSA compliance program.[29] SEC has the authority to examine brokers and dealers in securities mutual funds

[26]31 U.S.C. § 5330; 31 C.F.R. § 1022.380.

[27]As part of the process for obtaining a charter from a federal or state chartering authority, a depository institution typically provides information about its structure and ownership, as well as financial and managerial information and plans for compliance with applicable laws, including the BSA.

[28]For the purposes of this report, we use "federal banking regulators" to refer collectively to the regulators of depository institutions (federally insured banks, thrifts, and credit unions). Federal banking regulators include the Office of the Comptroller of the Currency (OCC), Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and National Credit Union Administration (NCUA). Although CFPB has supervisory and enforcement authority over federal consumer financial law for certain entities, including large banks and certain nondepository institutions, we did not include CFPB in our definition of federal banking regulators because CFPB does not examine for compliance with or enforce BSA. *See* 12 U.S.C. §§ 5514, 5515.

[29]The appropriate federal prudential regulators are required to prescribe regulations requiring the insured depository institutions under their supervision to establish and maintain procedures that are reasonably designed to assure and monitor the compliance of such institutions with the BSA. 12 U.S.C. §§ 1786(q), 1818(s). Regulations requiring the establishment of BSA compliance programs are codified at 12 C.F.R. § 21.21 (OCC); 12 C.F.R. § 208.63 (Federal Reserve); 12 C.F.R. §§ 326.8, 390.354 (FDIC); 12 C.F.R. § 748.2 (NCUA).

for BSA compliance, while the CFTC has such authority with respect to futures commission merchants, introducing brokers in commodities.[30] The IRS has the authority to examine for BSA compliance financial institutions, such as money transmitters, that are subject to the BSA but are not currently examined by federal banking regulators for safety and soundness.[31]

To ensure consistency in the application of the BSA requirements, in 2008 FinCEN issued a BSA examination manual for use in reviewing money transmitters, including for IRS and state regulators. Similarly, in 2005 the federal banking regulators collaborated with FinCEN on a BSA examination manual that was issued by the Federal Financial Institutions Examination Council (FFIEC).[32] The manual is intended for federal bank examiners conducting BSA examinations of depository institutions. It was updated most recently in 2014 to further clarify supervisory expectations and regulatory changes.[33]

Depository institutions and money transmitters—in some states—are subject to safety and soundness examinations.[34] These on-site examinations are done periodically and assess an institution's adherence to laws and regulations such as the BSA, among other things. Federal banking regulators take a risk-based approach to BSA examinations—that is, they

[30]*See* 31 C.F.R. § 1010.810(b)(6),(9).

[31]Certain entities are specifically excluded from IRS's examination authority, including brokers or dealers in securities, mutual funds, futures commission merchants, introducing brokers in commodities, and commodity trading advisors. 31 C.F.R. § 1010.810(b)(8). As noted above, those entities are subject to examination by SEC and CFTC.

[32]FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by its member agencies and to make recommendations to promote uniformity in the supervision of financial institutions. The constituent agencies are the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Bureau of Consumer Financial Protection, and State Liaison Committee, which consists of five representatives from state regulatory agencies that supervise financial institutions.

[33]Federal Financial Institutions Examination Council, *Bank Secrecy Act/ Anti-Money Laundering Examination Manual* (2014).

[34]Federal and state banking regulators conduct safety and soundness examinations of depository institutions. State regulators may examine depository institutions chartered within their jurisdiction. State regulators may also conduct safety and soundness examinations of nondepository financial institutions, such as money transmitters. The authority of states to regulate money transmitters varies from state to state.

target key areas of risk or specific problems. In our prior work, we found that the risk-based approach allowed regulators to apply the appropriate scrutiny and devote resources to business lines or areas within institutions that pose the greatest risk for BSA noncompliance.[35]

FinCEN has overall authority for enforcement and compliance under the BSA, and may impose civil penalties and issue injunctions to compel compliance with BSA.[36] In addition, each of the federal banking regulators has the authority to initiate enforcement actions against supervised institutions for violations of law.[37] Federal banking regulators can also impose civil money penalties for BSA violations.[38] Under the BSA, IRS has certain authority that is delegated by FinCEN, and also has authority for investigating criminal violations.[39] The Department of Justice (DOJ) prosecutes violations of federal criminal money laundering statutes and violations of the BSA, and several law enforcement agencies can conduct BSA-related criminal investigations.

We did not identify any current federal requirement to verify the legal immigration status of a remittance sender. Federal legislation has been proposed that would require such verification. For example, the Remittance Status Verification Act of 2015, if enacted, would require each

[35]GAO, *Bank Secrecy Act: Opportunities Exist for FinCEN and the Banking Regulators to Further Strengthen the Framework for Consistent BSA Oversight*, GAO-06-386 (Washington, D.C.: Apr. 28, 2006), 5.

[36]31 U.S.C. §§ 5320, 5321; 31 C.F.R. § 1010.810(a),(d). See 31 U.S.C. § 310; 67 Treasury Order 180-01, Fed. Reg. 64,697 (Sept. 26, 2002) for the source of FinCEN's overall enforcement and compliance authority.

[37]*See* 12 U.S.C. §§ 1786(b), (q) (federally insured credit unions), 1818(b), (c), (s) (depository institutions other than credit unions).

[38]*See* 12 U.S.C. §§ 1786(k)(2) (federally insured credit unions), 1818(i) (depository institutions other than credit unions).

[39]31 C.F.R. § 1010.810(b)(8), (c)(2), (g). The authority to enforce certain provisions has been delegated from FinCEN to the Commissioner of Internal Revenue by means of a Memorandum Agreement between FinCEN and IRS, which provides that IRS has the authority to, among other things, assess and collect civil penalties under 31 U.S.C. § 5321 and 31 C.F.R. § 1010.810; investigate possible civil violations of these provisions; and issue administrative rulings under 31 C.F.R. pt. 1010, subpt. G. *See* 31 C.F.R. § 1010.810(g). IRS's Small Business/Self-Employed Division conducts BSA compliance examinations of money transmitters, and can refer cases to IRS Criminal Investigations if the examiners believe that a willful criminal violation may be involved. IRS Criminal Investigations investigate, among other types of criminal violations, BSA criminal violations.

remittance transfer provider to request from each remittance transfer sender proof of the sender's legal status under U.S. immigration laws, and impose a fine on the sender—7 percent of the transfer amount—if the sender is unable to provide proof of legal immigration status.[40] One state has passed and others have proposed legislation related to verifying the legal immigration status of a sender. In July 2009, Oklahoma enacted a law requiring that a fee be imposed on all remittances that originate in Oklahoma, and customers are entitled to an income tax credit equal to the amount they paid when filing an individual income tax return in Oklahoma with either a valid Social Security or taxpayer identification number.[41] We also identified legislation that has been proposed—but not enacted—in several states between 2005 and October 2015 that would impose a fee on customers sending remittances who are unable to prove legal immigration status. For example, a bill that was introduced in Texas in March 2015 would require providers to charge a fee equal to 10 percent of a money transmission made by individuals unable to show proof of legal immigration status.[42]

Bank Secrecy Act Requirements and Compliance-Related Challenges

Money transmitters and depository institutions are subject to similar requirements under the BSA. They are generally required to design and implement a written AML program, report certain transactions to Treasury, and meet recordkeeping and identity documentation requirements for funds transfers of $3,000 or more. In our interviews, money transmitters and depository institutions indicated that they took steps to comply with these requirements, but identified some compliance-related challenges. These challenges included the cost of compliance, and derisking—the practice of depository institutions ending their

[40]Remittance Status Verification Act of 2015, S. 79, 114th Cong. § 2 (2015).

[41]Okla. Stat. Ann. tit. 63, § 2-503.1j (West). Although this law does not require providers to verify legal immigration status of remitters, as noted, it imposes a fee on all remittances, regardless of remitters' legal status, and only those remitters who file income tax returns with the state may claim a credit for the fee paid. Since individuals who do not have proof of legal status are unlikely to have a valid Social Security number or tax identification number, they are unlikely to file income tax returns, and therefore unlikely to obtain a credit for the remittance fee paid. Legislation has been proposed in several other states that would impose a tax or fee on remittances with a later opportunity for a tax credit or refund—none of which have been enacted.

[42]H.B. 4120, 84th Leg., Reg. Sess. (Tex. 2015).The bill was left pending in committee as of April 2015.

relationships with money transmitters (who need bank accounts to conduct business) to avoid perceived regulatory concerns about facilitating money laundering.

Money Transmitters and Depository Institutions Are Subject to Similar BSA Requirements

AML Program Requirements

All financial institutions subject to the BSA—including money transmitters and depository institutions— are required to establish a written AML program.[43] At a minimum, each AML program must

- establish written AML compliance policies, procedures, and internal controls;
- designate an individual to coordinate and monitor day-to-day compliance;
- provide training for appropriate personnel; and
- provide for an independent audit function to test for compliance.[44]

FinCEN reported and the five money transmitters and four depository institutions we spoke with said that money transmitters and depository institutions had developed complex AML programs to meet FinCEN's requirements. Among the tools used were detailed software systems to help identify and monitor high-risk customers, and agent oversight and training.

[43]31 U.S.C. § 5318(h)(1). For specific AML program requirements for money services businesses, including money transmitters, *see* 31 C.F.R. § 1022.210; for banks, *see* 31 C.F.R. § 1020.210.

[44]Financial Crimes Enforcement Network's guidance, *Frequently Asked Questions: Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs*, FIN-2006-G012, September 22, 2006, clarifies that, for a money transmitter, an independent review is not a formal audit by a certified public accountant or third-party consultant. Accordingly, a money services business does not necessarily need to hire an outside auditor or consultant. The review may be conducted by an officer, employee, or group of employees, so long as the reviewer is not the designated compliance officer and does not report directly to the compliance officer.

- Money transmitters, depository institutions, and their respective industry associations told us they—or their members—used software systems that aided in their AML compliance, including what they described as robust monitoring programs that routinely evaluate high-risk customers. For example, one representative of a money transmitter we interviewed stated that the transmitter created a comprehensive member profile for each customer that identified their typical transactions. This system also automatically prevents the processing of transactions that seem abnormal based on a customer's profile. This representative indicated that they are developing a program that will provide a "risk score" for all customers as part of its efforts to conduct due diligence and monitor for suspicious activity.

- FinCEN has found that money transmitters have placed significant emphasis on AML program requirements including agent oversight, and consider compliance with BSA regulations part of their business models.[45] According to FinCEN, money transmitters try to mitigate agent risk by conducting due diligence on potential agents, making on-site visits to existing agents, reviewing and monitoring transactions, and engaging in mystery shopping—that is, unannounced testing of agents for money transmitters. A representative from a money transmitter industry association with whom we spoke said that money transmitters placed significant emphasis on agent training as a part of the steps they took to comply with AML program requirements.

IRS BSA examination data for fiscal years 2013 and 2014 showed that failure to comply with AML program requirements was the most frequently cited violation of money transmitters. See appendix II for more information.

Reporting Requirements

Depository institutions and money transmitters also must comply with certain reporting requirements. Money transmitters generally must file a suspicious activity report when a transaction involves or aggregates funds or other assets of at least $2,000 and they know, suspect, or have reason

[45]Financial Crimes Enforcement Network, *Financial Institutions Outreach Initiative: Report on Outreach to Money Services Businesses* (July 2010).

to suspect that the transaction is suspicious for one of several reasons.[46] Depository institutions are required to file a suspicious activity report when a transaction conducted by, at, or through the institution involves or aggregates at least $5,000 in funds or other assets and the institution knows, suspects, or has reason to suspect that the transaction is suspicious.[47]

According to a 2015 FinCEN report, suspicious activity reports play an integral role in law enforcement investigations and financial regulatory compliance at both the federal and state levels.[48] To ensure compliance, some money transmitters and depository institutions that we interviewed indicated that they filed suspicious activity reports on all suspicious transactions, regardless of size, and had designed programs to identify suspicious activity. A representative from another money transmitter told us that the institution did not file suspicious activity reports if it investigated a situation and found that there was a reasonable explanation for the transaction. However, the representative stated that the organization would file a suspicious activity report for a transaction of as little as $200 dollars if it suspected illicit activity. According to FinCEN, money transmitters have reportedly used social networking sites to verify identity during a suspicious activity report investigation, developed

[46]Specifically, a suspicious transaction is one that involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to evade any federal law or regulation, or any transaction reporting requirement under federal law or regulation. A suspicious transaction is also one that is designed, whether through structuring or other means, to evade any BSA requirements; one that serves no business or apparent lawful purpose and for which the reporting money transmitter knows of no reasonable explanation after examining the available facts; or one that involves use of the money transmitter to facilitate criminal activity. 31 C.F.R. § 1022.320(a)(2).

[47]A transaction is suspicious and requires reporting if it may involve potential money laundering or other illegal activity, is designed to evade the BSA or its implementing regulations, has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, 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. 31 C.F.R. § 1020.320(a)(2). Depository institutions are also required to file suspicious activity reports for criminal violations involving insider abuse of any amount, as well as violations aggregating $5,000 or more when a suspect can be identified and $25,000 or more even without a potential suspect. *See* 12 C.F.R. §§ 21.11(c)(1)-(3), 163.180(d)(3)(i)-(iii) (OCC); 12 C.F.R. § 208.62(c)(1)-(3) (Federal Reserve); 12 C.F.R. § 353.3(a)(1)-(3) (FDIC); 12 C.F.R. § 748.1(c)(1)(i)-(iii) (NCUA).

[48]Financial Crimes Enforcement Network, *SAR Stats Technical Bulletin* (October 2015).

proprietary systems to identify suspicious activity, and placed accounts on hold after filing a suspicious activity report in order to ensure that they do not conduct further business with that customer.

A representative from another money transmitter described a series of software programs that it had developed and said that 95 percent of the overall suspicious activity that they identified was identified with the software. According to the representative, these systems check transactions monthly and look for illicit activity under the reporting threshold. The systems also aggregate different types of transactions to see if the same individual is transferring an amount of money above the reporting threshold through different products. Further, one industry group we interviewed that represents depository institutions indicated that institutions filed suspicious activity reports if they saw a series of transactions to high-risk corridors, such as Ukraine or the Middle East.

According to IRS BSA examination data for fiscal years 2013 and 2014, failure to file suspicious activity reports was the second most frequently cited violation during examinations of money transmitters. See appendix II for more information.

Recordkeeping and Identity Verification

Under the BSA, money transmitters and depository institutions are required to obtain and retain specified information, including the name and address of the sender, for all transfers in the amount of $3,000 or more, regardless of whether the sender is an established customer of the financial institution.[49] Recordkeeping and other BSA-related requirements for money transmitters and depository institutions include

- verifying customer identification (ID) when a transaction is conducted in person and the sender is not an established customer,
- recording certain specified customer and transaction information,
- providing certain information to the receiving money transmitter or other receiving financial institution,[50] and

[49]31 C.F.R. § 1020.410(a) (recordkeeping requirements for banks); 31 C.F.R. § 1010.410(e) (recordkeeping requirements for nonbank financial institutions).

[50]31 C.F.R. § 1010.410(f).

- maintaining the record for 5 years from the date of transaction.

For transfers in the amount of $3,000 or more made by senders other than established customers, in person or not, money transmitters and depository institutions are required to obtain and retain a record of the name and address of the person placing the payment order, as well as the person's taxpayer identification number (Social Security number or employer identification number, for example).[51] If the person does not have a taxpayer identification number, the records must include an alien number, passport number and country of issuance, or notation in the record of the lack thereof.[52] For transfers made in person, money transmitters and depository institutions must, in addition to the items listed previously, also verify the identity of the person placing the order and obtain and retain a record of the type of identification reviewed as well as the number of the identification document. In verifying a sender's identity, institutions are required to examine a document—preferably with the person's name, address, and photograph—that is normally acceptable as a means of identification when cashing checks for persons other than established customers.

Depository institutions have some additional identification and verification requirements. As part of their BSA program requirements, depository institutions are required to implement a customer identification program appropriate for their size and type of business which, among other things, must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable.[53] The customer identification program must contain procedures for opening an account that specify the identifying information that will be obtained from each customer, which shall include, at a minimum, name, date of birth, address, and identification number. The program must also include procedures for making and maintaining a record of a description of the methods used and the results of any measures undertaken to verify the identity of the customer, including a description of the resolution of any substantive

[51]31 C.F.R. §§ 1010.410(e)(2), 1020.410(a)(2).

[52]An alien number is issued to noncitizens by U.S. Citizenship and Immigration Services. The alien identification number can be found on the permanent residence card, which gives the holder a way of proving his or her legal status to live and work permanently within the United States.

[53]31 C.F.R. § 1020.220(a)(2).

discrepancy discovered when verifying the identifying information obtained.[54]

Some money transmitters and depository institutions that we spoke with said that they took steps beyond the minimum requirements to comply with the recordkeeping and identity verification requirements. All four depository institutions that we interviewed said that they imposed stricter requirements than minimally required to comply with the recordkeeping and identity verification requirements. Generally, these institutions limit remittance transfers to their customers only. Depository institutions must verify and record identification upon forming a customer relationship due to customer identification program requirements. Thus these depository institutions said that they generally verified identification for all remittance transfers when they established the customer relationship. One representative from a depository institution detailed the depository institution's policy for the collection of two levels of identification—primary and secondary identification. The official noted that the primary identification is aimed at complying with AML and customer identification program requirements, while the secondary identification is used for fraud prevention and can be as simple as a student identification card.

According to FinCEN, some money transmitters are reportedly implementing company standards that go beyond BSA requirements.[55] One representative from a money transmitter stated that the organization implemented a lower threshold of $750 for verifying identification. A representative from a money transmitter industry group explained it was common for money transmitters to impose thresholds lower than $3,000 for identity verification.

[54]The preamble to the customer identification program final rule provides that the term "account" was limited to formal banking and business relationships established to provide "ongoing" services, dealings, or other financial transactions to make clear that this term is not intended to cover infrequent transactions such as the occasional purchase of a money order or a wire transfer. 68 Fed. Reg. 25,092, 25,092 (May 9, 2003). As a result, not all bank remittances transactions fall within the requirements of the customer identification program rule. According to OCC, most banks only permit "customers" with "accounts" to engage in remittance transfers; however, some do not and the customer identification program may not apply to these situations when a non-customer is permitted to engage in remittance transfers.

[55]Financial Crimes Enforcement Network, *Financial Institutions Outreach Initiative: Report on Outreach to Money Services Businesses* (July 2010).

According to IRS BSA examination data for fiscal years 2013 and 2014, inadequate recordkeeping was the third most frequently cited BSA violation during examinations of money transmitters. See appendix II for more information.

Expectations for Depository Institutions That Have Money Transmitters as Customers

Depository institutions open and maintain accounts for money transmitters. FinCEN and the federal banking regulators have provided interagency guidance for depository institutions that provide banking services to money transmitters, which outlines the following minimum due diligence expectations based on BSA requirements:

- applying the depository institution's customer identification program;
- confirming FinCEN registration, if required;
- confirming compliance with state or local licensing requirements, if applicable;
- confirming agent status, if applicable;[56] and
- conducting a basic BSA risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.[57]

A representative from a depository institution whom we interviewed stated that the institution conducted due diligence on money transmitter customers that included an on-site visit and a review of their financial

[56]A person who is a money transmitter solely because that person serves as an agent of another money services business (such as a money transmitter) is generally not required to register with FinCEN. 31 C.F.R. § 1022.380(a)(3). However, these agents are required to establish AML programs and comply with other recordkeeping and reporting requirements. See 31 C.F.R. § 1022.210(d)(1)(iii).

[57]In determining how much, if any, further due diligence is required for a money transmitter customer, depository institutions should consider the types of products and services the money transmitter offers, the location(s) and the market(s) it serves, anticipated account activity, and the purpose of the account. Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States* (April 2005). The Office of Thrift Supervision was abolished in 2010 by the Dodd-Frank Act. Pub. L. No. 111-203, § 313, 124 Stat. 1376, 1523 (codified at 12 U.S.C. § 5413).

statements. This representative also explained that the institution inspected the AML program that the money transmitter had in place. According to the interagency guidance for depository institutions that provide banking services to money transmitters, regulators expect the depository institution to conduct a risk assessment of the account and confirm the money transmitter's compliance with applicable licensing and registration requirements. The guidance notes that regulators do not expect depository institutions to uniformly review the AML program of all money transmitters that are customers, but that a depository institution's level of review of a money transmitters' AML program should be based on the assessed risks of the particular relationship.

Money Transmitters and Depository Institutions Identified Challenges Related to BSA Compliance

Money transmitters, depository institutions, and industry associations we interviewed identified some challenges in complying with BSA requirements, including suspicious activity report confidentiality requirements, derisking, monitoring and examining remittance data, and costs.

Suspicious Activity Report Confidentiality Requirements

Officials we spoke with from a money transmitter and an industry association representing depository institutions stated that suspicious activity report confidentiality requirements hindered global money transmitters and depository institutions from meeting their AML risk management and monitoring requirements. The BSA prohibits financial institutions that file a suspicious activity report from notifying any person involved in the transaction that the transaction has been reported.[58] FinCEN has explained that unauthorized disclosure of suspicious activity reports could undermine investigations by tipping off suspects, deterring financial institutions from filing suspicious activity reports, and threatening the safety and security of institutions and individuals filing such reports. FinCEN warns that the disclosure of suspicious activity reports compromises the essential role they play in protecting the financial system and in preventing and detecting financial crimes and terrorist financing.

[58]31 U.S.C. § 5318(g)(2).

According to FinCEN and the federal banking regulatory guidance, BSA's confidentiality provision generally prohibits a depository institution from disclosing or revealing a suspicious activity report.[59] FinCEN and the federal banking regulators have amended suspicious activity report confidentiality rules and provided guidance to clarify the confidentiality requirements for depository institutions. The 2006 guidance states that a U.S. branch or agency of a foreign depository institution may share a suspicious activity report with its head office outside the United States. In addition, it states that a U.S. depository institution may disclose a suspicious activity report to its controlling company, no matter where it is located. The depository institution must have written confidentiality agreements or arrangements in place specifying that the head office or controlling company must protect the confidentiality of suspicious activity reports through appropriate internal controls. In 2010, FinCEN issued further guidance stating that a depository institution may share a suspicious activity report or any information that would reveal the existence of such a report with domestic affiliates subject to a suspicious activity report regulation, but cannot share suspicious activity reports with foreign branches of U.S. banks.[60] In December 2010, FinCEN amended its BSA regulations on the confidentiality of suspicious activity reports to state that the confidentiality requirements do not prohibit the disclosure of the underlying facts, transactions, and documents upon which a suspicious activity report is

[59]There is an exception for when the disclosure is requested by FinCEN, bank supervisory agencies, or appropriate law enforcement agencies. Financial Crimes Enforcement Network, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, *Interagency Interpretive Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* (Jan. 20, 2006). The Office of Thrift Supervision was abolished in 2010 by the Dodd-Frank Act. Pub. L. No. 111-203, § 313, 124 Stat. 1376, 1523 (codified at 12 U.S.C. § 5413).*See also* 31 C.F.R. §§ 1020.320(e), 1022.320(d).

[60]Financial Crimes Enforcement Network, *Guidance on Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates* (Nov. 23, 2010). For purposes of this guidance, ''affiliate'' of a depository institution means any company under common control with, or controlled by, that depository institution. ''Under common control'' means that another company (1) directly or indirectly or acting through one or more other persons owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution; or (2) controls in any manner the election of a majority of the directors or trustees of the company and the depository institution. ''Controlled by'' means that the depository institution (1) directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or (2) controls in any manner the election of a majority of the directors or trustees of the company. See, e.g., 12 U.S.C. § 1841(a)(2).

based.[61] The preamble to the final rule clarifies that confidentiality rules do not apply to information shared with entities in the ordinary course of business that identify suspicious content but do not indicate whether the information was filed in a suspicious activity report.[62] One industry association requested further guidance—in addition to the language in FinCEN's 2010 final rule clarifying confidentiality rules—on what information could be shared when depository institutions provided information to foreign banks, but could not reveal the existence of a suspicious activity report.

Derisking

With respect to money transmitters, derisking—the practice of depository institutions limiting certain services or ending their relationships with entities to, among other things, avoid perceived regulatory concerns about facilitating money laundering—poses challenges for depository institutions and money transmitters.[63] Depository institutions face compliance challenges in managing risk appropriately while avoiding indiscriminately terminating or refusing to open accounts for money transmitters. Money transmitters need bank accounts to conduct business, including settling accounts among agents and other financial institutions. In 2014, FinCEN reported that some money transmitters are losing access to banking services with depository institutions due to derisking.[64] Additionally, three representatives from money transmitters and affiliated industry groups we spoke with described difficulties in maintaining and forming relationships with depository institutions. A representative from a money transmitter industry group told us that depository institutions should be able to rely on

[61]75 Fed. Reg. 75,593 (Dec. 3, 2010).

[62]75 Fed. Reg. at 75,595.

[63]Derisking can be the result of various drivers, such as concerns about profitability, prudential requirements, anxiety after a global financial crisis, and reputational risk. Financial Action Task Force, *FATF clarifies risk-based approach: case-by-case, not wholesale de-risking,* accessed November 2, 2015, http://www.fatf-gafi.org/documents/documents/rba-and-de-risking.html.

[64]Financial Crimes Enforcement Network, Statement on Providing Banking Services to Money Services Businesses (Nov. 10, 2014). For example, in September 2013, a global bank announced that it ended accounts with some of their money transmitter accounts—including those sending remittances to Somalia—due to the concerns regarding the regulatory risk of financial crimes, including terrorist financing occurring through these accounts. Barclays, *Barclays statement on Money Services Businesses,* accessed September 15, 2015, http://www.newsroom.barclays.com/r/2728/barclays_statement_on_money_service_busine.

the fact that money transmitters are subject to BSA requirements and examinations by state and federal regulators.

According to the FFIEC BSA/AML Examination Manual, however, a number of characteristics of money transmitters could expose depository institutions to risk.[65] For example, the manual specifies that, among other things, money transmitters lack ongoing customer relationships and require minimal or no identification from customers, engage in frequent currency transactions, and are subject to varying levels of regulatory requirements and oversight. Nearly all representatives from depository institutions and affiliated industry groups whom we interviewed said that they had difficulty doing business with money transmitters because of the increased regulatory risk. For example, representatives from all three depository institutions' industry associations added that it was sometimes easier to sever relationships with money transmitters than face the possibility of compliance failure.

Some federal banking regulators have acknowledged that some depository institutions have limited certain types of banking services because of concerns that money transmitter customers might not comply with the BSA. However, federal banking regulators and FinCEN encourage depository institutions to practice a risk-based approach when evaluating individual customers. According to FinCEN's public statement issued in 2014, money transmitters play an important role in the financial services sector.[66] Derisking related to money transmitters could reduce BSA reporting in the financial system if the transmitters went out of business and more remittance transfers were sent via informal methods, which are often outside the reporting system. FinCEN's 2014 public statement discouraged derisking and emphasized that institutions were expected to properly manage and mitigate any risks that money transmitters presented on a case-by-case basis. FDIC has provided similar guidance, and the Comptroller of the Currency has publicly echoed it by explaining that high-risk customers should be managed with strong risk management and controls rather than with a strategy of total

[65]Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2014).

[66]Financial Crimes Enforcement Network, Statement on Providing Banking Services to Money Services Businesses (Nov. 10, 2014).

avoidance.[67] According to a Treasury official, bank regulators have taken very few public enforcement actions against depository institutions for deficiencies related to the money transmitters who have accounts with them.

In a 2015 global Anti-Money Laundering Survey of AML specialists, the Association of Certified Anti-Money Laundering Specialists found that more than one-third of respondents reported that the institutions they worked for had exited lines or segments of business in the past 12 months due to perceived regulatory risk.[68] While this information was not specific to derisking and money transmitters, it speaks to the idea of depository institutions managing regulatory risk by exiting business lines that they perceive to be too risky. Furthermore, two World Bank surveys conducted in 2015, and the corresponding reports, found that some depository institutions are reducing access to financial services for remittance providers in some countries and regions.[69] One of these reports was on a survey of derisking, for which they use the Financial Action Task Force definition of the term—the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk. According to the report, the survey indicates that derisking exists in some countries. The main drivers cited for account closures of money transmitters mainly included: profitability, pressure from other entities involved—such as correspondent banks, fear of regulatory scrutiny, lack of confidence in money transmitters' procedures, and reputational risk. The reports make recommendations, including for governments to monitor correspondent banking and money transmitters' access to financial services, and to have legal and regulatory AML frameworks in place and ensure that financial institutions are being effectively supervised for compliance with these standards—including

[67]Federal Deposit Insurance Corporation, *Statement on Providing Banking Services*, FIL-5-2015 (Jan. 28, 2015). Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Association of Certified Anti-money Laundering Specialists (Mar. 17, 2014).

[68]Survey respondents included, among others, representatives from both depository institutions and money transmitters.

[69]World Bank, *Fact Finding Summary from De-risking Surveys*: *Withdrawal from Correspondent Banking: Where, Why, and What to Do about It and Report on the G20 Survey on De-risking Activities in the Remittance Market* (Washington D.C.: November 2015). The *G20 Survey on De-risking Activities in the Remittance Market* noted that there was a low response rate from banks and money transmitters, but considered the data to be reflective of the market since they had responses from money transmitters that covered a substantial portion of market share of the remittance market.

ensuring and communicating risk-based supervision and enforcement. The recommendations also suggest that money transmitters should improve their AML controls to reduce their risk profile, and national authorities and financial institutions need to improve and communicate their overall understanding of risk.

Challenges in Monitoring and Examining Remittance Data

Money transmitters and depository institutions that we interviewed indicated that they faced challenges in monitoring and examining data from remittance transactions. Representatives from three of the four depository institutions we spoke with described difficulties they faced in identifying and preventing illicit activity, including the need to constantly monitor and examine transactions and identify structuring activity. FinCEN similarly recently reported that one of the key challenges banks faced was adequately adapting their controls on a timely basis to eliminate vulnerabilities that criminals were exploiting. One money transmitter industry group representative told us that keeping money transmitters' monitoring systems up to date with the changing behavior of criminals was a challenge. This representative said that law enforcement and FinCEN are helpful in providing them with guidance and information on new patterns of activity. For example, FinCEN issued a notice in 2014 to be aware of illicit movement of money from the Los Angeles garment district to Mexico and Colombia on behalf of prominent drug trafficking organizations. In the 2015 Association of Certified Anti-Money Laundering Specialists survey, 38 percent of respondents cited insufficient/outdated technology as a compliance challenge that could serve as a possible barrier to the monitoring of remittance transactions.

Compliance Costs

Both money transmitters and depository institutions that we spoke with said that the costs of complying with BSA requirements and potential new rules presented a challenge. One money transmitter industry group representative told us that compliance cost is a challenge that is quite substantial for money transmitters. For example, one large money transmitter told us that they are implementing a system to better monitor their customers that is costing them millions of dollars. A representative from another money transmitter told us that there are costs associated with compliance, including additional expenses for training employees and integrating a system that helps the transmitter identify suspicious activity and prevent illicit transactions. Officials from a credit union we spoke with said that compliance cost is a challenge for smaller credit unions because establishing effective BSA and AML programs is expensive and smaller institutions have fewer resources to absorb such expenses. One industry association representing community banks added that it is especially difficult for smaller institutions that do not have

the resources to spend time and money to monitor and examine riskier customers that require enhanced due diligence. Furthermore, a representative from a large depository institution said that it was becoming increasingly expensive to keep up with compliance costs as the regulatory environment seems to be getting stricter with a recent number of consent orders and fines.

Personal Liability of Compliance Officers

Money transmitters and depository institutions that we spoke with identified concerns about the personal liability of compliance officers. In January 2014, FinCEN's director acknowledged that there had been calls for more accountability in compliance failures, in particular for a focus on individuals as well as institutions.[70] The director stressed the importance of holding accountable those who violated BSA requirements. In 2014, FinCEN assessed a $1 million civil money penalty against the Chief Compliance Officer of a large money transmitter concluding that he willfully violated the BSA requirements to implement and maintain an effective AML program and to report suspicious activity.[71] FinCEN found that as a result of the Chief Compliance Officer's AML failures, agents and outlets—that the money transmitter's personnel knew or suspected were involved in fraud and money laundering—were allowed to continue to use the money transmitter's money transfer system.

Officials we spoke with from six institutions representing money transmitters and depository institutions expressed concern about the liability of compliance officers under the BSA, but one official representing a credit union thought personal responsibility was long overdue. One money transmitter said that holding compliance officers personally accountable was inappropriate. An industry association representative said that it was counterproductive if a compliance officer was negligent and not complicit in illegal activity and stated that hiring and retaining compliance officers was becoming a challenge. Another industry association representing depository institutions told us that if there is a trend of holding compliance officers responsible for AML failures, it may become increasingly difficult to hire qualified people for the position. Officials from one credit union and two industry associations stated that the personal liability of compliance officers could cause compliance

[70]Remarks of Jennifer Shasky Calvery, Director, FinCEN, Securities Industry and Financial Markets Association, Anti-money Laundering and Financial Crimes Conference (Jan. 30, 2014).

[71]*In the Matter of Thomas E. Haider*, FinCEN Matter No. 2014-08 (Dec. 18, 2014).

officers to be more risk averse—potentially resulting in the decisions of depository institutions to derisk money transmitter accounts in order to avoid personal liability and scrutiny. However, an official from a credit union said that the shift toward compliance officer personal responsibility was probably long overdue. FinCEN and OCC issued statements and advisories promoting the culture of compliance and stating that an important aspect of a culture of compliance is leadership's responsibility for the performance, including the institution's compliance with BSA requirements.[72] DOJ has also issued a memo that stresses the importance of individual accountability to combat corporate fraud and other misconduct, and provides DOJ's policy for investigations of corporate misconduct that focuses on individual liability.[73]

Remittance Transfers Pose Money Laundering Risks

Remittance transfers are vulnerable to money laundering due to factors such as the large volume of transactions and the global reach of large remittance transfer companies. Stakeholders have identified money laundering risks of remittance transfers including risks involving agents, customers, geographic location, and products. Remittance transfers can be used to launder proceeds from different types of criminal activities, including drug trafficking, human smuggling, and consumer fraud.

Agents, Customers, Geographic Location, and Products Can Pose Money Laundering Risks

Agency officials, industry stakeholders (including money transmitters and depository institutions), and international organizations have identified several types of money laundering risks associated with remittance transfers, including risks involving agents, customers, geographic location, and products. Remittance transfers are vulnerable to money laundering due to factors such as the large volume of transactions, which can make it difficult to detect laundered funds, and the global reach of large remittance transfer companies, which can allow customers to move

[72]Financial Crimes Enforcement Network, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*, (Aug. 11, 2014), Remarks by Thomas J. Curry Comptroller of the Currency Before the Association of Certified Anti-Money Laundering Specialists (Mar. 17, 2014).

[73]Department of Justice, Deputy Attorney General, *Individual Accountability for Corporate Wrongdoing,* Memorandum for the Assistant Attorney General, Antitrust Division; Assistant Attorney General, Civil Division; Assistant Attorney General, Criminal Division; Assistant Attorney General, Environment and Natural Resources Division; Assistant Attorney General, National Security Division; Assistant Attorney General, Tax Division; Director, Federal Bureau of Investigation; Director, Executive Office for United States Trustees; All United States Attorneys (Washington D.C.: Sept. 9, 2015).

funds easily around the world. Furthermore, Treasury reported that deficient compliance with BSA requirements could leave money transmitters and depository institutions vulnerable to money laundering.[74] Additionally, FinCEN, law enforcement, and international organizations said that certain remittance transfer methods, such as unregistered informal value transfer systems discussed earlier, pose risks that are difficult to manage because law enforcement has limited visibility of these transactions. However, they cautioned that a single risk may not indicate money laundering, but risks should be considered in the aggregate.

Agent Risk

Money transmitters often work with a number of agents, and maintaining adequate oversight can be challenging, given the decentralized nature of the agent system. In a 2011 survey that FinCEN conducted, 170 money services businesses—often working in the capacity of a money transmitter—reported that they had over 230,000 agents—with 3 of these money services businesses reporting that they had over 20,000 agents each.[75] These agents present money laundering risks if they knowingly or unknowingly fail to follow BSA requirements or the policies and programs established by the money transmitter. For example, an agent may not follow the recordkeeping requirements for transfers above the regulatory funds transfer threshold or above lower thresholds that a remittance provider has self imposed.

Customer Risk

Customers are another source of risk, because in certain instances they may be able to launder money while remaining anonymous. For example, money launderers may use false identities or straw men (individuals hired to conduct transfers on behalf of others) in order to keep from being identified as the original source of the funds. Money launderers may also keep transactions below the regulatory recordkeeping and reporting requirements or the money transmitter's self-imposed recordkeeping requirements in order to remain anonymous. The FFIEC BSA/AML Examination Manual provides examples of suspicious customer activity that may indicate money laundering. These examples include identification documents that cannot be easily verified; the use of different taxpayer identification numbers with variations of the same name;

[74]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

[75]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

frequent or large transactions with no record of past or present employment; and reluctance to provide identification for transactions subject to identification requirements. Law enforcement officials added other indicators, such as receiving multiple transfers from different geographic locations (both domestic and international), and using variations of names and addresses that are inconsistent with the identification provided.

Geographic Location Risk

Agency officials, industry stakeholders, and international organizations generally agreed that certain geographic locations may be more vulnerable to money laundering via remittances. For example, FinCEN has noted the importance of factoring in geographic risk for both depository institutions and money transmitters. In addition, one regulator said that international transfers were at a high risk for money laundering because, depending on the destination country, transparency could be lost if the country receiving the remittance did not have the same AML standards as the United States. The FFIEC BSA/AML Examination Manual states that financial institutions with foreign offices or branches should comply with local requirements and be consistent with the U.S. bank's standards; however, foreign offices' or branches' standards may need to be tailored for local laws and regulations. The FFIEC BSA/AML Examination Manual also states that depository institutions should factor geographic location into their BSA risk assessments. While geographic location alone does not determine a customer's or transaction's money laundering risk level, according to the FFIEC BSA examination manual, certain characteristics can contribute to a location's designation as high risk.[76] A number of sources exist for money transmitters and depository institutions to identify high-risk geographic locations. Some of these include countries subject to Office of Foreign Assets Control sanctions, jurisdictions determined to be of "primary money laundering concern" by Treasury, High Intensity Financial Crime Areas, and those identified by

[76]These include the presence of offshore financial centers, a previous high-risk designation based on experience, and known money laundering risks as identified in the Department of State's annual International Narcotics Control Strategy Report. U.S. Department of State, *2015 International Narcotics Control Strategy Report, Volume II: Money Laundering and Financial Crimes* (March 2015).

the Financial Action Task Force as having deficient AML and counter-terrorist financial measures.[77]

Products/Services Risk

The U.S. financial system provides a wide range of products and services that help create a complex environment in which, according to Treasury, both legitimate and unlawful activity can take place. According to the FFIEC BSA/AML Examination Manual, certain products and services, such as funds transfers, may pose a higher risk of money laundering because of the degree of anonymity they can offer. For example, emerging technologies can offer a degree of anonymity and new providers entering the market may not be compliant with existing regulations. The Financial Action Task Force identified money laundering and terrorist financing risks associated with mobile payments because these services can sometimes allow for anonymous transactions depending on the level of AML measures the mobile payments provider has in place. The Financial Action Task Force also reported that virtual currency—digital representations of value that are not government-issued, such as Bitcoin—could facilitate international remittances as virtual currency-based products and services are developed. FinCEN recognizes money laundering vulnerabilities in virtual currencies. In 2013 FinCEN issued guidance clarifying that administrators and exchangers of virtual currency were considered money transmitters and thus were subject to the same BSA requirements.[78]

The FFIEC BSA/AML Examination Manual listed correspondent account relationships as services, in particular, for which depository institutions should manage risk. As discussed earlier, multiple depository institutions may be involved in remittance transfers—known as correspondent banking relationships—and assessing the risk of each of them can be

[77]The Office of Foreign Assets Control within Treasury administers and enforces sanctions such as blocking assets or restricting trade against countries and groups of individuals, such as terrorists and narcotics traffickers. Beginning in 2000, Treasury and Justice designated certain areas as High Intensity Financial Crime Areas: Chicago, Illinois; Los Angeles, California; San Francisco, California; Miami, Florida; San Juan, Puerto Rico; the southwest border (Texas and Arizona); and New York and New Jersey. High Intensity Financial Crime Area designations were designed to allow law enforcement to concentrate resources in areas where money laundering or related financial crimes were occurring at a higher-than-average rate.

[78]Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies Guidance,* FIN-2013-G001 (Mar. 13, 2013).

difficult. According to FinCEN, approximately 300 banks in the United States provide correspondent banking services to foreign financial institutions. U.S. banks may receive funds or instructions for a funds transfer from a foreign correspondent bank. While U.S. banks may have a relationship with the foreign bank, they probably do not have a relationship with the originator of the funds transfer. For this reason, the FFIEC BSA/AML Examination Manual and FinCEN stress the importance of conducting appropriate due diligence with foreign banks as part of risk management programs.

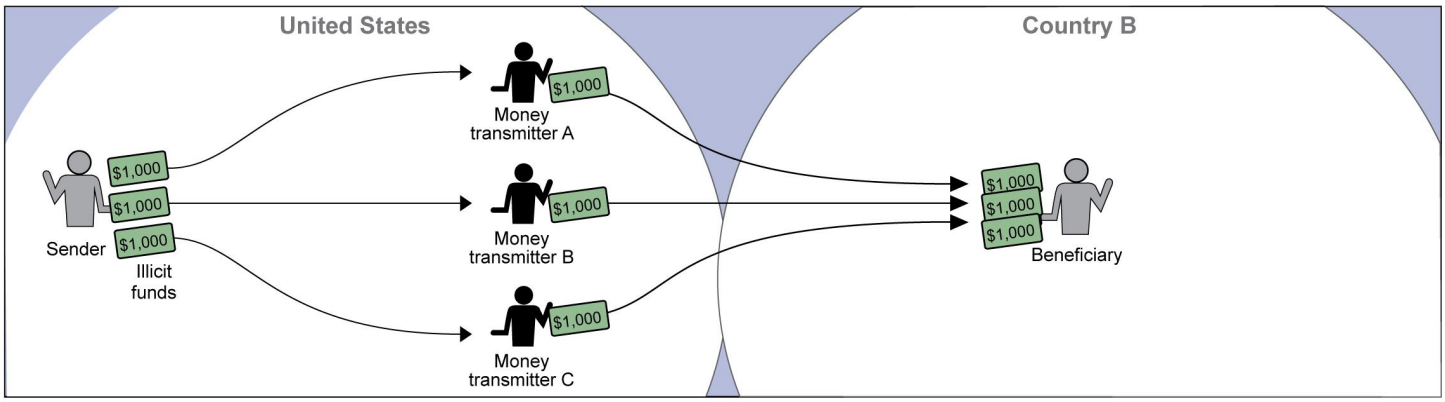
Remittances Have Been Used to Launder Proceeds from Criminal Activity

Federal agencies and international organizations have identified instances where remittances have been used to launder proceeds from illicit activities such as drug trafficking, human smuggling and trafficking, and consumer fraud. To transmit illicit funds, money launderers use underground providers such as couriers, hawaladars, and straw men (persons hired to conduct transfers for others), or transfers made by several people to the same beneficiary. They may also provide false information during the identification process for a remittance. Structuring is another means of disguising large proceeds from illicit activities. It generally involves dividing a large transaction into several smaller transactions to evade BSA reporting requirements.[79] As shown in figure 4, an individual could remit $1,000 to the same beneficiary in three separate transactions. Since each of the individual remittances is below the $3,000 reporting threshold, this activity avoids recordkeeping and reporting requirements. Structuring is considered both a criminal activity in itself and a potential method for hiding the proceeds of other suspicious activity.[80]

[79]Specifically, under BSA regulations, a person structures a transaction if that person, acting alone, or in conjunction with, on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, in any amount at one or more financial institutions, on one or more days, in any manner, for the purpose of evading specified reporting requirements. 31 C.F.R. § 1010.100(xx).

[80]*See* 31 U.S.C. § 5324, which prohibits structuring and imposes a criminal penalty.

Figure 4: Example of Structuring to Launder Illicit Funds



Source: GAO (analysis); Art Explosion (images). | GAO-16-65

In its 2015 National Money Laundering Risk Assessment, Treasury identified structuring as a common money laundering method used in the United States, and a money laundering vulnerability for money transmitters.[81] FinCEN data on suspicious activity report filings related to international remittances by money services businesses, including money transmitters, showed that structuring—after fraud—was the second most frequently cited suspicious activity category in 2014.[82] Treasury has identified instances in which structuring was used to hide and transmit illicit funds, such as the following:

- In 2007, a task force made up of federal, state, and local law enforcement in New York and New Jersey conducted a sting operation in which 27 money transmitters were prosecuted for facilitating money laundering. The money transmitters allegedly agreed to transfer drug proceeds to Colombia and structured the transactions in order to avoid federal recordkeeping and reporting requirements.[83]

[81]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

[82]Data on suspicious activity report filings related to international remittances have some limitations. See appendix I for more information.

[83]United States Attorney's Office, Eastern District of New York, Twenty-Seven Individuals Charged in Continuing Probe of Drug Money Laundering in Money Remitter Industry, news release, February 7, 2007.

- In 2008, in California, four family members were indicted for running a small human smuggling ring that had allegedly been bringing illegal immigrants into the United States from Mexico since 1996, earning approximately $50,000 a year.[84] According to the indictment, the defendants instructed the sponsors of the illegal immigrants to pay the smuggling fee, which ranged from $1,000 and $3,000 per person, via nonbank wire transfer and to structure the payment across multiple wires.

- In a 2011 case, seven people were sentenced for money laundering and drug trafficking involving the transfer of drugs from the Virgin Islands to Alaska. Hundreds of thousands of dollars in payment for the drugs were sent using a large money transmitter to send wire transfers in amounts averaging less than $2,000 per wire.[85]

Drug trafficking

Transactions made using cash generated from drug trafficking can be structured to remain below the recordkeeping and reporting thresholds. In 2010 a Florida bank was charged with willfully failing to establish an adequate AML program. The charge followed a criminal investigation into $13 million of wire transfers initiated by Mexican casas de cambio (exchange houses) from correspondent accounts at the bank to pay for aircraft subsequently used to transport illegal drugs to the United States.[86] In addition, officials at the Department of Homeland Security (DHS) told us that employees of a money transmitter helped launder over $1 million in drug proceeds to the Dominican Republic.

Human smuggling and human trafficking

Human smuggling involves bringing or attempting to bring undocumented immigrants into the United States.[87] Human trafficking involves the use of

[84]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington D.C.).

[85]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

[86]USA v. Wachovia Bank N.A., Deferred Prosecution Agreement, 10-20165-CR-Lenard, March 16, 2010; See also OCC, In the Matter of Wachovia Bank, National Association, Consent Order for a Civil Money Penalty, #2010-036, March 10, 2010. OCC found that Wachovia N.A. "failed to implement adequate policies, procedures, or monitoring controls governing the repatriation of nearly $14 billion of USD bulk cash for high risk casa de cambio and other foreign correspondent customers."

[87]*See* 8 U.S.C. § 1324.

force, fraud or coercion to recruit, harbor, transport, provide, or obtain persons for purposes including forced labor and sexual exploitation.[88] There are a number of stages involved in human smuggling and in human trafficking during which smugglers and traffickers may need to interact with remittance providers. For example, to avoid detection, smugglers may make multiple remittance payments below the recordkeeping and reporting thresholds to people who are paid to move undocumented immigrants to the United States. In 2010 a large money transmitter entered into a $94 million settlement with the state of Arizona after it was accused of processing over $500 million in payments to human smugglers annually between 2003 and 2007.[89]

One money transmitter we spoke with provided internal guidance that it relies on to help identify possible human smuggling payments. This guidance included the following examples:

- A customer picks up money transfers in agent locations along the U.S. border from multiple senders in various parts of the United States. All of the transactions are for similar dollar amounts.

- A customer picks up a money transfer at an agent location along the U.S. border and is accompanied by another person. The other person appears to be telling the customer what to do. After the transaction is completed, the customer gives the money to the other person.

FinCEN has issued guidance to financial institutions listing red flags that could indicate human smuggling or trafficking.[90] The guidance encourages financial institutions to file a suspicious activity report if they suspect a transaction has no legitimate business purposes and could be related to human smuggling or trafficking.

[88]*See* Financial Crimes Enforcement Network, *Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags*, FIN-2014-A008 (Sept. 11, 2014) (citing 18 U.S.C. §§ 1581, 1584, 1589, 1590, 1591, 2421, 2422, 2423, 2425; The Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386 (2000)).

[89]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

[90]Financial Crimes Enforcement Network, *Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags*, Advisory FIN-2014-A008 (Sept. 11, 2014).

This FinCEN guidance also states that no single transaction by itself is a clear indicator of human smuggling or human trafficking but that several warning signs can indicate this type of behavior. These include multiple wire transfers below the $3,000 threshold sent to a common beneficiary from various locations, wire transfers from countries with high migrant populations, and the existence of a potential funnel account.[91] The amounts wired may be kept below the reporting threshold and occur in locations where the customer does not reside. According to Treasury, efforts by state and federal law enforcement to curb the use of money transmitters to pay human smugglers along the southwest border has resulted in a shift to funnel accounts, using the banking system rather than money transmitter networks.

However, law enforcement officials from the southwest border High Intensity Financial Crime Area told us that, in their experience, a large percentage of human smuggling fees were sent using money transmitters because these providers offered a quick and reliable method of transfer with some degree of perceived anonymity for the smugglers and their couriers. These officials said that over $12 million in suspected illicit human smuggling proceeds were sent to Texas border cities through money transmitters in the 4-month period between January and April 2015.

Consumer fraud

Money transmitters and depository institutions have been used to facilitate consumer fraud, such as lottery scams or scams involving a relative's stolen identity, as identified in a recent enforcement action, Federal Trade Commission (FTC) consumer complaint data, and by the Internet Crime Complaint Center—the federal cybercrime complaint organization. The Internet Crime Complaint Center describes various schemes that defraud consumers into wiring funds directly to fraudsters, resulting in virtually unrecoverable losses to the victim and with little recourse. One federal banking regulatory official explained that fraudsters request victims to use wire transfer services to send funds because the money moves fast and they can take the money before the victim discovers the scam.

[91]According to FinCEN, a funnel account is a bank account located in one geographic area that receives multiple deposits, often in amounts below the cash reporting threshold. Funds are often withdrawn from someone in a different geographic location with little time elapsing between deposits and withdrawals. *See* FinCEN (May 2014) Advisory FIN-2014-A005 for a detailed description of funnel accounts.

In 2012, DOJ found that a large money transmitter's agents knowingly participated in a scheme in which U.S. customers wired funds to Canada in response to fraudulent claims that they were required to pay a fee or tax before receiving a lottery winning that they were falsely told was due them.[92] The large money transmitter agreed with DOJ to address the problems in its AML program that facilitated fraud. According to recent FTC consumer compliant data, the highest reported payment method used in cross-border fraud complaints in 2014 was a wire transfer.[93] This consumer complaint data showed that 55 percent of the complaints from U.S. consumers who paid companies located in Canada reported wire transfer as the payment method, and 78 percent of the complaints from U.S. consumers who paid other foreign companies reported that wire transfers were the payment methods. Treasury reported that, along with drug trafficking, fraud generates a large amount of illicit proceeds in the United States each year.[94] According to FinCEN data on suspicious activity report filings related to international remittances by money services businesses, including money transmitters, fraud was the most frequently cited suspicious activity in 2014.[95]

[92]Moneygram Deferred Prosecution Agreement, Statement of Facts, November 9, 2012.

[93]Federal Trade Commission, International Consumer Complaints, January – December 2014 (June 2015).

[94]Department of the Treasury, *2015 National Money Laundering Risk Assessment* (Washington, D.C.).

[95]Data on suspicious activity report filings related to international remittances have some limitations. See appendix I for more information.

Many Stakeholders Supported Lowering the Funds Transfer Threshold, but Cited Concerns with Verifying Remitters' Legal Immigration Status

Many stakeholders, including law enforcement officials, four of the five money transmitters we spoke with, and all four depository institutions, told us they generally supported or were already using a funds transfer threshold lower than the existing $3,000 for obtaining identification and other information on remittances. For example, law enforcement officials said that a centralized database of remittance transfers—one result of a proposed rule that would require remittance providers to report certain remittance data at low dollar thresholds—would help identify illicit activity and be useful in assisting AML efforts. Most larger money transmitters and larger depository institutions we spoke with were already using thresholds below $3,000. However, some stakeholders said that a lower threshold could negatively affect small providers. For example, federal and state banking regulators said that a lower threshold would likely create additional recordkeeping requirements and costs for some providers and customers. But, stakeholders generally said that a requirement to check the legal immigration status of remittance senders would not significantly benefit AML efforts, noting that the requirement could lead senders to use less detectable forms of transmitting money.

Many Stakeholders Supported a Lower Threshold, but Some Were Concerned about Additional Recordkeeping Requirements and Costs

Law enforcement officials generally stated that a funds transfer threshold lower than the existing $3,000 threshold would benefit agencies' AML efforts. Several law enforcement agencies, including DHS, DOJ, and IRS, indicated in 2006 that additional information collected as a result of lowering or eliminating the threshold would prove beneficial to investigations including money laundering.[96] The law enforcement officials added at that time that lowering or eliminating the threshold could disrupt illicit transfers and make them more expensive for perpetrators. For example, DOJ law enforcement officials stated that a lower threshold would increase the cost of laundering money, because more transfers would have to be structured to stay below the threshold. DHS officials we spoke with recommended a $500 funds transfer threshold, which they said would be low enough to limit structuring capabilities but would not impede legitimate transactions. DOJ officials, while noting the benefits of a lower threshold, also identified some concerns. For example, DOJ's

[96]Financial Crimes Enforcement Network, Federal Reserve, Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds, Joint Advance Notice of Proposed Rulemaking, 71 Fed. Reg. 35,564 (June 21, 2006). Several law enforcement agencies commented on this advance notice of proposed rulemaking.

letter commenting on the 2006 advance notice of proposed rulemaking (2006 advance notice) stated that there were no specific data showing that a lower threshold would benefit law enforcement, as transactions structured at smaller values could approach the range of legitimate transactions and thus become more difficult to detect.[97]

Many law enforcement officials supported a requirement for reporting information on remittances. BSA requirements generally focus on recording funds transfers rather than reporting them, unless they constitute certain types of transactions such as suspicious transactions. Several law enforcement agencies supported and noted the benefits of adding such a reporting requirement in a 2006 FinCEN study.[98] Furthermore, DHS and DOJ officials we spoke with for this report said that information on remittance senders that could be collected in a centralized database could be analyzed to help identify illicit activity and would be useful in AML efforts. DHS officials noted that they used a comprehensive database to track remittances from 10 of the largest money transmitters that report remittance data along the southwest border to identify human smuggling networks. These officials said that having these type of data at the federal level would be useful. One DOJ official stated that the option most favorable to law enforcement in investigating illicit transfers would be FinCEN's 2010 proposed rule, Cross-Border Electronic Transmittals of Funds (2010 proposed rule), which would require depository institutions and money transmitters to report cross-border electronic transmittals at a zero dollar threshold and $1,000 threshold, respectively—lower dollar thresholds than providers are currently required to use.[99] The reporting requirement would provide a searchable database of remittances for law enforcement to analyze, while information provided by a lower funds transfer threshold without a reporting requirement would have to be requested by law enforcement on a case-by-case basis. FinCEN is still evaluating ways to implement the 2010 proposed rule in a way that takes into account industry concerns such as the cost to financial institutions and the government's ability to implement, manage, and support a reporting

[97]A DOJ official we interviewed said that the observations from this letter were generally still valid.

[98]Financial Crimes Enforcement Network, *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* (October 2006).

[99]Financial Crimes Enforcement Network, Cross-Border Electronic Transmittals of Funds, Notice of Proposed Rulemaking, 75 Fed. Reg. 60,377 (Sept. 30, 2010).

system. FinCEN also continues to consider the appropriate reporting thresholds.

Four of the five money transmitters we spoke with, and all four depository institutions, told us they generally supported or were already using a lower funds transfer threshold for obtaining identification and other information on remittances. Stakeholders we spoke with noted that these providers were generally already collecting and maintaining information at lower thresholds. Larger depository institutions often used a zero dollar threshold. For example, all four of the depository institutions we spoke with said they were already using a zero dollar threshold as part of their customer identification and recordkeeping practices. Also, in FinCEN's studies of the 2010 proposed rule, FinCEN determined that banks, by and large, keep records for funds transfers regardless of dollar value.

Nearly all of the money transmitters we interviewed also said that they already had self-imposed thresholds of around $1,000 for verifying and collecting information on funds transfers, and that most of their transactions were significantly below the $3,000 funds transfer threshold. The $1,000 threshold is an industry and international standard recommended by the Financial Action Task Force and, according to FinCEN in the 2010 proposed rule, adopted by many countries, which money transmitters must follow when operating in their jurisdictions. Some states have also implemented a recordkeeping threshold below the federal requirement that money transmitters in those states must comply with. For example, Arizona and Oklahoma have implemented a $1,000 threshold for recording certain information, including some identifying information.[100]

In the 2010 proposed rule, FinCEN stated that through extensive consultation with the industry, the threshold for money transmitters to report on international transfers of $1,000 or more was appropriate because the industry in large part already observed this threshold. Money transmitters we spoke with or stakeholders that commented on the 2006 advance notice generally did not advocate reducing the threshold for money transmitters to zero dollars, noting that eliminating the funds transfer threshold would be burdensome for them and would likely drive transactions underground. Similarly, law enforcement officials from DHS,

[100]*See* Ariz. Rev. Stat. Ann. § 6-1241(E); Okla. Admin. Code § 85:15-7-5.

DOJ, and IRS indicated that they did not support reducing the threshold to zero for money transmitters because doing so could impede legitimate transactions and cause remitters to resort to alternative methods of laundering proceeds. DHS officials noted that they would still have the authority to investigate alternative remittance systems.

Some stakeholders had concerns about a lower threshold, however, largely because of the additional recordkeeping and costs that would be involved. Some of these stakeholders also indicated that information already collected was sufficient, and that the additional cost to monitor the information at a lower amount would not be worth the benefits of law enforcement tracking such small amounts. Federal and state banking regulators we spoke with generally did not advocate for a lower funds transfer threshold. Officials from these regulators believed that reducing the threshold would require increased recordkeeping for banks, and one state regulator believed that it could increase costs for both providers and regulators which would need to review more transactions. In our review of the published comments to FinCEN's 2006 advance notice we found that nearly half (12 of the 25 commenters) recommended no change in the threshold largely because of the additional recordkeeping and costs involved. The comments opposed to lowering the threshold were mostly from or referred to relatively small community banks or credit unions that were opposed to the additional recordkeeping, in part because they were not already collecting and maintaining information for transactions below the federal threshold. Some of these commenters noted that additional recordkeeping and verification requirements would increase costs that would be passed on to customers, who then might turn to alternate forms of transmitting money.

Most Stakeholders Raised Concerns That Requirements to Verify Legal Immigration Status Would Increase the Use of Less Detectable Forms of Remittances

Most parties we spoke with, including officials from law enforcement, money transmitters, depository institutions, industry associations, and policy and consumer advocacy groups, voiced concerns about the implications of requiring verification of legal immigration status of remittance senders. Law enforcement officials we spoke with told us that a requirement to verify legal immigration status might not assist AML efforts and could lead senders to use less detectable forms of transmitting money, as the following examples illustrate.

- IRS officials said that the Remittance Status Verification Act would, if passed, effectively require an identification verification threshold of near zero and the collection of information on de minimis, or very minor, transaction amounts.[101] IRS concluded that verifying identities and collecting information at a near zero dollar threshold would not be useful and could cause remitters to resort to off-the-book methods.

- DHS officials we spoke with said that, in general, collecting identification information would be beneficial to investigations but that verifying legal immigration status would not necessarily hurt or help their investigations. They added that a lower funds transfer threshold was more crucial to their investigations. DHS officials did say that knowing senders' legal immigration status could be beneficial if DHS was looking at potentially removing illegal immigrants from the country. But they added that the verification requirements could drive remitters to informal remittance systems. One official noted that although criminals could turn to alternative methods of transferring money to avoid being identified, it could take several years to establish a new criminal financial network, and could result in a positive AML effect for a time—at least until the criminals identified alternative networks.

In interviews with us, officials from the five money transmitters, four depository institutions, six of their respective industry associations, and three policy and consumer advocacy groups nearly all raised concerns about asking for information from remittance senders about their legal immigration status in the United States. Among other things, they said doing so would likely contribute to pushing remittances out of formal financial systems to less detectable methods. Officials from two money transmitters we spoke with compared the potential outcomes to those they observed when the state of Oklahoma imposed a requirement they

[101]As discussed previously, the Remittance Status Verification Act would amend the Electronic Fund Transfer Act (EFTA), so the proposed law, if passed, would be subject to EFTA's definition of remittance transfer. 15 U.S.C. § 1693o-1(g)(2). Regulation E, which implements EFTA, excludes small value transactions of $15 or less from its definition of remittance transfer. 12 C.F.R. § 1005.30(e)(2)(i).

felt had similar implications.[102] According to these officials, the enactment of the Oklahoma legislation led to a significant drop of around 28 percent in their Oklahoma remittances shortly after the law was passed. However, an official from one of these money transmitters stated that the volume of transfers in surrounding states increased by as much as half during the same time period—indicating that some customers went to bordering states to conduct remittances to avoid the fee in Oklahoma. An official from the Oklahoma Bureau of Narcotics & Dangerous Drugs Control stated that he believed that the Oklahoma remittance fee had helped reduce transfers of proceeds from illicit activity from Oklahoma, adding that the amount collected annually in wire transmitter fees had increased.[103]

Agency Comments and Our Evaluation

We provided a draft of this report to CFPB, DHS, DOJ, Federal Reserve, FDIC, FTC, IRS, NCUA, OCC, Treasury, and USPS for review and comment. NCUA and USPS provided written comments that are described below and reprinted in appendixes III and IV. Officials from DHS, Federal Reserve, FDIC, OCC, and Treasury provided technical comments, which we incorporated as appropriate. CFPB, DOJ, FTC, and IRS had no comments on the report. In its letter, USPS said that they had no comments. In its letter, NCUA noted that the scale and scope of international remittances raise significant public policy issues, and that this report will go far toward informing the debate about constructive remittance policy.

[102]As discussed previously, Oklahoma enacted a law in July 2009 requiring that a fee be imposed on all remittances that originate in Oklahoma. Although this law does not require providers to verify legal immigration status of remitters, it imposes a fee on all remittances, regardless of remitters' legal status, and only those remitters who file income tax returns with the state may claim a credit for the fee paid. Since individuals who do not have proof of legal status are unlikely to have a valid Social Security number or tax identification number, they are unlikely to file income tax returns, and therefore unlikely to obtain a credit for the remittance fee paid.

[103]For wire transmitter fee collections increasing in Oklahoma, see *Oklahoma Tax Commission, Annual Reports* (Oklahoma City, OK: June 30, 2011 through 2015). Also, there may be other economic factors contributing to the increase in Oklahoma wire transfer collections, including generally low remittance revenue during the recession from 2007 through 2009. See Suírez-Orozco, Marcelo M., *The Remittance Hole*, Americas Quarterly, vol. 3, no. 2 (Spring 2009), 85-89.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to CFPB, DHS, DOJ, Federal Reserve, FDIC, FTC, IRS, NCUA, OCC, Treasury, USPS, the appropriate congressional committees and members, and others. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-8678 or evansl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

Lawrance L. Evans, Jr.
Director, Financial Markets and Community Investment

Appendix I: Objectives, Scope, and Methodology

Our objectives were to examine (1) the Bank Secrecy Act (BSA) remittance requirements that exist for remittance providers and related challenges that remittance providers face in complying with these requirements; (2) the money laundering risks that remittance transfer methods pose; (3) stakeholders' views on the extent to which requiring remittance providers to verify identification and collect information at a lower dollar transaction amount than is currently required, or adding a requirement to verify legal immigration status, would assist federal agencies' anti-money laundering (AML) efforts.[1]

To examine BSA remittance requirements for remittance providers, we reviewed relevant laws and regulations and obtained information from remittance providers on their efforts to comply with BSA (including their methods and practices) and the challenges they faced in these efforts. We also obtained and analyzed available data on money transmitters' compliance with BSA-related requirements. Compliance data we reviewed included Internal Revenue Service (IRS) BSA-related violation and exam data on money transmitters for fiscal years 2013 and 2014. We assessed the reliability of data provided to us by IRS by reviewing related documentation of the database from which the data come and also through interviews with agency officials, and found the data to be reliable for purposes of this report.

To examine the money laundering risks posed by remittance transfers, we reviewed and summarized available reports and documents that the Financial Crimes Enforcement Network (FinCEN), federal law enforcement, regulatory agencies, international organizations, and remittance providers maintained on money laundering through remittance transfers. We also collected and reviewed information from the Department of Justice (DOJ) and Department of Homeland Security (DHS) on closed money laundering cases from fiscal year 2006 to April 2015 involving remittance providers.

[1]We obtained stakeholder views on both (1) lowering or eliminating the reporting dollar threshold for collecting and retaining information on funds transfers and (2) imposition of a requirement that individuals document immigration status for funds transfers beginning at a near-zero threshold. Because imposing these requirements beginning at a low dollar threshold may result in similar challenges and benefits for law enforcement, stakeholders views on a lower dollar threshold for required BSA recordkeeping may inform our discussion of the potential effects of the immigrant status documentation requirement GAO has ongoing work underway that will be reporting on the reliability of remittance estimates in a separate report that it plans to issue in fiscal year 2016.

We also reviewed FinCEN data on the number of suspicious activity reports filed by money transmitters related to remittance transfers to determine the most frequently reported categories of suspicious activity. FinCEN noted that there were some limitations regarding the data on suspicious activity report filings related to international remittances. The totals of suspicious activities reported could exceed the actual number of reports filed because some reports can reflect more than one type of suspicious activity. For example, a single suspicious activity report may be counted in "Money Laundering" and "Structuring" because both categories in that report were selected. The data we reviewed were based on the number of money transmitters that selected "funds transfer" when reporting the type of payment mechanism involved in the suspicious activity; however, the statistics are incomplete because some filers (about 40 percent) did not fill out the payment mechanism. Additionally, the data are incomplete because the filers may not have filled out relevant fields that would identify whether a transfer was a remittance. We assessed the reliability of suspicious activity report data through interviews with agency officials and comparing information to published data. Although FinCEN noted limitations with the data, we found the data to be reliable for purposes of reporting the top two categories of suspicious activity filed by remittance providers, which were consistent with common methods of money laundering identified in the Department of the Treasury's 2015 *National Money Laundering Risk Assessment*.

For purposes of our report, stakeholders included officials from 30 entities: FinCEN, federal law enforcement entities—including representatives from a High Intensity Financial Crime Area, federal and state regulators, industry associations, money transmitters, depository institutions, and policy and consumer advocacy groups. To examine stakeholders' views on the extent to which lowering the funds transfer threshold for complying with recordkeeping requirements or adding a legal immigration status verification requirement would assist agencies' AML efforts we reviewed an advance notice of proposed rulemaking, a proposed rule, and proposed legislation related to remittance transfers—including 25 public comment letters available on the advance notice and proposed rule. We also obtained, through interviews, the views of stakeholders on the extent to which lowering the funds transfer threshold or adding a legal immigration status verification requirement (which could include requiring certain identification for transfers at the near zero dollar threshold) would further AML efforts. We researched and reviewed information on international customer identification standards for remittance transfers. Sources for this information included, among others: the Financial Action Task Force report, *International Standards on*

Combating Money Laundering and the Financing of Terrorism and Proliferation: The Financial Action Task Force Recommendations (February 2012); the Financial Action Task Force, *Money Laundering through Money Remittance and Currency Exchange Providers* (June 2010); Department of State report, *Country Reports on Terrorism 2013*; FinCEN's report, *Feasibility of a Cross Border Electronic Funds Transfer System under the Bank Secrecy Act*; and PricewaterhouseCoopers, *Anti Money Laundering – Know Your Customer Quick Reference Guide* (January 2014).

For all objectives, we interviewed officials from FinCEN and federal law enforcement entities—including DHS, DOJ, and DHS representatives from the Southwest High Intensity Financial Crime Area. We also interviewed federal banking regulators and officials from the Conference of State Banking Supervisors, which included representatives from state banking regulators. In addition, we interviewed agency officials at the Consumer Financial and Protection Bureau and the Federal Trade Commission. We interviewed officials from depository institution industry associations including the American Bankers Association, The Clearing House, and Independent Community Bankers of America. We also interviewed money transmitter industry associations including The Money Services Roundtable, The National Money Transmitters Association, and the Association of Certified Anti-Money Laundering Specialists—representing both money transmitters and depository institutions. Additionally, we interviewed representatives from a policy group, Inter-American Dialogue, and two consumer advocacy groups—National Council of La Raza and Appleseed. Furthermore, we interviewed a selection of money transmitters and depository institutions. We judgmentally selected a cross-section of medium and large money transmitters and depository institutions that included five nondepository money transmitters and four depository institutions (two banks and two credit unions) based on a number of factors, including the volume of remittances and diversity of countries serviced. For all objectives, we also reviewed reports and guidance published by FinCEN and international organizations such as the World Bank and the Financial Action Task Force.

We conducted this performance audit from October 2014 to December 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: IRS Bank Secrecy Act Examinations of Money Transmitters

Under delegated authority from the Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS) examines nondepository financial institutions—including money transmitters—for compliance with the Bank Secrecy Act (BSA).[1] According to IRS data, the results of examinations of money transmitters from fiscal years 2013 and 2014 showed that the top three most frequently cited violations were failure to comply with AML program requirements, failure to file suspicious activity reports, and inadequate recordkeeping of funds transfers.

Table 1: Summary of IRS Bank Secrecy Act Examinations of Money Transmitters, Fiscal Years 2013-2014

	Fiscal year 2014	Fiscal year 2013
Number of exams	**2,729**	**3,073**
Number of violations	**6,104**	**8,659**

Top 3 most frequently occurring violations:	Fiscal year 2014	Fiscal year 2013
AML program requirements[a]	3,191	3,554
Reports of suspicious activity[b]	1,323	2,893
Recordkeeping—funds transfers[c]	531	838

Source: IRS data and GAO analysis. | GAO-16-65

[a]AML Compliance Program Violations 1022_210, 1022_210(d)(1), 1022_210(d)(2), 1022_210(d)(3), 1022_210(d)(4). These subcategory violations are all requirements for maintaining an adequate AML program. Subcategories include policies, procedures, and internal controls; designation of compliance officer; training; and independent review, respectively.

[b]Reporting violations 1022_320(a), 1022_320(b), 1022_320(c) . Money transmitters are required to file reports of any suspicious transaction relevant to a possible violation of law or regulation. 31 C.F.R. § 1022.320.

[c]Recordkeeping violation 1010_410(e). Money transmitters are required to obtain and retain specific information, such as the name and address of the sender, for each transfer of $3,000 or more. 31 C.F.R. § 1010.410(e).

[1]*See* 31 C.F.R. § 1010.810(b)(8).

Appendix III: Comments from the National Credit Union Administration

National Credit Union Administration
Office of the Executive Director

October 29, 2015

Lawrance L. Evans, Jr.
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Evans:

We have reviewed the U.S. General Accountability Office's report, entitled *International Remittances: Money Laundering Risks and Views on Enhanced Customer Verification and Record Keeping Requirements* (GAO-16-65).

NCUA agrees with the report's underlying premise – namely, the scale and scope of international remittances (and the role of depository institutions in these remittances) raises significant public-policy issues. The report implicitly acknowledges the first step in developing a sound policy response is systematic exploration of all aspects of the issue. To that end, it provides an excellent primer on the attendant money-laundering risks. At the same time, it also strikes a delicate balance in weighing the benefits of stricter controls and record-keeping (such as lowering the current reporting threshold of $3,000) against the cost of driving remittance activity underground.

NCUA believes this report will go far to informing the debate about constructive remittance policy. Thank you for the opportunity to comment.

Sincerely,

Mark Treichel
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320

Appendix IV: Comments from the United States Postal Service

JOSEPH CORBETT
CHIEF FINANCIAL OFFICER
EXECUTIVE VICE PRESIDENT

UNITED STATES POSTAL SERVICE

October 30, 2015

Mr. Lawrance L. Evans, Jr.
Director, Financial Markets and Community Investment
United States Government Accountability Office
441 G Street, Northwest
Washington, DC 20548-0001

Dear Mr. Evans, Jr.:

Thank you for the opportunity to review and comment on the draft GAO report to Congress titled *International Remittances: Money Laundering Risks & Views on Enhanced Customer Verification and Recordkeeping Requirement (GAO-16-65).*

We have reviewed the draft report and have no comments to add beyond those already reflected in the document.

Thank you,

Joseph Corbett

cc: Mr. Nickerson
Mr. Berthold
Ms. Hitzeroth

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-5000
202-268-5272
FAX: 202-268-4364
www.usps.com

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Lawrance L. Evans, Jr. (202) 512-8678 or evansl@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Andrew Pauline (Assistant Director), Verginie Tarpinian (Analyst-in-Charge), Tonita Gillich, Elvira Josifi, Daniel Kaneshiro, Angela Messenger, and Ashton Warren made key contributions to this report. Also contributing to this report were Emily Chalmers, Pamela Davidson, Marc Molino, and Patricia Moye.

Appendix VI: Accessible Data

Agency Comment Letter

Text of Appendix III: Comments from the National Credit Union Administration

Page 1

National Credit Union Administration

Office of the Executive Director

1775 Duke Street, Alexandria, VA

October 29, 2015

Lawrance L. Evans, Jr.

Director, Financial Markets and Community Investment

U.S. Government Accountability Office

441 G Street, NW Washington, D.C. 20548

Dear Mr. Evans:

We have reviewed the U.S. General Accountability Office's report, entitled International Remittances: Money Laundering Risks and Views on Enhanced Customer Verification and Record Keeping Requirements (GA0-16-65).

NCUA agrees with the report's underlying premise - namely, the scale and scope of international remittances (and the role of depository institutions in these remittances) raises significant public-policy issues. The report implicitly acknowledges the first step in developing a sound policy response is systematic exploration of all aspects of the issue. To that end, it provides an excellent primer on the attendant money-laundering risks. At the same time, it also strikes a delicate balance in weighing the benefits of stricter controls and record-keeping (such as

lowering the current reporting threshold of $3,000) against the cost of driving remittance activity underground.

NCUA believes this report will go far to informing the debate about constructive remittance policy. Thank you for the opportunity to comment.

Sincerely,

Mark Treichel

Executive Director

Text of Appendix IV: Comments from the United States Postal Service

Page 1

JOSHEP CORBETT

CHIEF FINANCIAL OFFICER

EXECUTIVE VICE PRESIDENT

UNITED STATES POSTAL SERVICE

October 30, 2015

Mr. Lawrance L. Evans, Jr.

Director, Financial Markets and Community Investment

United States Government Accountability Office

441 G Street, Northwest

Washington, DC 20548-0001

Dear Mr. Evans, Jr.:

Thank you for the opportunity to review and comment on the draft GAO report to Congress titled International Remittances: Money Laundering Risks & Views on Enhanced Customer Verification and Recordkeeping Requirement (GA0-16-65).

We have reviewed the draft report and have no comments to add beyond those already reflected in the document.

Thank you,

Joseph Corbett

cc:

Mr. Nickerson

Mr. Berthold

Ms. Hitzeroth

475 L’ENFANT PLAZA SW

WASHINGTON, DC 20260-5000

202-268-5272

F.AX:202-268-4364

www.usps.com