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

December 30, 2019

The Honorable Sheldon Whitehouse
Ranking Member
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

The Honorable Bill Cassidy, M.D.
United States Senate

The Honorable Marco Rubio
United States Senate

Countering Illicit Finance and Trade: U.S. Efforts to Combat Trade-Based Money Laundering

The breadth and depth of the U.S. financial system make it a prime target for transnational criminal organizations to launder the illicit proceeds of their crimes, as well as for terrorists and other hostile actors to hide the source of the funds that finance their activities. The Financial Action Task Force, an intergovernmental body that sets internationally recognized standards for developing regimes to counter money laundering and the financing of terrorism, identifies trade-based money laundering (TBML) as one of the primary means that criminal organizations use to launder illicit proceeds. TBML is the process of moving the value of the proceeds of crime through trade transactions to attempt to disguise its origins and integrate it into the formal economy.[1] According to the Department of the Treasury (Treasury), TBML is one of the most challenging forms of money laundering to investigate because of the complexities of trade transactions and the sheer volume of international trade.[2] In addition to TBML, criminal organizations may also be involved in other trade-facilitated financial crimes, such as customs fraud or tax evasion. U.S. law enforcement agencies believe there has been an increase in TBML activity attributable, in part, to U.S. financial institutions' improved compliance with Bank Secrecy Act (BSA) requirements, such as cash reporting requirements and anti-money laundering (AML) laws.[3]

You asked us to provide information on U.S. efforts to combat TBML. This report describes (1) TBML-related vulnerabilities in the U.S. financial and trade systems; (2) the types of criminal

[1] The basic techniques of TBML include over- and under-invoicing of goods and services; multiple invoicing of goods and services; over- and under-shipments of goods and services; and falsely describing goods and services.

[2] In addition to basic TBML schemes, more complex schemes include the black market peso exchange, which evolved in part to circumvent restrictive currency exchange policies in Colombia but is not limited to specific geographic locations. Department of the Treasury, *National Money Laundering Risk Assessment* (Washington, D.C.: June 12, 2015).

[3] Department of the Treasury, *2018 National Money Laundering Risk Assessment* (Washington, D.C.: Dec. 20, 2018).

organizations that seek to exploit those vulnerabilities; (3) U.S. agencies' use of available data to detect and combat TBML and related schemes; and (4) efforts to develop and employ new tools and technologies that could address vulnerabilities to TBML and related schemes.[4] This report includes the slides we provided to your staff on December 10, 2019 (see enclosure I).

To address these objectives, we reviewed reports and other documentation from the Departments of Commerce, Homeland Security, Justice, and the Treasury, and the federal banking regulators (Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, National Credit Union Administration, and Office of the Comptroller of the Currency), which examine financial institutions to ensure compliance with Bank Secrecy Act and anti-money laundering regulations.[5] We also interviewed officials from the Departments of Homeland Security, Justice, and the Treasury (including the Internal Revenue Service), as well as the U.S. Postal Service and the federal banking regulators. We interviewed law enforcement officials from two interagency task forces focused on combating transnational organized crime: the Organized Crime Drug Enforcement Task Force and the El Dorado Task Force.

We reviewed reports by international organizations, financial institutions, academics, and others that identify TBML-related risks and vulnerabilities. We also interviewed representatives from the private sector, including two banks with large trade finance and correspondent banking operations, the shipping industry, technology firms, international organizations, and other subject-matter experts.

We reviewed documentation related to the information systems and sources of data used by U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement's Homeland Security Investigations (HSI). We reviewed a CBP report on a proof-of-concept pilot project exploring the use of blockchain technology as a digital replacement for CBP's existing paper-based system of processing trade-related documents.[6] We interviewed technology providers that are exploring the use of blockchain for the international shipping and marine cargo insurance industries. We also interviewed representatives of a large financial institution that is piloting a new technology to streamline its trade finance operations. While we identified these efforts as having the potential to address challenges related to TBML vulnerabilities, we did not evaluate their efficacy at doing so.

We conducted this performance audit from January 2019 to December 2019 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

[4] This review is one of multiple reviews that address your request. We have additional reviews that are evaluating other issues related to TBML, including practices international organizations and selected countries recommend for detecting and combating TBML and U.S. agencies' collaboration with international organizations to combat TBML, among other things.

[5] For more information about the Bank Secrecy Act and its implementing regulations, including requirements of financial institutions and the role of the federal financial regulators, see GAO, *Bank Secrecy Act: Agencies and Financial Institutions Share Information but Metrics and Feedback Not Regularly Provided*, GAO-19-582 (Washington, D.C.: Aug. 27, 2019).

[6] Distributed ledger technology (e.g., blockchain) allows users to carry out digital transactions without the need for a centralized authority. For more information on distributed ledgers and blockchain, see GAO, *Science and Tech Spotlight: Blockchain & Distributed Ledger Technologies*, GAO-19-704SP (Washington, D.C.: Sept. 16, 2019).

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

BSA and AML regulations provide important tools in federal law enforcement efforts to detect and deter the use of financial institutions for criminal activity. Treasury's Financial Crimes Enforcement Network (FinCEN), as the administrator of the BSA, has responsibilities that include collecting, analyzing, and disseminating information received from covered institutions (such as banks).[7] FinCEN primarily relies on federal financial regulators to conduct examinations of U.S. financial institutions to determine compliance with BSA/AML requirements and has delegated BSA/AML examination authority to these regulators.[8] Law enforcement agencies play a role in conducting criminal investigations related to money laundering and BSA noncompliance, and the Department of Justice prosecutes violations of federal criminal statutes, including money laundering offenses. Additionally, CBP enforces the customs and trade laws of the United States and collaborates with law enforcement agencies on civil and criminal cases involving trade fraud.

According to Treasury, since 2013 there has been a consistent decrease in bulk cash seizures reported by agencies throughout the United States that suggests that transnational criminal organizations may be increasing their use of international funds transfers to wire money across borders as part of TBML schemes.

U.S. Financial and Trade Systems Have Vulnerabilities That Criminal Organizations Seek to Exploit

Financial institutions have responsibilities based on Bank Secrecy Act and anti-money laundering requirements to, among other things, report suspicious financial transactions to the Department of the Treasury. However, financial institutions have limited visibility into the underlying documentation of the majority of trade transactions for which they process the payments, which makes it more difficult for them to identify suspicious activity. For example, one of the primary vulnerabilities of the U.S. financial and trade systems is open-account trade, in which the transaction is not financed by a bank. In open-account trade, the financial transaction between the buyer and seller—which underpins the trade transaction—is usually processed

[7] Covered financial institutions, including banks, are required to have policies and procedures that include key AML requirements based on the BSA that, at a minimum, must (1) establish a system of internal controls to ensure ongoing compliance; (2) conduct AML compliance training for appropriate personnel; (3) provide for independent testing of BSA compliance—such as testing transactions for adherence to recordkeeping and reporting requirements and reviewing filing of suspicious activity reports and currency transaction reports; (4) designate a person or persons responsible for managing BSA compliance; and (5) establish risk-based customer due diligence procedures. In addition, a customer identification program, which enables the institution to form a reasonable belief of the true identity of the customer, must be included as part of the BSA/AML compliance program.

[8] FinCEN has delegated its BSA examination authority to other federal agencies, including the federal banking regulators, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Federal Housing Finance Authority. See 31 C.F.R. § 1010.810(b). The Internal Revenue Service and CBP have also been delegated authority to investigate criminal BSA violations. See 31 C.F.R. § 1010.810(c). The federal banking regulators also have authority to examine banks for compliance with BSA requirements under 12 U.S.C. § 1818(s). In general, to ensure compliance with the BSA, the federal financial regulators examine institutions' AML policies and procedures, transaction monitoring systems, and suspicious activity reporting, using a risk-based approach with the flexibility to apply greater scrutiny to business lines that pose a higher level of risk to the institution.

through a bank’s automatic payment systems, without human intervention, by the bank sending the payment on behalf of its customer. As such, the financial institution has limited visibility into the underlying reason for the payment.

Additionally, the large volume and complexities of international trade transactions, as well as the limited resources and varying priorities of customs agencies to identify and investigate illicit trade, make the U.S. financial and trade systems attractive for illicit activity, including TBML and related schemes. Criminal organizations commonly commingle legitimate trade with illicit trade, further complicating the identification of suspicious activity.

U.S. Agencies Primarily Identified Transnational Criminal Organizations, Particularly Narcotics Trafficking Organizations, as Employing TBML and Related Schemes

U.S. law enforcement agencies told us that the types of organizations using TBML schemes are primarily transnational criminal organizations involved in narcotics trafficking, customs fraud, and financial fraud schemes, as well as professional money launderers and terrorist organizations. Narcotics trafficking organizations use a particular kind of TBML—known as black market peso exchange schemes—to transfer the value of U.S. dollars earned from narcotics sales in the United States into other countries’ currencies. In black market peso exchange schemes, the contents, prices, and quantities of goods exported and imported can be correctly reported to customs agencies, with no use of fraudulent trade documents, complicating the identification of anomalies in patterns of behavior based on those categories. Although U.S. agencies have primarily identified organizations involved in narcotics trafficking as using black market peso exchange schemes, other criminal organizations are engaged in TBML and related schemes.

U.S. Agencies Use Trade, Financial, and Law Enforcement Data in Their Efforts to Detect and Investigate TBML and Related Schemes

U.S. agencies, such as HSI, use import and export data, suspicious financial activity reported by financial institutions, and law enforcement investigative data to identify patterns and anomalies in financial and trade transactions. Law enforcement agencies and FinCEN also use these data to develop leads for and support ongoing investigations of TBML and related schemes. For example, in 2010 FinCEN issued an advisory to financial institutions based on its analysis of suspicious activity reports (SAR) filed by financial institutions. FinCEN highlighted the increasing use of TBML schemes by criminal organizations—particularly narcotics trafficking organizations in the Western Hemisphere—and potential indicators of TBML that financial institutions should consider as they evaluate potential suspicious activity. Additionally, suspicious financial activity review teams have been established in 94 federal districts around the country, and they bring together investigators and prosecutors from different agencies to regularly review BSA reports, such as SARs and currency transaction reports, related to their geographic area of responsibility.

U.S. Agencies and Private-Sector Entities Are Exploring New Tools and Technologies to Address TBML-Related Vulnerabilities

Several efforts we examined explored the use of distributed ledger technology, including blockchain, to improve supply chain visibility and integrity, both for regulatory agencies and market participants. Additionally, a large bank is piloting a project to digitize and automate its document review process for trade finance transactions. These tools could address challenges related to TBML—such as the use of fraudulent documentation and the general lack of visibility into the underlying documentation of individual transactions on behalf of regulatory agencies and other market participants—in international trade, supply chain integrity, and trade finance.

Agency Comments

We provided a draft of this report to the Departments of Commerce, Homeland Security, Justice, and the Treasury (including the Internal Revenue Service), as well as the federal banking regulators (Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, National Credit Union Administration, and Office of the Comptroller of the Currency) for review and comment. The Departments of Homeland Security and the Treasury, as well as the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, provided technical comments, which we incorporated as appropriate.

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 the appropriate congressional committees, agencies, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://gao.gov.

If you or your staff have any questions about this report, please contact us at (202) 512-8678 or ClementsM@gao.gov or (202) 512-6722 or SheaR@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Michael Clements

Michael Clements
Director, Financial Markets and Community Investment

Rebecca Shea

Rebecca Shea
Director, Forensic Audits and Investigative Service

Enclosures – 2

Countering Illicit Finance and Trade

U.S. Efforts to Combat Trade-Based Money Laundering

December 10, 2019

For more information, contact Michael Clements, (202) 512-8678 or ClementsM@gao.gov; or Rebecca Shea, (202) 512-6722 or SheaR@gao.gov.

Table of Contents

Introduction

- Trade-based money laundering (TBML) is the process of moving the value of proceeds of crime through trade transactions to attempt to disguise its origins and integrate it into the formal economy.
- The Financial Action Task Force (FATF) is an intergovernmental body that sets internationally recognized standards for developing regimes to counter money laundering and the financing of terrorism. FATF identifies TBML as one of the primary means that criminal organizations use to launder illicit proceeds.
- According to FATF and the Department of the Treasury (Treasury), TBML is one of the most challenging forms of money laundering to investigate because of the complexities of trade transactions and the sheer volume of international trade.[1]
- In addition to TBML, criminal organizations can also be involved in other trade-facilitated criminal activity, such as customs fraud, trafficking in counterfeit goods, and tax evasion.

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

Objectives

- What are the TBML-related vulnerabilities in the U.S. financial and trade systems?
- What types of criminal organizations seek to exploit those vulnerabilities?
- How do U.S. agencies use available data to detect and combat TBML and related schemes?
- What new tools or technologies could address vulnerabilities to TBML and related schemes?

Scope and Methodology

- Reviewed reports and other documents from the Departments of Commerce, Homeland Security, Justice, and the Treasury, and the federal banking regulators (Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, National Credit Union Administration, and Office of the Comptroller of the Currency).
- Interviewed officials from the Departments of Homeland Security, Justice, and the Treasury—including the Internal Revenue Service—as well as the U.S. Postal Service and the federal banking regulators.
- Interviewed law enforcement officials from two interagency task forces focused on combating transnational organized crime and illicit finance: the Organized Crime Drug Enforcement Task Force and the El Dorado Task Force.
- Interviewed representatives from two banks with large trade finance and correspondent banking operations, the shipping industry, technology firms, international organizations, and other subject-matter experts.

Scope and Methodology (continued)

- Reviewed reports by international organizations, banks and other financial institutions (such as money services businesses), academics, and others that identify TBML-related risks and vulnerabilities.
- Reviewed documentation related to the information systems and sources of data used by U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement's Homeland Security Investigations (HSI). Reviewed a CBP report exploring use of blockchain technology as a digital replacement for CBP's existing paper-based system of processing trade-related documents.[2]
- Interviewed two technology providers that are exploring the use of blockchain for the international shipping and marine insurance industries. Interviewed representatives of a large bank that is piloting a new tool to streamline its trade finance operations. We identified these projects as examples of efforts to explore new tools or technologies through our discussions with federal agencies and subject-matter experts and our review of publicly available materials. While we identified these efforts as having the potential to address challenges related to TBML vulnerabilities, we did not evaluate their efficacy at doing so.

[2] Distributed ledger technology (e.g., blockchain) allows users to carry out digital transactions without the need for a centralized authority. For more information on distributed ledgers and blockchain, see GAO, *Science and Tech Spotlight: Blockchain & Distributed Ledger Technologies*, GAO-19-704SP (Washington, D.C.: Sept. 16, 2019).

Background – Trade-Based Money Laundering

- The basic techniques of TBML involve the misinvoicing of goods and services, such as through over- and under-invoicing (i.e., trade fraud). However, no single activity by itself is a clear indication of TBML, and criminal organizations attempt to exploit vulnerabilities in anti-money laundering (AML) and trade enforcement efforts in the United States.
- More complicated TBML schemes include the black market peso exchange (BMPE), where merchants—wittingly or not—accept payment in illicitly derived funds, often from third parties to a trade transaction, for exports of goods.
- In 2010, Treasury's Financial Crimes Enforcement Network (FinCEN) estimated that between January 2004 and May 2009 over $276 billion in financial transactions reported as suspicious by financial institutions, including banks, were potentially related to TBML schemes.[3]
- Treasury estimates that the bulk of the illicit proceeds generated in the United States comes from criminal organizations involved in fraud, drug trafficking, human smuggling, human trafficking, organized crime, and corruption, with fraud and narcotics trafficking being the two largest sources of illicit proceeds.[4]

[3] FinCEN, *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering* (Washington, D.C.: Feb. 18, 2010).

[4] Department of the Treasury, *2018 National Money Laundering Risk Assessment* (Washington, D.C.: Dec. 20, 2018).

Background – International Trade

- International trade involves two discrete, but related, transactions, each with its own unique parties to the transaction, along with unique vulnerabilities.
  1) The financial component involves the purchaser and seller and their respective financial institutions, and the payment for the transaction is settled on agreed-upon terms.
  2) The trade component—the physical shipment of goods—also involves the purchaser and seller, but can include many more parties to the transaction, including shipping companies, insurance companies, port and terminal operators, and customs agents in both the exporting and importing countries.

Background – Bank Secrecy Act / Anti-Money Laundering Requirements

- Bank Secrecy Act (BSA) and AML regulations provide important tools in federal law enforcement efforts to detect and deter the use of financial institutions for criminal activity.
- FinCEN, as the administrator of the BSA, has responsibilities that include collecting, analyzing, and disseminating information received from covered institutions (such as banks).
- Covered financial institutions, including banks, are required to have policies and procedures that include key AML requirements based on the BSA that, at a minimum, must
  - establish a system of internal controls to ensure ongoing compliance
  - conduct AML compliance training for appropriate personnel
  - provide for independent testing of BSA compliance—such as testing transactions for adherence to recordkeeping and reporting requirements and reviewing filing of suspicious activity reports (SAR) and currency transaction reports (CTR)[5]
  - designate a person or persons responsible for managing BSA compliance
  - establish risk-based customer due diligence procedures

[5] SARs are reports certain financial institutions are required to file, generally if a transaction 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 (1) involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation, including transaction reporting requirements; (2) is designed to evade any other BSA requirements; or (3) has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction. CTRs are reports institutions generally must file when customers make large cash transactions, currently defined by regulation as those exceeding $10,000.

Background – Bank Secrecy Act / Anti-Money Laundering Requirements (continued)

- FinCEN primarily relies on federal financial regulators to conduct examinations of U.S. financial institutions to determine compliance with BSA/AML requirements and has delegated BSA/AML examination authority to these regulators.[6]
- In general, to ensure compliance with the BSA, the federal financial regulators examine institutions' AML policies and procedures, transaction monitoring systems, and suspicious activity reporting, using a risk-based approach with the flexibility to apply greater scrutiny to business lines that pose a higher level of risk to the institution.

[6] FinCEN has delegated its BSA examination authority to other federal agencies, including the federal banking regulators, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Federal Housing Finance Authority. See 31 C.F.R. § 1010.810(b). IRS and CBP have also been delegated authority to investigate criminal BSA violations. See 31 C.F.R. § 1010.810(c). The federal banking regulators also have authority to examine banks for compliance with BSA requirements under 12 U.S.C. § 1818(s).

Background – Law Enforcement Agencies

- Law enforcement agencies play a role in detecting illicit activity and conducting criminal investigations related to money laundering and BSA noncompliance, and the Department of Justice prosecutes violations of federal criminal statutes, including money laundering offenses.
    - For example, HSI targets transnational criminal organizations, and agents investigate money laundering, illicit finance, and other financial crimes related to how those criminal organizations receive, move, launder, and store their illicit funds.
    - HSI operates the Trade Transparency Unit, which was established to identify global TBML trends and conduct ongoing analysis of trade data provided through partnerships with other countries' trade transparency units.
    - IRS–Criminal Investigations investigates complex and significant money laundering activity, including vital national priorities such as terrorism financing, and transnational organized crime.
    - Other law enforcement task forces, the Organized Crime Drug Enforcement Task Force (part of the Department of Justice) and the El Dorado Task Force (led by HSI), investigate transnational criminal organizations and seek to dismantle the financial networks that support them.
- CBP enforces the customs and trade laws of the United States and collaborates with HSI on civil and criminal cases involving trade fraud.

Background – Recent Trends

- U.S. law enforcement agencies believe there has been an increase in TBML attributable, in part, to U.S. financial institutions' improved compliance with BSA requirements, such as cash reporting requirements and AML laws.[7]
- According to Treasury, since 2013 there has been a consistent decrease in reported bulk cash seizures by agencies throughout the United States that suggests that transnational criminal organizations may be increasing their TBML activity using international funds transfers to wire money across borders as part of TBML schemes.[8]
- Although precise estimates of the magnitude around the world are not available, U.S. agency officials, subject-matter experts, and representatives of international organizations believe the amount of illicit funds laundered through TBML and related schemes—which would include illicit funds derived in other countries that are then laundered into the U.S. financial system—to be large and growing.

[7] Treasury, *2018 National Money Laundering Risk* Assessment.

[8] For more information on international funds transfers, see GAO, *Bank Secrecy Act: Examiners Need More Information on How to Assess Banks' Compliance Controls for Money Transmitter Accounts*, GAO-20-46 (Washington, D.C.: Dec. 3, 2019).

Vulnerabilities of the U.S. Financial and Trade Systems – Open-Account Trade

- One of the primary vulnerabilities of the U.S. financial and trade systems is open-account trade, in which the transaction is not financed by a bank.[9]
- In open-account trade, the financial transaction between the buyer and seller—which underpins the trade transaction—is usually processed through a bank's automatic payment systems, without human intervention, by the bank sending the payment on behalf of its customer. As such, the financial institution has limited visibility into the underlying reason for the payment.
- According to the Wolfsberg Group, 80 percent of international trade that is processed through financial institutions is open-account trade.[10]
  - Financial institutions generally apply standard AML compliance processes and procedures, including sanctions screening, when processing payments for open-account trade transactions.
  - Covered financial institutions that process these funds transfers, or engage in the financing of trade transactions, are required to file SARs with FinCEN for certain transactions that exhibit indicators of potential TBML.

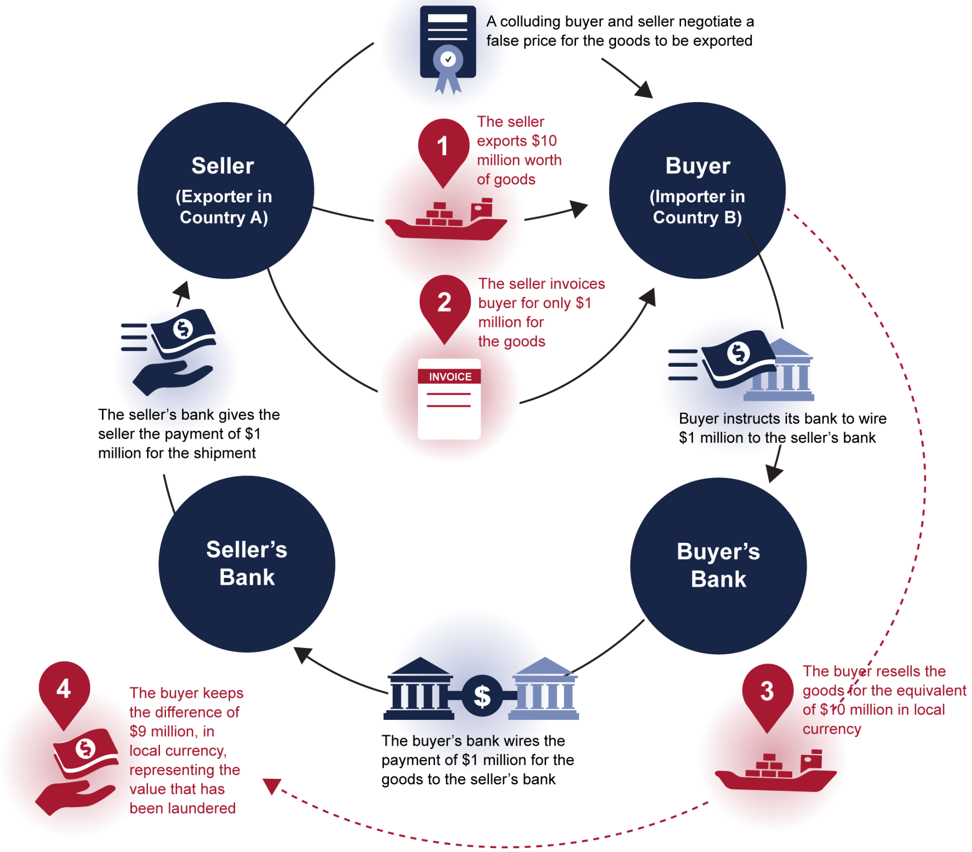
[9] According to the Bankers Association for Finance and Trade, transactions in which a financial institution provides some form of financing to a party in the transaction, such as a letter of credit, are referred to as documentary transactions. In documentary transactions, banks generally process documentation, such as a bill of lading, invoice, or packing list, in order to review the information underlying the transaction for evidence of red flags or indicators of money laundering.

[10] The Wolfsberg Group is an association of 13 global banks that aims to develop frameworks and guidance for the management of financial crime risks.

Vulnerabilities of the U.S. Financial and Trade Systems – Open-Account Trade (continued)

Figure 1: Trade-Based Money Laundering: Open-Account Transactions

Trade-based money laundering is the process of disguising proceeds of crime by moving value through trade transactions to legitimize their illicit origin, often by under- or over-invoicing the payment for the goods. In open-account transactions, the buyer and seller negotiate the terms of the transaction, and their banks process the payments for the transaction often without access to the documents underlying the transaction, such as an invoice or a description of the goods.



A colluding buyer and seller negotiate a false price for the goods to be exported

1 The seller exports $10 million worth of goods

2 The seller invoices buyer for only $1 million for the goods

Buyer instructs its bank to wire $1 million to the seller's bank

The buyer's bank wires the payment of $1 million for the goods to the seller's bank

The seller's bank gives the seller the payment of $1 million for the shipment

3 The buyer resells the goods for the equivalent of $10 million in local currency

4 The buyer keeps the difference of $9 million, in local currency, representing the value that has been laundered

Source: Bankers Association for Finance and Trade. | GAO-20-314R

Vulnerabilities of the U.S. Financial and Trade Systems – Open-Account Trade (continued)

- Subject-matter experts and representatives of banks we spoke with told us that a bank’s ability to identify indicators associated with TBML is limited for open-account transactions.
    - Banks generally do not review documentation such as invoices, bills of lading, or customs declarations in open-account transactions—as would be the case for transactions that are financed by the bank and where the bank is exposed to greater financial risk.
    - FATF has identified a number of indicators that can be used by banks to identify potential instances of TBML, such as the following situations:
        - Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.
        - Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value.
        - The type of commodity being shipped appears inconsistent with the exporter's or importer’s regular business activities.[11]
- However, in open-account transactions, banks would not be examining many of these documents that could allow them to identify suspicious activity associated with the trade transaction, such as under- or over-invoicing.

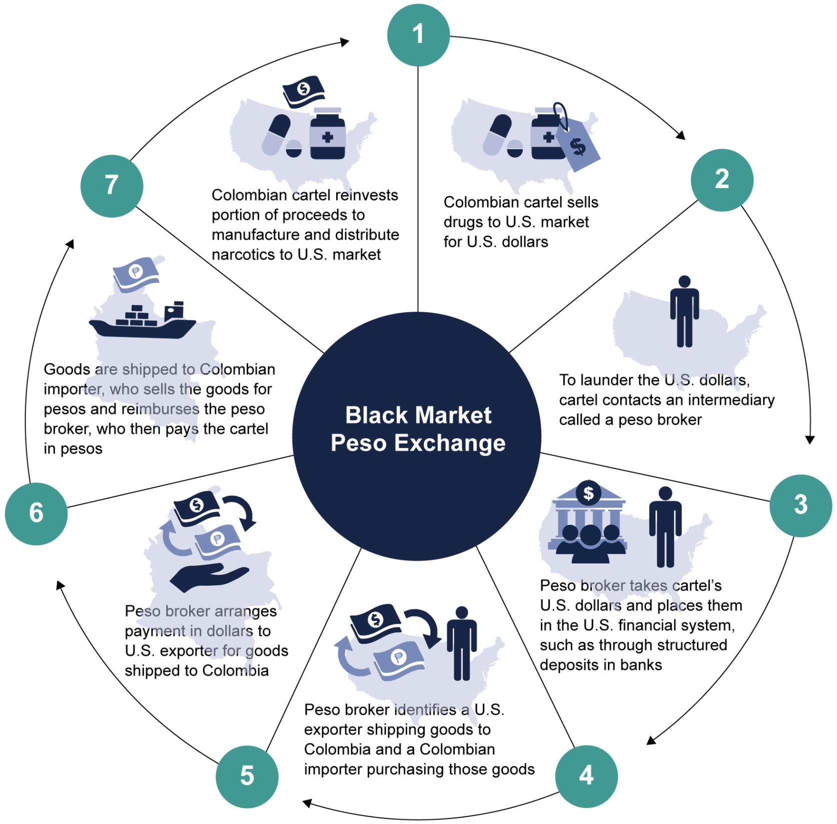
[11] Financial Action Task Force, *Trade Based Money Laundering* (Paris, France: June 23, 2006).

Vulnerabilities of the U.S. Financial and Trade Systems – Large Volume and Complexity of Trade

- According to FATF and U.S. agency officials we spoke with, the large volume of international trade transactions and the limited resources of customs agencies to identify and investigate illicit trade make trade attractive for illicit activity, including TBML and related schemes.[12]
- FATF also identifies the commingling of legitimate trade with illicit trade as a common technique of criminal organizations.
  - For example, in BMPE schemes the contents, prices, and quantities of goods exported and imported can be correctly reported to customs agencies, with no use of fraudulent trade documents, making detection of illicit activity more difficult.

Figure 2: Black Market Peso Exchange

The black market peso exchange is a complex form of trade-based money laundering, typically associated with Colombian narcotics trafficking organizations. The scheme is designed to turn the illicit proceeds from narcotics sales in the United States from U.S. dollars into Colombian pesos (or other local currency). The scheme relies on complicit merchants engaged in regular trade, and the contents, prices, and quantities of goods exported and imported can be correctly reported to customs agencies, with no use of fraudulent trade documents.



Colombian cartel sells drugs to U.S. market for U.S. dollars

To launder the U.S. dollars, cartel contacts an intermediary called a peso broker

Peso broker takes cartel's U.S. dollars and places them in the U.S. financial system, such as through structured deposits in banks

Peso broker identifies a U.S. exporter shipping goods to Colombia and a Colombian importer purchasing those goods

Peso broker arranges payment in dollars to U.S. exporter for goods shipped to Colombia

Goods are shipped to Colombian importer, who sells the goods for pesos and reimburses the peso broker, who then pays the cartel in pesos

Colombian cartel reinvests portion of proceeds to manufacture and distribute narcotics to U.S. market

Source: Department of the Treasury and Department of Homeland Security. | GAO-20-314R

[12] For fiscal year 2018, CBP reported processing $2.65 trillion in imports through more than 300 ports of entry.

Criminal Organizations That Exploit TBML-Related Vulnerabilities

- Law enforcement officials told us that the types of organizations using TBML schemes are primarily transnational criminal organizations involved in narcotics trafficking, customs fraud, and financial fraud schemes, as well as professional money launderers and terrorist organizations.[13]
  - Narcotics trafficking organizations use TBML to repatriate the illicit proceeds of narcotics sales in the United States to other countries in the Western Hemisphere.
  - Terrorist organizations also use TBML to transfer the value of funds internationally, usually to disguise the origin of the funds; to avoid sanctions or other restrictions to countries that are known to be state sponsors of terrorism; or to avoid sanctions to designated terrorist organizations or individuals.
- HSI officials told us that, based on their reporting, the most frequently used method of TBML is BMPE and variations of those schemes, where complicit merchants accept payment in illicitly derived funds for their exports.

[13] According to FATF, professional money launderers are individuals, organizations, and networks that are involved in third-party laundering for a fee or commission. *See* FATF, *Professional Money Laundering* (Paris, France: July 26, 2018).

Criminal Organizations That Exploit TBML-Related Vulnerabilities (continued)

- Organized Crime Drug Enforcement Task Force officials told us the narcotics trafficking organizations they target primarily use BMPE schemes, and in recent years they have seen an increase in the involvement of entities from China.[14]
- Similarly, El Dorado Task Force officials said that the drug trafficking organizations they target primarily use BMPE and related schemes.
  - Recent trends identified by the El Dorado Task Force include the increasing use of shell companies by Chinese entities as well as wire transfers for goods from Chinese companies.
  - According to prosecutors we interviewed at two U.S. Attorney's Offices that have prosecuted TBML cases related to narcotics trafficking organizations, the cases are challenging because of their complexity and because of the amount of time and resources required to investigate and prosecute them. Another major challenge to prosecution of BMPE cases in particular is demonstrating that merchants knowingly accepted illicit funds as payment for their exports.[15]

[14] The Drug Enforcement Administration reported that illicit fentanyl and other synthetic opioids—the most lethal category of opioids used in the United States—are primarily sourced from China and Mexico. See Drug Enforcement Administration, *2018 National Drug Threat Assessment* (Washington, D.C.: Oct. 2, 2018).

[15] In its 2018 *National Money Laundering Risk Assessment*, Treasury reported on an example of a TBML-related prosecution that resulted in guilty pleas. According to Treasury, in December 2017, in Los Angeles, Pacific Eurotex Corp., a textile company, and its owners pleaded guilty to using the business to receive bulk cash that they knew or believed to be the proceeds of narcotics trafficking and part of a BMPE scheme. The owners received approximately $370,000 in cash delivered on four separate occasions as payment for goods shipped to Mexico, Guatemala, and other countries in Latin America.

Criminal Organizations That Exploit TBML-Related Vulnerabilities – FinCEN Advisories to the Private Sector

- In 2010, FinCEN issued an advisory to financial institutions based on its analysis of SARs filed by financial institutions.
  - FinCEN highlighted the increasing use of TBML schemes by criminal organizations—particularly narcotics trafficking organizations in the Western Hemisphere—and potential indicators of TBML that financial institutions should consider as they evaluate potential suspicious activity.
  - Examples of suspicious activity included third-party payments for goods or services made by an intermediary apparently unrelated to the seller or purchaser of goods and a customer's inability to produce appropriate documentation (i.e., invoices) to support a requested transaction.
- In response to law enforcement concern about TBML, FinCEN also issued a geographic targeting order (GTO) in October 2014 that imposed additional reporting and recordkeeping obligations on certain businesses located within the Los Angeles Fashion District in an effort to identify persons and businesses believed to be involved in accepting illicit funds as payment from narcotics trafficking organizations.
- In April 2015, FinCEN, in coordination with HSI and IRS–Criminal Investigations, issued a GTO to several hundred businesses in Miami that export electronics to gather additional information on cash transactions that were potentially related to money laundering schemes used by drug cartels.

U.S. Agencies’ Use of Data to Identify TBML – HSI

- HSI’s Trade Transparency Unit operates the Data Analysis and Research for Trade Transparency System (DARTTS), which its agents use to analyze trade and financial data to generate leads for HSI investigations of TBML and other illicit trade activities.
    - DARTTS incorporates trade data (U.S. imports and exports) reported to CBP and financial data (such as SARs and CTRs) reported to FinCEN.
    - The Trade Transparency Unit also shares and receives import and export data from its counterparts in 17 partner countries, most of which are in the Western Hemisphere.
- HSI Trade Transparency Unit officials we spoke with told us that they typically use DARTTS to support ongoing investigations, particularly when HSI agents in the field have an investigative lead. Trade Transparency Unit analysts can query DARTTS to identify any linkages, generally at the financial or trade transaction level, to provide further information for investigative purposes.
    - Trade Transparency Unit analysts can also use import and export data from their foreign counterparts to identify anomalies in values, contents, or quantities reported to customs agencies.
    - For example, the Trade Transparency Unit can analyze trade pricing data to identify over- or under-pricing of goods, which may be an indicator of TBML.

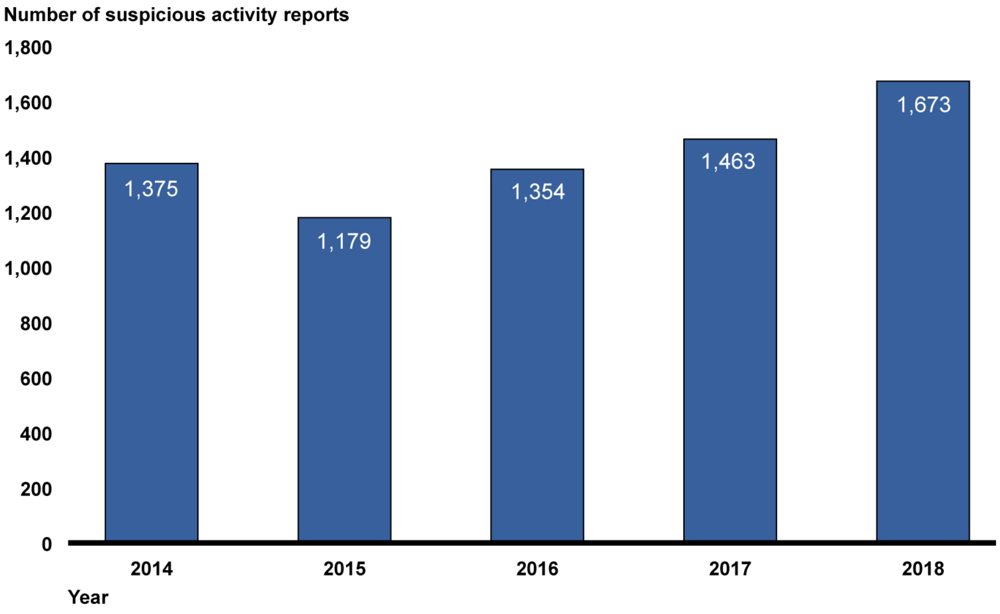
U.S. Agencies' Use of Data to Identify TBML – CBP

- CBP uses the Automated Targeting System (ATS) to identify individuals and cargo that require additional scrutiny before entering or leaving the United States.
  - ATS includes data on incoming cargo, such as bills of lading, importer of record information, descriptions of the goods and the manufacturer, country of origin, and tariff code.
  - CBP analysts use ATS to compare existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, analysis of trends of suspicious activity, law enforcement cases, and raw intelligence.
- CBP officials told us that there is no specific method for targeting suspected TBML schemes in ATS because they cannot confirm any schemes until a shipment and its associated documentation are reviewed.
  - In 2017, ATS began including a broad range of BSA data filed by financial institutions—such as SARs and CTRs—which are incorporated into CBP's traveler, cargo, and conveyance analysis and risk assessments.
  - According to CBP, its analysts use BSA data in ATS to, among other things, identify entities or persons who may need additional scrutiny due to a possible connection to illicit money, drugs, weapons, and terrorism-related activities.

U.S. Agencies’ Use of Data to Identify TBML – FinCEN

- In its 2010 advisory to financial institutions regarding TBML, FinCEN analyzed more than 17,000 SARs covering activity that occurred between January 2004 and May 2009 to identify reports that could be related to TBML schemes.[16]
- In 2012, FinCEN added an option on its SAR form for financial institutions to specifically select “Trade Based Money Laundering / Black Market Peso Exchange” as a type of suspicious activity.
  - Financial institutions filed 7,044 SARs specifically indicating suspected TBML/black market peso exchange activity from 2014-2018 (see fig. 3). During the same period, financial institutions filed more than 9.6 million SARs.
  - However, financial institutions may not have enough information on the suspicious activity to determine whether it is related to TBML schemes, and suspicious activity related to TBML schemes could be reported under different categories.
- FinCEN officials told us they considered updating their analysis of SARs for TBML-related activity, but that agencies with access to trade data, such as HSI and CBP, are better positioned to analyze potential patterns of suspicious financial and trade activity.

Figure 3. Suspicious Activity Reports Filed by Covered Financial Institutions Specifically Indicating Trade Based Money Laundering, 2014-2018



Source: GAO analysis of the Financial Crimes Enforcement Network suspicious activity reports. | GAO-20-314R

Note: Data are as of December 2019. Many factors can contribute to the number of suspicious activity reports filed, such as the amount of global trade and the types of financial institutions involved in those transactions.

[16] According to FinCEN, the financial institutions that filed the SARs clearly identified the activity as TBML or BMPE in 24 percent of the SAR narratives FinCEN analyzed.

U.S. Agencies’ Use of Data to Identify TBML – SAR Review Teams

- SAR Review Teams have been established in 94 federal districts around the country, and they bring together investigators and prosecutors from different agencies to regularly review BSA reports, such as SARs and CTRs, related to their geographic area of responsibility.
- Officials from IRS–Criminal Investigations who lead a SAR Review Team in New York City told us that they search and review SARs based on key terms, often based on the priorities of their office.
  - As previously mentioned, IRS–Criminal Investigations has authority to investigate a wide variety of money laundering crimes in addition to tax crimes, and IRS–Criminal Investigations is a major user of BSA data.
  - According to officials, their review of BSA data significantly contributes to their detection of potential crime and initiation of investigations. Officials also told us that they have recently begun to focus on third-party money launderers and have seen an increase in activity connected to China.[17]

[17] According to FATF, third-party money launderers are persons not involved in the commission of the underlying criminal activity that generated the illicit funds. FATF considers professional money laundering involving individuals, organizations, or networks to be a subset of third party money laundering.

Efforts to Develop and Employ New Tools and Technologies – Overview

- Government agencies and private-sector entities are exploring new technologies that could address challenges related to TBML—such as the use of fraudulent documentation and the general lack of visibility in trade transactions—in international trade, supply chain integrity, and trade finance.
- For example, we spoke with representatives of entities that are exploring the use of distributed ledger technologies that, according to the representatives, could limit the ability of bad actors to manipulate documents associated with trade transactions, such as invoices and forms reported to customs agencies.
- As previously mentioned, while we identified these efforts as having the potential to address challenges related to TBML vulnerabilities, we did not evaluate their efficacy at doing so.

Efforts to Develop and Employ New Technologies – CBP Blockchain Proof-of-Concept

- In 2018, CBP piloted a proof-of-concept assessment to evaluate the application of blockchain technology to the process of submitting documents for cargo entry associated with the North American Free Trade Agreement/Central America Free Trade Agreement.
- The goal of the assessment was to prove that a standards-based, fully digital system could be created to replace the existing paper-based system to improve auditability, increase transparency, and more clearly identify suppliers and manufacturers, which could help better identify fraudulent documentation, among other things.
- Participants in the proof-of-concept included CBP auditors, import and entry specialists, CBP legal and policy personnel, importers, technology companies, and suppliers.

Efforts to Develop and Employ New Technologies – TradeLens

- In January 2018, Maersk and IBM announced their intention to establish a new platform—TradeLens—to provide more efficient and secure methods for conducting global trade using blockchain technology.[18]
- According to a TradeLens press release, the platform is intended to provide timely end-to-end supply-chain visibility for businesses and authorities along the supply chain.
- According to Maersk and IBM, the TradeLens platform is also designed to enable regulatory and customs authorities to closely monitor the flow of goods, carry out risk assessments, and perform regulatory processing in an efficient manner, thereby reducing the risk of illicit activity, including TBML.
- IBM representatives told us that different entities on the platform—manufacturers, shippers, logistics companies, and government regulators—could have different incentives, but improving visibility, auditability, immutability, and trust are shared goals.

[18] Maersk, based in Denmark, is the largest container shipping company in the world.

Efforts to Develop and Employ New Technologies – Guardtime

- Guardtime is a software security company that developed a digital signature system based on blockchain technology. According to a press release, Guardtime worked with Ernst and Young in a joint venture to develop Insurwave, a blockchain-enabled insurance platform for marine cargo.
- Insurwave aims to digitize and automate processes in the commercial insurance industry. It is designed to improve the speed and accuracy for settlements and claims, potentially reducing the risks of entities fraudulently manipulating documents related to trade transactions. The platform went live in 2018.

Efforts to Develop and Employ New Technologies – Bank Trade Finance Operations

- A bank with large trade finance operations announced recently that it is piloting a project to automate and digitize the screening of trade transactions.
  - Bank representatives told us that trade finance has traditionally been a resource-intensive manual process because global trade still depends on paper documents.
  - Bank representatives also told us that because trade is more document-based than other banking activities, it can be susceptible to documentary fraud, exposing the bank to risks of money laundering, terrorist financing, or the circumvention of sanctions.
- As part of the pilot, the bank receives and scans trade transaction documents, such as the bill of lading, into digital format. Those documents are then processed by a character and noun recognition program to detect and classify reportable phrases based on Treasury and Department of Commerce guidelines, such as sanctions screening and export controls.
- According to bank representatives, the pilot is leveraging analytics, machine learning, and statistical transaction monitoring techniques to identify information, trends, connections, and anomalies indicative of TBML or other illicit finance schemes such as fraud.[19]

[19] Officials from the bank’s regulator said they continue to engage with the bank concerning the pilot program to ensure that the bank deploys appropriate risk governance around these initiatives.

Enclosure II: GAO Contact and Staff Acknowledgments

GAO Contacts

Michael Clements at (202) 512-8678 or ClementsM@gao.gov or Rebecca Shea at (202) 512-6722 or SheaR@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Toni Gillich (Assistant Director), Jeff Harner (Analyst in Charge), Georgette Hagans, Pamela Davidson, Dan Luo, Sarah Nielsen, Maria McMullen, Jennifer Schwartz, Tyler Spunaugle, and Mollie Todd made key contributions to this report. Other staff who made key contributions to this report were Ming Chen, Kim Gianopoulos, Juan Gobel, Joyce Y. Kang, and Ryan Vaughan.

(103265)