United States Government Accountability Office

Report to Congressional Requesters

November 2021

COUNTERING ILLICIT FINANCE AND TRADE

Better Information Sharing and Collaboration Needed to Combat Trade-Based Money Laundering

GAO-22-447

GAO@100 Highlights

Highlights of GAO-22-447, a report to congressional requesters

November 2021

COUNTERING ILLICIT FINANCE AND TRADE

Better Information Sharing and Collaboration Needed to Combat Trade-Based Money Laundering

Why GAO Did This Study

Criminal organizations and other malign actors exploit vulnerabilities in the U.S. financial and trade systems to obscure the source and destination of ill-gotten proceeds and further their illicit activity. TBML is one of the most challenging forms of money laundering to investigate because of the complexities of trade transactions and the large volume of international trade. U.S. agencies report there has been an increase in TBML activity, in part because criminals are using more sophisticated schemes to avoid detection.

GAO was asked to provide information on U.S. efforts to combat TBML. This report examines, among other things, (1) vulnerabilities in the U.S. financial and trade systems that are exploited to facilitate TBML, (2) the data U.S. agencies use to detect and combat TBML, and (3) the extent to which U.S. agencies collaborate to share information to combat TBML. GAO reviewed U.S. agency reports, data, and other documentation. GAO also interviewed U.S. agency officials and representatives of private-sector entities, including from the financial, trade, and technology sectors.

What GAO Recommends

GAO recommends that (1) the Department of the Treasury establish an interagency mechanism to promote greater information sharing and data analysis, and (2) the Department of Homeland Security take steps to allow the sharing of TTU data with relevant agencies. Treasury emphasized the importance of the TTU sharing data with other agencies. DHS did not concur. GAO continues to believe the recommendation is warranted.

View GAO-22-447. For more information, contact Michael Clements at (202) 512-8678 or ClementsM@gao.gov or Rebecca Shea at (202) 512-6722 or SheaR@gao.gov.

What GAO Found

Trade-based money laundering (TBML) is one of the primary mechanisms criminal organizations and others use to launder illicit proceeds, and the basic techniques involve the mis-invoicing of goods and services, such as through over- and under-invoicing. The Bank Secrecy Act requires, among other things, financial institutions to report suspicious financial transactions to the Department of the Treasury. But for most trade transactions, financial institutions lack visibility into the types of documentation that would allow them to identify suspicious activity. Also, many trade-related documents, such as purchase orders, invoices, and customs documents, are vulnerable to fraudulent manipulation. Criminal organizations exploit these vulnerabilities for other trade-related financial crimes, such as customs fraud, trafficking in counterfeit goods, and sanctions evasion.

The Department of Homeland Security (specifically, U.S. Immigration and Customs Enforcement's Homeland Security Investigations) established the Trade Transparency Unit (TTU) to combat TBML through the analysis of financial and trade data, including import and export data exchanged with partner countries. The TTU uses the Data Analysis and Research for Trade Transparency System (DARTTS) to analyze trade and financial data to identify suspicious transactions that may warrant investigation for money laundering or other crimes. TTU officials told GAO that they conduct most of their analysis in response to specific requests from agents in the field to support ongoing investigations.

TBML schemes often involve many types of illicit activity—such as the trade of counterfeit goods and sanctions evasion—that cut across multiple agencies' roles and responsibilities. However, current federal collaborative efforts to combat TBML do not include some key agencies involved in overseeing trade, and information on suspicious financial and trade activity is siloed among different agencies. For example:

- Treasury's national strategy for combating money laundering does not incorporate the views and perspectives of several agencies positioned to identify illicit trade, as well as private-sector entities, such as freight forwarders. There is no formal collaboration mechanism focused on combating TBML, such as a working group or task force, among federal agencies with anti-money laundering and trade enforcement responsibilities. Such a mechanism could facilitate the sharing of information and data on trade-facilitated financial crimes between federal agencies and with private-sector entities.
- According to agency officials familiar with DARTTS, data from this system are not proactively analyzed to, among other things, identify emerging trends or patterns of illicit activity. Further, the data and analysis are not shared with other relevant agencies involved in combating illicit finance and trade that could potentially identify suspicious activity. TTU officials told GAO that the TTU's data-sharing agreements with partner countries limit its ability to share DARTTS data, but the TTU could take steps to explore ways to incorporate interagency data sharing into those agreements. With access to relevant data, U.S. agencies may be able to better identify emerging risks and trends related to TBML and other illicit trade schemes.

Contents

Letter		1
	Background	5
	Vulnerabilities in U.S. Financial and Trade Systems Include Limited Visibility into Underlying Documentation, Large Volume of Trade, and E-Commerce	12
	Transnational Criminal Organizations and Others Seeking to Undermine U.S. Interests Engage in TBML Schemes	22
	Multiple Federal Entities Use Data to Identify High-Risk Trade Transactions and Support Enforcement Duties	27
	Lack of Government-wide Collaboration Mechanism on Illicit Finance and Trade Limits Agencies' Information Sharing	34
	Banking Regulators Use a Risk-Based Approach To BSA/AML Examinations, and Banks Incorporate Public and Private Data into Their Risk Assessments	43
	Conclusions	45
	Recommendations for Executive Action	45
	Agency Comments and Our Evaluation	46
Appendix I	Private-Sector Entities and U.S. Agencies Are Exploring New Technologies to Better Evaluate Risks of Trade Transactions	49
Appendix II	Comments from the Department of Homeland Security	51
Appendix III	Comments from the Department of the Treasury	54
Appendix IV	GAO Contacts and Staff Acknowledgments	57

Figures

Figure 1: Key U.S. Agencies with Anti-Money Laundering and Trade Enforcement Responsibilities	11
Figure 2: Trade-Based Money Laundering: Open-Account Transactions	14
Figure 3: Example of a Black Market Peso Exchange Scheme	24

Figure 4: Illustration of U.S. Customs and Border Protection's Trade Digitalization Pilot Project Goals to Digitize Global Trade 50

Abbreviations

ACE	Automated Commercial Environment
AML	anti-money laundering
ATS	Automated Targeting System
BMPE	Black Market Peso Exchange
CBP	U.S. Customs and Border Protection
DARTTS	Data Analysis and Research for Trade Transparency System
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FATF	Financial Action Task Force
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve System
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
IRS-CI	Internal Revenue Service Criminal Investigations Division
MARAD	U.S. Maritime Administration
MSB	money services business
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
SAR	Suspicious Activity Report
TBML	trade-based money laundering
Treasury	Department of the Treasury
TTU	Trade Transparency Unit
UNODC	United Nations Office on Drugs and Crime
USTR	U.S. Trade Representative

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

November 30, 2021

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

The Honorable Chuck Grassley
United States Senate

The Honorable Marco Rubio
United States Senate

The Honorable Sheldon Whitehouse
United States Senate

Criminal organizations, terrorists, and other malign actors engage in money laundering—exploiting vulnerabilities in the global financial system to obscure the source and destination of ill-gotten proceeds and further their illicit activity. The size of the U.S. financial system and the prevalence of the U.S. dollar in international trade make the United States an attractive destination for transnational criminal organizations and others seeking to launder their illicit proceeds, often in complex ways.[1]

The Financial Action Task Force (FATF), an intergovernmental body that sets internationally recognized standards for countering money laundering and the financing of terrorism and proliferation, identifies trade-based money laundering (TBML) as a primary means of money laundering. FATF defines TBML as the process of disguising proceeds of crime and moving value through trade transactions to legitimize their illicit origin.[2] 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, the substantial volume of international trade, and criminal organizations' increasing reliance on

[1]The U.S. dollar serves a wide range of uses in international financial transactions, including almost 60 percent of global central banks' reserves, broadly as an invoicing currency to fund international commercial activities, and non-U.S. banks' foreign currency holdings. Also, a number of internationally traded commodities, such as crude oil, are priced in dollars.

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

professional money laundering networks that specialize in TBML schemes.[3]

You asked us to provide information on U.S. efforts to combat TBML.[4] This report (1) describes vulnerabilities in the U.S. financial and trade systems to TBML schemes, (2) describes the entities that exploit these vulnerabilities for TBML schemes, (3) describes how U.S. agencies use available data to detect and combat TBML schemes, (4) examines the extent to which U.S. agencies and private-sector entities that combat illicit trade and finance collaborate to analyze and share information, and (5) describes how banking regulators and financial institutions assess risks of TBML schemes.

To address our first and second objectives, we reviewed reports and other documentation from the Departments of Commerce, Homeland Security, Justice, 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). The banking regulators examine financial institutions to ensure compliance with Bank Secrecy Act (BSA) and anti-money laundering (AML) regulations. We also interviewed officials from the Departments of Homeland Security, Justice, and the Treasury, including the Internal Revenue Service (IRS), as well as the U.S. Postal Service and the federal banking regulators. In addition, we spoke with relevant subject-matter experts (identified through prior work or experience related to TBML) about the role of financial and nonfinancial parties in trade transactions and potential vulnerabilities to TBML schemes.[5] We also interviewed law enforcement officials from two interagency task forces focused on combating transnational organized

[3]Department of the Treasury, *National Money Laundering Risk Assessment* (2015) and *National Strategy for Combating Terrorist and Other Illicit Financing* (2020). Basic TBML schemes include misrepresenting the price and quantity of goods and services (over- and under-invoicing).

[4]At the time of this request, Sen. Whitehouse was Ranking Member, Subcommittee on Crime and Terrorism, Committee on the Judiciary.

[5]GAO, *Countering Illicit Finance and Trade: U.S. Efforts to Combat Trade-Based Money Laundering*, GAO-20-314R (Washington, D.C.: Dec. 30, 2019) and *Trade-Based Money Laundering: U.S. Government Has Worked with Partners to Combat the Threat, but Could Strengthen Its Efforts*, GAO-20-333 (Washington, D.C.: Apr. 2, 2020).

crime: the Organized Crime Drug Enforcement Task Forces and the El Dorado Task Force.

We reviewed an illustrative sample of court documents from federal TBML-related prosecutions and Department of Justice press releases that described the mechanics of TBML-related schemes, federal agencies' roles in identifying and investigating these criminal schemes, and how evidence was used in prosecutions.[6] We also interviewed officials from U.S. Attorneys' Offices that have prosecuted TBML and related schemes.[7] 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 banks with large trade finance and correspondent banking operations, nonfinancial entities involved in trade, technology firms, international organizations, and other subject-matter experts.[8]

To address our third objective, we analyzed documentation related to the information systems and sources of data used for investigative and targeting purposes by U.S. Customs and Border Protection (CBP), Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), and Treasury's Financial Crimes Enforcement Network (FinCEN). We examined the types of data contained in their systems, which agencies have access to these sources and systems, and how agencies are analyzing and using available data to inform their trade or AML enforcement efforts. Further, we reviewed policies, guidance, and methodologies used by HSI's Trade Transparency Unit (TTU), CBP, and other agencies to inform investigations of TBML and related activity. We also analyzed suspicious activity reports filed by financial institutions with FinCEN from 2016 through 2020 to identify recent trends in TBML-related reporting. We interviewed officials from these agencies to better understand how they use available data for identifying and investigating illicit financial and trade activity.

[6]The illustrative examples were identified by requesting examples of closed TBML-related cases from law enforcement agencies, using keyword searches of the Department of Justice's website, and reviewing relevant academic and agency documents that highlighted TBML cases.

[7]We interviewed officials from the U.S. Attorneys' Offices in the Central District of California, Eastern District of New York, Southern District of New York, and Southern District of Florida. These offices prosecuted most of the adjudicated cases we identified.

[8]Examples of nonfinancial parties to a trade transaction include import/export companies, brokers, freight forwarders, shipping companies, and port terminal operators.

To address our fourth objective, we examined reports and other documents from the Departments of Commerce, Defense, Homeland Security, Justice, and the Treasury; the U.S. Trade Representative (USTR); and the federal banking regulators to determine how they share information and collaborate with other agencies to identify and investigate potential trade-related illicit activity, including how they may use or share relevant data. We identified efforts HSI, CBP, and other agencies have taken to collaborate in the use of available information and data to incorporate known risks and vulnerabilities to TBML-related schemes into their assessments and targeting efforts. We compared these efforts against relevant statutes, agency strategies, federal internal control principles, and key practices for enhancing interagency collaboration.

We also interviewed relevant officials from other agencies with a role in combating illicit trade and with access to TBML-related information—including ICE's National Intellectual Property Rights Coordination Center, USTR, the Maritime Administration (MARAD), and the Department of Defense's U.S. Southern Command—to identify any challenges to accessing data and information and to identify opportunities to mitigate any barriers to collaboration and coordination in efforts to combat TBML and related schemes.

To address our fifth objective, we reviewed the federal banking regulators' examination manual and other related documents regarding how they ensure compliance with BSA/AML regulations and address identified risks. We interviewed officials from Treasury and the federal banking regulators to understand how regulators evaluate the risks to financial institutions of TBML schemes and those institutions' compliance with BSA/AML regulations. Further, we interviewed representatives of international banks with large trade finance operations and correspondent banking relationships and the Bankers Association for Finance and Trade, an industry group for large international banks involved in trade finance activities. We also interviewed the Money Services Business Association, an association representing money services businesses (MSB), to understand these financial institutions' role in facilitating trade transactions, their BSA/AML compliance responsibilities, their due diligence processes, and their efforts to coordinate with federal agencies in identifying suspicious activity. We also reviewed a CBP report exploring the use of blockchain technology as a digital replacement for CBP's existing paper-based system of processing trade-related documents. We interviewed representatives of technology firms exploring the use of new technologies to ensure trade integrity, and we also interviewed

representatives of a large bank piloting the use of machine learning to automate parts of its trade finance activities.

We conducted this performance audit from January 2020 to November 2021 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

The BSA and its implementing regulations provide the legal and regulatory framework that requires covered financial institutions to assist the federal government in efforts to detect and prevent money laundering.[9] In January 2021, Congress expanded the BSA with the passage of the Anti-Money Laundering Act of 2020, which strengthens Treasury's AML and counter-terrorist finance programs, improves communication and processes, and establishes new beneficial ownership reporting requirements, among other things.[10] As the administrator of the BSA, Treasury's FinCEN issues regulations and interpretive guidance,

[9]The Currency and Foreign Transactions Reporting Act, its amendments, and the other statutes relating to the subject matter of that act have come to be referred to as the Bank Secrecy Act. These statutes are codified in scattered sections of Titles 12, 18, and 31 of the U.S. Code. The BSA's implementing regulations can be found primarily at 31 C.F.R. Chapter X, and generally require financial institutions to, for example, collect and retain various records of customer transactions, maintain AML programs, and file reports with FinCEN related to certain transactions. For the purposes of this report, we use "financial institutions" generally to mean banks and money transmitters (see 31 C.F.R. § 1010.100(ff)(5)) because of their role in facilitating cross-border financial transactions. This differs from the broader usage of "financial institution" in the BSA and its implementing regulations. See 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

[10]The Joint Explanatory Statement for the National Defense Authorization Act, 2021, noted that the current U.S. AML/countering the financing of terrorism framework is grounded in the BSA, first passed in 1970, and the regime is generally built around mechanisms that contemplate aging, decades-old technology. Division F of the act, better known as the Anti-Money Laundering Act of 2020, represents a comprehensive update to this framework to recognize new compliance technology, challenges, and priorities. The act expanded the purpose of the BSA to include preventing money laundering and terrorism finance through financial institutions' reasonably designed risk-based programs; facilitating tracking of criminal and terrorism-linked money; assessing risk of money laundering, terrorism finance, tax evasion, and fraud to financial institutions, products, or services to protect the financial system and safeguard national security; and establishing frameworks for information sharing among financial institutions, regulators, law enforcement, and related associations to identify, stop, and apprehend money launderers and those who finance terrorism.

such as advisories to financial institutions concerning money laundering and terrorist financing threats and vulnerabilities, and pursues enforcement actions when warranted.[11]

Treasury reported in 2018 that U.S. law enforcement agencies believe that there has been an increase in TBML, in part because criminals are using increasingly sophisticated money laundering techniques. According to Treasury, law enforcement agencies attribute this shift to TBML schemes, in part, to U.S. financial institutions' improved compliance with BSA obligations, such as cash reporting requirements, and AML laws more generally.[12] In addition, Treasury reported in 2018 that bulk cash seizures had decreased since 2013, potentially because transnational criminal organizations were relying more heavily on international funds transfers to wire money across borders as part of TBML schemes. For example, Treasury reported in 2020 that drug trafficking organizations and transnational criminal organizations are relying more on Asian (primarily Chinese) professional money launderers that facilitate exchanges of Chinese and U.S. currency or serve as money brokers in traditional TBML schemes.[13] Estimating the extent of TBML activities is challenging, but one academic researcher estimated, for instance, that trade price manipulation (mis-invoicing, including under- or over-invoicing) accounted for approximately $278 billion moved out of, and $435 billion moved into, the United States in 2018.[14] Another study estimated that potential trade mis-invoicing to and from 148 developing countries accounted for between $0.9 trillion and $1.7 trillion in 2015.[15]

[11]According to FinCEN, it also provides outreach to regulated industries; examines and works with other federal financial regulators to examine financial institutions for BSA compliance; delegates examination authority to financial regulators; and coordinates with federal, state, and local agencies to communicate financial crime trends and to provide support for investigations.

[12]Department of the Treasury, *National Money Laundering Risk Assessment* (2018).

[13]Department of the Treasury, *National Strategy*.

[14]The researcher used unit-price analysis to develop his estimates. See John Zdanowicz, "Trade-Based Money Laundering and Terrorist Financing," *Review of Law and Economics*, vol. 5, no. 2 (2009): pp. 855–878. We previously reported that unit-price analysis has several limitations. See GAO-20-333.

[15]Global Financial Integrity, *Illicit Financial Flows to and from 148 Developing Countries: 2006–2015* (Washington, D.C.: 2019). Estimates of trade price manipulation, or trade mis-invoicing, may include activity that is broader than TBML alone, such as income tax avoidance or evasion, among other things.

The primary role of financial institutions such as banks and money transmitters—entities that transfer money for their customers to recipients domestically or internationally—in international trade is to provide settlement of payment for cross-border transactions, financing, and risk mitigation for parties involved in international trade.[16] Trade transactions in which a financial institution processes the payment but does not provide some type of financing—such as a letter of credit—are referred to as open-account transactions.[17] According to a joint report from the Wolfsberg Group, the International Chamber of Commerce, and the Bankers Association for Finance and Trade, open-account trade constitutes about 80 percent of international trade transactions.[18] For the remaining 20 percent of trade, banks or other financial institutions provide some type of financing, such as a letter of credit.

Financial institutions that process the payments for trade transactions or engage in the financing of trade transactions are generally required to file suspicious activity reports (SAR) with FinCEN for those transactions that

[16]Under FINCEN's BSA/AML regulations, money transmitters are a type of MSB. Other types of MSB include, subject to exception, dealers in foreign exchange, check cashers, issuers or sellers of traveler's checks or money orders, providers or sellers of prepaid access (such as prepaid cards), and the U.S. Postal Service. 31 C.F.R. § 1010.100(ff).

[17]According to the Bankers Association for Finance and Trade, open-account trade transactions differ from documentary transactions, or transactions in which a financial institution provides some form of financing to a party in the transaction, such as a letter of credit. In documentary transactions, banks generally process documentation, such as a bill of lading, invoice, or packing list, to review the information underlying the transaction for evidence of red flags or indicators of money laundering, in addition to evaluating the financial risk to the institution of a default or nonpayment.

[18]The Wolfsberg Group, the International Chamber of Commerce, and the Bankers Association for Finance and Trade, *Trade Finance Principles* (March 2019). The Wolfsberg Group is an association of 13 global banks that aims to develop frameworks and guidance for the management of financial crime risks. The International Chamber of Commerce represents more than 45 million companies across more than 100 countries and advocates for and promotes international trade, among other things. The Bankers Association for Finance and Trade is an industry association for international transaction banking.

may exhibit red flags for potential TBML.[19] However, no single activity by itself is a clear indication of TBML. FinCEN encourages financial institutions to evaluate indicators of potential TBML in combination with other indicators and transaction activity before determining suspicious activity, and financial institutions may need to conduct additional investigation and analysis based on available information.[20] Banks and other financial institutions are examined for compliance with BSA regulations by their supervisory agencies, to which FinCEN has delegated BSA/AML examination authority.[21] The banking regulators—Treasury's Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA)—conduct risk-focused examinations of the banks under their supervision, and they tailor examination plans and procedures based on the risk profile of each bank.[22] FinCEN also relies heavily on both federal and state examinations of MSBs in its supervisory oversight

[19]See 31 U.S.C. § 5318(g).Under FinCEN's regulations, banks are required to file a SAR if a transaction involves insider abuse or aggregates at least $5,000 in funds or other assets and the bank knows, suspects, or has reason to suspect that the transaction involves funds derived from or intended to disguise illegal activities, is designed to evade any BSA requirements, or has no business or apparent lawful purpose or is not the type of transaction in which the customer would normally be expected to engage and the bank knows of no reasonable explanation for the transaction. See 31 C.F.R. § 1020.320; see also § 1022.320. Each federal banking regulator has also established additional criteria for the filing of a SAR by financial institutions under their supervision, such as a requirement to file a SAR for suspicious activity involving suspected insider abuse at any dollar amount. See 12 C.F.R. §§ 21.11, 163.180 (OCC); 208.62 (Federal Reserve); 748.1(c) (NCUA); 353.3(a)(1) (FDIC).

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

[21]The federal banking regulators also have separate authority pursuant to 12 U.S.C. §§ 1786(q) and 1818(s) to ensure that banking organizations comply with BSA laws and regulations. Banking regulators also examine banks for compliance with Office of Foreign Assets Control (OFAC) regulations. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals, entities, and jurisdictions such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime. While OFAC regulations are not part of the BSA, regulators examine a bank's policies, procedures, and processes for ensuring compliance with OFAC sanctions.

[22]Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision* (July 22, 2019).

of MSBs.[23] For example, IRS has been delegated authority to examine money transmitters and other types of MSBs not examined by the banking regulators or other supervisory agencies for BSA compliance.[24]

Law enforcement agencies play a role in detecting illicit activity and conducting criminal investigations related to money laundering and BSA noncompliance (see fig. 1). For example:

- Within the Department of Homeland Security (DHS), ICE's 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. ICE established the Trade Transparency Unit (TTU) within HSI to identify global TBML trends and conduct ongoing analysis of trade data provided through partnerships with other countries' trade transparency units.[25] TTU is collocated at CBP's National Targeting Center.[26]
- CBP, located within DHS, enforces the civil customs and trade laws of the United States, and refers issues to ICE HSI for criminal investigation and prosecution, as appropriate.
- The Internal Revenue Service Criminal Investigations Division (IRS-CI), within Treasury, investigates complex and significant money

[23]In 2008, FinCEN issued a BSA examination manual to guide reviews of money transmitters and other types of MSBs, including reviews by IRS and state regulators. In 2019, we reported that IRS has 44 memorandums of understanding with states and that IRS uses state reports of examination in its risk scoping of examinations of MSBs. IRS also has procedures in place to conduct concurrent examinations with states on a voluntary basis. 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).

[24]31 C.F.R. § 1010.810(b)(8).

[25]The U.S. government's key international effort to counter TBML is the trade transparency unit program. ICE set up trade transparency units in 18 partner countries with the goal of exchanging and analyzing trade data to identify potential cases of TBML.

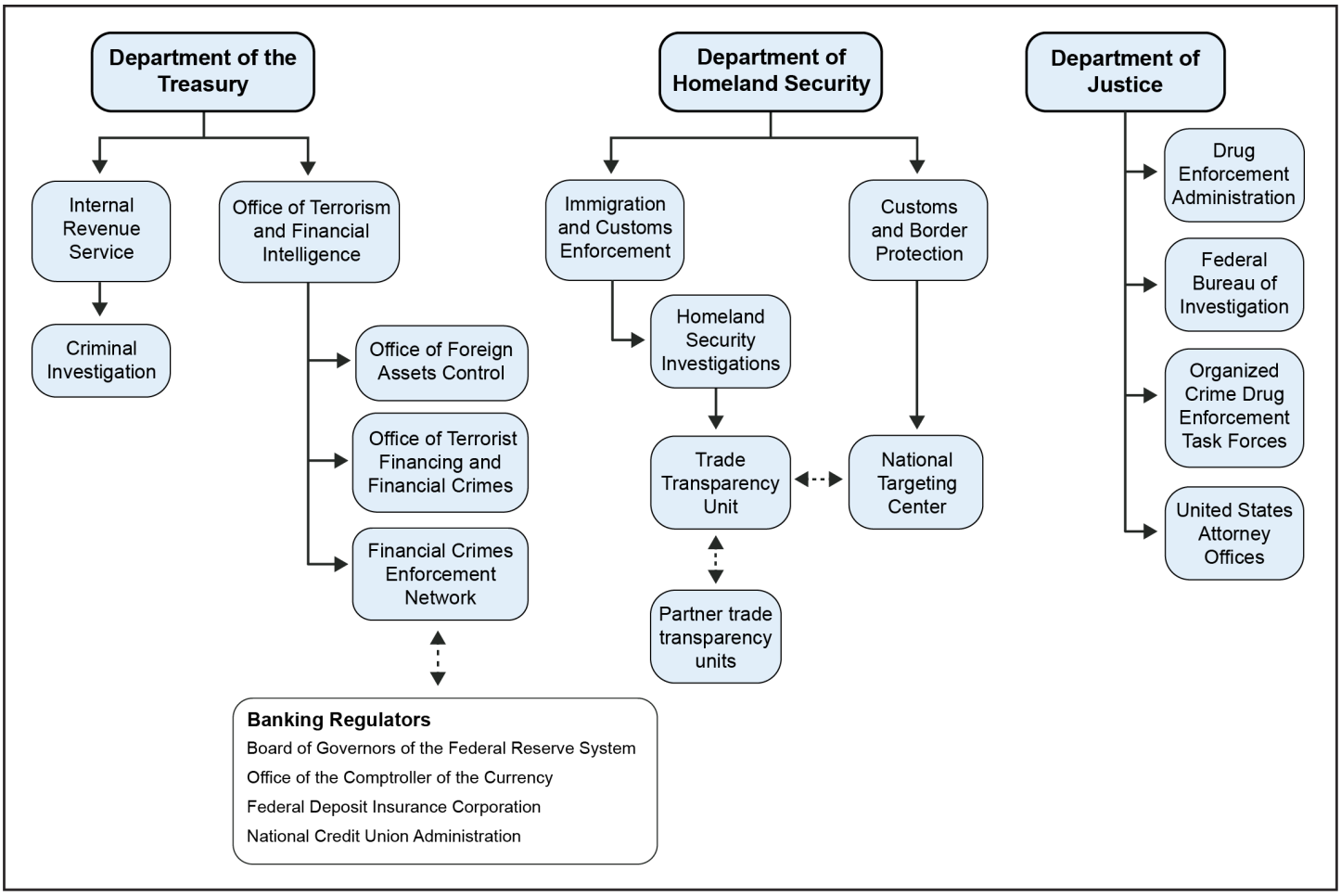
[26]The National Targeting Center leads all of CBP's predeparture targeting and vetting efforts. The center is a 24/7 operations entity responsible for providing advance information and research about high-risk cargo and travelers and facilitating coordination between law enforcement and intelligence agencies in support of CBP's antiterrorism mission and efforts to keep high-risk cargo and individuals from boarding U.S.-bound flights.

laundering activity, including that related to terrorism financing and transnational organized crime.

- The Drug Enforcement Administration and the Federal Bureau of Investigation, both components within the Department of Justice, investigate drug trafficking organizations and transnational criminal organizations. This includes investigations into money laundering activities conducted by these criminal organizations.
- Law enforcement task forces, such as the Organized Crime Drug Enforcement Task Forces (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.[27] The Department of Justice prosecutes violations of federal criminal statutes, including money laundering offenses.

[27]The Organized Crime Drug Enforcement Task Forces are an independent component of the Department of Justice. Established in 1982, it is the centerpiece of the Department of Justice's strategy to combat transnational organized crime and to reduce the availability of illicit narcotics in the nation by using a prosecutor-led, multiagency approach to enforcement. Established in 1992, the El Dorado Task Force is the largest anti-money laundering task force in the nation. It consists of more than 200 members from more than 30 law enforcement agencies in New York and New Jersey—including federal agents; international, state, and local police investigators; intelligence analysts; and federal prosecutors. The El Dorado Task Force is headquartered at the HSI New York Special Agent in Charge Office and operates at locations throughout the New York/New Jersey metropolitan area.

Figure 1: Key U.S. Agencies with Anti-Money Laundering and Trade Enforcement Responsibilities



Legend: ⟶ Direct authority ⟷ Collaboration

Source: GAO analysis of agency documents. | GAO-22-447

The Trade Facilitation and Trade Enforcement Act of 2015 codified many existing CBP capabilities to enforce U.S. trade laws and regulations, streamline and facilitate the movement of legitimate trade, and interdict noncompliant trade.[28] Enforcing trade laws also includes protecting revenue, which means ensuring that the duties and taxes owed on goods imported into the United States are collected. The act also strengthened CBP's and ICE's ability to protect U.S. economic security through trade

[28]Pub. L. No. 114-125, 130 Stat. 122 (2016).

enforcement, collaborate with the private sector through direct engagement, and streamline and modernize processes through business transformation initiatives to meet the demands and complexities of a rapidly evolving global supply chain.

Vulnerabilities in U.S. Financial and Trade Systems Include Limited Visibility into Underlying Documentation, Large Volume of Trade, and E-Commerce

Four key vulnerabilities in the U.S. financial and trade systems to TBML schemes are (1) banks' and other financial institutions' limited visibility into the trade documentation needed to evaluate suspicious activity; (2) fraudulent documentation in trade finance; (3) the extensive volume of international trade, including the growth of e-commerce and limited sharing of customs data between countries; and (4) relaxed oversight in free-trade zones.[29]

Financial Institutions' Limited Visibility into Underlying Transaction Documentation and Parties Is a Vulnerability

Financial institutions have limited visibility into the documentation of open-account trade, which constitutes most trade transactions. In open-account trade, the role of banks is limited to processing the payments between the buyer and seller. For this reason, a bank's ability to identify indicators of TBML, such as discrepancies in the type, amount, or price of the commodity being shipped, is limited, according to representatives of banks, bank regulators, and subject-matter experts with whom we spoke. In open-account transactions, banks may not always be aware that the particular payment involves a trade transaction and generally do not review documentation such as invoices, bills of lading, or customs declarations.[30] Banks process the payment from the buyer to the seller through their automatic payment systems, usually without human

[29]Generally, we adopt Treasury's use of the terms "vulnerability" and "risk." A vulnerability is what facilitates or creates the opportunity for money laundering. It may relate to a specific financial sector or product or a weakness in regulation, supervision, or enforcement. It may also reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity. Risk is a function of threat—that is, the criminal activity that generates the illicit funds—and vulnerability, and it represents a summary judgment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement. See Department of the Treasury, *National Money Laundering Risk Assessment* (2018).

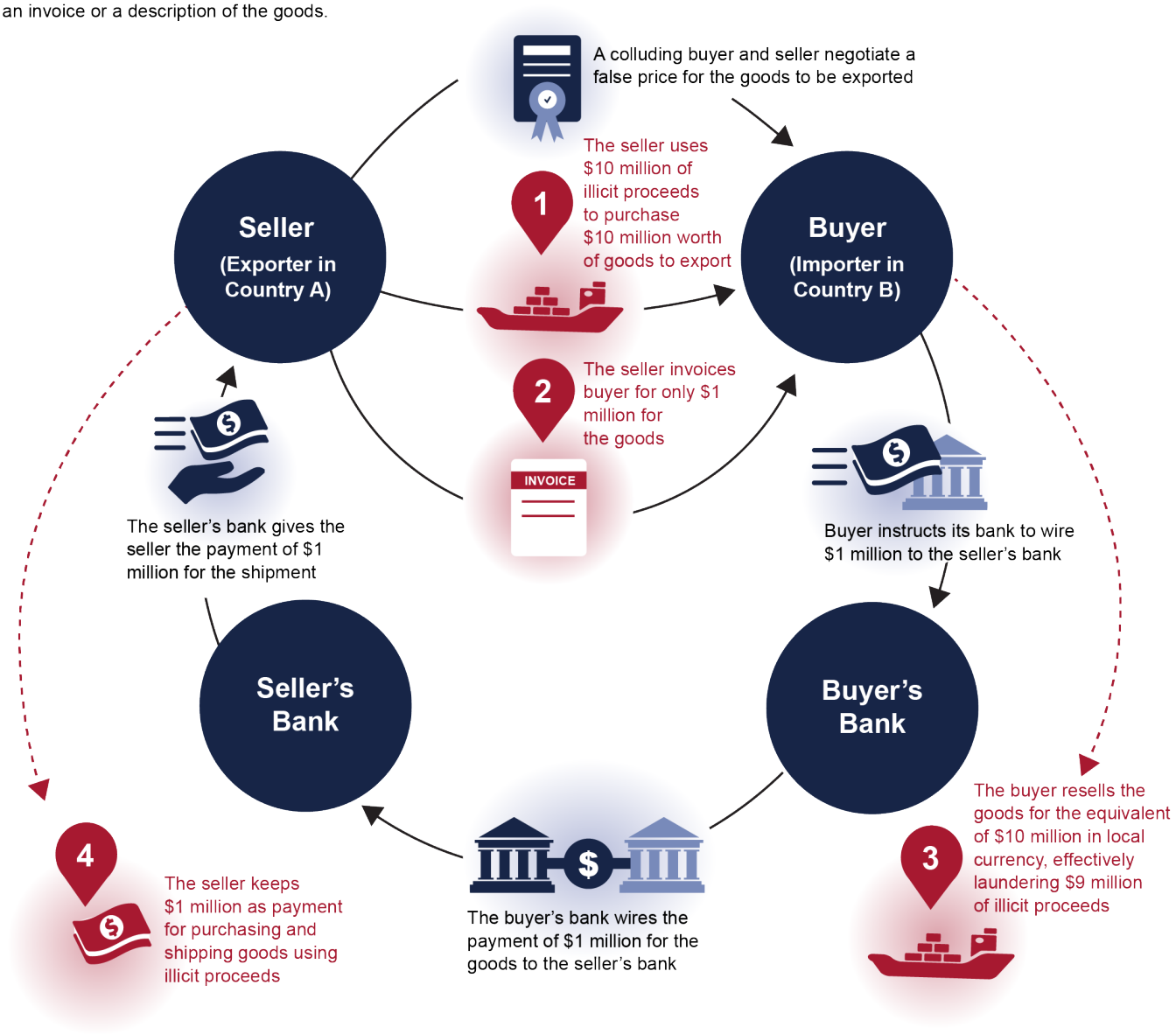
[30]According to FATF, a bill of lading is a document issued by a carrier or its agent to acknowledge receipt of cargo for shipment.

intervention. Banks generally apply standard AML compliance processes and procedures, including screening for compliance with economic sanctions, when processing payments for open-account trade transactions.

Criminals can exploit this limited visibility to launder illicit funds through the financial system by, for example, falsely stating the value of goods being exported. In such a scheme, after the goods are shipped and the payment is processed, the goods are sold for their real value in local currency in the importing country, effectively laundering the difference in the value between the invoiced amount and the real, higher value of the goods (see fig. 2). Because banks generally do not see the underlying documentation of such transactions, they cannot identify them as potential money-laundering schemes.

Figure 2: 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.



Source: Bankers Association for Finance and Trade. | GAO-22-447

Having multiple banks or other financial institutions involved in a transaction can also limit a given bank's visibility into all the parties to a transaction, which affects its ability to detect suspicious activity. Trade transactions often rely on correspondent banking relationships and can be processed through several banks, depending in part on the complexity of the correspondent banking relationships of the buyer's and seller's banks.[31] For example, for a simple wire transfer to process the payment for a trade transaction, in addition to the buyer's and seller's respective banks, the transaction could involve one or more intermediary banks that receive and transmit the payment instructions from the buyer's bank to the seller's bank. Banks also rely on, among other things, their customer due diligence procedures. In the case of foreign correspondent banking relationships, these include enhanced due diligence procedures such as monitoring transactions to, from, or through the correspondent for suspicious activity.

According to FATF, cross-border transactions that involve correspondent banking relationships are inherently vulnerable to illicit financial activity, in part because banks are processing transactions for a third party that is not their customer.[32] Representatives of banks we spoke with said they continually evaluate the BSA/AML risks that their correspondent banking relationships may present to them.[33] To develop a risk profile for transactions conducted with correspondent banks, they seek to understand their correspondents' AML controls and processes for

[31]According to FATF, correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. They provide respondent banks with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, check clearing, and foreign exchange services.

[32]FATF's standards do not require financial institutions such as banks to conduct customer due diligence on their customer's customer. FATF recommends that banks monitor their respondents' transactions to determine if there are changes in their risk profile, implementation of risk mitigation measures, unusual activity, or any deviation from the agreed-upon terms of the correspondent relationship. See Financial Action Task Force, *Correspondent Banking Services* (Paris: October 2016).

[33]Financial institutions are required to establish a due diligence program that includes appropriate, specific, risk-based and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the bank to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by a financial institution in the United States for a foreign financial institution. 31 C.F.R. § 1010.610(a).

onboarding new customers, customer due diligence, and transaction monitoring processes.

U.S. banking regulators examine banks for compliance with BSA/AML regulations, which can include expanded examination procedures for high-risk activity such as cross-border correspondent banking transactions. In alignment with FATF standards, and under BSA regulations, banks are required to establish a risk-based due diligence program related to correspondent banking that is reasonably designed to enable the bank to detect and report money laundering.[34] U.S. banking regulators do not generally expect banks to conduct customer due diligence on customers of the foreign financial institution. However, U.S. banks must verify that the foreign financial institution customer is not, and does not provide services to, a foreign shell bank. The BSA/AML examination manual of the Federal Financial Institutions Examination Council (FFIEC)—a formal interagency body of federal and state financial regulators that prescribes standards for the examination of banks and other financial institutions—states that U.S. banks should generally understand and assess the quality of the AML controls at the foreign correspondent financial institution. These controls include customer due diligence practices, suspicious activity identification processes, and recordkeeping documentation.[35] In a 2019 joint statement, the banking regulators also emphasized that they expect banks to structure their compliance programs to be risk-based, which enables banks to allocate compliance resources commensurate with their risk.[36]

In 2008, FATF identified several indicators that banks and other entities can use to identify potential instances of TBML, and in 2021 FATF published updated indicators intended to inform financial service providers, law enforcement, freight forwarders, and customs brokers.[37] However, because the role of banks and other financial institutions, such

[34]31 C.F.R. § 1060.610(a).

[35]FFIEC's members are a governor of the Federal Reserve, and the heads of the FDIC, NCUA, OCC, the Consumer Financial Protection Bureau, and the State Liaison Committee (five representatives from state regulatory agencies that supervise financial institutions).

[36]Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Joint Statement*.

[37]FATF and Egmont Group, *Trade-Based Money Laundering Risk Indicators* (Paris: March 11, 2021).

as money transmitters, is limited to processing the payments for most trade transactions, they are not positioned to evaluate many of these indicators. For example, FATF identified several risk indicators related to trade documents that banks have limited ability to identify, including:

- Elements across contracts, invoices or other trade documents may be inconsistent, such as contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.
- Contracts, invoices, or other trade documents display fees or prices that do not seem to be in line with commercial considerations, are inconsistent with market value, or significantly fluctuate from previous comparable transactions.
- Contracts, invoices, or other trade documents have vague descriptions of the traded commodities—for example, the subject of the contract is only described generically or non-specifically.
- Trade or customs documents supporting the transaction are missing, appear to be counterfeits, include false or misleading information, are a resubmission of previously rejected documents, or are frequently modified or amended.

As a result, financial institutions generally report relatively little activity specifically identified as TBML. Less than 1/10 of 1 percent of all SARs filed from 2016 through 2020 specifically indicated TBML activity (8,749 out of almost 11 million SARs).[38] According to OCC, while many SARs do not specifically mention TBML, the banks' SAR filings may have included the reporting of transactions that were related to a TBML scheme. In other words, if a bank filed a SAR for suspicious wire transfer activity, while the bank may not have known the transaction was related to TBML, it still filed the SAR. Similarly, if the bank became aware that it was provided fraudulent documentation associated with a bank-financed trade transaction, it very well may have filed a SAR for fraudulent documentation rather than TBML.

Other financial institutions, such as money transmitters, may also lack information to detect TBML schemes when processing transmittals of

[38]This total includes all financial institutions covered by BSA reporting requirements, in addition to banks. Banks'—that is, depository institutions'—filings represented about 79 percent of the TBML-specific SARs during this period.

funds, or wire transfers. For example, Treasury has identified TBML schemes that used MSBs to wire money between the United States and Mexico where the purpose of the payments was fraudulently reported to the MSB to obscure the illicit transactions. A representative from the Money Services Business Association (which represents about 80 companies operating small- and medium-sized MSBs) told us MSBs processing international transmittals of funds to high-risk regions or for high-risk goods generally request invoices to examine and match the quantity and description of goods. However, like banks, they may be vulnerable to TBML schemes involving mis-invoicing because the prices and quantities on an invoice can be manipulated.

Fraudulent Documentation of Bank-Financed Trade Transactions Represents a Vulnerability

Fraudulent documentation represents another vulnerability, especially in trade finance, according to representatives of banks, banking regulators, and other subject-matter experts with whom we spoke. Trade finance refers to a bank's financing of a trade transaction—such as through a letter of credit—and stands in contrast to open-account trade, where the bank's only role is to process payments. Bank representatives told us that trade finance is a very manual, resource-intensive business area because international trade is largely paper-driven, which exposes banks to fraud because the documents can be manipulated. In addition, banks have different roles and responsibilities depending on their role in letter-of-credit transactions, according to OCC. For example, a bank may be the issuing bank, the confirming bank, or the receiving bank, and the responsibilities from a BSA perspective are different depending on the role that the bank plays.

For example, trade finance products like letters of credit are more susceptible to documentary fraud because they require a large number of documents relative to other areas of banking, according to OCC. Banks process payments based on information stated in the documents rather than based on physical evidence of the goods being traded, and the more documentation they have to review, the greater the likelihood that fraudulent documentation can evade detection. According to banks, agency officials, and subject-matter experts with whom we spoke, criminals can, for example, also use obscure goods or part numbers, for which there are no available pricing data for banks to evaluate, on invoices in order to under- or over-invoice as part of TBML or related schemes. In addition, trade finance documents can originate with multiple parties in addition to the buyer and seller, including shipping companies, freight forwarders, warehouses, port authorities, terminal operators, and insurance companies—all of which are vulnerable to exploitation, have varying levels of oversight, and may wittingly or unwittingly become

involved in illicit trade schemes. Criminals can manipulate the invoice to, for example, falsify the quantity of a product to be shipped, and banks do not have access to shipments beyond the accompanying documentation to verify that quantities are accurate.

Generally, to satisfy their own risk mitigation policies and depending on the role of the bank in the letter-of-credit transaction (i.e., issuing bank, confirming bank, receiving bank, etc.), banks require documentary evidence for certain parts of a transaction for which they are providing financing—a contract between the buyer and seller, evidence of shipment, evidence of receipt, and evidence that the terms of the contract have been met. Transactions are screened for red flags, and the banks determine a risk tolerance level based on the number and severity of red flags that are identified.

Large Volume of Shipments and Limited Sharing of Customs Data Create Vulnerabilities

The extensive volume of international trade creates vulnerabilities for criminal organizations and other entities to exploit. According to the World Trade Organization, there was nearly $19 trillion of trade in merchandise globally in 2019. CBP collects information on cargo destined for U.S. ports of entry to identify high-risk shipments. However, representatives of banks, law enforcement officials, and subject-matter experts told us that criminal organizations can use any type of goods in TBML schemes. Further, differences in prices or quantities of goods shipped would be difficult, if not impossible, to determine in any given shipment without thorough inspection of the contents of the container and commodity-specific expertise.[39]

In addition, e-commerce is a growing area of vulnerability to TBML schemes such as trafficking in counterfeit goods because it involves a large volume of goods that enforcement officials have limited ability to inspect. According to law enforcement officials, criminal organizations may be able to more easily over-invoice counterfeit goods in e-commerce-related TBML schemes. Further, criminal organizations may use e-commerce to ship illicit goods in small packages, which are perceived to be a lower inspection risk with less severe consequences if the package is confiscated by customs authorities. We reported in September 2020 that European Union and U.S. agencies have connected

[39]CBP has a dual role of both trade enforcement and trade facilitation. Officials from CBP's Office of Field Operations told us that physically inspecting every shipment of cargo would be impractical and cost-prohibitive, particularly with the growth in e-commerce of smaller-dollar items shipped internationally.

increases in small packages sent through e-commerce with increased trade in counterfeit goods.[40]

CBP and other agency officials told us that the key challenge in identifying TBML schemes is the inability to inspect every container to determine, for example, that the contents of a container match the description on a bill of lading or invoice for quantity and price. Instead, CBP officials told us they use risk-based analysis and intelligence to prescreen, assess, and examine 100 percent of suspicious containers, and remaining cargo is cleared for entry into the United States using advanced inspection technology. CBP officials also told us they devote most of their inspection resources to inbound containers, with fewer resources devoted to outbound containers. However, for inbound containers, CBP officials told us they physically inspect, based on risk assessments, a limited portion of the arriving cargo at ports of entry, some of which see tens of thousands of containers a day. For example, the Port of Los Angeles, the largest container port in the United States, processed the equivalent of 9.2 million containers in 2020.[41]

In addition, limited exchange of customs data internationally hinders enforcement agencies' ability to compare import and export data to identify potentially suspicious activity, according to the World Customs Organization.[42] FATF identified as a best practice for combating TBML the sharing of trade data directly with foreign counterparts so that customs and law enforcement authorities can match import and export data to identify discrepancies. However, as we reported in April 2020, the U.S. effort to develop and expand trade transparency units with partner countries has experienced various challenges. These include lapses in information sharing between ICE and the partner trade transparency units, differing priorities between ICE and partner trade transparency units

[40]GAO, *Intellectual Property: CBP Has Taken Steps to Combat Counterfeit Goods in Small Packages but Could Streamline Enforcement*, GAO-20-692 (Washington, D.C.: Sept. 24, 2020).

[41]Port of Los Angeles, *Facts and Figures* (Los Angeles, CA: Apr. 5, 2021).

[42]World Customs Organization, *The Role of Customs in Identifying Trade-Based Money Laundering* (Brussels: February 2013). The World Customs Organization is an independent intergovernmental body that represents 183 customs agencies across the world.

in pursuing TBML investigations, and limitations in the data system that ICE and the trade transparency units use.[43]

Relaxed Oversight in Free-Trade Zones Creates Vulnerabilities

According to FATF, the generally relaxed oversight of free-trade zones makes them vulnerable to TBML and other illicit trade schemes.[44] Free-trade zones are designated areas within jurisdictions in which incentives are offered to support the development of exports, foreign direct investment, and local employment. These incentives may include exemptions from duties and taxes, simplified administrative procedures, and the duty-free importation of raw materials, machinery, parts, and equipment.

FATF further concluded these incentives can result in a reduction in finance and trade controls and enforcement, creating opportunities for money laundering and the financing of terrorism. The reduced oversight in free-trade zones makes it more challenging to detect illicit activity and provides an opportunity for misuse, both to launder illicit proceeds through TBML schemes and to engage in related illicit activity. Further, the size and scope of these zones make it difficult to effectively monitor incoming and outgoing cargo and the repackaging and relabeling of goods.[45]

In its 2018 report on notorious markets for counterfeit goods, the U.S. Trade Representative (USTR) highlighted the connection between free-trade zones and trade in counterfeit goods.[46] Similarly, the Organization for Economic Cooperation and Development found a positive correlation between the number of free-trade zones and the volume of trade in counterfeit goods.[47] The organization estimated in 2018 that counterfeit

[43]GAO-20-333.

[44]See Financial Action Task Force, *Money Laundering Vulnerabilities of Free Trade Zones* (Paris: March 2010).

[45]According to the World Bank, various reports put the number of free-trade zones at approximately 4,300. However, no exact counts exists, in part because the definition of these zones varies across countries. See World Bank, *Special Economic Zones: An Operational Review of Their Impacts* (Washington, D.C.: Nov. 21, 2017).

[46]U.S. Trade Representative, *2018 Out-of-Cycle Review of Notorious Markets* (April 2019).

[47]Organization for Economic Cooperation and Development, *Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends* (Paris: Mar. 15, 2018).

trade through the world's 1,843 free-trade zones represented about 2.5 percent of all exports.[48]

Transnational Criminal Organizations and Others Seeking to Undermine U.S. Interests Engage in TBML Schemes

Primary Threat Actors Include Transnational Criminal Organizations

Law enforcement officials told us that the types of organizations using TBML schemes are primarily transnational criminal organizations involved in drug trafficking, customs fraud, and financial fraud schemes, as well as professional money launderers and terrorist organizations.

- **Drug trafficking organizations.** These organizations use TBML to repatriate the illicit proceeds of drug sales in the United States primarily to other countries in the Western Hemisphere. Treasury officials identified drug trafficking as one of the main sources of illicit funds laundered through the U.S. financial system.
- **Professional money launderers.** FATF and Treasury have highlighted the role of professional money laundering networks in using TBML schemes to launder the proceeds of trade-related crimes, such as drug trafficking, fraud, human trafficking, and trafficking in counterfeit goods.[49] As previously stated, in its 2020 National Strategy for Combating Terrorist and Other Illicit Financing, Treasury noted that drug trafficking organizations and transnational criminal organizations are relying more on professional money launderers from Asia (primarily China) that facilitate exchanges of Chinese and U.S. currency or serve as money brokers in traditional TBML networks.
- **Terrorist organizations.** Terrorist organizations may also use TBML schemes to transfer the value of funds internationally to disguise the

[48]According to the organization, the share of counterfeit and pirated exports were calculated over the total value exports from economies for which information on the value of counterfeit and pirated trade was available.

[49]Financial Action Task Force, *Professional Money Laundering* (Paris: July 2018).

origin of the funds, avoid sanctions or other restrictions to countries known to be state sponsors of terrorism, or avoid sanctions to designated terrorist organizations or individuals.

A subset of TBML schemes typically associated with drug trafficking organizations in Mexico and Central and South America involves black market peso exchanges. In these 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 ability of law enforcement to identify anomalies in patterns of behavior (see fig. 3).

Figure 3: Example of a Black Market Peso Exchange Scheme

The black market peso exchange is a complex form of trade-based money laundering, originally developed by Colombian drug cartels, but is now used by criminal organizations in a number of countries. 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.

Source: Department of the Treasury and Department of Homeland Security. | GAO-22-447

Based on the documents we analyzed and interviews with law enforcement officials, TBML-related criminal prosecutions generally focused on the U.S.-based merchants that accepted illicit funds for payment of exports to countries where drugs are produced (or where the drug trafficking organization is located) to convert the illicit proceeds from U.S. dollars into local currency. According to prosecutors from U.S. Attorneys' Offices we spoke to, TBML cases—particularly drug trafficking-related black market peso exchange schemes—are complex, require significant time, resources, and expertise, and often span years, making them difficult to prosecute. Attorneys who prosecuted many of these cases told us the most difficult part of developing a case and bringing charges was establishing that the merchants who accept illicit funds as payment for their goods did so knowingly.[50]

Threat Actors Exploit TBML Vulnerabilities to Evade Economic Sanctions and Taxes

Criminal organizations exploit TBML-related vulnerabilities to engage in related illicit activity. For example, U.S. agencies have identified economic sanctions evasion schemes that exploit similar vulnerabilities, with red flag indicators of suspicious activity like those used for identifying TBML. Recent guidance developed by the Department of State, the Office of Foreign Assets Control (OFAC), and the U.S. Coast Guard for the maritime shipping industry describes best practices for identifying potential sanctions violations.[51] The guidance highlights deceptive shipping practices for evading sanctions, such as falsifying bills of lading, certificates of origin, invoices, packing lists, proof of insurance, and customs entry forms—practices prevalent in TBML schemes. The guidance encourages entities involved in trade to exercise heightened due diligence measures for shipments and transactions that transit areas determined to present high risk.

[50]Generally, prosecutors in money laundering cases have to show that defendants acted with intent to promote the carrying on of specified unlawful activity or had knowledge that the funds involved in the transaction represented the proceeds of some form of specified unlawful activity. Of the cases we reviewed, more than half were prosecuted by four U.S. Attorneys' Offices: the Southern District of New York, the Central District of California, the Eastern District of New York, and the Southern District of Florida. Department of Justice officials told us these are larger districts with more resources to prosecute complex cases. The officials also told us that attorneys from the department's Money Laundering and Asset Recovery Section with expertise in prosecuting complex money laundering cases can provide additional support to districts that have more limited expertise or resources.

[51]Department of State, Department of the Treasury, and U.S. Coast Guard, *Guidance to Address Illicit Shipping and Sanctions Evasion Practices* (May 14, 2020).

One federally prosecuted case we reviewed involved efforts to circumvent certain sanctions designations related to financial transactions with Iranian entities.[52] Individuals working for a bank in London manipulated Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages sent between financial institutions to mask the Iranian interests involved in the transactions.[53] Bank employees also conspired with an Iranian beneficiary to conduct financial transactions through commercial bank accounts in the United Arab Emirates, used as fronts for Iranian businesses. According to the Department of Justice, one purpose of this scheme was to provide access to U.S. dollars for sanctioned entities in violation of the International Emergency Economic Powers Act.[54] Subject-matter experts we interviewed told us that criminals can exploit the large volume of SWIFT messages that banks routinely process to mask illicit transactions.

Customs fraud schemes to evade taxes and duties use similar methods to exploit TBML-related vulnerabilities, such as over- and under-invoicing of exports and imports, and can lead to significant tax revenue losses. For example, an exporter that over-invoices the value of goods shipped may be able to significantly increase the value of the export tax credit or value-added tax rebate. Similarly, an importer that under-invoices the value of the goods received may be able to reduce the value of the import duties or customs taxes paid. IRS-CI officials we spoke with highlighted a scheme that involved methods similar to those in a TBML scheme—use of fraudulent import and export documents and falsely described goods and prices—to defraud Mexico's government of tax refunds. The scheme also used the same methods to then launder the value of the illicit funds through the U.S. financial system.

[52]Amended Deferred Prosecution Agreement, United States of America v. Standard Chartered Bank, 1:12-cr-00262 (D.D.C. Apr. 9, 2019). According to the Department of Justice, these sanctions arose in response to Iran's repeated support for international terror against the United States and its allies and the proliferation of weapons of mass destruction.

[53]SWIFT is organized as a cooperative under Belgian law and is owned and controlled by its shareholders. It provides the standards that enable member banks to exchange financial information needed to make payments and is one of the most commonly used means of sending cross-border transactions. As of 2021, it serves over 200 countries and over 11,000 financial and corporate entities.

[54]This act provides the President broad authority to regulate a variety of economic transactions following a declaration of national emergency. 50 U.S.C. §§ 1701-08.

Additionally, a federal prosecution of a trade-related money laundering scheme involving imports of clothing from China into the United States illustrates how criminals can combine multiple activities that exploit trade-related vulnerabilities.[55] The scheme involved declaring the clothing items as samples to avoid paying import duties. The illicit proceeds of the scheme were then laundered back to accounts or other parties in Asia through MSB money transfers.

Multiple Federal Entities Use Data to Identify High-Risk Trade Transactions and Support Enforcement Duties

Multiple federal agencies and offices collect and use data for trade enforcement responsibilities.[56] The TTU analyzes financial and trade data, including import and export data exchanged with foreign TTU counterparts. CBP evaluates import and export data to identify high-risk trade transactions. FinCEN provides guidance and has issued geographic targeting orders to assist TBML enforcement. Other agencies, such as the Coast Guard and the Department of Commerce, also use systems to evaluate import and export data to identify high-risk trade or financial transactions to mitigate trade-related violations based on mission priorities.

TTU and CBP Analyze Import and Export Data to Identify High-Risk Entities and Shipments

Trade Transparency Unit

HSI's TTU has about 15 staff who, among other things, examine trade between countries by comparing export records and corresponding import records.[57] TTU staff do this by using a data analysis tool—the Data Analysis and Research for Trade Transparency System (DARTTS)—to

[55]Memorandum of Plea Agreement, U.S. v. Dung Hanh Dao, No. 1:13-cr-00036-LJO (E.D. Cal. Feb. 12, 2014); Memorandum of Plea Agreement, U.S. v. Hoang Minh Nguyen, No. 1:13-cr-00036-LJO (E.D. Cal. Feb. 12, 2014).

[56]For example, we previously reported that 22 agencies have responsibilities for clearing or licensing goods for import or export (see GAO, *Customs and Border Protection: Automated Trade Data System Yields Benefits, but Interagency Management Approach Is Needed*, GAO-18-271 (Washington, D.C.: Mar. 14, 2018)), and 13 agencies have responsibilities related to implementing and enforcing economic sanctions (see GAO, *Economic Sanctions: Treasury and State Have Received Increased Resources for Sanctions Implementation but Face Hiring Challenges*, GAO-20-324 (Washington, D.C.: Mar. 11, 2020)).

[57]According to TTU officials, HSI funds four full-time employees, and other DHS components, such as CBP, fund the remainder.

analyze trade and financial data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes.[58] DARTTS incorporates import and export data reported to CBP, BSA reports filed with FinCEN, law enforcement investigative data, and foreign import and export data. According to TTU officials, the TTU analyzes financial and trade data and other information, including trade data exchanged with its foreign counterparts, to identify potential illicit activity, including violations of U.S. and foreign criminal trade laws. Specifically, HSI analysts use DARTTS to conduct three types of analysis:

1. **International trade discrepancy analysis.** U.S. and foreign import and export data are compared to identify anomalies and discrepancies that warrant further investigation for potential fraud or other illegal activity.
2. **Unit price analysis.** Trade pricing data are analyzed to identify over- or under-valuation of goods, which may be indicative of TBML or other import-export crimes.
3. **Financial data analysis.** Financial reporting data are analyzed to identify patterns of activity that may indicate money laundering schemes. These data include the import and export of currency, reports of suspicious financial activities, and the identities of parties to these transactions.

DARTTS analyses are designed to generate leads for and otherwise support ongoing investigations of TBML, smuggling, commercial fraud, and other crimes within the jurisdiction of HSI. Generally, according to TTU officials, if a field agent receives credible information from a reliable source, TTU staff can search DARTTS for specific data points. DARTTS can provide trade or financial transactions associated with those data points, which can help to determine where to focus investigative resources. In fiscal year 2018, the TTU's analysis provided support to 258 investigations, and in fiscal year 2019, the TTU referred 17 investigative leads to domestic and partner countries' investigative agencies.

Since its establishment in 2004, the TTU has helped establish 18 foreign-partner trade transparency units globally, mostly in the Western Hemisphere, to share their import and export data. These foreign partners can view a limited interface within DARTTS of U.S. import and export

[58]HSI, in addition to leading the TTU, is the primary law enforcement agency that investigates trade-related illicit activity, such as bulk cash smuggling, commercial fraud, and intellectual property theft.

data, but not other countries' data. The TTU also receives data from and works directly with its foreign trade transparency unit partners to help support their investigations and to develop leads. They can then use Customs Mutual Assistance Agreements to obtain original evidence from foreign partner agencies to support criminal investigations.[59]

Currently, when using DARTTS, TTU analysts are limited to manual identification of corresponding export entries from one country and import entries in another country, or vice versa, and have no automatic way to link those entries. As a result, their ability to perform more systematic analysis to identify trends or patterns is limited. According to TTU officials, part of the difficulty arises from the lack of standardized forms, translation difficulties, and intentional obfuscation by criminal organizations.

For example, import and export entries may correspond to each other, but may have different spellings of names, entities, or shipment contents, or they may be in different languages, which limits the TTU's ability to match data. To address these issues, the TTU has worked with Johns Hopkins University–Applied Physics Laboratory to facilitate analysis of foreign partner data with U.S. data. The project used data analytics and "fuzzy matching"—that is, algorithms to identify likely matching transactions based on shared factors. According to the TTU and Johns Hopkins officials, they have made progress in reconciling trade data between certain partner countries, but need further research and development before they can systematically link mirrored transactions.

Customs and Border Protection

The Trade Facilitation and Trade Enforcement Act of 2015 requires CBP to coordinate trade facilitation and enforcement efforts among federal agencies to facilitate legitimate international trade and enforce U.S. and foreign customs and trade laws. This includes collecting, assessing, and

[59]As we reported in 2020, according to HSI officials, as a precondition for setting up a trade transparency unit, a country must have a Customs Mutual Assistance Agreement or similar information-sharing agreement with the United States. CBP and ICE negotiate Customs Mutual Assistance Agreements with customs agencies in partner countries on behalf of the U.S. government. According to CBP documents, although the specific terms vary by country, the agreements, which are legally binding, help facilitate the exchange of information, intelligence, and documents that will support the prevention and investigation of customs offenses. As of March 2019, the U.S. government had signed 80 Customs Mutual Assistance Agreements with customs agencies around the world. See GAO-20-333.

disseminating information as appropriate and in accordance with any law regarding cargo destined for the United States.

CBP uses its Automated Targeting System (ATS) to evaluate import and export data reported to CBP, identify high-risk trade transactions, and assist CBP in mitigating trade-related violations based on its Priority Trade Issues.[60] According to CBP, ATS was designed to efficiently conduct risk assessments on information pertaining to import and export shipments and international travelers attempting to enter or leave the United States, as well as to flag certain cargo and goods for inspection or enhanced documentation review.[61] CBP also receives and assesses required information from customs brokers or importers on incoming cargo, such as bills of lading and descriptions of the goods, through two other data systems—the Automated Commercial Environment (ACE) and Automated Export System. The data captured through these systems are copied and transmitted to ATS.[62]

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. For example, CBP officials told us post-seizure analysis of shipments related to TBML schemes can provide critical details which can be leveraged to create targeting rules for future shipments. In 2017, ATS also started incorporating BSA data such as SARs to better identify trade

[60]According to CBP, Priority Trade Issues represent high-risk areas that can cause significant revenue loss, harm the U.S. economy, or threaten the health and safety of the American people. CBP's seven Priority Trade Issues are Agriculture and Quota, Antidumping and Countervailing Duty, Import Safety, Intellectual Property Rights, Revenue, Textiles/Wearing Apparel, and Trade Agreements. For more information on CBP's Priority Trade Issues, see GAO, *Customs and Border Protection: Improved Planning Needed to Strengthen Trade Enforcement*, GAO-17-618 (Washington, D.C.: June 12, 2017).

[61]CBP uses ATS to target potentially unlawful import and export activities such as high-risk shipments by leveraging data reported to CBP and data available through multiple applications and databases, including intelligence and law enforcement information, by creating user-defined rules and user queries. In fiscal year 2019, CBP processed 35.5 million entries and more than 28.7 million imported cargo containers at U.S. ports of entry, valued at $2.7 trillion.

[62]ACE is CBP's system for the electronic processing of imports and exports and is the backbone of its trade information processing and risk management activities. According to CBP, ACE allows efficient facilitation of imports and exports and serves as the primary system used by U.S. agencies to process cargo and passengers.

risks, such as where there may be a nexus between illicit financial activity, terrorist financing, and trade activity.

CBP's analysts also use ATS to collaborate with the TTU. According to TTU officials, to detect potential instances of TBML, the TTU works with CBP analysts at the National Targeting Center to analyze import and export information to create user-defined rules in ATS. For example, if TTU analysts identify a suspicious pattern of activity associated with a certain entity, they can work with CBP analysts to create rules in ATS that would flag other bills of lading from that same entity as part of CBP's targeting duties.[63]

FinCEN Has Provided Guidance and Issued Geographic Targeting Orders to Assist TBML Enforcement

In 2010, FinCEN issued a TBML-related advisory to financial institutions based on its analysis of SARs filed by financial institutions. The advisory highlighted the increasing use of TBML schemes by criminal organizations, particularly drug trafficking organizations in the Western Hemisphere. It also cited potential indicators of TBML that financial institutions should consider as they evaluate potential suspicious activity.[64] For its advisory, FinCEN analyzed more than 17,000 SARs covering activity between January 2004 and May 2009 to identify reports potentially related to TBML schemes. As a result of the review, in 2012 FinCEN added an option on its SAR form for financial institutions to report "Trade Based Money Laundering / Black Market Peso Exchange" as a type of suspicious activity. Examples of suspicious activity included third-party payments for goods or services made by an intermediary apparently unrelated to the buyer or seller goods and a customer's inability to produce appropriate documentation.

[63]The National Targeting Center works to prevent dangerous and unlawful travelers and cargo from entering and exiting the United States by reviewing and segmenting them across inbound and outbound modes of transportation. According to TTU officials, the four TTU staff that have access to DARTTS are co-located within the National Targeting Center with other CBP and HSI staff.

[64]In 2018, FinCEN organized a conference on TBML for several U.S. agencies involved in combatting TBML, including HSI, CBP, and IRS-CI, in addition to government officials from partner countries and nongovernment participants. The conference provided presentations on a range of issues related to TBML, such as the vulnerabilities in the gold industry that make it susceptible to TBML and the evolution of the black-market peso exchange. In 2019, FinCEN organized an additional conference focused on TBML and bulk cash smuggling. See GAO-20-333.

In response to law enforcement concern about TBML, FinCEN also issued a geographic targeting order in October 2014.[65] The order imposed additional reporting and recordkeeping obligations on certain businesses in the Los Angeles Fashion District to identify persons and businesses believed to be involved in accepting illicit funds from drug trafficking organizations. In April 2015, FinCEN, in coordination with HSI and IRS–CI, issued a geographic targeting order to several hundred businesses in Miami that export electronics to gather additional information on cash transactions potentially related to TBML schemes used by drug cartels to better understand how the schemes were occurring.[66]

In January 2021, Congress enacted the Corporate Transparency Act as part of the National Defense Authorization Act for Fiscal Year 2021, which requires certain legal entities to report beneficial ownership information to FinCEN pursuant to regulations that Treasury is required to issue.[67] Although FinCEN's existing Customer Due Diligence Rule requires covered financial institutions to identify and verify the beneficial owners of legal entity customers at the time of account opening and conduct risk-based monitoring to maintain and update customer information, the

[65]A geographic targeting order is an order issued by FinCEN (usually at the request of law enforcement) that imposes additional reporting and recordkeeping requirements on businesses in a specified geographic area. See GAO, *Anti-Money Laundering: FinCEN Should Enhance Procedures for Implementing and Evaluating Geographic Targeting Orders,* GAO-20-546 (Washington, D.C.: July 14, 2020).

[66]Since 2015, U.S. law enforcement, including FinCEN, has seen an increase in complex schemes to launder proceeds through TBML—for example, from the sale of illegal narcotics—by facilitating the exchange of cash proceeds from Mexican drug trafficking organizations to Chinese citizens residing in the United States. As a result of the collection of information, law enforcement developed a better understanding that these money laundering schemes are designed to sidestep two separate obstacles: (1) drug trafficking organizations' inability to repatriate drug proceeds into the Mexican banking system due to dollar deposit restrictions imposed by Mexico in 2010 and (2) Chinese capital flight law restrictions on Chinese citizens located in the United States that prevent them from transferring large sums of money held in Chinese bank accounts for use abroad. See Department of the Treasury, *National Strategy*.

[67]Pub. L. No. 116-283, div. F, tit. LXIV, 134 Stat. 4604.The act defines a beneficial owner, with respect to an entity, as an individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise, (1) exercises substantial control over the entity or (2) owns or controls not less than 25 percent of the ownership interests of the entity, subject to some exceptions. According to the sense of Congress statement in the act, most or all states did not require information about beneficial owners at the time of company formation, and federal legislation was needed to set a clear federal standard and to benefit U.S. commerce and national security.

current lack of obligation to report beneficial ownership information for certain entities to the federal government limits visibility into who owns or controls the account and may facilitate money laundering. To address this, the act provides additional tools for FinCEN to collect and analyze required beneficial ownership data it receives and subsequently provide intelligence to law enforcement to combat illicit trade based on those data. The act will also provide authorized U.S. law enforcement access to the collected beneficial ownership information, which can help law enforcement to better target complicit merchants, businesses, and individuals that act as facilitators in illicit trade schemes. In April 2021, FinCEN began soliciting public input related to its efforts to implement the beneficial ownership information reporting provisions of the act.

Other Agencies and Offices Use Trade Data to Mitigate Trade-Related Violations Based on Mission Priorities

Several federal entities serve as partner agencies to CBP and HSI to support trade enforcement responsibilities.[68] Among the agencies with responsibilities for regulating international trade are the Coast Guard; the Department of Commerce, including the Bureau of Industry and Security; the Department of Defense; the Department of Agriculture; the Food and Drug Administration; the Department of Justice; Treasury; and the U.S. Postal Inspection Service.[69]

These agencies use CBP import and export data and other trade data to identify risks and perform their respective enforcement responsibilities.[70] Partner agencies have ongoing access to CBP's ACE, and they examine imports of merchandise falling within their trade enforcement responsibilities. ACE enables a centralized online access point to connect CBP, trade representatives, and partner agencies involved in importing goods into the United States. For example, the Food and Drug Administration has integrated its systems with ACE and uses ACE data to review imports under its jurisdiction and target public health risks.

Not all partner agencies have full access to ACE data. We previously found that partner agencies have varying levels of access to ACE based

[68]As we previously reported in March 2018, a partner government agency is an agency with responsibility for clearing or licensing cargo that has signed a memorandum of understanding with CBP that allows access to ACE and details the information the agency will receive through the system, according to CBP officials. GAO-18-271.

[69]GAO-18-271.

[70]For example, under the Trade Facilitation and Trade Enforcement Act of 2015, federal agencies with authority to detain and release merchandise are to ensure coordination in the release of such merchandise through ACE.

on their responsibilities for clearing or licensing goods for import or export.[71] For example, Department of the Interior's Fish and Wildlife Service has limited access to monitor wildlife trade and prevent the illegal importation or exportation of species, fauna, and flora into and out of the United States. The Coast Guard uses ACE to conduct regulatory inspections in the ports, including inspecting vessels and containers that transport imported and exported cargo.

Other partner agencies or offices supplement ACE data with other data sources. For example, officials from the Department of Transportation's MARAD told us they often use private sources of data on maritime shipping to fulfill their trade monitoring responsibilities, instead of ACE. USTR has access to ACE, but officials told us they rely instead on other trade data to develop their reports on notorious markets for counterfeit goods.[72]

Lack of Government-wide Collaboration Mechanism on Illicit Finance and Trade Limits Agencies' Information Sharing

No Government-wide Collaboration Mechanism Exists to Help Agencies and the Private Sector Collaborate and Share Information

TBML-related schemes represent cross-cutting criminal activity that spans numerous agencies' responsibilities and involves multiple private-sector players, as previously discussed. Financial institutions are generally required to identify and report on suspicious financial activity, but for most international trade they have limited visibility into the underlying trade transaction that would enable them to evaluate documentation for red flag indicators, such as mis-invoicing. Law enforcement efforts have focused on drug trafficking organizations using

[71]GAO-18-271.

[72]USTR is responsible for negotiating directly with foreign governments to create trade agreements, resolve disputes, and participate in global trade policy organizations. The Notorious Markets Report highlights prominent and illustrative examples of online and physical markets that reportedly engage in or facilitate substantial piracy or counterfeiting. A goal of the report is to motivate appropriate action by the private sector and governments to reduce piracy and counterfeiting. U.S. Trade Representative, *2020 Review of Notorious Markets for Counterfeiting and Privacy* (January 2021).

black market peso exchange schemes, wherein the trade transactions that transfer illicit funds can be legitimate and can involve witting or unwitting merchants. Current federal collaborative efforts to combat TBML do not include some key agencies involved in overseeing trade. Additionally, information on suspicious financial and trade activity is siloed across different agencies and is not widely shared, and information sharing and interactions with key private-sector entities are limited.

Existing government strategies do not include a robust focus on TBML activities or input from some key agencies involved in overseeing trade transactions. For example, Treasury's National Strategy for Combating Terrorist and Other Illicit Financing is supported by high-level risk assessments it conducted covering money laundering (including TBML), terrorist financing, and proliferation financing.[73] Treasury incorporated published and unpublished research and analysis, insights, and observations from a variety of law enforcement and other agencies with roles related to combating illicit finance into its risk assessments, including HSI, the Drug Enforcement Administration, the Federal Bureau of Investigation, the Department of State, and its own agencies such as FinCEN and IRS. Treasury's risk assessments explain how TBML works and provide case studies, and Treasury officials told us they are dependent on contributions from other federal agencies. However, the assessments did not include the views and perspectives of other agencies positioned to identify illicit trade, such as USTR, MARAD, the Department of Defense, or the Department of Agriculture, which could enrich their understanding of TBML. Further, the risk assessments did not include the views of customs brokers, freight forwarders, maritime shipping companies, or other private-sector entities positioned to identify illicit trade activity, such as fraudulent manipulation of trade-related documents.

Data and analyses are not widely shared and are fragmented among various agencies. Specifically, officials we spoke with from agencies with trade enforcement responsibilities told us that trade enforcement, including data collection and analysis, exists in silos among federal agencies, affecting potential information-sharing and collaboration. For example:

[73]Treasury most recently published two strategies for combating terrorist and other illicit financing in December 2018 and February 2020. Its February 2020 strategy includes a high-level overview of TBML.

- USTR officials told us that they do not know the types of data shared between CBP and the TTU and their foreign partners and do not have a full understanding of the Customs Mutual Assistance Agreements that CBP and ICE enter with other countries. USTR officials are not involved in negotiating the agreements, and there is no other mechanism for them to learn about the agreements. They told us that without full understanding of the U.S. government's relationship with trading partners, their ability to negotiate and enforce trade agreements could be affected.
- Officials from MARAD told us that they do not receive all the available information that CBP collects on ships and shipping transactions and instead rely on private sources of data as part of their Jones Act-related responsibilities.[74] MARAD officials also told us that they occasionally identify suspicious patterns of activity that could be related to illicit trade schemes. However, officials told us they do not have a full understanding of the types of risks of illicit trade and associated red flags that would better position them to identify that activity, and they do not have a mechanism to share that information with relevant agencies.
- Officials from U.S. Southern Command, within the Department of Defense, told us the lack of aggregated TBML-related data collected by U.S. agencies limits the data's usefulness for identifying illicit activity.[75] Officials said they use data from other federal agencies, as well as private-sector sources, for analytic purposes. However, the data across agencies are structured differently, which, in addition to the text-heavy nature of data in several databases from other agencies, limits Southern Command's ability to perform more sophisticated analysis of illicit trade and financial activity in their area of responsibility.

Government agencies and private-sector entities generally do not share sufficient information to help them identify suspicious activities. Private-sector entities involved in international trade, including banks, MSBs,

[74]The Merchant Marine Act of 1920, better known as the Jones Act, generally requires that vessels transporting cargo from one U.S. point to another U.S. point be U.S.-built and be owned and crewed by U.S. citizens.

[75]U.S. Southern Command is responsible for providing contingency planning, operations, and security cooperation in its assigned area of responsibility, which includes Central America, South America, and the Caribbean (except U.S. commonwealths, territories, and possessions). U.S. Southern Command works with federal agencies and regional partners to counter threats from transnational criminal organizations that traffic drugs, weapons, counterfeit items, money, and people.

shippers, and customs brokers, also told us that better information sharing with government agencies could help identify suspicious activity.

- As noted earlier, banks and MSBs have limited visibility into some of the indicators of suspicious activity related to TBML and similar schemes. Representatives of banks and MSBs told us that information from federal agencies about risks—for example, about high-risk goods, regions, and criminal organizations—could help them better identify and report on suspicious activity. Representatives from banks and other private-sector entities we spoke to told us that they are familiar with the TTU and the unique data the TTU has access to, but they have not received any information about specific risks that could help them identify potentially suspicious activity. They told us that having more information from U.S. agencies about areas of risk or patterns of potential illicit activity could help them identify and report on suspicious activity related to TBML.
- Representatives of a large customs broker told us that information about high-risk goods from U.S. agencies such as CBP or the TTU could help them identify and share information on suspicious activity. They also told us that they have a good understanding of their customers' patterns of activity—for example, to whom manufacturers generally sell their goods and in what quantities, and who their suppliers are—that could be useful for identifying anomalous or suspicious behavior, but they have no way to share that information with CBP or other U.S. agencies.
- Representatives of another large global maritime shipping company told us that the data it collects from its customers allow it to see significant parts of the complete trade transaction—from the purchase order between a customer and a manufacturer, to the bill of lading, through delivery—providing the company with full supply chain visibility. The company believes its data is more comprehensive than what customs agencies generally collect for purposes of importing and exporting goods.

Other agencies with trade enforcement responsibilities have identified the role of private-sector entities in helping to identify and combat illicit trade-related activity and have mechanisms for collaboration. For example, in 2018 HSI published an e-commerce strategic plan that identified goals to leverage the assets of private industry and law enforcement partners to

combat criminal activity in e-commerce.[76] The strategy emphasizes the importance of sharing information to accomplish a common goal of disrupting criminal activity through all avenues of e-commerce, including targeting the flow of illicit proceeds and tracking and interdicting the movement of illicit goods.[77] HSI has directly engaged banks, MSBs, digital payment processors, and brokerage firms through HSI relationships with private-sector entities. For example, HSI has engaged with the National Cyber-Forensics and Training Alliance and other private-sector partnerships that focus on better information sharing between U.S. agencies and industry partners to leverage expertise related to enforcing intellectual property rights.[78]

Trade and AML enforcement agencies engage the private sector across a range of issues to incorporate their perspective and promote collaboration. For example:

- CBP co-chairs the Commercial Customs Operations Advisory Committee, an advisory committee made up of industry members who have regular meetings to discuss issues such as global supply chain security and facilitation, CBP modernization and automation, air cargo security, customs broker regulations, trade enforcement, revenue modernization, and protection of intellectual property rights. The committee advises CBP and Treasury components on, among other things, recommendations to the Secretaries of the Treasury and Homeland Security on improvements to the commercial operations of CBP, but it is not designed to share information about illicit trade risks.
- The Bank Secrecy Act Advisory Group (BSAAG) is chaired by FinCEN and consists of representatives from law enforcement and

[76]U.S. Immigration and Customs Enforcement Homeland Security Investigations, *E-Commerce Strategic Plan* (Washington, D.C.: Feb. 14, 2018). According to ICE, its e-commerce strategic plan complements other existing national strategies and, similarly, stresses the importance of working in a cooperative environment with both industry and other law enforcement partners.

[77]ICE's e-commerce strategic plan, in describing its alignment with other strategies, cites the Office of the Intellectual Property Enforcement Coordinator's *U.S. Joint Strategic Plan on Intellectual Property Enforcement (FY2017–2019)*. Specifically, ICE cites guidance that agencies should integrate awareness of intellectual property crime and its illicit proceeds into broader efforts to combat money laundering and the financing of transnational organized crime networks as an influence on its strategy.

[78]The National Cyber-Forensics and Training Alliance is a nonprofit corporation founded in 2002 by industry, academic, and law enforcement entities for the purpose of sharing information to combat cyber threats.

financial regulatory agencies, financial institutions, and industry trade groups. The BSAAG provides a forum for Treasury to receive advice regarding the operations of the BSA, and as chair, the Director of FinCEN is responsible for ensuring that relevant issues are placed before the BSAAG for review, analysis, and discussion. The BSAAG is not designed for sharing illicit finance risks with private-sector entities.[79]

The limitations of these collaboration efforts in addressing TBML are in part due to the absence of a formal mechanism—such as a working group or task force—to analyze data and share information on the risks of trade-facilitated financial crimes across federal agencies and with private-sector entities positioned to identify suspicious activity. Treasury has identified interagency task forces as essential tools for U.S. law enforcement efforts to disrupt money laundering and other criminal activity, and it has stated that efforts to raise awareness among private-sector entities about specific TBML-related risks should be communicated through outreach and working groups.[80] Though FinCEN has taken efforts to better share information about TBML risks with other U.S. agencies, FinCEN officials told us it does not plan to establish any type of TBML-focused working group because the TTU is best positioned to combat TBML because of its access to partner countries' trade data. However, as described below, the TTU does not share its data with other relevant agencies and is limited in its analytical capacity. We have also identified key practices that can help sustain collaboration among federal agencies, including, among other things, agreeing upon agency roles and responsibilities; establishing compatible policies, procedures, and other means to operate across agency boundaries; and identifying and

[79]In 2018 and 2019, separate from its role as BSAAG chair, FinCEN held TBML-focused conferences with law enforcement agencies and other agency experts to share case studies and best practices related to investigating TBML schemes. However, because of the sensitive nature of the information shared, banks and other financial institutions did not participate.

[80]Department of the Treasury, *National Strategy*.

addressing needs by leveraging resources.[81] Recent legislation requires Treasury to propose strategies to combat TBML.[82]

Without a mechanism—such as a working group or task force—to both share information with and incorporate the views of relevant agencies and private-sector entities, Treasury and other agencies are missing opportunities to better collaborate with relevant stakeholders that could help to identify the risks of illicit activity associated with TBML and similar schemes and the criminal organizations or entities that benefit from them. The mechanism could inform Treasury's TBML strategy development and help determine roles for agencies that are positioned to identify and combat trade-facilitated illicit financial activity but are without AML responsibilities, such as MARAD. The mechanism could also address the siloed nature of trade enforcement and leverage private-sector resources.

TTU Supports Ongoing Investigations but Does Not Fully Analyze Relevant Data or Share Them with Other Federal Agencies

According to ICE, the TTU was established to identify global TBML trends and conduct ongoing analysis of trade data provided through partnerships with other countries' trade transparency units. TTU officials explained that this mission is largely carried out by conducting analyses in response to specific requests from agents in the field to support ongoing investigations. As such, the TTU's analysis of the data for emerging patterns and trends is limited. However, the data available to the TTU and related analyses could be relevant to the work of other agencies that are involved in trade enforcement and AML efforts. Additionally, other agencies that told us they have more resources to conduct extensive analyses do not have access to TTU's data and are not able to use the data to inform their own AML or trade enforcement responsibilities.

HSI and other U.S. agency officials familiar with the trade data in DARTTS told us that the TTU and other agencies do not analyze the import and export data to, for example, identify emerging trends or patterns of activity that could be relevant for identifying TBML-related risks.[83] The data also are not analyzed for purposes of identifying other

[81]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

[82]The 2021 National Defense Authorization Act included a provision for Treasury to conduct a study, in consultation with appropriate private-sector stakeholders, academic and other international trade experts, and U.S. agencies, on TBML, and to submit to Congress proposed strategies to combat TBML. National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 6506, 134 Stat. 3388, 4631.

[83]TTU officials told us they currently examine high risk trade commodities and trade practices linked to partner trade transparency units.

illicit activity, such as tax evasion, trafficking in counterfeit goods, or sanctions evasion. HSI officials at the TTU told us they would like to conduct systematic analysis, such as data mining, but a number of factors present challenges to performing such analysis, such as the inability in DARTTS to, for example, match imports into the United States with exports from other countries without a common identifier. HSI officials also told us that the TTU has limited resources for conducting more robust analysis of the trade data in DARTTS to identify patterns and emerging trends.

Officials from the TTU, Treasury, law enforcement, and other agencies also told us DARTTS data, and the TTU's analyses of those data, are not widely shared or understood throughout the government because most of the TTU's analyses are conducted in response to specific requests from agents in the field to support ongoing investigations.[84] For example, Treasury's risk assessments—which underpin the National Strategy for Combating Terrorist and Other Illicit Financing—did not include analysis of relevant data available to the TTU, such as import and export data shared between partner trade transparency units, because the data were not shared with Treasury.

CBP has emphasized its use of advanced data analytics, particularly at the National Targeting Center, to identify trends and inform trade enforcement activities, and CBP and HSI officials told us that CBP has more analytical resources and that its data analysis and targeting systems are more sophisticated than DARTTS, which has more limited analytical tools. U.S. Southern Command officials also told us their data analysis tools are designed for analyzing large amounts of data and could incorporate the TTU's trade data into their analyses. According to Treasury, improved data analytics on trade data should be shared among law enforcement to better identify and investigate TBML.[85] FinCEN officials told us that if FinCEN could partner with U.S. law enforcement and other agencies like OFAC and CBP to obtain that "context" needed to

[84]We also reported in 2020 that ICE had not developed a strategy to increase the effectiveness of the TTU program. See GAO-20-333. We recommended that the Secretary of Homeland Security direct the Director of ICE to develop a strategy for the trade transparency unit program to ensure that ICE has a plan to guide its efforts to effectively partner with existing trade transparency units, and to expand the program, where appropriate, into additional countries. As of November 2021, ICE is developing a TTU strategic plan to guide efforts to enhance collaboration with partner countries to combat TBML and to identify a strategic methodology to guide the growth of ICE's international partnerships.

[85]Department of the Treasury, *National Strategy*.

query the BSA and TTU trade data, and conduct analysis on companies that have been identified by U.S. law enforcement in their investigations involving potential TBML, their analyses could better inform the banks, regulators, and other U.S. agencies on TBML trends, patterns, and vulnerabilities. These data—whether analyzed by CBP, Treasury, or another agency—could potentially improve Treasury's and other agencies' ability to identify patterns of illicit activity and vulnerabilities to TBML and related schemes and adapt a strategy appropriately to identified risks.

TTU officials told us the memorandums of understanding signed between ICE and partner countries for sharing trade data preclude them from sharing data with other U.S. agencies. However, the memorandums of understanding we reviewed include a provision that would allow ICE to share the data with other U.S. agencies if ICE requests and receives written permission from the partner country. ICE officials also told us that certain safeguards on data sharing could be explored that would, under certain circumstances, permit other agencies with more analytic resources to have access to the trade data it collects from partner trade transparency units. Additionally, since ICE negotiates the data-sharing agreements with partner trade transparency units and provides resources and training to those partners, it could explore ways to incorporate data sharing in those agreements. For those agencies without a need for access to the trade data, the TTU could also share analysis of trends and emerging risks based on the trade information the TTU receives from partners, which could inform risk assessments or investigative efforts of agencies with trade enforcement or AML responsibilities.

Federal internal control standards state that management should identify, analyze, and respond to risks related to achieving the defined objectives and that management should use quality information to achieve the entity's objectives.[86] The standards also state that management should communicate quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system. Unless ICE takes steps to enable the sharing of the TTU's trade data, the TTU and other U.S. agencies may not be able to identify emerging risks and trends related to

[86]GAO, *Standards for Internal Control in the Federal Government* (Washington, D.C.: Sept. 10, 2014).

TBML and other illicit trade schemes and allocate investigative resources appropriately.

Banking Regulators Use a Risk-Based Approach To BSA/AML Examinations, and Banks Incorporate Public and Private Data into Their Risk Assessments

Banking Regulators Take a Risk-Focused Approach to Examining Banking Activity at Risk for TBML and Related Schemes

According to banking regulators, examiners use the FFIEC BSA/AML examination manual to evaluate banks' compliance with BSA requirements. The manual includes procedures for assessing banks' BSA/AML compliance programs and assessing compliance with BSA regulatory requirements and risks associated with money laundering and terrorist financing for certain banking activities.[87] Examiners generally begin a BSA/AML examination by reviewing and assessing the adequacy of the bank's money laundering and terrorist financing risk assessment. This review includes determining whether bank management has developed a risk assessment that adequately identifies the money laundering and terrorist financing and other illicit financial activity risks within its banking operations. Next, examiners evaluate the bank's compliance with BSA requirements. This evaluation can use expanded examination procedures, including, for example, additional testing procedures on higher-risk accounts, such as those for U.S. banks with foreign correspondent accounts. U.S. banking regulators also examine banks for compliance with sanctions administered by OFAC, often in

[87]Banking regulators and FinCEN emphasize a risk-focused approach to BSA/AML examinations. Under this approach, examinations are tailored to each individual bank's unique risk profile considering the varying degrees of risk associated with its products, services, customers, and geographic locations. Examiners apply a risk-focused approach to evaluate a bank's processes and procedures for compliance with BSA requirements, as opposed to investigating specific types of money laundering. See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, *Joint Statement*.

tandem with the BSA/AML examinations. The manual identifies risks to financial institutions from sanctions evasion activities involving certain financial products and services similar to those for TBML, such as foreign correspondent bank accounts, cross-border funds transfers, and trade finance products.

Banking regulators have taken recent enforcement actions against banks for alleged weaknesses in areas that are vulnerable to TBML and related schemes. For example, in 2019, OCC issued a cease and desist consent order to three federal branches of MUFG Bank Ltd., Tokyo, Japan, a foreign bank with operations in the United States, that highlighted alleged weaknesses in transaction monitoring for international funds transfers, its due diligence program for correspondent accounts for foreign financial institutions, and its processes and procedures for trade finance monitoring.[88] In 2019, the Federal Reserve issued a cease and desist order and assessed civil money penalties to Standard Chartered, a foreign bank with operations in the United States, finding, among other things, that the bank processed hundreds of millions of dollars in transactions in violation of U.S. sanctions regimes and had deficiencies in compliance procedures related to international funds transfers.[89]

Banks Incorporate Advisories and Public and Private Data Sources into Their Risk Assessments

According to representatives of banks we spoke with, the banks rely on their customer due diligence processes, which include establishing a risk profile and a baseline for expected activity when onboarding a new client engaged in international trade. Bank representatives told us they rely on information, such as trends and patterns of potential illicit activity, from international organizations such as FATF, the Bankers Association for Finance and Trade, the Wolfsberg Group, and others to inform their risk assessments of new clients. Further, such information aids in conducting ongoing monitoring to identify and report suspicious activity and maintain and update customer information. Banks also may incorporate open-source information, advisories, and guidance from FinCEN, OFAC, and financial regulators into their due diligence and monitoring processes, consistent with the examiner instruction and background information provided in the FFIEC BSA/AML examination manual. According to

[88]Consent Order, In the Matter of MUFG Bank, Ltd, AA-EC-2019-7 (2019). The cease and desist order did not find that the banks engaged in, or were party to, TBML-related schemes, but that their processes and procedures had alleged weaknesses that could be exploited.

[89]Order to Cease and Desist and Order of Assessment of Civil Money Penalty Issued Upon Consent, In the Matter of Standard Chartered PLC, 19-011-B-FB, 19-011-CMP-FB (2019).

representatives of a banking association, some banks also rely on commercially available products that, for example, track maritime ships and publicly available bill-of-lading data to better understand patterns of shipping, the markets and prices for certain products, and other information that can help them to understand the risks of certain transactions and to identify anomalies. For more information on efforts to develop technological solutions for analyzing illicit trade risks, see appendix I.

Conclusions

TBML and related schemes are some of the most complex forms of illicit activity used by transnational criminal organizations, terrorists, and other entities to launder ill-gotten proceeds and finance activities that threaten U.S. national security. These schemes often involve many types of illicit activity—the trade of counterfeit goods, falsification of customs forms and other documentation, money laundering, and sanctions evasion—that cut across multiple agencies' roles and responsibilities. However, there is no formal mechanism among federal agencies to analyze and share information and data on the risks of trade-facilitated financial crimes between federal agencies and with private-sector entities positioned to identify suspicious activity. Without a mechanism to promote greater information sharing and collaboration—including with private-sector entities involved in international trade—U.S. agencies are missing opportunities to better analyze and distribute information that could help inform strategy development and identify potential investigative leads to better combat TBML and related schemes.

The TTU is also missing opportunities to better analyze and distribute information that could help investigative and enforcement agencies to identify suspicious activity. The TTU analyzes trade and financial data to support ongoing investigations related to TBML schemes. However, it does not analyze these data systematically or share the data more broadly with relevant U.S. agencies with trade enforcement and AML responsibilities, despite its CBP partners and other agencies having the analytic capability conduct such analysis. Without access to data that could be useful for identifying illicit trade and illicit financial activity, U.S. agencies may not be able to identify emerging risks and trends related to TBML and other illicit trade schemes, which could inform investigative priorities and resource allocation.

Recommendations for Executive Action

We are making two recommendations, including one to the Department of the Treasury and one to the Department of Homeland Security:

The Secretary of the Treasury, in collaboration with partner agencies, should establish an interagency collaboration mechanism to promote greater information sharing and data analysis between federal agencies and with relevant private-sector entities on issues related to trade-based money laundering and other illicit trade schemes. (Recommendation 1)

The Secretary of Homeland Security should ensure the Director of Immigration and Customs Enforcement takes steps to enable and implement sharing of the Trade Transparency Unit's trade data—including for the purposes of trade data analysis about patterns or trends of illicit activity related to trade-based money laundering and similar schemes—with U.S agencies with roles and responsibilities related to enforcing trade laws and combating illicit financial activity, as appropriate. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Commerce, Defense, Homeland Security, Justice, State, Transportation, and the Treasury, as well as the Office of National Drug Control Policy, the U.S. Trade Representative, the U.S. Postal Service, and the federal banking regulators (the Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and National Credit Union Administration). The Departments of Homeland Security, Justice, Transportation, and the Treasury and the federal banking regulators provided technical comments, which we incorporated as appropriate. DHS and Treasury also provided written comments, which are reproduced in appendixes II and III, respectively.

In its written comments, the Department of Homeland Security did not concur that the Director of Immigration and Customs Enforcement should take steps to enable and implement sharing of the TTU's trade data with U.S. agencies with roles and responsibilities related to enforcing trade laws and combating illicit financial activity. DHS noted that ICE remains committed to using its legal authority to investigate and combat TBML, smuggling, commercial fraud, and other crimes within the jurisdiction of Homeland Security Investigations. In noting that it did not concur with our recommendation, DHS stated that ICE leadership is concerned with our findings that the TTU should expand data sharing with the private sector. However, data sharing with the private sector was not part of our findings or recommendation. We clarified to DHS that its concerns seemed to be based on a misreading of the draft report, and that our recommendation specifically focused on data sharing between U.S. agencies with roles and responsibilities related to enforcing trade laws and combating illicit financial activity. We also provided an opportunity for DHS to reexamine

its response to our recommendation before publication of this report. DHS again responded with the same concerns. We reiterate that the focus remains on data sharing between U.S. agencies.

Additionally, DHS stated that the TTU program's primary mission is to establish partnerships with foreign law enforcement and provide them with information tools, such as the Data Analysis and Research for Trade and Transparency System (DARTTS), to facilitate the exchange of data between trade transparency units. However, according to DHS's website, "ICE established the Trade Transparency Unit to identify global TBML trends and conduct ongoing analysis of trade data provided through partnerships with other countries' trade transparency units." Additionally, documents the TTU provided to us and interviews with TTU officials indicated that the primary mission of the TTU is to combat TBML and other trade-facilitated financial crimes. While the establishment of partnerships with foreign governments to share trade data is important to achieving the broader mission of the TTU, our findings show that the TTU is limited in its ability to analyze those data, and that the data would help other U.S. agencies with trade enforcement and anti-money laundering responsibilities achieve their missions. Furthermore, in technical comments, DHS officials noted their willingness to share their unique data with other federal agencies—for example, partnering with relevant agencies to analyze data and identify trends within a working group capacity.

In its written comments, Treasury neither agreed nor disagreed with our recommendation that it establish an interagency collaboration mechanism, noting that the success of any interagency coordination mechanism would rely on DHS and the TTU making data more broadly available to Treasury, law enforcement, and other agencies. Specifically, Treasury stated that it believes that access to and analysis of trade data outside of DHS should be recognized as a critical component to any coordination effort. Treasury also stated that it is engaged in an effort, in partnership with other agencies, that will eventually inform mitigation strategies to combat TBML. Though access to the TTU's unique data could help identify patterns and trends, including particular risks to TBML, we continue to believe that without a collaboration mechanism, Treasury is missing key inputs and perspectives from other federal agencies and private sector entities related to assessing TBML risks and developing a strategy to mitigate them.

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 of this report to the Departments of Commerce, Defense, Homeland Security, Justice, State, Transportation, and the Treasury; the Office of National Drug Control Policy; the U.S. Trade Representative; the U.S. Postal Service; and the federal banking regulators, as well as the appropriate congressional committees. 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 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. GAO staff who made key contributions to this report are listed in appendix IV.

Michael Clements
Director, Financial Markets and Community Investment

Rebecca Shea
Director, Forensic Audits and Investigative Service

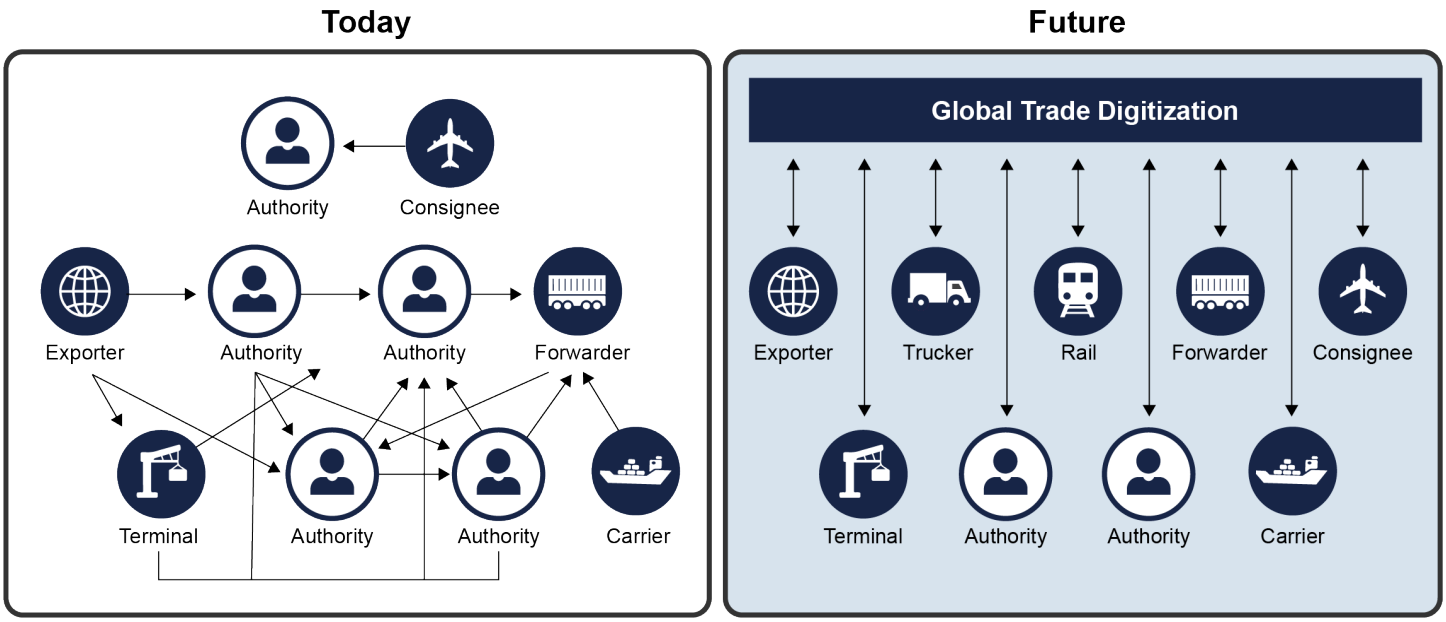
Appendix I: Private-Sector Entities and U.S. Agencies Are Exploring New Technologies to Better Evaluate Risks of Trade Transactions

Private-sector entities, including banks, are exploring new technologies that could address challenges related to trade-based money laundering (TBML) in international trade, supply chain integrity, and trade finance. For example, we spoke with representatives of shipping, technology, and financial companies 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.[1] Representatives from one technology firm serving the maritime shipping industry told us their platform is designed to provide more efficient and secure methods for conducting global trade using blockchain technology by, for instance, better enabling regulatory and customs authorities to closely monitor the flow of goods, carry out risk assessments, and perform regulatory processing, thereby reducing the risk of illicit activity, including TBML. The platform operates as a consortium and is intended to include a role for manufacturers, shipping companies, insurance companies, customs authorities, and banks. Additionally, a bank with large trade finance operations announced in 2019 that it is piloting a project to automate and digitize the screening of trade transactions, which is intended to improve the bank's ability to review documentation associated with providing trade financing, traditionally a manual and labor-intensive process.

In 2018, U.S. Customs and Border Protection (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 (see fig. 4). 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. CBP noted some issues that may prevent rapid implementation of the project, such as that few private-sector entities have adopted blockchain technology, but recommended to proceed with pursuing proof-of-concept.

[1]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).

Figure 4: Illustration of U.S. Customs and Border Protection's Pilot Project Goals to Digitize Global Trade



Source: GAO analysis of U.S. Customs and Border Protection information. | GAO-22-447

Note: As of July 2021, data are communicated via a centralized, paper-based mechanism. The future functionalities provided by the digital pilot include a decentralized platform, increased speed and assurance of correspondence between Customs and Border Protection users and the trade, the elimination of paper documents, and improved facilitation of the auditing process.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 26, 2021

Michael Clements
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Rebecca Shea
Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-447, "COUNTERING ILLICIT FINANCE AND TRADE: Better Information Sharing and Collaboration Needed to Combat Trade-Based Money Laundering"

Dear Mr. Clements and Ms. Shea:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the U.S. Immigration and Customs Enforcement (ICE) as the primary law enforcement agency investigating trade-based money laundering (TBML) and that ICE, Homeland Security Investigations (HSI), has established foreign Trade Transparency Units (TTU) in other countries to facilitate the creation and analyzing of import and export data for use in law enforcement investigations. HSI TTU obtains foreign data through memorandums of understanding (MOUs), usually based on established Customs Mutual Assistance Agreements (CMAAs), which are binding international customs-to-customs agreements, negotiated and concluded on behalf of the United States by U.S. Customs and Border Protection (CBP) and ICE. In addition, ICE operates within foreign country customs and law enforcement authorities and does not share information when the political climate is not supportive to the United States presence. ICE remains committed to using its legal

authority to investigate and combat TBML, smuggling, commercial fraud, and other crimes within the jurisdiction of HSI.

However, ICE leadership is concerned with GAO's findings that ICE HSI TTU should expand data sharing, including with private sector entities. ICE does not agree that it is appropriate to share this data and analysis with private sector entities. ICE is not a public-facing agency for export and import data, and any data collected and analyzed is for law enforcement investigative purposes to cover a broad range of areas encompassed by cargo safety and security, and smuggling prevention, including national security threats, the importation and exportation of contraband (including illegal arms exports), trade-facilitated financial crimes, commercial fraud, human trafficking, narcotics smuggling, and child pornography/exploitation.

The draft report contained two recommendations, including one for DHS with which the Department non-concurs. Attached find our detailed response to the DHS recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2021.10.26 12:59:52 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendation Contained in GAO-22-447

GAO recommended that the Secretary of Homeland Security ensure the Director of ICE:

Recommendation 2: Takes steps to enable and implement sharing of the TTU's trade data analysis about patterns or trends of illicit activity related to TBML and similar schemes—with U.S. agencies with roles and responsibilities related to enforcing trade laws and combating illicit financial activity, as appropriate.

Response: Non-concur. The ICE HSI TTU program's primary mission is to establish partnerships with foreign law enforcement, and provide them with information tools, such as the Data Analysis and Research for Trade and Transparency System (DARTTS), to facilitate the exchange of data between TTUs. DARTTS incorporates: (1) import and export data reported to CBP; (2) Bank Secrecy Act reports filed with the Financial Crimes Enforcement Network; (3) law enforcement investigative data; and (4) foreign import and export data, which HSI TTU uses to identify suspicious transactions that may warrant investigation for money laundering or other import-export crimes. ICE HSI has access to this data through established data-sharing agreements (i.e., MOUs and CMAAs) that clearly document what data are being shared, and how the data can be used.

However, the agreements serve to protect the agency providing the data, ensure the data will not be misused, and prevent any miscommunication on the part of the provider and receiver of the data; and ICE protects the integrity and privacy of this data accordingly. As ICE is not the owner of this data and does not have the authority to share the data with other entities, it is appropriate that data-sharing agreements with foreign countries prohibit the sharing of their information, and that data sharing agreements among U.S. law enforcement agencies provide a mechanism to request access and authorization if an agency needs access to data related to enforcing trade laws and combating illicit financial activity. These measures were established to protect the data and comply with federal statutes, regulations, and standards, such as 19 USC 1415(a)(3)(F), the 2002 Federal Information Security Management Act (Public Law 107-347), and those defined by the National Institute of Standards and Technology. Ultimately, these measures protect government information, operations, and assets against threats by ensuring that access to this data is at the least privilege and on a need-to-know basis.

DHS requests that GAO consider this recommendation resolved and closed.

3

Appendix III: Comments from the Department of the Treasury

Financial Crimes Enforcement Network
U.S. Department of the Treasury

Washington, D.C. 20220

October 29, 2021

Michael Clements
Director, Financial Markets and Community Investment
Rebecca Shea
Director, Forensic Audits and Investigative Service
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Clements and Ms. Shea:

Thank you for providing the Financial Crimes Enforcement Network (FinCEN) the opportunity to review the Government Accountability Office (GAO) report, "Countering Illicit Finance and Trade: Better Information Sharing and Collaboration Needed to Combat Trade-Based Money Laundering" (GAO-22-447) (the Report).

The Report includes the following findings:

- There is no formal mechanism among federal agencies to analyze and share information and data on the risks of trade-facilitated financial crimes between federal agencies and with private sector entities positioned to identify suspicious activity.
- Without a mechanism to promote greater information sharing and collaboration—including with private-sector entities involved in international trade—U.S. agencies are missing opportunities to better analyze and distribute information that could help inform strategy development and identify potential investigative leads to better combat TBML and related schemes.

The Report also contains the finding that FinCEN "could incorporate the [Trade Transparency Unit's (TTU)] trade data into their analyses." Based on these and other factual predicates described in the Report, GAO recommends that Treasury establish an interagency coordination mechanism to promote greater information sharing and data analysis between federal agencies and with relevant private sector entities on issues related to TBML and other illicit trade schemes (Recommendation 1). GAO also recommends that the Department of Homeland Security (DHS) should ensure that U.S. Immigration and Customs Enforcement takes steps to enable and implement sharing of the trade data maintained by the TTU—including for the purposes of trade data analysis about patterns or trends of illicit activity related to trade-based money laundering (TBML)—with U.S. agencies with roles and responsibilities related to enforcing trade laws and combating illicit financial activities, as appropriate (Recommendation 2).

www.fincen.gov

Treasury Management's Analysis of Recommendation 1

GAO Recommendation 1: "The Secretary of the Treasury, in collaboration with partner agencies, should establish an interagency collaboration mechanism to promote greater information sharing and data analysis between federal agencies and with relevant private sector entities on issues related to TBML and other illicit trade schemes."

As identified in the report, Treasury agrees that TBML is one of the most challenging forms of money laundering to investigate. Treasury also agrees that raising awareness among financial institutions through outreach and working groups and efforts to improve data analytics on trade data sharing may assist law enforcement in better identifying and investigating TBML.[1] Treasury already coordinates and shares information with numerous federal agencies, including law enforcement, in support of TBML-related efforts. While Treasury could seek to promote greater formal coordination among federal agencies on TBML to improve information sharing and data analysis, the effectiveness and success of such a coordination mechanism to combat illicit finance schemes would ultimately rely on DHS and the TTU data being made broadly available to Treasury, law enforcement, and other agencies.

However, there are additional steps that Treasury can take in the meantime, even given limited resources and competing mission obligations, to support the fight against TBML. For instance, FinCEN can leverage its FinCEN Exchange program to enhance collaboration on TBML between Treasury, law enforcement, and the financial sector. The FinCEN Exchange is FinCEN's voluntary public-private information sharing partnership that convenes law enforcement, financial institutions, and others to effectively and efficiently combat money laundering, terrorism financing, organized crime, and other financial crimes; protect the financial system from illicit use; and promote national security.[2] FinCEN can also continue to work with the TTU and law enforcement to highlight TBML trends and investigative leads identified in Bank Secrecy Act reporting. Treasury's Office of Terrorism Financing and Financial Crimes will continue to raise global awareness of TBML via the Financial Action Task Force, Treasury Risk Assessments and Strategies, and through foreign and domestic private and public engagements.

Finally, as GAO is aware, FinCEN is currently working with a contractor on a TBML study consistent with Section 6506 of the AML Act of 2020.[3] That study will eventually inform proposed mitigation strategies to combat TBML in partnership with other agencies. It may be

[1] Treasury, *2020 National Strategy for Combating Illicit Finance*. See page 45, Priority 3.
[2] FinCEN launched the FinCEN Exchange on December 4, 2017, to provide financial institutions with additional information about priority issues on a more regular basis. Section 6103 of the AML Act, codified at 31 U.S.C. § 310(d), formally established the FinCEN Exchange.
[3] The AML Act of 2020 is Division F of the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (January 1, 2021).

premature to reach the conclusion that Treasury should develop and lead a formal interagency collaboration mechanism to promote greater information sharing and data analysis regarding TBML while a Treasury study on TBML is underway.

If GAO retains Recommendation 1, Treasury believes that the lack of access to and analysis of trade data outside of DHS should be recognized as a critical component to any coordination effort. Treasury suggests that Recommendation 2 be prioritized.

Sincerely,

Anna L. Tirol Digitally signed by Anna L. Tirol Date: 2021.10.29 10:52:16 -04'00'

AnnaLou Tirol
Deputy Director

Appendix IV: GAO Contacts 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), Pamela Davidson, Georgette Hagans, Maria McMullen, Jennifer Schwartz, and Tyler Spunaugle made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548