U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

December 30, 2019

Accessible Version

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 organizations that seek to exploit those vulnerabilities; (3) U.S. agencies' use of available data

[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).

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 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.

---

[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).

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 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.

---

[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.

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

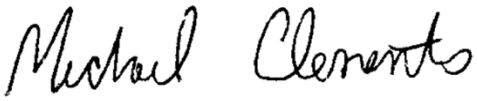
Several efforts we examined explored the use of distributed ledger technology, including blockchain, to improve supply chain visibility and integrity, both for regulatory agencies and market participants. Additionally, a large bank is piloting a project to digitize and automate its document review process 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
Director, Financial Markets and Community Investment

Rebecca Shea
Director, Forensic Audits and Investigative Service

Enclosures – 2

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)