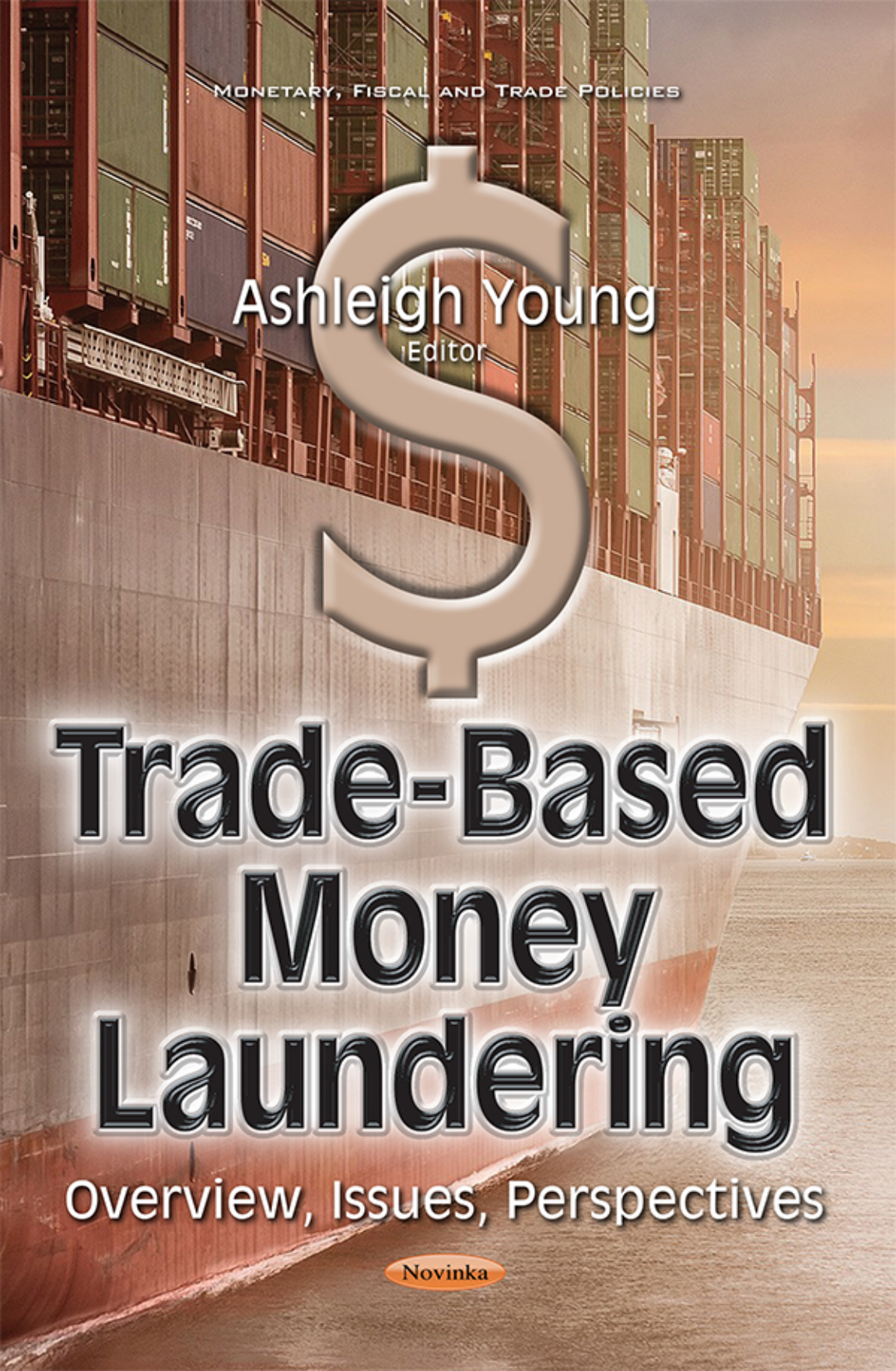

Monetary, Fiscal and Trade Policies
Ashleigh Young
Editor
Trade-Based Money Laundering
Overview, Issues, Perspectives
Novinka

MONETARY, FISCAL AND TRADE POLICIES

TRADE-BASED MONEY LAUNDERING

OVERVIEW, ISSUES, PERSPECTIVES

MONETARY, FISCAL AND TRADE POLICIES

Additional books in this series can be found on Nova's website under the Series tab.

Additional e-books in this series can be found on Nova's website under the e-book tab.

MONETARY, FISCAL AND TRADE POLICIES

TRADE-BASED MONEY LAUNDERING

OVERVIEW, ISSUES, PERSPECTIVES

ASHLEIGH YOUNG
EDITOR

New York

NOTICE TO THE READER

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-53610-544-5 (eBook)

Published by Nova Science Publishers, Inc. † New York

CONTENTS

PREFACE

Trade-based money laundering (TBML) involves the exploitation of the international trade system for the purpose of transferring value and obscuring the true origins of illicit wealth. TBML schemes vary in complexity but typically involve misrepresentation of the price, quantity, or quality of imports or exports. Financial institutions may wittingly or unwittingly be implicated in TBML schemes when such institutions are used to settle, facilitate, or finance international trade transactions (e.g., through the processing of wire transfers, provision of trade finance, and issuance of letters of credit and guarantees). TBML activity is considered to be growing in both volume and global reach. Although TBML is widely recognized as one of the most common manifestations of international money laundering, TBML appears to be less understood among academics and policymakers than traditional forms of money laundering through the international banking system and bulk cash smuggling. This book discusses the scope of the TBML problem and analyzes selected U.S. government policy responses to address TBML. It includes a listing of hearings in the 114th Congress that addressed TBML.

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 1

TRADE-BASED MONEY LAUNDERING: OVERVIEW AND POLICY ISSUES*

Rena S. Miller, Liana W. Rosen and James K. Jackson

SUMMARY

Trade-based money laundering (TBML) involves the exploitation of the international trade system for the purpose of transferring value and obscuring the true origins of illicit wealth. TBML schemes vary in complexity but typically involve misrepresentation of the price, quantity, or quality of imports or exports. Financial institutions may wittingly or unwittingly be implicated in TBML schemes when such institutions are used to settle, facilitate, or finance international trade transactions (e.g., through the processing of wire transfers, provision of trade finance, and issuance of letters of credit and guarantees). TBML activity is considered to be growing in both volume and global reach. Although TBML is widely recognized as one of the most common manifestations of international money laundering, TBML appears to be less understood among academics and policymakers than traditional forms of money laundering through the international banking system and bulk cash smuggling. Nevertheless, TBML has emerged as an issue of growing interest in the 114th Congress, especially as Members and committees examine tools to counter terrorist financing.

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, R44541, dated June 22, 2016.

The U.S. government has historically focused on TBML schemes involving drug proceeds from Latin America, particularly the Black Market Peso Exchange (BMPE). Although a number of anecdotal case studies in recent years have revealed instances in which TBML is used by known terrorist groups and other non-state armed groups, including Hezbollah, the Treasury Department's June 2015 *National Terrorist Financing Risk Assessment* concluded that TBML is not a dominant method for terrorist financing.

The United States is combating TBML in a number of ways:

- The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issues advisories and geographic targeting orders and applies special measures to jurisdictions determined to be of primary money laundering concern.
- The United States is also an active participant in the intergovernmental Financial Action Task Force (FATF), created in 1989 to develop and promote guidelines on anti-money laundering and combating the financing of terrorism (AML/CFT). FATF has addressed TBML methods and best practices to combat TBML in periodic reports and mutual evaluations of its members.
- The U.S. Department of Homeland Security (DHS), through its Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI) unit, maintains a Trade Transparency Unit (TTU) in Washington, DC. The TTU has U.S. Department of State funding and Treasury Department support. DHS has since developed a network of counterpart TTUs in almost a dozen countries abroad. The TTUs examine trade anomalies and financial irregularities associated with TBML, customs fraud, contraband smuggling, and tax evasion.

This report discusses the scope of the TBML problem and analyzes selected U.S. government policy responses to address TBML. It includes a listing of hearings in the 114th Congress that addressed TBML.

WHAT IS TRADE-BASED MONEY LAUNDERING?

Trade-based money laundering (TBML) involves the exploitation of the international trade system for the purpose of transferring value and obscuring the true origins of illicit wealth. The Financial Action Task Force (FATF), an intergovernmental standard-setting body on anti-money laundering and combating the financing of terrorism (AML/CFT), has defined TBML as the

process of disguising proceeds of crime and moving value through trade transactions to legitimize their illicit origin. This process varies in complexity, but typically involves the misrepresentation of the price, quantity, or quality of imports or exports.[1] When used by terrorist groups to finance their activities, move money, or otherwise disguise the source and beneficiaries of their funds, TBML schemes are sometimes referred to as TBML/FT. Financial institutions are wittingly or unwittingly implicated in TBML and TBML/FT schemes when they are used to settle, facilitate, or finance international trade transactions (e.g., through processing wire transfers, providing trade finance, and issuing letters of credit and guarantees).

In June 2015, the U.S. Department of the Treasury issued two reports related to money laundering: a *National Money Laundering Risk Assessment* and a *National Terrorist Financing Risk Assessment*. The *National Money Laundering Risk Assessment* identified TBML as among the most challenging and pernicious forms of money laundering to investigate.[2] Citing information from U.S. Immigration and Customs Enforcement (ICE), Treasury described TBML schemes as capable of laundering billions of dollars annually. A February 2010 advisory on TBML, issued by the Treasury Department's Financial Crimes Enforcement Network (FinCEN), stated that more than 17,000 Suspicious Activity Reports (SARs) described potential TBML activity between January 2004 and May 2009, which involved transactions totaling in the aggregate more than $276 billion.[3]

In addition to TBML, criminal organizations and terrorist financiers use the international financial system itself and the physical movement of cash through couriers to disguise their activities. In particular, criminal organizations and terrorist financiers take advantage of the size and complexity of the international trade and finance system to obscure individual transactions through (1) the complexities involved with multiple foreign exchange transactions and diverse trade financing arrangements; (2) the co-mingling of legitimate and illicit funds; and (3) the limited resources that most customs agencies have available to detect suspicious trade transactions.[4] In addition, money launderers have exploited vulnerabilities in the use of letters of credit and other financial arrangements that are necessary for facilitating cross-border trade to launder funds. According to FATF, TBML techniques "vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail."[5]

In most cases, TBML activities comprise efforts to misrepresent the price, quality, or quantity of goods as they transit across borders or through supply chains. The basic TBML techniques include the following:

- *Over- and under-invoicing of goods and services*. According to the FATF, money laundering through over- and under-invoicing goods and services is one of the most commonly used methods for laundering funds across borders. By invoicing a good or service below market value, an exporter can shift funds to the importer because the payment to the exporter is less than the value that the importer receives when the goods are sold at market value. Similarly, by invoicing a good or service at a price higher than market value, the exporter transfers value from the importer because the payment to the exporter is greater than the value the importer receives when the goods or services are sold at market value. These types of transactions generally require collusion by both parties and can have significant tax implications. Also, complex products and products that travel through supply chains are more apt to be used in these types of over- and under-invoicing activities because they complicate the ability of customs officials to determine the true market value of such goods and services.
- *Multiple invoicing of goods and services*. By providing multiple invoices for the same transaction, a money launderer or terrorist financier can justify multiple payments for the same goods or services. In addition, by using a number of financial institutions to make these multiple payments, a money launderer or terrorist financier can increase the level of complexity of the transaction and complicate efforts at detection. If the transaction is detected, a launderer can offer a number of plausible explanations that compound efforts by officials to detect the activities.
- *Over- and under-shipments of goods and services.* In addition to manipulating the prices of goods and services, a money launderer can misstate the quantity of goods and services that are exported or imported. In the extreme, exporters and importers can collude in not shipping any goods at all but proceed with processing the necessary shipping and customs documents. Banks and other financial institutions may be unaware that these “phantom” transactions are occurring.

- *Falsely described goods and services.* Money launderers also can misstate the quality or the type of a good or service that is being traded. Such a misstatement creates a discrepancy between the value of a good that is stated on the shipment or customs forms and what is actually shipped.

Combining several of these common TBML techniques is a classic scheme involving the laundering of drug proceeds from Latin America, called the Black Market Peso Exchange (BMPE). BMPE emerged as a major money-laundering method when Colombian drug traffickers used sophisticated trade-based schemes to disguise as much as $4 billion in annual narcotics profits in the 1980s.[6] For further illustration, see *Text Box* below.

Black Market Peso Exchange (BMPE): An Illustration

Although Latin America and the United States are used in the example below, similar arrangements have been widely used in many countries to repatriate the proceeds of various types of crimes. These transactions combine legal and illegal activities and multiple actors across international jurisdictions that wittingly or unwittingly facilitate TBML.

Illustrative steps of a black market peso exchange

1 Drug traffickers smuggle illegal drugs into the United States and sell them for U.S. dollars ("narco dollars"). 2 Drug traffickers sell the narco dollars at a discount to a peso broker. 3 The peso broker consolidates the narco dollars in a U.S. bank account and 4 pays the drug traffickers with pesos from a Latin American bank account. 5 The peso broker uses narco dollars to pay a U.S. exporter for legitimate goods on behalf of a Latin American importer. 6 The Latin American importer receives the legitimate goods and 7 sells them in Latin America for pesos. 8 The Latin American importer repays the peso broker with pesos.

Source: Financial Action Task Force, Trade Based Money Laundering, June 23, 2006, p. 8.

Key Concepts Associated with BMPE Schemes

[A] Money Laundering has three phases: (1) Structuring, when "dirty" cash is introduced into the financial system;

2 Layering, when a series of financial transactions are conducted to camouflage the illicit origins of the cash; and

3 Integration, when the seemingly legitimate cash becomes free to move anywhere in the financial system.

[B] A shell company is a company without active business operations serving as a vehicle for business transactions. A shelf company is a shell company with a long history of transactions. Both shell and shelf companies might serve legitimate purposes. On the other hand, a front company is a company with active business operations that serves as a front for illegal activities.

[C] Trade fraud techniques include variations on false invoicing: under-invoicing (used when importing goods/services to move money abroad); over-invoicing (used when exporting goods/services to receive money coming from abroad); and multiple invoicing. Supporting documents might also be manipulated, by providing false descriptions of goods or services or by falsifying bill of ladings, cargo manifests, and customs declarations. Shipment fraud techniques include short shipping (to move cash abroad); over-shipping (to receive money coming from abroad); and phantom shipping.

[D] Financial institutions are involved in TBML schemes when they are used to settle, facilitate, or finance international trade transactions, including through (1) letters of credit (in which a bank guarantees for one of its customers that the goods/services ordered to a seller abroad will be paid in full; the bank additionally insures its customer that payment will not be processed prior to confirmed receipt of shipped items); (2) letters of guarantee (similar to letters of credit, but when a bank only guarantees a sum of money to the beneficiary); (3) provisions of trade financial services; and (4) wire transfers.

SCOPE OF THE PROBLEM

TBML is widely recognized as one of the most common manifestations of international money laundering as well as a known value transfer and reconciliation method used by terrorist organizations. Nevertheless, TBML

appears to be less understood among academics and policymakers than traditional forms of money laundering through the international banking system and bulk cash smuggling. Considering the volume of global trade and the value of such transactions, however, TBML's effects can result in substantial consequences for international commerce and government revenue. The *National Money Laundering Risk Assessment* concludes that

> TBML can have a more destructive impact on legitimate commerce than other money laundering schemes. According to ICE HSI [Homeland Security Investigations], transnational criminal organizations may dump imported goods purchased with illicit proceeds at a discount into a market just to expedite the money laundering process. The below-market pricing is a cost of doing business for the money launderer, but it puts legitimate businesses at a competitive disadvantage. This activity can create a barrier to entrepreneurship, crowding out legitimate economic activity. TBML also robs governments of tax revenue due to the sale of underpriced goods, and reduced duties collected on undervalued imports and fraudulent cargo manifests.[7]

The global trends that facilitated a quadrupling of global trade over the past quarter century, measured at $16.4 trillion in 2015, are also being used by drug smugglers and other criminal organizations to hide the gains of illegal or illicit activities. In particular, advances in communications and lower transportation costs, combined with the digital revolution, global value chains, and greater urbanization, have produced more interconnected economies and societies that link together national economies and create vast new market opportunities. Reportedly, organized crime has followed these trends and expanded its activities into new markets.[8]

According to a research report by the Organization for Economic Cooperation and Development (OECD), these global markets offer criminal organizations new markets to reduce their overall risks by diversifying into profitable activities with low probability of being detected. According to the OECD's report, "Illicit trade needs to be presented within the context of global market trends.... Criminal groups adopted new types of activity and trade to overcome the challenge of connecting production to distant consumers. These new synergies created economies of scale and other efficiencies common to legitimate trade, and the opportunity to diversify into new illicit markets."[9] The OECD further concluded that such illegal trade and the attendant financial flows not only present a challenge for law enforcement but also potentially

could have wide-ranging economic and development consequences, particularly as illegal transfers of money and capital out of developing countries may result in reductions of domestic expenditure and investment.[10]

Vulnerabilities

The potential is vast for criminal organizations and terrorist groups to exploit the international trade system with relatively low risk of detection. According to FATF, key characteristics of the international trade system have made it both attractive and vulnerable to illicit exploitation. According to FATF, vulnerabilities include the following:

- "The enormous volume of trade flows, which obscures individual transactions and provides abundant opportunity for criminal organizations to transfer value across borders;
- The complexity associated with (often multiple) foreign exchange transactions and recourse to diverse financing arrangements;
- The additional complexity that can arise from the practice of comingling illicit funds with the cash flows of legitimate business;
- The limited recourse to verification procedures or programs to exchange customs data between countries; and
- The limited resources that most customs agencies have available to detect illegal trade transactions."[11]

Global Hotspots

According to FinCEN, TBML activity is growing in both volume and global reach. In an analysis of SARs between January 2004 and May 2009, TBML activity was most frequently identified in transactions involving Mexico and China. Panama was ranked third, potentially due to TBML activity linked to the Panama Colon Free Trade Zone, whereas the Dominican Republic and Venezuela were identified as "countries with the most rapid growth in potential TBML activity."[12]

According to the U.S. Department of State's 2016 annual report on money laundering and financial crimes, TBML concerns have surfaced in countries or jurisdictions including Afghanistan, Australia, Belize, Brazil, Cambodia,

Canada, China, Colombia, Greece, Guatemala, Hong Kong, India, Iran, Iraq, Japan, Kenya, Lebanon, Mexico, Pakistan, Panama, Paraguay, the Philippines, Singapore, Saint Maarten, Switzerland, Taiwan, the United Arab Emirates (UAE), Uruguay, Venezuela, and the West Bank and Gaza.[13] The State Department's *Country Reports on Terrorism 2015* (released in 2016) noted that TBML unrelated to terrorist financing also occurs in Trinidad and Tobago. Based on these reports, TBML is often associated with significant losses in potential customs and tax revenue, circumvention of foreign exchange capital restrictions, corruption of customs authorities, exploitation of free trade zones, laundering of proceeds associated with black and grey market goods, counter-valuation among informal money brokers (e.g., *hawaladars*), and trade in gold and precious gems.

Links to Terrorism

Although a number of anecdotal case studies in recent years have revealed instances in which known terrorist groups and other non-state armed groups, including Hezbollah, used TBML, the Treasury Department's June 2015 *National Terrorist Financing Risk Assessment* concluded that TBML is not a dominant method for terrorist financing.[14] It stated,

> Broadly speaking, based on an analysis of U.S. law enforcement investigations and prosecutions relating to TF [terrorist financing], two methods of moving money to terrorists and terrorist organizations have been predominate in the convictions and cases pending since 2001: the physical movement of cash and the movement of funds through the banking system.... The physical movement of cash accounted for 28 percent of these cases while movement directly through banks constituted 22 percent, movement through licensed MSBs [money services businesses] 17 percent, and movement by individuals or entities acting as unlicensed money transmitters constituted 18 percent."[15]

The footnote following the sentence quoted above continued: "The remaining 15 percent were a mix of checks, wire transfers through unspecified financial institutions, and TBML."[16]

In its latest *Country Reports on Terrorism*, the State Department identified TBML as a terrorism-related concern in Tunisia and Syria, particularly as a technique used by *hawala* brokers in conjunction with corrupt customs and

immigration officials.[17] *Hawala* refers to an informal method for transferring funds that is commonly used in parts of the Middle East and South Asia where the formal banking system has limited presence. A *hawala* transfer typically involves a network of trusted money brokers, or *hawaladars*, who rely on each other to accept and disburse funds to third-party clients on their behalf. Settlement of account balances among *hawaladars* takes place subsequently, but not necessarily through bank and nonbank financial institutions. Such informal value transfer systems are often preferred because of their perceived quickness, reliability, and lower cost. Unregulated *hawala* systems, however, are perceived by government authorities as lacking sufficient transparency and investigations have revealed that they are vulnerable to abuse by terrorist groups.[18]

The State Department's 2016 annual report on money laundering and financial crimes also identified some specific countries that may be vulnerable to TBML/FT schemes. For example, the report notes that expanded trade cooperation pursuant to the 2011 Afghanistan/Pakistan Transit Trade Agreement encompasses trade routes that are known for TBML and that "pass through key locations where insurgent and terrorist groups operate."[19]

In Lebanon, the State Department reports that individuals are involved in a TBML scheme involving trade in vehicles, sometimes co-mingled with weapons, to launder drug proceeds linked to Hezbollah (for further discussion, see case study below on "Hezbollah-Linked TBML"):

> U.S. law enforcement identified money wires coming into the United States from Jordanian and Lebanese entities to various domestic vehicle dealerships. These funds are used to purchase vehicles subsequently exported to Lebanon and Jordan. In some instances, there are weapons secreted within the exported vehicles. The transactions that occur in the United States appear to be legitimate, but the ultimate destination of the vehicles is unknown and the proceeds may be directed back to Hizballah in Lebanon.[20]

TBML schemes have long prevailed in Paraguay's Tri-Border Area with Brazil and Argentina, where the cross-border cigarette smuggling market, believed to be worth approximately $1 billion per year, is also used for money-laundering purposes, enriching criminal organizations, corrupt officials, and, at least in the past, potentially also terrorist organizations.

In the United Arab Emirates, the State Department reports that TBML schemes "might support sanctions-evasion networks and terrorist groups in Afghanistan, Pakistan, Iran, Iraq, Syria, Yemen, and Somalia."[21]

SELECTED CASE STUDIES

Hezbollah-Linked TBML

In February 2011, the Department of the Treasury designated the Lebanese Canadian Bank (LCB) as a financial institution of primary money-laundering concern, stating that, according to U.S. government information, Hezbollah "derived financial support" from these drug and money laundering schemes, which involved TBML.[22] Treasury noted that an international narcotics trafficking and money laundering network "move[d] illegal drugs from South America to Europe and the Middle East via West Africa and launder[ed] hundreds of millions of dollars monthly through accounts held at LCB, as well as through trade-based money laundering involving consumer goods throughout the world, including through used car dealerships in the United States."[23]

In one such scheme, LCB facilitated wire transfers to U.S. banks to purchase used cars in the United States.[24] Cars were purchased in the United States and shipped to countries in West Africa and elsewhere, and the proceeds from the car sales would reportedly be repatriated back to Lebanon through bulk cash deposits among conspiring exchange houses. In another scheme associated with the same Hezbollah-linked drug trafficking network, Asian-supplied consumer goods were shipped to Latin America and the proceeds were laundered through a BMPE-styled scheme. The funds sent to pay for the consumer goods were reportedly funneled through LCB's U.S. correspondent accounts.[25]

Ultimately, Lebanon's central bank and monetary authority, the Banque du Liban, revoked LCB's banking license in September 2011 and LCB's former shareholders sold its assets and liabilities to the Lebanese Societé Generale de Banque au Liban. Some of the individuals and entities associated with this illicit network have also variously been subject to financial sanctions and law enforcement investigations in the United States.[26]

Toys-for-Drugs BMPE Scheme

According to U.S. and international reports, in the late 2000s, owners of the Los Angeles-based toy wholesaler Woody Toys, Inc. received millions of dollars in cash payments generated from Colombian and Mexican narcotics trafficking and laundered such funds in a BMPE scheme. The cash payments reportedly were placed directly into the company's bank account from multiple locations in small deposits that were consistently under $10,000 to avoid reporting requirements (i.e., structuring). The toy company used the cash deposits to purchase toys from China, which, in turn, were exported to Colombia. The Colombian pesos generated by the toy sales in Colombia were used to reimburse the Colombian drug traffickers through the BMPE. Some of the employees of Woody Toys had previously worked for Angel Toy Company, whose owners had also been implicated in a similar toys-for-drugs BMPE scheme. The law enforcement investigation into this case benefitted from an information sharing arrangement between the United States and Colombia on trade data through the Trade Transparency Units (TTUs) established in both countries (see section below on "U.S. Department of Homeland Security's Trade Transparency Units").[27]

Trade Finance and *Hawala* Networks

According to the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, another scheme to launder funds derived in the early 2000s from multiple major international drug traffickers involved cash couriers, money transfer services, alternate value transfer systems (e.g., *hawala*), and formal mechanisms of trade finance, managed and directed by an Indian national living in Dubai.[28] The individual involved operated numerous businesses in Dubai as well as numerous affiliates in Europe, Asia, Africa, and the United States.

In Dubai, the individual opened letters of credit (LCs) through his different companies for various importers. These LCs were opened to benefit various affiliated exporters in India and other locations and were in amounts substantially higher than the market value of the exports. In opening the LCs, the individual used his businesses' connections with certain issuing and advising banks to transmit the LCs to the affiliated exporters in India. The individual also arranged for bogus trade documents that reflected the inflated

value of the exports to satisfy the issuing and advising banks. The LCs, with inflated export values, along with drug trafficking funds, were remitted to the exporters in India, essentially moving money through the financial system in the guise of trade financing. Once in India, the exporters distributed the drug proceeds to the various affiliates and sold the exports at market value.

In addition, that same Indian national used various techniques to move funds offshore through *hawala* operators. In one scheme, he facilitated trade in banned goods by falsifying trade documents through his network of businesses in India to export banned goods from India. To circumvent the restrictions, the goods were falsely described and valued in the trade documents. *Hawala* operators were used to settle the difference between the true value of the exported goods and the fraudulent value of the goods.[29]

SELECTED POLICY RESPONSES

Several of the primary U.S. government policy responses and tools to address TBML include U.S. participation in the international Financial Action Task Force; a number of Treasury Department regulatory responses; and use of the Department of Homeland Security's Trade Transparency Units, which are discussed below.

U.S. Participation in the Financial Action Task Force

FATF was organized to develop and promote AML/CFT guidelines.[30] It currently comprises 34 member countries and territories and 2 regional organizations.[31] Although FATF has no enforcement capabilities, it relies on a combination of annual self-assessments and periodic mutual evaluations on the compliance of its members to FATF guidelines. It can suspend member countries that fail to comply on a timely basis with its guidelines. Since its inception in 1989, FATF was charged with examining money laundering techniques and trends, reviewing actions already taken, and setting out the measures to be taken to combat money laundering. In 1990, FATF issued a new report containing 40 recommendations,[32] which provided a comprehensive plan of action to fight against money laundering.

The Treasury Department's Office of Terrorist Financing and Financial Crimes (TFFC) leads the U.S. interagency delegation to the FATF, advancing the FATF's global efforts in combating money laundering, terrorist financing,

and other illicit financing threats that pose a risk to the integrity of the international financial system.[33] The United States has been a strong supporter of the FATF. Treasury staff members chair the U.S. delegation to the FATF, and it has been an important organizational resource in centralizing efforts to combat money laundering and terrorist financing. The delegation includes members of the Departments of State and Justice, the National Security Council, and federal financial regulators. It develops U.S. positions; represents the United States at FATF meetings; and implements actions domestically to meet U.S. commitments to the FATF.

In February 2012, FATF members adopted a revised set of the FATF 40 Recommendations (subsequently updated again October 2015), which integrated CFT guidelines into the core set of recommendations and added the proliferation of financing of weapons of mass destruction to FATF's areas of surveillance. The new mandate is intended to

- deepen global surveillance of evolving criminal and terrorist threats;
- build a stronger, practical, and ongoing partnership with the private sector; and
- support global efforts to raise standards, especially in low capacity countries.

In addition, the revised recommendations address new and emerging threats, while clarifying and strengthening many of the existing obligations. The new standards strengthen the requirements for higher-risk situations and allow countries to take a more focused approach to areas where high risks remain or where implementation could be enhanced. The standards also address transparency requirements related to the adequate, accurate, and timely information on the beneficial ownership and control of legal persons and arrangements to address tax transparency, corporate governance, and various types of criminal activity.

Recommendations specifically to counter TBML, however, are not included in the current set of FATF 40 Recommendations, despite recognition that the rapid growth and complexity of the international trade and financing system has multiplied the opportunities for abuse of this system by money launderers and terrorist financiers. FATF, however, has occasionally issued stand-alone reports that address TBML and best practices.[34]

Surveys conducted by the FATF indicate, however, that there is no comprehensive data set on the extent and magnitude of the TBML issue. In

part, the FATF determined that this lack of data reflected the fact that most jurisdictions do not identify TBML as a separately identifiable activity under the general topic of money laundering and, therefore, did not collect data on this specific type of activity. The FATF also concluded that most jurisdictions do not offer training specifically related to TBML activities that would assist trade and finance specialists in identifying TBML activities.[35] As part of its efforts to promote best practices regarding training for detecting TBML, the FATF recommended that jurisdictions develop training programs that are specific to TBML and could focus on financial and trade data analysis for identifying trade anomalies and identifying criminal activities, among other reforms.[36]

What is the Financial Crimes Enforcement Network?

The Financial Crimes Enforcement Network (FinCEN) is a bureau within the U.S. Department of the Treasury whose mission is to safeguard the financial system through the collection, analysis, and dissemination of financial intelligence to law enforcement. FinCEN's director is appointed by the Secretary of the Treasury and reports to the Under Secretary of the Treasury for Terrorism and Financial Intelligence. FinCEN also acts as the U.S. financial intelligence unit (FIU), one of the more than 100 FIUs that comprise the Egmont Group, an international body focused on information sharing and cooperation among FIUs.[37] FinCEN receives data, such as suspicious activity reports (SARs) from banks and other financial firms, analyzes the data, and disseminates it to law enforcement. It also cooperates with foreign FIUs in exchanging information, largely through its membership and participation in the Egmont Group.

FinCEN exercises regulatory functions primarily under the Currency and Financial Transactions Reporting Act of 1970,[38] as amended by Title III of the USA PATRIOT Act of 2001[39] and other legislation, together commonly referred to as the Bank Secrecy Act (BSA).

The BSA is the United States' first and most comprehensive Federal AML/CFT statute. It authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to establish AML programs and to file reports on financial activity that may have relevance for criminal, tax, and regulatory investigations or for intelligence or counterterrorism.

U.S. Department of the Treasury Regulatory Actions

Central to the Treasury Department's efforts to combat TBML is FinCEN, which issues advisories and geographic targeting orders and applies special measures to jurisdictions determined to be of primary money laundering concern.

Advisories

In general, a FinCEN advisory red flags for financial institutions activities that may be indicative of certain types of money laundering, in line with recent investigations, to assist financial institutions in filing SARs. FinCEN first highlighted TBML in November 1997 and then again in June 1999 with advisories on BMPE.[40]

In February 2010, FinCEN issued an advisory on TBML, based on law enforcement experience involving U.S. trade with Central and South America.[41] The advisory was to aid financial institutions in reporting suspicious activity related to TBML. The advisory noted the basic schemes behind TBML and offered more specific red flags. It further noted that reporting on suspected TBML was inconsistent and requested that financial institutions include the abbreviation TBML or BMPE on SARs.[42] FinCEN also described substantial delays in reporting suspected TBML activity.[43]

In May 2014, FinCEN issued an updated TBML advisory on increased TBML activity involving funnel accounts following the restrictions on U.S. currency in Mexico.[44] A funnel account is an individual or business account in one geographic area receiving multiple cash deposits, often below the jurisdiction's cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.[45] The advisory provides several specific red flags associated with such activity conducted by Mexican criminal and drug trafficking organizations.

Geographic Targeting Orders

In recent years, FinCEN appears to have also begun to rely more heavily on Geographic Targeting Orders (GTOs), a tool that was first authorized in 1988. A GTO imposes additional, but time-limited, recordkeeping and reporting requirements on domestic financial institutions or nonfinancial businesses in a particular geographic area to assist regulators and law enforcement agencies in identifying criminal activity. In the absence of extensions, GTOs may only remain in effect for a maximum of 180 days.

Violators may face substantial civil or criminal liability. Several recent GTOs have been used to enhance U.S. efforts to combat TBML.

- In April 2015, FinCEN issued a GTO that lowered cash reporting thresholds and triggered additional recordkeeping requirements for certain financial transactions for about 700 Miami-based electronics exporters.[46] The GTO required targeted businesses to file forms with FinCEN reporting any single transaction or related transactions in which they receive more than $3,000 in cash—a stricter standard than the ordinary $10,000 filing threshold for cash transactions imposed pursuant to BSA. FinCEN stated that the new reporting requirements are aimed at combating complex TBML-related schemes employed by the Sinaloa and Los Zetas drug and transnational crime organizations. In October 2015, FinCEN renewed the GTO for an additional 180 days.[47]
- In October 2015, FinCEN issued a similar GTO that also lowered cash reporting to $3,000 and triggered additional recordkeeping requirements. This GTO targeted businesses in the Los Angeles Fashion District in an effort to frustrate suspected Mexican and Colombian drug traffickers who had been exploiting fashion industry businesses to engage in BMPE schemes.[48]

Special Measures

Pursuant to BSA, as amended by the USA PATRIOT Act, FinCEN may require financial institutions and agencies within U.S. jurisdiction to take certain regulatory special measures against a foreign jurisdiction, foreign financial institution, class of transaction, or type of account determined to be of "primary money laundering concern."[49] The enumerated five special measures, which may be imposed individually, in any combination, and in any sequence, range from requiring enhanced due diligence to prohibiting the opening or maintaining of correspondent or payable-through accounts. In some cases, such action corresponds with other administrative actions taken by the Treasury Department, including by the Office of Foreign Asset Control (OFAC), which is responsible for administering financial sanctions that target specially designated foreign nationals and entities. Among the eight active cases, two were designated for their involvement in TBML, including the Halawi and Rmeiti Exchanges.

In April 2013, FinCEN separately designated two Lebanese exchange houses, Halawi Exchange and Rmeiti Exchange, as financial institutions of

primary money laundering concern. According to U.S. government information, both exchange houses facilitated transactions associated with a large-scale TBML scheme, involving the purchase of used cars in the United States for export to West Africa. Moreover, U.S. authorities claim that both exchange houses had been providing money laundering services for an international narcotics trafficking and money laundering network linked to Hezbollah.[50]

U.S. Department of Homeland Security's Trade Transparency Units

Within the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI) established the first Trade Transparency Unit in Washington, DC, in 2004. Using a specialized computer system called the "Data Analysis and Research for Trade Transparency System," TTUs examine trade anomalies and financial irregularities in domestic and foreign trade data to identify instances of TBML, customs fraud, contraband smuggling, and tax evasion that warrant further law enforcement investigation. Often with funding support from the Department of State's Bureau for International Narcotics and Law Enforcement Affairs (INL), HSI and Treasury have stood up or established relationships with TTUs in the countries listed in *Table 1*, below.

According to the State Department, these TTUs form the basis of broader plans to develop an international network of TTUs, similar to the Egmont Group of FIUs.[51] The 2007 *National Money Laundering Strategy* established attacking TBML at home and abroad as a national goal and specifically called on the deployment of ICE-led TTUs to facilitate the exchange and analysis of trade data among trading partners. The State Department further reports that "the number of TBML investigations emerging from TTU activity continues to grow."[52] According to one estimate, more than $1 billion has been seized since the creation of the U.S.- and foreign-based TTU effort.[53]

Table 1. Foreign Countries with Trade Transparency Units as of June 2016

Countries with TTUs	Year TTU Established
Australia	2012
Argentina	2006
Colombia	2005
Dominican Republic	2013
Ecuador	2011
Guatemala	2012
Mexico	2008
Paraguay	2007
Panama	2010
Peru	2016
Philippines	2013
Uruguay	2016

Source: State Department response to CRS, June 15, 2016.

Notes: State Department funds assisted in either establishing or furthering the TTUs listed above.

ISSUES FOR CONGRESS

The 114th Congress has addressed TBML specifically in several hearings that have explored TBML links with respect to specific terrorist groups, such as Hezbollah, and regional security priorities, particularly in Latin America. It has also addressed TBML in more general hearings focused on policy responses to address anti-money laundering and terrorist financing. A list of these hearings (prior to the publication of this CRS report) appears in the *Appendix*. Several hearing witnesses have questioned the effectiveness of and challenges confronting U.S. and international efforts to combat TBML, in particular the role of and resources allocated to TTUs. Others have questioned whether U.S. trade policy, including negotiations related to free trade agreements, could be linked to mutual commitments to combat TBML and also relevant financial information and trade data, potentially through the establishment and maintenance of TTUs.[54]

The 114th Congress has been particularly interested in links between TBML and terrorist financing. The Treasury Department, in its June 2015 national risk assessments on money laundering and terrorist financing,

appeared to downplay the relationship between terrorism and TBML. Yet some policymakers remain concerned about such links, often pointing to various examples that implicate Hezbollah in TBML schemes, among others.

In December 2015, the 114th Congress enacted the Hizballah International Financing Prevention Act of 2015,[55] which directed the President to apply additional financial restrictions on Hezbollah-linked foreign financial institutions with U.S. correspondent or payable-through accounts. It also required the President to report to selected congressional committees on various aspects of Hezbollah's financing operations—including its use of TBML as a method for raising and transferring funds; and requires the Secretaries of State and Treasury to periodically brief congressional committees on Hezbollah's assets and financing activities.

On April 15, 2016, OFAC issued a final rule for implementing the Hizballah International Financing Prevention Act of 2015. President Barack Obama has stated that his Administration is "committed to continuing to take strong action, such as imposing sanctions, to counter the activities of Hizballah operatives and supporters, wherever they are located."[56] In June 2016 testimony, the Treasury Department stated that it intends to implement the Hizballah International Financing Prevention Act of 2015 "robustly, but in a manner that is consistent with preserving the strength and health of the Lebanese financial system."[57] Congress may seek to continue to monitor the implementation of the Hizballah International Financing Prevention Act of 2015 and other financial tools available to address TBML.

APPENDIX. 114TH CONGRESS HEARINGS THAT INCLUDED DISCUSSION OF TRADE-BASED MONEY LAUNDERING

The following list includes hearings in the 114th (as of publication) in which trade-based money laundering (TBML) was discussed in testimony or during the question and answer sessions. One hearing, *Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance,* dealt specifically with the topic of TBML.

House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities and House Foreign Affairs Committee, Subcommittee on Terrorism, Nonproliferation and Trade, Stopping the Money Flow: The

War on Terror Finance, June 9, 2016. https:// armedservices.house.gov/legislation/hearings/joint-hearing-stopping-money-flow-warterror-finance.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, The Enemy in our Backyard: Examining Terror Funding Streams from South America, June 8, 2016. http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=400715.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, Stopping Terror Finance: A Coordinated Government Effort, May 24, 2016. http://financialservices.house.gov/calendar/ eventsingle.aspx?EventID=400670.

House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, Current Terrorist Financing Trends, May 12, 2016. https://homeland.house.gov/hearing/following-money-examining-current-terrorist-financingtrends-threat-homeland/.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, Preventing Cultural Genocide: Countering the Plunder and Sale of Priceless Cultural Antiquities by ISIS, April 19, 2016. http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=400550.

House Financial Services Committee, The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System, March 22, 2016. http://financialservices.house.gov/calendar/ eventsingle.aspx?EventID=400462.

Senate Armed Services Committee, United States Strategic Command, United States Northern Command, and United States Southern Command programs and budget in review of the Defense Authorization Request for Fiscal Year 2017 and the Future Years Defense Program, March 10, 2016. http://www.armed-services. senate.gov/imo/media/doc/16-29_3-10-16.pdf.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, Helping the Developing World Fight Terror Finance, March 1, 2016. http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=400338.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance, February 3, 2016. http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=400192.

House Foreign Affairs Committee, Subcommittee on Terrorism, Nonproliferation, and Trade, Terrorist Financing: Kidnapping, Antiquities Trafficking, and Private Donations, November 17, 2015. http://docs.house.gov/meetings/FA/FA18/20151117/104202/HHRG-114-FA18-Transcript20151117.pdf.

Senate Judiciary Committee, Oversight of the Administration's Misdirected Immigration Enforcement Policies: Examining the Impact on Public Safety and Honoring the Victims, July 21, 2015. http://www.judiciary.senate.gov/meetings/oversight-of-the-administrations-misdirected-immigration-enforcement-policies-examining-the-impact-on-public-safety-and-honoring-the-victims.

House Homeland Security Committee, Subcommittee on Border and Maritime Security, The Outer Ring of Border Security: DHS's International Security Programs, June 2, 2015. https://homeland.house.gov/hearing/subcommittee-hearing-outer-ring-border-security-dhs-sinternational-security-programs/.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, A Dangerous Nexus: Terrorism, Crime and Corruption, May 21, 2015. http://financialservices.house.gov/uploadedfiles/114-27.pdf.

House Financial Services Committee, Task Force to Investigate Terrorism Financing, A Survey of Global Terrorism and Terrorism Financing, April 22, 2015. http://financialservices.house.gov/uploadedfiles/114-15.pdf.

House Judiciary Committee, Immigration and Customs Enforcement Oversight Issues, April 14, 2015. https://judiciary.house.gov/wp-content/uploads/2016/02/114-27_94183.pdf.

Senate Homeland Security and Governmental Affairs Committee, Securing the Border: Assessing the Impact of Transnational Crime, March 24, 2015. http://www.hsgac.senate.gov/hearings/securing-the-border-assessing-the-impact-of-transnationalcrime.

House Foreign Affairs Committee, Subcommittee on Western Hemisphere and Subcommittee on Middle East and North Africa, Iran and Hezbollah in the Western Hemisphere, March 18, 2015. http://docs.house.gov/meetings/FA/FA07/20150318/103177/HHRG-114-FA07-Transcript20150318.pdf.

House Financial Services Committee, *The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System*, March 17, 2015. http://financialservices.house.gov/uploadedfiles/114-7.pdf.

End Notes

[1] Financial Action Task Force (FATF), Trade Based Money Laundering, June 23, 2006. The basic techniques of trade-based money laundering (TBML) include over- and under-invoicing of goods and services, multiple-invoicing of goods and services; over- and under-shipment (i.e., short shipping) of goods and services; and falsely described goods and services, including phantom shipping.

[2] U.S. Department of the Treasury, National Money Laundering Risk Assessment, June 12, 2015, at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/Natio nal%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

[3] Financial Crimes Enforcement Network (FinCEN), Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering, advisory, FIN-2010-A001, February 18, 2010.

[4] FATF, Trade Based Money Laundering, June 23, 2006.

[5] FATF, Trade Based Money Laundering, June 23, 2006.

[6] Broadly, the Black Market Peso Exchange (BMPE) facilitated the "swap" of dollars owned by drug cartels in the United States for pesos already in Colombia by selling the dollars to Colombian businessmen who sought to buy U.S. goods for export. See FinCEN, Colombian Black Market Peso Exchange, advisory, issue 9, November, 1997; U.S. Government National Money Laundering Strategy, May 3, 2007; and FATF, Trade Based Money Laundering, June 23, 2006.

[7] U.S. Department of the Treasury, National Money Laundering Risk Assessment, June 12, 2015, p. 29, at https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/Natio nal%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

[8] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, at http://www.keepeek.com/Digital-Asset-Management/oecd/governance/charting-illicittrade_9789264251847-en#page3.

[9] Ibid.

[10] Ibid.

[11] FATF, Trade Based Money Laundering, June 23, 2006.

[12] FinCEN, Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering, advisory, FIN-2010-A001, February 18, 2010.

[13] U.S. Department of State, International Narcotics Control Strategy Report (INCSR), vol. 2, March 2016.

[14] U.S. Department of the Treasury, National Terrorist Financing Risk Assessment, June 12, 2015.

[15] Ibid.

[16] Ibid.

[17] U.S. Department of State, Country Reports on Terrorism 2014, June 2015.

[18] See FinCEN, "Informal Value Transfer Systems," Advisory, FIN-2010-A011, September 1, 2010.

[19] U.S. Department of State, INCSR, vol. 2, March 2016.

[20] Ibid.

[21] Ibid.

[22] Treasury Identifies Lebanese Canadian Bank Sal as a "Primary Money Laundering Concern, U.S. Department of the Treasury, Press Release, Feb. 2, 2011, at https://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx.

[23] Ibid.

[24] For additional details on these schemes, please see, for example.: Asia/Pacific Group on Money Laundering (APG), APG Typology Report on Trade Based Money Laundering, July 20, 2012; Jo Becker, "Beirut Bank Seen As Hub of Hezbollah's Finances," New York Times, December 13, 2011; Sebastian Rotella, "Government Says Hezbollah Profits from U.S. Cocaine Market Via Link to Mexican Cartel," ProPublica, December 13, 2011; "Prosecutors Say Hezbollah Laundered Millions of Dollars into U.S.," Associated Press, December 15, 2011, at http://www.foxnews.com/us/2011/ 12/15/prosecutors-say-hezbollah-laundered-millions-dollars-into-us.html; Devlin Barrett, "U.S. Intensifies Bid to Defund Hezbollah," Wall Street Journal, December 16, 2015.

[25] Jo Becker, "Beirut Bank Seen As Hub of Hezbollah's Finances," New York Times, December 13, 2011; Sebastian Rotella, "Government Says Hezbollah Profits from U.S. Cocaine Market Via Link to Mexican Cartel," ProPublica, December 13, 2011; "Prosecutors Say Hezbollah Laundered Millions of Dollars into U.S.," Associated Press, December 15, 2011; Devlin Barrett, "U.S. Intensifies Bid to Defund Hezbollah," Wall Street Journal, December 16, 2015.

[26] Asia/Pacific Group on Money Laundering (APG), APG Typology Report on Trade Based Money Laundering, July 20, 2012; Jo Becker, "Beirut Bank Seen As Hub of Hezbollah's Finances," New York Times, December 13, 2011; Sebastian Rotella, "Government Says Hezbollah Profits from U.S. Cocaine Market Via Link to Mexican Cartel," ProPublica, December 13, 2011; "Prosecutors Say Hezbollah Laundered Millions of Dollars into U.S.," Associated Press, December 15, 2011; Devlin Barrett, "U.S. Intensifies Bid to Defund Hezbollah," Wall Street Journal, December 16, 2015.

[27] See APG, APG Typology Report on Trade Based Money Laundering, July 20, 2012; U.S. Immigration and Customs Enforcement (ICE), "Co-Owner of Los Angeles-Area Toy Company Sentenced in Drug Money Laundering Case," press release, May 6, 2013, at https://www.ice.gov/news/releases/co-owner-los-angeles-area-toy-company-sentenceddrug-money-laundering-case.

[28] APG, APG Typology Report on Trade Based Money Laundering, July 20, 2012.

[29] Ibid.

[30] For additional information on the FATF, please see CRS Report RS21904, The Financial Action Task Force: An Overview, by James K. Jackson.

[31] FATF members are Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, People's Republic of China, Portugal, Russian Federation, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States; the two international organizations are the European Commission, and the Gulf Cooperation Council. The following organizations have observer status: Asia/Pacific Group on Money Laundering; Caribbean Financial Action Task Force; Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures; Eastern and Southern Africa Anti-Money Laundering Group; Financial Action Task Force on Money Laundering in South America; and other international organizations, including the African Development Bank, Asia Development Bank, European Central Bank, International Monetary Fund, Organization of American States, Organization for Economic Cooperation and Development, United Nations Office on Drugs and Crime, and the World Bank.

[32] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations, adopted on February 16, 2012, and updated in 2013 and 2015.

[33] Kook, Sabina, Financial Action Task Force (FATF) Evolving in its Effort to Combat Money Laundering and Terrorist Financing, Department of Treasury, Treasury Notes, March 23, 2013, at https://www.treasury.gov/connect/ blog/Pages/Financial-Action-Task-Force-%28FATF%29-Evolving-in-its-Effort-to-Combat-Money-Laundering-andTerrorist-Financing.aspx.

[34] FATF, Best Practices on Trade-Based Money Laundering, June 20, 2008.

[35] Ibid.

[36] Ibid.

[37] A financial intelligence unit (FIU) is a national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime and potential financing of terrorism or as otherwise required by national legislation or regulation, in order to combat money laundering and terrorism financing. See FinCEN, "What We Do," at https://www.fincen.gov/ about_fincen/wwd/.

[38] 31 U.S.C. 5311 et seq.

[39] P.L. 107-56.

[40] The two early FinCEN advisories on TBML were also followed in 2005 by additional sections in the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual, issued in collaboration with FinCEN, aimed to provide bank examiners more guidance on assessing the adequacy of bank systems on risks associated with trade finance activities. See http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

[41] FinCEN, Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering, advisory, FIN-2010-A001, February 18, 2010.

[42] Ibid. Of the approximately 17,000 SARs between January 2004 and May 2009 that FinCEN determined may have indicated TBML activity, only 24% of them clearly identified TBML as the suspected activity. The remaining 76% were identified by FinCEN based on complex queries, including trade and other terms derived from various red flags.

[43] Ibid. For example, 14% of suspected TBML activity reported in SARs in 2004 occurred in 2004. However, 30% of such activity was not reported by financial institutions until 2009, five years after the activity occurred.

[44] FinCEN, Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, advisory, FIN-2014-A005, May 28, 2014.

[45] Ibid.

[46] FinCEN, Geographic Targeting Order, April 15, 2015; see also FinCEN, "FinCEN Targets Money Laundering Infrastructure with Geographic Targeting Order in Miami: 'GTO' Addresses Trade-Based Money Laundering Activity Involving Drug Cartels," press release, April 21, 2015.

[47] FinCEN, Geographic Targeting Order, October 20, 2015; see also FinCEN, "FinCEN Renews Geographic Targeting Order (GTO) Requiring Enhanced Reporting and Recordkeeping for Electronics Exporters Near Miami, Florida," press release, October 23, 2015.

[48] FinCEN, Geographic Targeting Order, September 26, 2014; see also FinCEN, "FinCEN Issues Geographic Targeting Order Covering the Los Angeles Fashion District as Part of Crackdown on Money Laundering for Drug Cartels," press release, October 2, 2014.

[49] 31 U.S.C. 5318A, as added by Section 311 of Title III of the USA PATRIOT Act (P.L. 107-56), and subsequently amended.

[50] FinCEN, Notice of Finding that Halawi Exchange Co. is a Financial Institution of Primary Money Laundering Concern, April 23, 2013; FinCEN, Notice of Finding that Kassem Rmeiti and Co. For Exchange is a Financial Institution of Primary Money Laundering Concern, April 23, 2013.

[51] U.S. Department of State, INCSR, vol. 2, March 2015, p.11.

[52] Ibid., p.7.

[53] John Cassara, Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement (Hoboken, NJ: John Wiley and Sons, 2016).

[54] John Cassara, prepared statement for a hearing of the House Financial Services Committee Task Force to Investigate Terrorism Financing on "Trading with the Enemy: Trade Based Money Laundering is the Growth Industry in Terror Finance," February 3, 2016.

[55] P.L. 114-102.

[56] White House, "Statement by the Press Secretary on the Hizballah International Financing Prevention Act of 2015," December 18, 2015.

[57] U.S. Department of the Treasury, Assistant Secretary for Terrorist Financing Daniel Glaser, prepared statement for a joint hearing of the House Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, and the House Armed Services Subcommittee on Emerging Threats and Capabilities," June 9, 2016.

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 2

THE FINANCIAL ACTION TASK FORCE: AN OVERVIEW*

James K. Jackson

SUMMARY

The National Commission on Terrorist Attacks Upon the United States, or the 9/11 Commission, recommended that tracking terrorist financing "must remain front and center in U.S. counterterrorism efforts" (see *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, U.S. Government Printing Office, July, 2004. p. 382). As part of these efforts, the United States plays a leading role in the Financial Action Task Force on Money Laundering (FATF). The independent, intergovernmental policy-making body was established by the 1989 G-7 Summit in Paris as a result of growing concerns among the summit participants about the threat posed to the international banking system by money laundering. After September 11, 2001, the body expanded its role to include identifying sources and methods of terrorist financing and adopted nine special recommendations on terrorist financing to track terrorists' funds. The scope of activity of FATF was broadened as a result of the 2008-2009 global financial crisis, since financial systems in distress can be more vulnerable to abuse for illegal activities. More recently, the FATF added the proliferation of financing of weapons of mass destruction as

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, RS21904, dated March 13, 2014.

one of its areas of surveillance. In April, 2012, the member countries adopted a remodeled set of Forty Recommendations and renewed the FATF's mandate through December 31, 2020. This report provides an overview of the task force and of its progress to date in gaining broad international support for its recommendations.

INTRODUCTION

The Financial Action Task Force on Money Laundering is comprised of 34 member countries and territories and two regional organizations[1] and was organized to develop and promote policies to combat money laundering and terrorist financing, referred to as anti-money laundering/ combatting the financing of terrorism (AML/CFT) measures.[2] The FATF relies on a combination of annual self-assessments and periodic mutual evaluations that are completed by a team of FATF experts to provide information and to assess the compliance of its members to the FATF guidelines. FATF has no enforcement capability, but can suspend member countries that fail to comply on a timely basis with its guidelines. For instance, the FATF warned Turkey in early 2013 that its membership would be suspended unless it became more aggressive in criminalizing money laundering. The FATF is housed at the headquarters of the Organization for Economic Cooperation and Development (OECD) in Paris and occasionally uses some OECD staff, but the FATF is not part of the OECD. The presidency of the FATF is a one-year appointed position, currently held by Mr. Vladimir Nechaev of the Russian Federation, who will serve through June 30, 2014, when Mr. Roger Wilkins of Australia is to assume the presidency. At the ministerial meeting in April 2012, the member countries renewed the FATF's mandate through December 31, 2020.

The FATF focuses on six key areas that are intended to reduce the potential for the abuse of financial systems and financial crimes.

- FATF Recommendations. The FATF issued its Forty Recommendations to serve as global standards to protect the integrity of the international financial system and enhance international co-operation on AML/CFT by increasing transparency and assisting countries in successfully taking action against the illicit use of their financial system.
- High-risk and Non-cooperative Jurisdictions. FATF attempts to identify those countries that are not complying with the FATF

recommendations. On the basis of reviews by the International Co-operation Review Group (ICRG), jurisdictions may be publicly identified in one of the two FATF public documents that are issued three times a year: 1) FATF's Public Statement identifies jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply and jurisdictions which have deficiencies but have not made progress in addressing the deficiencies or have not committed to an action plan to address the deficiencies; and 2) Improving Global AML/CFT Compliance: On-Going Process in which the FATF identifies those jurisdictions that have AFL/CFT deficiencies but have provided a high-level political commitment to address the deficiencies through a plan developed with the FATF.

- Financing of Proliferation. The FATF updated its standards to include measures on the implementation of targeted financial sanctions related to proliferation of weapons of mass destruction.
- Mutual Evaluations. The FATF conducts peer reviews of each member on an ongoing basis to assess levels of implementation of the FATF Recommendations, providing an in-depth description and analysis of each country's system for preventing criminal abuse of the financial system.
- Methods and Trends. FATF monitors and updates the constant evolution of the methods used to launder proceeds of criminal activities and finance illicit activities. Recently, FATF surveyed the vulnerability of Hawalas and other similar service providers to money laundering and terrorist financing as a result of their use of non-bank settlement methods. The FATF also surveyed the vulnerabilities and risks of the diamond trade to money laundering, including production, rough diamond sale, cutting and polishing, jewelry manufacturing and jewelry retailers.
- Corruption. FATF focuses on the linkage between corruption and money laundering, both of which are generally committed to obtain or hide financial gain.

THE MANDATE

When it was established in 1989, the FATF was charged with examining money laundering techniques and trends, reviewing the actions

which had already been taken, and setting out the measures that still needed to be taken to combat money laundering. In 1990, the FATF issued a report containing a set of 40 recommendations,[3] which provided a comprehensive plan of action to fight against money laundering. Following the terrorist attacks of September 11, 2001, the FATF redirected its efforts to focus on money laundering and terrorist financing. On October 31, 2001, the FATF issued a new set of guidelines and a set of eight special recommendations on terrorist financing.[4] At that time, the FATF indicated that it had broadened its mission beyond money laundering to focus on combating terrorist financing and that it was encouraging all countries to abide by the new set of guidelines. A ninth special recommendation was added in 2005. In 2005, the United Nations Security Council adopted Resolution 1617 urging all U.N. Member States to implement the FATF 40 recommendations on money laundering and the nine special recommendations on terrorist financing.

The FATF completed a review of its mandate and proposed changes that were adopted at the May 2004 ministerial meeting. In 2006, FATF adopted a new surveillance process, known as the International Cooperation Review Group, to identify, examine, and engage with vulnerable jurisdictions that are failing to implement effective AML-CFT systems. In addition, the FATF revised its mandate in 2008 to indicate that FATF "will intensify its surveillance of systemic criminal and terrorist financing risks to enhance its ability to identify, prioritize, and act on these threats." The FATF also expressed its support for the development of national threat assessments through best practice guidance and the establishment of stronger and more regular mechanisms for sharing information on risks and vulnerabilities. In addition, the FATF indicated its determination to remain at the center of international efforts to protect the integrity of the global financial system against new risks from criminals and terrorists.

At the G-20 (Group of 20) Summit in Pittsburgh in 2009, the national leaders affirmed their commitment to deal with tax havens, money laundering, corruption, terrorist financing, and prudential standards. They called on the FATF to improve transparency and exchange of information so countries can fully enforce their laws. The G-20 members also called on the FATF to issue a public list of high-risk jurisdictions. In 2010, the FATF published guidelines for insurance companies and the cross-border transportation of cash and bearer bonds. The FATF also adopted a set of guidelines regarding tax amnesty laws and asset repatriation. In 2010, the FATF also published a report on the

vulnerabilities of free trade zones for misuse in money laundering and terrorist financing. At the conclusion of the November 2010 G-20 Summit in Seoul, the members urged the FATF to "update and implement" the FATF standards calling for transparency of cross-border wire transfers, beneficial ownership, customer due diligence, and due diligence for "politically exposed persons."

At the Cannes 2011 Summit, the G-20 leaders declared that "corruption is a major impediment to economic growth and development," and encouraged all jurisdictions to adhere to the international standards in the tax, prudential, and AML/CFT areas. The leaders also stated that, "We stand ready, if needed, to use our existing countermeasures to deal with jurisdictions which fail to meet these standards" (par. 36).[5] The G-20 leaders also stated:

> We support the work of the Financial Action Task Force (FATF) to continue to identify and engage those jurisdictions with strategic Anti-Money Laundering/Counter-Financing of Terrorism (AML/CFT) deficiencies and update and implement the FATF standards calling for transparency of cross-border wires, beneficial ownership, customer due diligence, and enhanced due diligence.

At the November 4-5, 2012, meeting of G-20 finance ministers and central bank governors in Mexico City, the officials reaffirmed their support for FATF by concluding that "We remain committed and encourage the FATF to continue to pursue all its objectives and notably to continue to identify and monitor high-risk jurisdictions with strategic Anti-Money Laundering/Counter-Terrorist Financing (AML/CFT) deficiencies."[6] In addition, the final communique from the July 2013 meeting of G-20 finance ministers and central bank governors in Moscow concluded: "We reiterate our commitment to FATF's work in fighting money laundering and terrorism financing and its key contribution to tackling other crimes such as tax crimes, corruption, terrorism, and drug trafficking. In particular, we support the identification and monitoring of high risk jurisdictions with strategic AML/CFT deficiencies while recognizing the countries' positive progress in fulfilling the FATF's standards. We encourage all countries to tackle the risks raised by opacity of legal persons and legal arrangements...."[7]

On February 15, 2012, the FATF members adopted a revised and updated set of the FATF Forty Recommendations, which added the proliferation of financing of weapons of mass destruction to FATF's areas of surveillance. The new mandate is intended to: 1) deepen global surveillance of evolving criminal and terrorist threats; 2) build a stronger, practical and ongoing partnership with

the private sector; and 3) support global efforts to raise standards, especially in low capacity countries. In addition, the revised recommendations address new and emerging threats, while clarifying and strengthening many of the existing obligations. The new standards strengthen the requirements for higher risk situations and allow countries to take a more focused approach to areas where high risks remain or where implementation could be enhanced. The standards also significantly strengthen requirements in the area of transparency regarding the adequate, accurate and timely information on the beneficial ownership and control of legal persons and arrangements to address issues of tax transparency, corporate governance, and various types of criminal activity.

The risk-based approach adopted by FATF encourages countries to identify, assess, and understand the risks posed by money laundering and terrorist financing and to adopt the appropriate measures to address those risks, providing for a more flexible set of measures for countries to target resources in the most effective way. In addition, the new standards address the challenge of terrorist financing by integrating standards for combating terrorist financing throughout the Recommendations, thereby eliminating the need for the nine Special Recommendations. In particular, the new standards recommend: that terrorist financing should be criminalized (Recommendation 5); that countries should implement targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6); that countries should implement targeted financial sanctions related to the prevention, suppression, and disruption of proliferation of weapons of mass destruction and its financing (Recommendation 7); and that countries review their laws and regulations to ensure that non-profit organizations are not used to finance terrorism (Recommendation 8).

In addition to the revised and updated Recommendations, the FATF members adopted on April 20, 2012, a new mandate for the FATF and renewed FATF's mandate through December 31, 2020. The new mandate specifies a number of functions and tasks for the FATF, including:

1. Identifying and analyzing money laundering, terrorist financing, and other threats to the integrity of the financial system, including the methods and trends involved; examining the impact of measures designed to combat misuse of the international financial system; supporting national, regional, and global threat and risk assessments.
2. Developing and refining the international standards for combating money laundering and the financing of terrorism and weapons proliferation.

3. Assessing and monitoring its Members through "peer reviews" (mutual evaluations) and follow-up processes to determine the degree of technical compliance, implementation, and effectiveness of systems to combat money laundering and the financing of terrorism and proliferation; refining the standard assessment methodology and common procedures for conducting mutual evaluations and evaluation follow-up.
4. Identifying and engaging with high-risk, non-cooperative jurisdictions and those with strategic deficiencies in their national regimes, and coordinating action to protect the integrity of the financial system against the threat posed by them.
5. Promoting full and effective implementation of the FATF Recommendation by all countries through the global network of FATF-style regional bodies and international organizations; ensuring a clear understanding of the FATF standards and consistent application of mutual evaluation and follow-up processes throughout the FATF global network and strengthening the capacity of the FATF regional bodies to assess and monitor their member countries.
6. Responding as necessary to significant new threats to the integrity of the financial system consistent with the needs identified by the international community, including the United Nations Security Council, the G-20, and the FATF itself; preparing guidance as needed to facilitate implementation of relevant international obligations in a manner compatible with the FATF standards.
7. Assisting jurisdictions in implementing financial provisions of the United Nations Security Council resolutions on non-proliferation, assess the degree of implementation and the effectiveness of these measures in accordance with the FATF mutual evaluation and follow-up process, and preparing guidance as needed to facilitate implementation of relevant international obligations in a manner compatible with the FATF standards,
8. Engaging and consulting with the private sector and civil society on matters related to the overall work of the FATF, including regular consultation with the private sector and through the consultative forum.
9. Undertaking any new tasks agreed by its Members in the course of its activities and within the framework of this Mandate and taking on these new tasks only where it has a particular additional contribution to make while avoiding duplication of existing efforts elsewhere.

PROGRESS TO DATE

An essential part of the FATF activities is assessing the progress of its members in complying with the FATF recommendations. As previously indicated, the FATF attempts to accomplish this activity through assessments performed annually by the individual members and through mutual evaluations. As part of an on-going process, the FATF completes mutual evaluations of all the FATF members. According to the FATF assessment of February 2014, only a few countries are considered to be non-cooperative countries. The countries in this group include Iran and the Democratic Peoples' Republic of Korea (North Korea), which FATF considers to have significant deficiencies in its anti-money laundering and terrorist financing regime and urged other jurisdictions to protect themselves by applying counter-measures. The FATF identified nine countries— Algeria, Ecuador, Ethiopia, Indonesia, Myanmar, Pakistan, Syria, Turkey, and Yemen—that have not made sufficient progress in addressing their deficiencies or have not committed to an action program developed with the FATF to address the deficiencies. Other countries that are improving their AML/CFT regimes, but are considered have strategic AML/CFT deficiencies for which they have developed an action plan with the FATF are: Albania, Angola, Argentina, Cuba, Iraq, Kenya, Kuwait, Kyrgyzstan, Lao PDR, Mongolia, Namibia, Nepal, Nicaragua, Papua New Guinea, Tajikistan, Tanzania, Uganda, and Zimbabwe. Jurisdictions that were assessed as not making sufficient progress are: Afghanistan and Cambodia. Finally, jurisdictions that are no longer subject to monitoring are: Antigua and Barbuda, Bangladesh, and Vietnam.

In addition to monitoring the progress of countries in meeting the FATF recommendations regarding AML/CFT, the FATF has taken a number of steps since the 2008-2009 financial crisis to protect the international financial system from abuse. These actions include identifying jurisdictions that may pose a risk to the international financial system and updating reports on such topics as: Best Practices on Confiscation (asset recovery); best practices on Managing the Anti-Money Laundering and Counter-Terrorist Financing Policy Implications of Voluntary Tax Compliance Programs; and Trade Based Money Laundering. In addition, FATF issued a statement on February 22, 2013 indicating that it intended to suspend Turkey's membership in the organization as a result of its "continued failure to take action to fully criminalize terrorist financing and establish an adequate legal framework for identifying and freezing terrorist assets consistent with the FATF Recommendations."[8] The FATF encouraged Turkey to: 1) adopt legislation to

remedy deficiencies in its terrorist financing laws; and 2) establish a legal framework for identifying and freezing terrorist assets consistent with the FATF Recommendations. In February 2014, FATF indicated that Turkey had taken steps towards improving its CFT regime by complying with the FATF standard on criminalizing terrorist financing through court decisions and, therefore, did not suspend Turkey's membership. The FATF indicated, though, that it remained concerned over Turkey's framework for identifying and freezing terrorist assets.[9]

The FATF faces a number of difficulties in determining how fully member countries are complying with the special recommendations. A large part of this difficulty arises from the challenges in reaching a mutual understanding of what the recommendations mean and how a country should judge its performance relative to the recommendations, since the recommendations are periodically revised and new methodologies for analyzing money laundering and terrorist financing evolve over time. In addition, a number of the recommendations require changes to laws and other procedures that take time for member countries to implement. To assist member countries in complying with the recommendations, the FATF has issued various interpretative notes to clarify aspects of the recommendations and to further refine the obligations of member countries.

In February 2004, the FATF adopted a revised version of the 40 recommendations that significantly broadened the scope and detail of the recommendations over previous versions. Also, the FATF adopted a new methodology to track and identify money laundering and terrorist financing that applied to the 40 recommendations and the eight (nine) special recommendations. As a result of the significant length and additional detail of these new requirements, the FATF decided that it would no longer conduct self-assessment exercises based on the previous method, but will initiate follow-up reports to mutual evaluations.

In 2005, the FATF issued revised standards related to wire transfers of funds. The new standards require financial institutions to include the name, address, and account number of the originator on all fund transfers. The standards also lower the reporting threshold from $3,000 to $1,000. Two FATF-style regional bodies were also created—the Eurasian Group and the Middle East and North Africa Financial Action Task Force. The first round of mutual evaluations for these two bodies was scheduled for 2006. In 2007, the FATF adopted new measures to protect the international financial system from abuse, including calling on Iran to strengthen its money-laundering and counter-terrorist financing controls and a new commitment to produce a

regular global threat assessment detailing key issues of concern related to criminal and terrorist financing.

Since the start of the global financial crisis, the FATF has taken a number of steps to help governments guard against abuse of their financial systems by groups or individuals engaging in terrorist financing or money laundering. As part of these efforts, the FATF has:

- Issued a statement warning all FATF members and all jurisdictions to protect their financial systems from risks associated with Iran's failure to address ongoing deficiencies in its anti-money laundering regime and in combating financial terrorism
- Completed an analysis of the impact of the global financial and economic crises on international cooperation in the area of money laundering and terrorist financing and reported to the G-20 in September 2009 on responses to the financial crisis.
- Completed a report on the potential for money laundering and other vulnerabilities in the football (soccer) sector.[10]
- Issued a list of best practices that can assist member countries in implementing measures to freeze the assets or funds of terrorists or of terrorist-related activities. The FATF argues that freezing these assets or funds is important because it 1) denies funds to terrorists, which forces them to use more costly and higher risk ways to finance their operations; 2) deters those who might be willing to finance terrorism; and 3) is one element of a broader effort to follow the money trail of terrorists, terrorist groups and terrorist activity.
- Issued a report on money laundering and the risk posed under New Payment Methods (prepaid cards, mobile payments, and Internet payment services).[11]
- Completed research on the use of Trusts and Company Service Providers for money laundering, indicating that Trusts and Company Service Providers have often been misused, wittingly or not, in money laundering activities.[12]
- Published a report on the rise in organized piracy on the high seas and related kidnapping for ransom.[13]
- Published a report analyzing money laundering methods used for corruption, identifying key vulnerabilities of the current AML/CFT system, and discussed the barriers for the recovery of corrupt proceeds once they are discovered.[14]

- Published a report on the extent and nature of trade-based money laundering, which FATF identifies as one of the three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy.[15]
- Published a report on the illegal money flows associated with money laundering and trafficking in human beings and smuggling of migrants.[16]
- Published a report on money laundering and financial inclusion, which focuses on AML/CFT measures that meet national goals of facilitating access to formal services for financially excluded and underserved groups, including low income, rural sectors and undocumented groups.[17]
- Published a report on the vulnerabilities of legal professionals in witting/unwitting criminal ML/TF activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialized legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism.[18]
- Published a report on the vulnerability of politically exposed persons, which is defined as an individual who is or has been entrusted with a prominent public function that potentially can be abused for the purpose of committing money laundering offences and related activities, including corruption and bribery, as well as conducting activity related to terrorist financing.[19]
- Has approved a report on money laundering counterfeiting currency and the risk that counterfeit currency can seriously destabilize a country's currency and as such represents a serious threat to national economies. The report examines the methods that are used for putting the proceeds of the illicit trade in counterfeit currency into the regular financial system and how counterfeit currency is used for the purpose of terrorist financing and other crimes.[20]

As the FATF begins its fourth round of country evaluations, it adopted in 2013 a new methodology for countries to use in evaluating their compliance with the FATF Recommendations.[21] The Methodology is comprised of two components:

1. The first is a technical compliance assessment that will address the specific requirements of each of the FATF Recommendations, principally as they relate to the relevant legal and institutional framework of the country, and the powers and procedures of competent authorities.
2. The second is an effectiveness assessment that will assess the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyze the extent to which a country's legal and institutional framework is producing the expected results.

ROLE OF THE IMF AND WORLD BANK

Between 2002 and 2003, the International Monetary Fund (IMF) and the World Bank participated in a year-long pilot program to conduct assessments of national approaches to detecting and controlling money laundering and terrorist financing in various countries[22] using the methodology developed by the FATF.[23] In March 2004, the IMF and World Bank agreed to make the program a permanent part of their activities. The IMF has worked with the World Bank and the FATF to conduct over 70 AML/CFT assessment and has contribute to the design of AML/CFT-related program measures, and provided a large number of technical assistance and research projects, at an annual cost of approximately $6 million.[24] The FATF has incorporated an AML/CFT evaluation as part of its annual Article IV country consultations,[25] and country Financial Sector Assessment Programs (FSAP).[26] In 2009, the IMF spearheaded a donor-sponsored trust fund to finance technical assistance in AML/CFT to strengthen AML/CFT regimes. In a public statement, the IMF indicated that:

> ...it is concerned about the possible consequences money laundering, terrorist financing, and related governance issues have on the integrity and stability of the financial sector and the broader economy. These activities can undermine the integrity and stability of financial institutions and systems, discourage foreign investment, and distort international capital flows. They may have negative consequences for a country's financial stability and macroeconomic performance, resulting in welfare losses, draining resources from more productive economic activities, and even have destabilizing spillover effects on the economies of other

countries. In an increasingly interconnected world, the negative effects of these activities are global, and their impact on the financial integrity and stability of countries is widely recognized.[27]

The IMF's efforts are driven in part by its conclusion that money laundering, terrorist financing, and associated criminal activities are crimes that have real effects on the economy, on financial sector stability, and on external stability more generally. In general, the potential economic effects that arise from such financial crimes are:[28]

- Loss of access to global financial markets.
- Destabilizing capital inflows and outflows. Money laundering or terrorist financing activities may give rise to significant levels of criminal proceeds or "hot money" flowing into and out of financial institutions in a country in ways that are destabilizing. In such cases, financial flows are not driven by the economic fundamentals, but by differences in controls and regulations that make money laundering a safer activity in some countries than in others.
- Financial Sector Fraud. Money laundering may also be associated with broader problems of financial sector fraud. Such fraud can undermine confidence in a country's financial system which can lead to large outflows of capital from the banking system, or the loss of access to international financial markets as a result of deterioration in the country's reputation.
- Financial Sector Supervision. Money laundering and terrorist financing may reflect deeper problems with the supervision of the financial system in a country. Where important financial institutions within a country are owned or controlled by criminal elements, the authorities may encounter difficulty supervising these institutions or in identifying and addressing problems before domestic financial stability is undermined.
- Economic Paralysis. Incidents of terrorism and terrorist financing may undermine the stability of a country's financial system, either as a result of a history of terrorist incidents or through the effect of a single, but significant, incident.
- Tax Fraud. Money laundering associated with tax fraud potentially can undermine financial or macroeconomic activity by: 1) affecting the government's revenue stream to a point where its fiscal balance is

significantly undermined; and 2) threatening the stability of a country's banking system through volatile financial inflows and outflows by injecting large amounts of "hot money" arising from tax evasion. The IMF estimates that large scale tax fraud is the most prevalent and significant of all proceeds-generating crimes.

- Problems with economic policy-making. Where the illegal sector forms a significant part of the economy and criminal proceeds remain in cash outside the banking system, such activities can distort consumption, investment and savings, trade and exchange rates, and the demand for money. As a result, official data on economic fundamentals may not fully reflect the underlying economic realities and economic policymakers may be thwarted in assessing the state of the economy and in making economic policy.
- Adverse effects on growth. Corruption, especially corruption at the national level, has the potential to negatively affect fiscal balances, foreign direct investment, and growth. In extreme cases, unchecked criminal activity can threaten state functions and the rule of law, with associated adverse economic effects.
- Money laundering, terrorist financing and related crimes may undermine the stability of the country in which they originate and have adverse spillover effects on the stability of other countries.

In 2011, the IMF published the results of its assessment of the effectiveness of the AML/CFT program.[29] This survey concluded that:

- Of the 161 countries surveyed between 2004 and 2011 by the IMF, compliance with all of the FATF Recommendations was 42.5% and full compliance on any of the FATF Recommendations was rare, occurring in just 12.3% of the cases. The survey also indicated that it appears to be easier for countries to adopt legislation and to establish government institutions than it is to ensure that the system functions well on an on-going basis.
- Compliance is expensive because countries must invest in building institutions and promote active interagency coordination and international cooperation in order to achieve relatively high levels of compliance. As a result, countries with higher per capita income levels and more well-developed frameworks for financial regulation and fighting corruption have achieved relatively high levels of

compliance. Compliance by many emerging market and low-income countries, however, is impeded by a relatively poor understanding of AML/CFT best practices, inadequate budgets for training staff, and the absence of important preconditions (e.g., rule of law, transparency, and good governance) for the effective implementation of AML/CFT measures.

- The costs of performing a country evaluation are high in terms of time and resources for both the country being assessed and for the assessors. An IMF assessment of the criteria set out in the FATF assessment methodology, requires that the assessor bodies engage in long missions, extensive interviews with a broad range of representatives of the official and private sectors (both financial and nonfinancial), and protracted follow-up discussions. Some of these costs are shared with other assessor bodies.
- Country assessments attempt to focus not only on the country's formal compliance with the AML/CFT recommendations, but on how effectively the standards have been implemented.
- The comprehensive nature of the current methodology for assessing a country's compliance with the AML/CFT standards in some cases does not allow assessors the flexibility of focusing on issues that may be of greatest relevance to a particular country.

As a result of the conclusions reached above, the IMF and the World Bank proposed two changes in the AML/CFT policy framework:

1. Future assessments should adopt a more flexible, targeted approach, since most of the IMF's members have undergone an initial assessment. This approach will concentrate on: 1) areas where countries have a record of poor compliance; 2) key or core areas of the standard or where the standard has been amended; and/or 3) areas where individual countries face particular risks, either domestic or cross border.
2. Country assessments should be conducted with a more targeted, risk-based approach aimed at assessing a country's compliance with the AML/CFT standards. It is anticipated that such an approach would allow assessors to engage in more targeted and focused assessments based on the circumstances of the country whose framework is being

assessed. FATF moved in this direction when it adopted its new methodology in 2012.

ISSUES FOR CONGRESS

Following the 9/11 attacks, Congress passed P.L. 107-56 (the USA PATRIOT Act) to expand the ability of the Treasury Department to detect, track and prosecute those involved in money laundering and terrorist financing. In 2004, the 108th Congress adopted P.L. 108-458, which appropriated funds to combat financial crimes, made technical corrections to P.L. 107-56, and required the Treasury Department to report on the current state of U.S. efforts to curtail the international financing of terrorism. The experience of the Financial Action Task Force in tracking terrorist financing, however, indicates that there are significant national hurdles that remain to be overcome before there is a seamless flow of information shared among nations. While progress has been made, domestic legal issues and established business practices, especially those that govern the sharing of financial information across national borders, continue to hamper efforts to track certain types of financial flows across national borders. Continued progress likely will depend on the success of member countries in changing their domestic laws to allow for greater sharing of financial information, criminalizing certain types of activities, and improving efforts to identify and track terrorist-related financial accounts.

The economic implications of money laundering and terrorist financing pose another set of issues that argue for gaining greater control over this type of activity. According to the IMF, money laundering accounts for between $600 billion and $1.6 trillion in economic activity annually. Money launderers exploit differences among national anti-money laundering systems and move funds into jurisdictions with weak or ineffective laws. In such cases, organized crime can become more entrenched and create a full range of macroeconomic consequences, including unpredictable changes in money demand, risk to the soundness of financial institutions and the financial system, contamination effects on legal financial transactions and increased volatility of capital flows and exchange rates due to unprecedented cross-border transfers.[30]

End Notes

[1] The FATF members are Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, People's Republic of China, Portugal, Russian Federation, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States; the two international organizations are the European Commission, and the Gulf Cooperation Council. The following organizations have observer status: Asia/Pacific Group on Money Laundering; Caribbean Financial Action Task Force; Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures; Eastern and Southern Africa Anti-Money Laundering Group; Financial Action Task Force on Money Laundering in South America; other international organizations including the African Development Bank; Asia Development Bank; European Central Bank; International Monetary Fund; Organization of American States, Organization for Economic Cooperation and Development; United Nations Office on Drugs and Crime; and the World Bank.

[2] To be admitted to the FATF, a country must (1) be fully committed at the political level to implement the 40 recommendations within a reasonable time frame (three years) and to undergo annual self-assessment exercises and two rounds of mutual evaluations; (2) be a full and active member of the relevant FATF-style regional body; (3) be a strategically important country; (4) have already made the laundering of the proceeds of drug trafficking and other serious crimes a criminal offense; and (5) have already made it mandatory for financial institutions to identify their customers and to report unusual or suspicious transactions.

[3] For the 40 recommendations, see http://www.oecd.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html.

[4] FATF Cracks Down on Terrorist Financing. Washington, FATF, October 31, 2001, p. 1.

[5] Cannes Summit Final Declaration, G-20, November 4, 2011.

[6] Communique of Ministers of Finance and Central Bank Governors of the G-20, Mexico City, 4-5 November 2012, par. 20.

[7] Communique: G-20 Meeting of Finance Ministers and Central Bank Governors, Moscow, July 20, 2013, para. 20.

[8] Outcomes of the Plenary Meeting of the FATF, Paris, 17-19 October 2012, FATF, October 19, 2012.

[9] FATF Public Statement, February 14, 2014.

[10] Money Laundering Through the Football Sector, July 2009.

[11] Money Laundering Using New Payment Methods, Financial Action Task Force, October 2010.

[12] Money Laundering Using Trust and Company Service Providers, Financial Action Task Force, October 2010.

[13] Organized Maritime Piracy and Related Kidnapping for Ransom, Financial Action Task Force, July 2011.

[14] Laundering the Proceeds of Corruption, Financial Action Task Force, July 2011.

[15] APG Typology Report on Trade Based Money Laundering, Financial Action Task Force, July 20, 2012.

[16] Money Laundering Risks Arising From Trafficking in Human Beings and Smuggling of Migrants, Financial Action Task Force, July 2011.

[17] Anti-Money Laundering and Terrorist Financing Measures for Financial Inclusion, Financial Action Task Force, February 2013.

[18] Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, Financial Action Task Force, June 2013.

[19] Politically Exposed Persons, Financial Action Task Force, June 2013.

[20] Money Laundering and Terrorist Financing Related to Counterfeiting of Currency, Financial Action Task Force, forthcoming.

[21] Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, Financial Action Task Force, February 2013.

[22] This group of countries is not the same as those surveyed by the FATF, although there is some overlap in coverage between the FATF and the IMF/World Bank assessments.

[23] Twelve-Month Pilot Program of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Assessments: Joint Report on the Review of the Pilot Program. The International Monetary Fund and the World Bank, March 10, 2004.

[24] Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) Report on the Effectiveness of the Program, International Monetary Fund, May 11, 2011, p. 37.

[25] An Article IV consultation, required by Article IV of the IMF's Articles of Agreement, is part of the IMF's surveillance program of member countries' economic and financial policies and includes discussions with government and central bank officials and representatives of business, labor, and civil society.

[26] The Financial Sector Assessment Program (FSAP) is a comprehensive and in-depth analysis of a country's financial sector. The assessment is comprised of two components: a financial stability assessment, and a financial development assessment.

[27] The IMF and the Fight Against Money Laundering and the Financing of Terrorism, International Monetary Fund.

[28] Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) Report on the Effectiveness of the Program, Annex 4.

[29] Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) Report on the Effectiveness of the Program.

[30] The IMF and the Fight Against Money Laundering and the Financing of Terrorism. IMF Factsheet, April 2003. http://www.imf.org/external/np/exr/facts/aml.htm.

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 3

MEMORANDUM TO MEMBERS OF THE COMMITTEE ON FINANCIAL SERVICES FOR THE HEARING ON "TRADING WITH THE ENEMY: TRADE-BASED MONEY LAUNDERING IS THE GROWTH INDUSTRY IN TERROR FINANCE"*

UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES

M E M O R A N D U M

To:	Members of the Committee on Financial Services
From:	FSC Majority and Minority Staff
Date:	January 21, 2016
Subject:	January 26, 2016, Task Force to Investigate Terrorism Financing hearing titled "Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance"

* This is an edited, reformatted and augmented version of a memorandum dated January 21, 2016 from the Staff of the House Committee on Financial Services.

The Task Force to Investigate Terrorism Financing will hold a hearing entitled "Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance" on Tuesday, January 26, 2016, at 10:00 a.m. in room 2128 of the Rayburn House Office Building. This will be a one-panel hearing with the following witnesses:

- Mr. John Cassara, former U.S. Intelligence Officer and Treasury Special Agent
- Mr. Louis Bock, former Senior Special Agent, U.S. Customs and Border Protection
- Mr. Farley Mesko, Co-Founder and Chief Executive Officer, Sayari Analytics
- Mr. Nikos Passas, Professor of Criminology and Criminal Justice, College of Social Sciences and Humanities, Northeastern University

INTRODUCTION[1]

Trade-based money laundering (TBML) involves the exploitation of the international trade system for the purpose of transferring value and obscuring the true origins of illicit wealth. The Financial Action Task Force (FATF), an intergovernmental standard-setting body on anti-money laundering and combating the financing of terrorism (AML/CFT), has described TBML as the process of disguising proceeds of crime and moving value through trade transactions in order to legitimize their illicit origin—a process that varies in complexity, but typically involves the misrepresentation of the price, quantity, or quality of imports or exports.[2] When used by terrorist groups to finance their activities, move money, or otherwise disguise the source and beneficiaries of their funds, TBML schemes are sometimes referred to as TBML/ Financing of Terrorism (FT). Financial institutions are wittingly or unwittingly implicated in TBML and TBML/FT schemes when they are used to settle, facilitate, or finance international trade transactions (e.g., through the processing of wire transfers, provision of trade finance, and issuance of letters of credit and guarantees).

In June 2015, the U.S. Department of the Treasury issued two reports related to money laundering: a National Money Laundering Risk Assessment and a National Terrorist Financing Risk Assessment. The National Money Laundering Risk Assessment identified TBML as among the most challenging

and pernicious forms of money laundering to investigate.[3] Citing information from U.S. Immigration and Customs Enforcement (ICE), Treasury described TBML schemes as capable of laundering billions of dollars annually. An earlier advisory on TBML, issued by the Treasury Department's Financial Crimes Enforcement Network (FinCEN) in February 2010, stated that more than 17,000 Suspicious Activity Reports (SARs) described potential TBML activity between January 2004 and May 2009, which involved transactions totaling in the aggregate more than $276 billion.[4]

SCOPE OF THE PROBLEM

Although TBML is widely recognized as one of the most common manifestations of international money laundering as well as a known value transfer and reconciliation method used by terrorist organizations, TBML appears to be less understood among academics and policymakers, in contrast with traditional forms of money laundering through the international banking system and through bulk cash smuggling. Considering the volume of global trade and the value of such transactions, however, TBML's effects can result in substantial consequences for international commerce and government revenue. The *National Money Laundering Risk Assessment* concludes that:

> TBML can have a more destructive impact on legitimate commerce than other money laundering schemes. According to ICE HSI [Homeland Security Investigations], transnational criminal organizations may dump imported goods purchased with illicit proceeds at a discount into a market just to expedite the money laundering process. The below-market pricing is a cost of doing business for the money launderer, but it puts legitimate businesses at a competitive disadvantage. This activity can create a barrier to entrepreneurship, crowding out legitimate economic activity. TBML also robs governments of tax revenue due to the sale of underpriced goods, and reduced duties collected on undervalued imports and fraudulent cargo manifests.

GLOBAL HOTSPOTS

The U.S. government has historically focused on TBML schemes involving drug proceeds from Latin America, particularly the Black Market

Peso Exchange (BMPE). BMPE emerged as a major money laundering method when Colombian drug traffickers used sophisticated trade-based schemes to disguise as much as $4 billion in annual narcotics profits in the 1980s.[5] According to FinCEN, TBML activity is growing in both volume and global reach. In an analysis of SARs between January 2004 and May 2009, TBML activity was most frequently identified in transactions involving Mexico and China. Panama was ranked third, potentially due to TBML activity linked to the Panama Colon Free Trade Zone (FTZ), while the Dominican Republic and Venezuela were identified as "countries with the most rapid growth in potential TBML activity."[6]

According to the U.S. Department of State's March 2015 edition of its annual report on money laundering and financial crimes, Volume II of the *International Narcotics Control Strategy Report*, TBML concerns have surfaced in countries or jurisdictions such as Afghanistan, Belize, Brazil, Canada, China, Colombia, Greece, Hong Kong, India, Iran, Iraq (and "the surrounding region"), Kenya, Lebanon, Mexico, Pakistan, Panama, Paraguay, Singapore, St. Maarten, Taiwan, the United Arab Emirates (UAE), Uruguay, Venezuela,[7] and the West Bank and Gaza.[8]

LINKS TO TERRORISM

Although a number of anecdotal case studies in recent years have revealed instances in which TBML is used by known terrorist groups and other non-state armed groups, including Hezbollah, the Treasury Department's June 2015 *National Terrorist Financing Risk Assessment* concluded that TBML is not a dominant method for terrorist financing.[9] It stated:

> Broadly speaking, based on an analysis of U.S. law enforcement investigations and prosecutions relating to TF [terrorist financing], two methods of moving money to terrorists and terrorist organizations have been predominate in the convictions and cases pending since 2001: the physical movement of cash and the movement of funds through the banking system.... The physical movement of cash accounted for 28 percent of these cases while movement directly through banks constituted 22 percent, movement through licensed MSBs [money services businesses] 17 percent, and movement by individuals or entities acting as unlicensed money transmitters constituted 18 percent.

The footnote following the last sentence quoted above continued: "The remaining 15 percent were a mix of checks, wire transfers through unspecified financial institutions, and TBML."

In its latest *Country Reports on Terrorism*, issued in June 2015, the State Department identified TBML as a terrorism-related concern in Tunisia and Syria, particularly as a technique used by *hawala* brokers in conjunction with corrupt customs and immigration officials (*hawala* is an informal value transfer system, often used to send remittances, that can operate outside the formal international financial system to move funds internationally and anonymously).[10] The State Department's March 2015 report on money laundering and financial crimes also identified some specific countries that may be vulnerable to TBML/ Financing of Terrorism (FT) schemes. For example, the report notes that TBML in the United Arab Emirates (UAE), particularly linked to *hawala* transactions and counter-valuation through trading companies, "might support sanctions-evasion networks and terrorist groups in Afghanistan, Pakistan, and Somalia."[11]

VULNERABILITIES

The potential is vast for criminal organizations and terrorist groups to exploit the international trade system with relatively low risk of detection. According to FATF, key characteristics of the international trade system have made it both attractive and vulnerable to illicit exploitation. Quoting FATF, vulnerabilities include the following:

> The enormous volume of trade flows, which obscures individual transactions and provides abundant opportunity for criminal organizations to transfer value across borders;
>
> The complexity associated with (often multiple) foreign exchange transactions and recourse to diverse financing arrangements;
>
> The additional complexity that can arise from the practice of comingling illicit funds with the cash flows of legitimate business;
>
> The limited recourse to verification procedures or programs to exchange customs data between countries; and
>
> The limited resources that most customs agencies have available to detect illegal trade transactions.[12]

SELECTED CASE STUDIES

Hezbollah-Linked TBML

In an elaborate TBML scheme purported to be linked to Hezbollah, a Lebanon-based group that was designated in 1997 by the State Department as a Foreign Terrorist Organization (FTO), U.S. officials claimed that the Lebanese Canadian Bank (LCB) and multiple foreign exchange houses had facilitated the laundering of South American drug proceeds through the Lebanese financial system and through TBML schemes involving used cars and consumer goods.

In one such scheme, LCB facilitated wire transfers to U.S. banks for the purchase of used cars in the United States. Cars would be purchased in the United States and shipped to countries in West Africa and elsewhere while the proceeds from the car sales would reportedly be repatriated back to Lebanon through the use of bulk cash deposits among conspiring exchange houses. In another scheme associated with the same Hezbollah-linked drug trafficking network, Asian-supplied consumer goods would be shipped to Latin America while the proceeds would be laundered through a BMPE-styled scheme. The funds sent to pay for the consumer goods were reportedly sent through LCB's U.S. correspondent accounts.

In its February 2011 designation of LCB as a financial institution of primary money laundering concern, FinCEN stated that, according to U.S. government information, Hezbollah "derived financial support" from these drug and money laundering schemes. Ultimately, Lebanon's central bank and monetary authority, the Banque du Liban, revoked LCB's banking license in September 2011 and LCB's former shareholders sold its assets and liabilities to the Lebanese Societé Generale de Banque au Liban SAL (SGBL). Some of the individuals and entities associated with this illicit network have also variously been subject to financial sanctions and law enforcement investigations in the United States.[13]

Toys-for-Drugs BMPE Scheme

In a BMPE scheme involving a Los Angeles-based toy wholesaler, Woody Toys, Inc., its owners received millions of dollars in cash payments generated from Colombian and Mexican narcotics trafficking. The cash payments reportedly were placed directly into the company's bank account

from multiple locations in small deposits that were consistently under $10,000 to avoid reporting requirement (i.e., structuring). The toy company used the cash deposits to purchase toys from China, which, in turn, were exported to Colombia. The Colombia pesos generated by the toy sales in Colombia were used to reimburse the Colombian drug traffickers through the BMPE. Some of the employees of Woody Toys had previously worked for Angel Toy Company, whose owners had also been implicated in a similar toys-for-drugs BMPE scheme. The law enforcement investigation into this case benefitted from an information sharing arrangement between the United States and Colombia on trade data through the Trade Transparency Units (TTUs) established in both countries. [14]

Trade Finance and *Hawala* Networks

According to the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body (FSRB), another scheme to launder funds derived from multiple major international drug traffickers involved cash couriers, money transfer services, alternate value transfer systems (e.g., *hawala*), and formal mechanisms of trade finance, managed and directed by an Indian national living in Dubai. The individual involved operated numerous businesses in Dubai as well as numerous affiliates in Europe, Asia, Africa, and the United States.

In Dubai, the individual opened letters of credit (LCs) through his various companies for various importers, also located in Dubai. These LCs were opened to benefit various affiliated exporters located in India and in other locations and were in amounts that were substantially higher than the market value of the exports. In opening the LCs, the individual used his businesses connections with certain issuing banks and certain advising banks to transmit the LCs to the affiliated exporters in India. The individual also arranged for trade documents to be prepared that reflected the inflated value of the exports in order to make them acceptable to the issuing and advising banks. Next, the LCs, with inflated export values, along with funds received from drug trafficking, were remitted to the exporters in India, essentially moving money through the financial system in the guise of trade financing. Once in India, the exporters distributed the drug proceeds to the various affiliates and sold the exports at market value.

The same Indian national also used various techniques to move funds offshore through *hawala* operators. In one scheme, the individual facilitated trade in banned goods (in this example, a "pulses," or agricultural crops) by

falsifying trade documents through his network of businesses in India to export banned goods from India. In order to circumvent the restrictions, the goods were falsely described and falsely valued in trade documents. *Hawala* operators were used to settle the difference between the true value of the exported goods and the falsely documented value of the goods.[15]

SELECTED POLICY RESPONSES

Role of the Financial Action Task Force (FATF)

FATF was organized to develop and promote AML/CFT guidelines.[16] It currently comprises 34 member countries and territories and two regional organizations.[17] Although FATF has no enforcement capabilities, FATF relies on a combination of annual self-assessments and periodic mutual evaluations on the compliance of its members to FATF guidelines. It can suspend member countries that fail to comply on a timely basis with its guidelines. When it was established in 1989, FATF was charged with examining money laundering techniques and trends, reviewing actions already taken, and setting out the measures to be taken to combat money laundering. In 1990, FATF issued a new report containing 40 recommendations,[18] which provided a comprehensive plan of action to fight against money laundering.

In February 2012, FATF members adopted a revised set of the FATF 40 Recommendations (subsequently updated again October 2015), which integrated CFT guidelines into the core set of recommendations and added the proliferation of financing of weapons of mass destruction to FATF's areas of surveillance. The new mandate is intended to:

- deepen global surveillance of evolving criminal and terrorist threats;
- build a stronger, practical and ongoing partnership with the private sector; and
- support global efforts to raise standards, especially in low capacity countries.

In addition, the revised recommendations address new and emerging threats, while clarifying and strengthening many of the existing obligations. The new standards strengthen the requirements for higher risk situations and allow countries to take a more focused approach to areas where high risks

remain or where implementation could be enhanced. The standards also address transparency requirements related to the adequate, accurate, and timely information on the beneficial ownership and control of legal persons and arrangements to address tax transparency, corporate governance, and various types of criminal activity.

Recommendations specifically to counter TBML, however, are not included in the current set of FATF's 40 Recommendations, despite recognition that the rapid growth and complexity of the international trade and financing system has multiplied the opportunities for abuse of this system by money launderers and terrorist financiers. FATF, however, has occasionally issued stand-alone reports that address TBML and best practices.[19] Surveys conducted by FATF, for example, indicate that there is no comprehensive data set on the extent and magnitude of TBML. In part, FATF determined that this lack of data reflected the fact that most jurisdictions do not identify TBML as a separately identifiable activity under the general topic of money laundering and, therefore, did not collect or share data on this specific type of activity. FATF also concluded that most jurisdictions do not offer training to trade and finance specialists specifically related to TBML activities.[20]

U.S. DEPARTMENT OF THE TREASURY

Central to the Treasury Department's efforts to combat TBML is FinCEN, which issues advisories and geographic targeting orders, and applies special measures to jurisdictions determined to be of primary money laundering concern.

Advisories

The purpose of a FinCEN advisory, in general, is to red flag for financial institutions activities that may be indicative of certain types of money laundering, in line with recent investigations, to assist financial institutions in filing suspicious activity reports (SARs). FinCEN first highlighted TBML in November 1997 and then again in June 1999 with advisories on the Black Market Peso Exchange (BMPE).[24]

What is FinCEN?

FinCEN's mission is to safeguard the financial system through the collection, analysis and dissemination of financial intelligence to law enforcement. FinCEN's Director is appointed by the Secretary of the Treasury and reports to the Under Secretary of the Treasury for Terrorism and Financial Intelligence. FinCEN also acts as the U.S. financial intelligence unit (FIU), one of the over 100 FIUs that comprise the Egmont Group, an international body focused on information sharing and cooperation among FIUs.[21] FinCEN receives data, such as suspicious transaction reports (SARs) from banks and other financial firms, analyzes the data, and disseminates it to law enforcement. It also cooperates with foreign FIUs in exchanging information, largely through its membership and participation in the Egmont Group.

FinCEN exercises regulatory functions primarily under the Currency and Financial Transactions Reporting Act of 1970,[22] as amended by Title III of the USA PATRIOT Act of 2001[23] and other legislation, together commonly referred to as the Bank Secrecy Act (BSA). The BSA is the United States' first and most comprehensive Federal AML/CFT statute. It authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to establish AML programs and to file reports on financial activity that may have relevance for criminal, tax, and regulatory investigations or for intelligence or counter-terrorism.

In February 2010, FinCEN issued an advisory on TBML, based on law enforcement experience involving U.S. trade with Central and South America.[25] The purpose of the advisory was to aid financial institutions in reporting suspicious activity related to TBML. The advisory noted the basic schemes behind TBML and offered more specific red flags. The 2010 advisory further noted that reporting on suspected TBML had been inconsistent and requested that financial institutions include the abbreviation TBML or BMPE on SARs.[26] FinCEN also described substantial delays in the reporting of suspected TBML activity.[27]

FinCEN issued an additional TBML advisory in May 2014 related to Mexican TBML activity involving funnel accounts.[28] A funnel account is an individual or business account in one geographic area receiving multiple cash deposits, often below the jurisdiction's cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.[29] The advisory also provides

several specific red flags associated with such activity conducted by Mexican criminal and drug trafficking organizations.

Geographic Targeting Orders

FinCEN appears to have also begun to rely more heavily on Geographic Targeting Orders (GTOs) in recent years, a tool that was first authorized in 1988. A GTO imposes additional, but time-limited, recordkeeping and reporting requirements on domestic financial institutions or nonfinancial businesses in a particular geographic area in order to assist regulators and law enforcement agencies in identifying criminal activity. In the absence of extensions, GTOs may only remain in effect for a maximum of 180 days. Violators may face substantial civil or criminal liability. Several recent GTOs have been used to enhance U.S. efforts to combat TBML.

In April 2015, FinCEN issued a GTO that lowered cash reporting thresholds and triggered additional recordkeeping requirements for certain financial transactions for about 700 Miami-based electronics exporters.[30] The GTO required targeted businesses to file forms with FinCEN reporting any single transaction or related transactions in which they receive more than $3,000 in cash—a stricter standard than the ordinary $10,000 filing threshold for cash transactions imposed pursuant to BSA. FinCEN stated that the new reporting requirements are aimed at combating complex TBML-related schemes employed by the Sinaloa and Los Zetas drug and transnational crime organizations. In October 2015, FinCEN renewed the GTO for an additional 180 days.[31]

In October 2015, FinCEN issued a similar GTO that also lowered cash reporting to $3,000 and triggered additional recordkeeping requirements. This GTO targeted businesses in the Los Angeles Fashion District in an effort to frustrate suspected Mexican and Colombian drug traffickers who had been exploiting fashion industry businesses to engage in BMPE schemes.[32]

Special Measures

Pursuant to BSA, as amended by the USA PATRIOT Act, FinCEN may require financial institutions and agencies within U.S. jurisdiction to take certain regulatory special measures against a foreign jurisdiction, foreign financial institution, class of transaction, or type of account determined to be

of "primary money laundering concern."[33] The enumerated five special measures, which may be imposed individually, in any combination, and in any sequence, range from requiring enhanced due diligence to prohibiting the opening or maintaining of correspondent or payable-through accounts. In some cases, such action corresponds with other administrative actions taken by the Treasury Department, including by the Office of Foreign Asset Control (OFAC), which is responsible for administering financial sanctions that target specially designated foreign nationals and entities. Among the 10 active cases, several were designated for their involvement in TBML, including the following:

Halawi Exchange and Rmeiti Exchange. In April 2013, FinCEN separately designated two Lebanese exchange houses, Halawi Exchange and Rmeiti Exchange, as financial institutions of primary money laundering concern. According to U.S. government information, both exchange houses facilitated transactions associated with a large-scale TBML scheme, involving the purchase of used cars in the United States for export to West Africa. Moreover, U.S. authorities claim that both exchange houses had been providing money laundering services for an international narcotics trafficking and money laundering network linked to Hezbollah.[34]

Banca Privada d'Andorra (BPA). In March 2015, FinCEN designated BPA as a financial institution of primary money laundering concern. FinCEN found high-level managers to have facilitated transactions on behalf of Third-Party Money Launderers (TPMLs) linked to individuals and organizations associated with organized crime, corruption, human trafficking, TBML, and fraud. One of these TPMLs laundered the proceeds of Venezuelan public corruption through TBML schemes, among others.[35]

U.S. DEPARTMENT OF HOMELAND SECURITY

Within the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI) established the first Trade Transparency Unit (TTU) in Washington, D.C., in 2004. Using a specialized computer system called the "Data Analysis and Research for Trade Transparency System" (DARTTS), TTUs examine trade anomalies and financial irregularities in domestic and foreign trade data to identify instances of TBML, customs fraud, contraband smuggling, and tax evasion that warrant further law enforcement investigation. With funding support from the Department of State's Bureau for International Narcotics and

Law Enforcement Affairs (INL), HSI has stood up TTUs in Argentina, Brazil, Colombia, Ecuador, Guatemala, Mexico, Panama, and Paraguay. According to the State Department, these eight international TTUs form the basis of broader plans to develop an international network of TTUs, similar to the Egmont Group of FIUs.[36] The 2007 *National Money Laundering Strategy* established attacking TBML at home and abroad as a national goal and specifically called on the deployment of ICE-led TTUs to facilitate the exchange and analysis of trade data among trading partners. According to one estimate, more than $1 billion has been seized since the creation of the U.S. - and foreign-based TTU effort.[37]

WITNESS BIOGRAPHIES

John Cassara, former U.S. Intelligence Officer and Treasury Special Agent

John Cassara retired after a 26 year career in the federal government intelligence and law enforcement communities. He is considered an expert in anti-money laundering and terrorist financing, with particular expertise in the areas of money laundering in the Middle East and the growing threat of alternative remittance systems and forms of trade-based money laundering and value transfer. He invented the concept of international "Trade Transparency Units," an innovative countermeasure to entrenched forms of trade-based money laundering and terrorist financing. A large part of his career was spent overseas. He is one of the very few to have been both a clandestine operations officer in the U.S. intelligence community and a Special Agent for the Department of Treasury.

His last position was as a Special Agent detailee to the Department of Treasury's Office of Terrorism Finance and Financial Intelligence (TFI). His parent Treasury agency was the Financial Crimes Enforcement Network (FinCEN), the U.S. Financial Intelligence Unit (FIU). He worked at FinCEN from 1996-2002. From 2002-2004, Mr. Cassara was detailed to the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) Anti-Money Laundering Section to help coordinate U.S. interagency international anti-terrorist finance training and technical assistance efforts.

Mr. Cassara has authored or co-authored several articles and books, including *Hide and Seek, Intelligence, Law Enforcement and the Stalled War*

on Terrorist Finance (2006 Potomac Books) and *On the Trail of Terror Finance - What Intelligence and Law Enforcement Officers Need to Know* (2010 Red Cell IG). In 2013, his first novel *was released - Demons of Gadara. Trade-Based Money Laundering: The Next Frontier in International Money Laundering* (Wiley) *is* due to be released in the fall of 2015.

Louis Bock, former Senior Special Agent, U.S. Customs and Border Protection

Mr. Bock is a successful U.S. government criminal investigator who has targeted various types of trade fraud and money laundering around the world. He is an expert in data preparation and visualization representing the flow and nexus of goods and money around the world and is highly respected both as visionary and expert in targeting trade-based money laundering through the use of big trade and financial data. From 2004-2013, Mr. Bock served as Chief Investigative Officer at Data Mining International. From 2002 - 2004, Mr. Bock was a Supervisory Special Agent at U.S. Immigration and Customs Enforcement (ICE) at the U.S. Department of Homeland Security. Previously, from 1991-2002, Mr. Bock was Supervisory Special Agent at U.S. Customs and Border Protection, and he also holds previous experience as a Senior Special Agent for U.S. Customs' field offices from 1986- 1991 and at U.S. Department of Agriculture's New York City offices from 1984-1986. Finally, Mr. Bock worked for the DEA as a Diversion Investigator from 1980-1984. Mr. Bock holds a BA in Behavioral and Statistical Measurement from Brooklyn College and a MA in Education and Behavioral Statistical Measurement from Kean College.

Farley Mesko, Co-founder and CEO, Sayari Analytics

Farley Mesko started Sayari Analytics after spending five years building C4ADS, a nonprofit organization focused on data-driven and technology-enabled analysis of conflict and security issues. His research on mapping and exposing illicit networks won C4ADS accolades from the highest levels of the security community and private technology sector, including being selected for a philanthropic partnership with Palantir Technologies and receiving a New Digital Age grant from Eric Schmidt, Executive Chairman of Google, as one of the top 10 most innovative organizations in the world using data and technology to solve pressing human challenges. He has worked as a consultant

for the World Bank and has briefed flag officers, ambassadors, and executive-level leadership at US combatant commands, joint task forces, the national security staff of the Office of the Vice President, and various embassies. He has presented his research at New America Foundation, Yale University, Google Ideas, and American University, and has authored reports for the United Nations and Brookings. Farley received his degree in Natural Resource Policy and Economics from Bowdoin College and has worked extensively in conflict zones across Africa, including Northern Mali and Southern Somalia, and speaks Arabic.

Nikos Passas, Professor of Criminology and Criminal Justice, Northeastern University

Nikos Passas is Professor of Criminology and Criminal Justice at Northeastern University, and co-Director of the Institute for Security and Public Policy. He is also Consortium Member and Distinguished Inaugural Professor of Collective Action, Business Ethics and Compliance at the International Anti-Corruption Academy, Vienna; Distinguished Visiting Professor at Beijing Normal University; Adjunct Professor and Distinguished Practitioner in Financial Integrity; Senior Fellow of the Financial Integrity Institute at Case Western Reserve Law School; and Distinguished Visiting Fellow at the TC Beirne School of Law, University of Queensland. He is also the Head of Sanctions Implementation Legal Review Services at Compliance Capacity International.

He has served as Corruption Program Director at the Ethics and Compliance Officer Association (ECOA) and Adjunct Law Professor at Case Western Reserve University. His law degree is from the Univ. of Athens (LL.B.), his Master's from the University of Paris-Paris II (D.E.A.) and his Ph.D. from the University of Edinburgh Faculty of Law. He is a member of the Athens Bar (Greece). He is fluent in 6 languages and plays classical guitar.

He specializes in the study of corruption, illicit financial/trade flows, sanctions, informal fund transfers, remittances, terrorism, white-collar crime, financial regulation, organized crime and international crimes. He has published more than 200 articles, book chapters, reports and books in 13 languages. His next books are entitled *Trade-Based Financial Crime and Illicit Flows* and *Corruption and Crisis in Greece*.

End Notes

[1] This memorandum was prepared by the Congressional Research Service at the Task Force's request, and has been reviewed and approved by the Financial Services Committee staff.

[2] Financial Action Task Force (FATF), Trade Based Money Laundering, June 23, 2006. The basic techniques of trade-based money laundering (TBML) include over- and under-invoicing of goods and services, multiple-invoicing of goods and services; over- and under-shipment (i.e., short shipping) of goods and services; and falsely described goods and services, including phantom shipping.

[3] U.S. Department of the Treasury, National Money Laundering Risk Assessment, June 12, 2015.

[4] Financial Crimes Enforcement Network (FinCEN), Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering, advisory, FIN-2010-A001, February 18, 2010.

[5] Broadly, the Black Market Peso Exchange (BMPE) facilitated the "swap" of dollars owned by drug cartels in the United States for pesos already in Colombia by selling the dollars to Colombian businessmen who sought to buy U.S. goods for export. See FinCEN, Colombian Black Market Peso Exchange, advisory, issue 9, November, 1997; U.S. government, National Money Laundering Strategy, May 3, 2007; and FATF, Trade Based Money Laundering, June 23, 2006.

[6] FinCEN, Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering, advisory, FIN-2010-A001, February 18, 2010.

[7] The 2015 report notes that "Venezuelan government officials—including the president, the executive vice president, an central bank president, a finance minister, and an interior minister—have all admitted publicly over the past 12-18 months that 30-40 percent of the roughly $53 billion the Venezuelan government spent on imports in 2013 were paid out for over-invoiced or completely fictitious transactions...." U.S. Department of State, International Narcotics Control Strategy Report (INCSR), Vol. 2, Money Laundering and Financial Crimes, March 2015.

[8] U.S. Department of State, INCSR, Vol. 2, March 2015.

[9] U.S. Department of the Treasury, National Terrorist Financing Risk Assessment, June 12, 2015.

[10] U.S. Department of State, Country Reports on Terrorism 2014, June 2015.

[11] U.S. Department of State, INCSR, Vol. 2, March 2015.

[12] FATF, Trade Based Money Laundering, June 23, 2006.

[13] Asia/Pacific Group on Money Laundering (APG), APG Typology Report on Trade Based Money Laundering, July 20, 2012; Jo Becker, "Beirut Bank Seen As Hub of Hezbollah's Finances," New York Times, December 13, 2011; Sebastian Rotella, "Government Says Hezbollah Profits from U.S. Cocaine Market Via Link to Mexican Cartel," ProPublica, December 13, 2011; "Prosecutors Say Hezbollah Laundered Millions of Dollars into U.S.," Associated Press, December 15, 2011, http://www.foxnews.com/us/2011/12/15/prosecutors-say-hezbollah-launderedmillions-dollars-into-us.html; Devlin Barrett, "U.S. Intensifies Bid to Defund Hezbollah," Wall Street Journal, December 16, 2015

[14] APG, APG Typology Report on Trade Based Money Laundering, July 20, 2012; U.S. Immigration and Customs Enforcement (ICE), "Co-Owner of Los Angeles-Area Toy Company Sentenced in Drug Money Laundering Case," press release, May 6, 2013; https://www.ice.gov/news/releases/co-owner-los-angeles-area-toy-companysentenced-drug-money-laundering-case.

[15] APG, APG Typology Report on Trade Based Money Laundering, July 20, 2012.

[16] For additional information, see CRS Report RS21904, The Financial Action Task Force: An Overview, by James K. Jackson.

[17] FATF members are Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, People's Republic of China, Portugal, Russian Federation, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States; the two international organizations are the European Commission, and the Gulf Cooperation Council. The following organizations have observer status: Asia/Pacific Group on Money Laundering; Caribbean Financial Action Task Force; Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures; Eastern and Southern Africa Anti-Money Laundering Group; Financial Action Task Force on Money Laundering in South America; other international organizations including the African Development Bank; Asia Development Bank; European Central Bank; International Monetary Fund; Organization of American States, Organization for Economic Cooperation and Development; United Nations Office on Drugs and Crime; and the World Bank.

[18] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations, adopted on February 16, 2012 and updated in 2013 and 2015.

[19] FATF, Best Practices Paper on Trade-Based Money Laundering, June 20, 2008.

[20] Ibid.

[21] An FIU is a national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime and potential financing of terrorism or as otherwise required by national legislation or regulation, in order to combat money laundering and terrorism financing. See https://www.fincen.gov/about fincen/wwd/.

[22] 31 U.S.C. 5311 et seq.

[23] P.L. 107-56.

[24] The two early FinCEN advisories on TBML were also followed in 2005 by additional sections in the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual, issued in collaboration with FinCEN, aimed at providing more guidance to bank examiners on assessing the adequacy of bank systems on risks associated with trade finance activities. See http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

[25] FinCEN, Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Trade-Based Money Laundering, advisory, FIN-2010-A001, February 18, 2010.

[26] Ibid. Of the approximately 17,000 SARs between January 2004 and May 2009 that FinCEN determined may have indicated TBML activity, only 24% of them clearly identified the suspected activity as TBML. The remaining 76% were identified by FinCEN based on complex queries including "trade" and other terms derived from various red flags.

[27] Ibid. For example, 14% of suspected TBML activity reported in SARs in 2004 occurred in 2004. However, 30% of such activity was not reported by financial institutions until 2009, five years after the activity occurred.

[28] FinCEN, Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, advisory, FIN-2014-A005, May 28, 2014.

[29] Ibid.

[30] FinCEN, Geographic Targeting Order, April 15, 2015; see also FinCEN, "FinCEN Targets Money Laundering Infrastructure with Geographic Targeting Order in Miami: 'GTO'

Addresses Trade-Based Money Laundering Activity Involving Drug Cartels," press release, April 21, 2015.

[31] FinCEN, Geographic Targeting Order, October 20, 2015; see also FinCEN, "FinCEN Renews Geographic Targeting Order (GTO) Requiring Enhanced Reporting and Recordkeeping for Electronics Exporters Near Miami, Florida," press release, October 23, 2015.

[32] FinCEN, Geographic Targeting Order, September 26, 2014; see also FinCEN, "FinCEN Issues Geographic Targeting Order Covering the Los Angeles Fashion District as Part of Crackdown on Money Laundering for Drug Cartels," press release, October 2, 2014.

[33] 31 U.S.C. 5318A, as added by Sec. 311 of Title III of the USA PATRIOT Act (P.L. 107-56), and subsequently amended.

[34] FinCEN, Notice of Finding that Halawi Exchange Co. is a Financial Institution of Primary Money Laundering Concern, April 23, 2013; FinCEN, Notice of Finding that Kassem Rmeiti and Co. For Exchange is a Financial Institution of Primary Money Laundering Concern, April 23, 2013.

[35] FinCEN, Notice of Finding that Banca Privada d'Andorra is a Financial Institution of Primary Money Laundering Concern, March 10, 2015.

[36] U.S. Department of State, INCSR, Vol. 2, March 2015.

[37] John Cassara, Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement (Hoboken, NJ: John Wiley and Sons, 2016).

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 4

STATEMENT OF JOHN A. CASSARA, FORMER U.S. INTELLIGENCE OFFICER AND TREASURY SPECIAL AGENT. HEARING ON "TRADING WITH THE ENEMY: TRADE-BASED MONEY LAUNDERING IS THE GROWTH INDUSTRY IN TERROR FINANCE"*

Chairman Fitzpatrick, Ranking Member Lynch and members of the Task Force to Investigate Terrorism Financing, thank you for the opportunity to testify today. It is an honor for me to be here.

Not long after the September 11 attacks, I had a conversation with a Pakistani entrepreneur. This businessman could charitably be described as being involved in international grey markets and illicit finance. We discussed many of the subjects addressed in this hearing including trade-based money laundering, terror finance, value transfer, hawala, fictitious invoicing, and counter-valuation. At the end of the discussion, he looked at me and said, "Mr. John, don't you know that your adversaries are transferring money and value right under your noses? But the West doesn't see it. Your enemies are laughing at you."

* This is an edited, reformatted and augmented version of a statement presented February 3, 2016 before the House Committee on Financial Services.

The conversation made a profound impact on me. I knew he was right. At the time of the conversation, the U.S. government and the international community had not focused attention or resources on the misuse of international trade to launder money, transfer value, avoid taxes, commit commercial fraud, and finance terror. It was completely under our radar screen. Our adversaries − terrorists, criminals, kleptocrats, and fraudsters − were operating in these areas with almost total impunity. And unfortunately, many years after that conversation and the tremendous expenditure of resources to counter illicit finance, trade-based money laundering and value transfer are still not recognized as significant threats. Perhaps as the Pakistani businessman inferred, it is because the subterfuges are "hiding in plain sight."

The Financial Action Task Force (FATF) has declared that there are three broad categories for the purpose of hiding illicit funds and introducing them into the formal economy. The first is via the use of financial institutions; the second is to physically smuggle bulk cash from one country or jurisdiction to another; and the third is the transfer of goods via trade.[1] The United States and the international community have devoted attention, countermeasures, and resources to the first two categories. Money laundering via trade has for the most part been ignored.

Trade-based money laundering and value transfer (TBML) is a very broad topic. FATF defines TBML as "the process of disguising the proceeds of crime and moving *value* through the use of trade transactions in an attempt to legitimize their illicit origins."[2] The key word in the definition is *value.*

MAGNITUDE OF THE PROBLEM

There are no official estimates on the magnitude of TBML as a whole. Since the issue impacts national security, law enforcement, and the collection of national revenue it is remarkable that TBML has never been systematically examined by the U.S. government.

I would like to give you just a few examples to demonstrate the enormity of the problem.

Dr. John Zdanowicz, an academic and early pioneer in the field of TBML, examined 2013 U.S. trade data obtained from the U.S. Census Bureau. By examining under-valued exports ($124,116,420,714) and over-valued imports ($94,796,135,280) Dr. Zdanowicz found that $218,912,555,994 was moved out of the United States in the form of value transfer! That figure represents 5.69% of U.S. trade. Examining over-valued exports ($68,332,594,940) and

undervalued imports ($272,753,571,621), Dr. Zdanowicz calculates that $341,086,166,561 was moved into the United States! That figure represents 8.87% of U.S. trade in 2013.[3]

I believe the United States has the most professional and vigorous customs enforcement service in the world. So if almost 6 to 9 percent of our trade is tainted by customs fraud and perhaps trade-based money laundering, what does that mean for the rest of the world, in particular countries with weak governance and high corruption?

By examining other forms of TBML the magnitude of the problem increases further. For example, TBML is also involved with customs fraud, tax evasion, export incentive fraud, VAT fraud, capital flight or the transfer of wealth offshore, evading capital controls, barter trade, underground financial systems such as hawala and the fei-chien – the Chinese "flying money system, the black market peso exchange (BMPE), and commercial trade-based money laundering such as trade diversion, transfer pricing, and abusive trade-misinvoicing.

The amount of trade-misinvoicing is staggering. According to Raymond Baker, the head of Global Financial Integrity (GFI) and a worldwide authority on financial crime, "Trade misinvoicing – a prevalent form of TBML – accounts for nearly 80 percent of all illicit financial outflows that can be measured by using available data."[4] According to a 2015 study by GFI, "Illicit financial flows from developing and emerging economies surged to $1.1 trillion in 2013." By just focusing on developing economies, cumulative illicit outflows were approximately $7.8 trillion between 2004 and 2013 in the GFI study, the last year for which data are available.[5]

TBML is found in every country in the world – both developed and developing. But the massive transfer of wealth offshore through abusive trade misinvoicing is particularly harmful to countries with weak economies, high corruption, and little adherence to the rule of law. The developmental, human and societal costs are staggering.

Trade-based value transfer has existed long before the advent of modern "Western" banking. In areas where our adversaries operate, trade-based value transfer is part of a way of life. It is part of their culture; a way of doing business. TBML is related to terrorist finance. In just one example of TBML and terrorist financing, a Pakistani madrassa – a fundamental Islamic religious school – was linked to radical jihadist groups. The madrassa received large amounts of money from foreign sources. It was engaged in a side business dealing in animal hides. In order to justify the large inflow of funds, the madrassa claimed to sell a large number of hides to foreign customers at

grossly inflated prices. This ruse allowed the extremists to "legitimize" the inflow of funds which were then passed to terrorists.[6]

In addition, trade-based value transfer is often used to provide "counter-valuation" or a way of balancing the books in many global underground financial systems - including some that have been used to finance terror. Trade-based value transfer is found in hawala networks and most other regional "alternative remittance systems."

The World Bank estimates that global remittances through official channels like banks and Western Union will reach $707 billion by 2016. Nobody has reliable estimates of remittances through *unofficial* channels. However, the International Monetary Fund believes, "unrecorded flows through *informal channels* are believed to be at least 50 percent larger than recorded flows."[7] Thus according to these World Bank and IMF estimates, unofficial remittances could be well over $1 trillion!

Our countermeasures for underground money remitters like hawaladars are not effective. Requirements for registration, licensing, and filing of financial intelligence have all failed – not only in the United States but in other countries where they have been tried. I believe that a systematic examination of TBML and value transfer and their links to underground finance could be the "back door" into hawala and other problematic alternative remittance systems – some used by our terrorist adversaries. Yet the U.S. and the international community have virtually ignored trade's role in underground financial systems.

TBML is also intertwined with the misuse of the Afghan Transit Trade, Iran/Dubai commercial connections, the Tri-Border region in South America, suspect international Lebanese/Hezbollah trading syndicates, non-banked lawless regimes such those in Somalia and Libya, territory controlled by ISIS in Syria and Iraq, and many more. The promotion of international trade transparency could provide clarity for these opaque value transfer systems.

To summarize, the argument can be made that TBML and value transfer, including all its varied forms, is perhaps the largest and most pervasive money laundering methodology in the world. Unfortunately, it is also the least understood, recognized, and enforced. In comparison to the annual volume of tens of trillions of dollars in international general merchandise trade, successful enforcement efforts are practically nil.

HOW DOES TBML WORK?

In its primary form, TBML revolves around invoice fraud and associated manipulation of supporting documents. When a buyer and seller work together, the price of goods (or services) can be whatever the parties want it to be. There is no invoice police! As Raymond Baker succinctly notes, "Anything that can be priced can be mispriced. False pricing is done every day, in every country, on a large percentage of import and export transactions. This is the most commonly used technique for generating and transferring dirty money."[8]

The primary techniques used for involve invoice fraud and manipulations are:

- Over-and-under invoicing of goods and services
- Multiple invoicing of goods and services
- Falsely described goods and services

Other common techniques related to the above include:

- Short shipping: this occurs when the exporter ships fewer goods than the invoiced quantity of goods thus misrepresenting the true value of the goods in the documentation. The effect of this technique is similar to over invoicing.
- Over shipping: the exporter ships more goods than what is invoiced thus misrepresenting the true value of the goods in the documentation. The effect is similar to under invoicing.
- Phantom shipping: No goods are actually shipped. The fraudulent documentation generated is used to justify payment abroad.

Invoice Fraud

Money laundering and value transfer through the over- and-under invoicing of goods and services is a common practice around the world. The key element of this technique is the misrepresentation of trade goods to transfer value between the importer and exporter or settle debts/balance accounts between the trading parties. The shipment (real or fictitious) of goods and the accompanying documentation provide cover for the transfer of money.

First, by under-invoicing goods below their fair market price, an exporter is able to transfer value to an importer while avoiding the scrutiny associated with more direct forms of money transfer. The value the importer receives when selling (directly or indirectly) the goods on the open market is considerably greater than the amount he or she paid the exporter.

For example, Company A located in the United States ships one million widgets worth $2 each to Company B based in Mexico. On the invoice, however, Company A lists the widgets at a price of only $1 each, and the Mexican importer pays the U.S. exporter only $1 million for them. Thus, extra value has been transferred to Mexico, where the importer can sell (directly or indirectly) the widgets on the open market for a total of $2 million. The Mexican company then has several options: it can keep the profits; transfer some of them to a bank account outside the country where the proceeds can be further laundered via layering and integration; share the proceeds with the U.S. exporter (depending on the nature of their relationship); or even transfer them to a criminal organization that may be the power behind the business transactions.

To transfer value in the opposite direction, an exporter can over-invoice goods above their fair market price. In this manner, the exporter receives value from the importer because the latter's payment is higher than the goods' actual value on the open market.

Invoice Manipulation Made Simple!
To move money/value out:

- Import goods at overvalued prices or export goods at undervalued prices To move money/value in:
- Import goods at undervalued prices or export goods at over-valued prices

For example, Figure 1[9] below shows the fluctuating value associated with thousands of refrigerators exported from Country A to Country B via a series of shipments. The darker shade represents the declared value of the refrigerators upon export from Country A, and the light shade represents their declared value upon arrival in Country B. The horizontal line represents the time period over which these shipments occurred. The vertical line represents the value expressed in dollars. In this case the refrigerators were over-invoiced. The export data came from the "shippers export declaration" (SED) that accompanies the shipments. The import data came from the importing

country's customs service. Obviously, the declared export price should match the declared import price. (There are some recognized but comparatively small pricing variables. In addition, the quantity and quality of refrigerators should also match - which occurred in this case.) The difference in price between the dark and light shades represents the transfer of value from the importer to the exporter. In this case, the transfer represented the proceeds of narcotics trafficking.

At the end of the chart the shaded colors start to converge. The colors or values between imports and exports begin to match because data was compared, anomalies noted, and joint enforcement action taken by the two countries involved. Trade transparency was achieved. The comparative stability at the end of the chart reflects true market conditions.

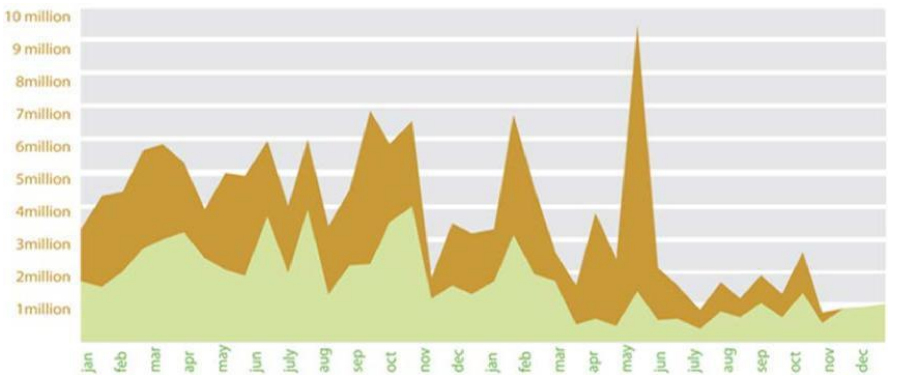


Figure 1.

There are incredible examples of trade-mispricing. For example, Dr. John Zdanowicz conducted a study analyzing U.S. trade data.[10] He found plastic buckets from the Czech Republic imported with the declared price of $972 per bucket! Toilet tissue from China is imported at the price of over $4,000 per kilogram. Bulldozers are being shipped to Colombia at $1.74 each! Of course, there are various reasons why the prices could be abnormal. For example, there could simply be a data "input" or "classification" error. However, recalling the above explanation of over-and-under invoicing, the abnormal prices could also represent attempts to transfer value in or out of the United States in the form of trade goods. At the very least, the prices should be considered suspicious. Only analysis and investigation will reveal the true reasons for such large discrepancies between market price and declared price.

Countermeasures – Data, Analytics, and Trade Transparency

Despite the enormity of TBML and the challenges briefly outlined above, I am hopeful. The reason for my optimism is that *theoretically* international trade transparency can be achieved. As opposed to other money laundering methodologies (for example, bulk cash smuggling) a growing volume of precise data exists that enable analysts and criminal investigators to follow the value transfer trails.

Over the last few years there has been an explosion in both government and commercial data related to trade. Overlaying financial intelligence, law enforcement and customs data, travel data, commercial records, shipping data, etc. further increases transparency and facilitates more clarity. Simultaneously, there has been incredible progress in advanced analytics. I am particularly excited about "predictive analytics" which helps analysts and investigators spot patterns, methods, and trends as well as prioritize investigative leads.

Time and space do not allow me to elaborate on how trade and associated data is produced and analyzed. Other witnesses, including my friend Lou Bock, the "godfather" of TBML, will elaborate on this in their remarks.

In order to champion trade transparency, in 2004 the United States government adopted a proposal Lou and I advanced and created the world's first trade transparency unit (TTU). It is located within Homeland Security Investigations (HSI). (For further information see the TTU website at: https://www.ice.gov/trade-transparency) The initiative seeks to identify global TBML trends and conduct ongoing analysis of trade data provided through partnerships with other countries because one of the most effective ways to identify instances and patterns of TBML is through the exchange and subsequent analysis of trade data for anomalies that would only be apparent by examining both sides of a trade transaction.

A TTU is formed when HSI and any of the United States trading partners agree to exchange trade data for the purpose of identifying comparison and analysis. To help analyze the data, the HSI has developed a specialized computer system. Containing both domestic and foreign trade data, the system allows users to see both sides of a trade transaction, making it transparent to both countries. As in the example of refrigerators in Figure 1 above, TTUs can easily identify trade anomalies that could be indicative of customs fraud, TBML, contraband smuggling, tax evasion, and even underground finance. Of course, investigations are still required. This investigative tool has been proven to be effective. Since the creation of the domestic and international TTU initiative, more than $1 billion has been seized.[11]

Another reason I am optimistic about the long-term prospects of achieving trade transparency is that it is a revenue enhancer. By systematically cracking down on various forms of customs fraud, hundreds of billions in dollars of lost revenue can be returned to cash-starved governments around the world. This could be particularly helpful in parts of the world where our adversaries operate and weak governments are starved for revenue. In cases where corruption is rife, effective trade analysis can be accomplished outside of the country. I have found that many times when I travel to the developing world and talk about the importance of anti-money laundering and counter-terrorist finance, the reception is sometimes cool. However, when I explain to the officials how much revenue they can obtain by cracking down on customs fraud they become very interested. In other words, the carrot of empowering our partners to strive for trade transparency and increased revenue can be much more effective than the stick of heavy handed measures that have proved unsuccessful.

RECOMMENDATIONS

1. As noted, I believe TBML could be the largest and most pervasive money laundering methodology in the world. However, we do not know for certain because the issue has never been systematically examined. This is even more surprising in the United States because annually we are possibly losing billions of dollars in lost taxes due to trade-mispricing alone. While not necessarily true for all money laundering methodologies, trade generates data. I believe it is possible for economists, statisticians, and analysts to come up with a fairly accurate estimate of the overall magnitude of global TBML and value transfer. Narrowing it down to specific problematic countries is easier still.

I suggest this Task Force urge the Department of Treasury's Office of Intelligence and Analysis (OIA) to at least examine U.S. related data and come up with an official estimate for the amount of TBML *in all its varied forms* that impacts the U.S. A generally accepted estimate of the magnitude of TBML is important for a number of reasons: a.) It will provide clarity; b). It will focus attention on the issue; c.) From an enforcement perspective, the supporting analysis should provide both excellent insight into specific areas where criminals are vulnerable and promising opportunities for targeting; and d.) A systematic crack down on TBML and customs fraud will translate into enormous revenue gain.

2. In the world of anti-money laundering/counter-terrorist finance (AML/CFT) enforcement, the FATF makes things happen. The FATF recognizes TBML is a huge concern. There is a special FATF typology report on TBML. However, in 2012 when the current FATF recommendations were reviewed and promulgated, TBML was not specifically addressed. It is past time this is done. I suggest the Task Force contact the U.S. Department of Treasury (which heads the U.S. FATF delegation) and urge that the U.S. introduce a resolution calling for the misuse of trade to launder money and transfer value be examined as a possible new FATF recommendation.

3. HSI continues to expand the network of operational TTUs, which now includes Argentina, Australia, Colombia, Dominican Republic, Ecuador, Guatemala, Mexico, Panama, Paraguay, Peru and Philippines. As part of the TTU initiative, HSI provides equipment and increased operational support to these TTU partners to ensure the network's successful development. I believe the TTU concept should be further developed and expanded. In the "next frontier of international money laundering enforcement," I believe a global TTU network should be created that is somewhat analogous to the Egmont Group of Financial Intelligence Units. Two wonderful aspects of this program are that data already exists and trade transparency is actually a net revenue enhancer – not only for the United States but for partner countries. I urge Congress to create a separate line item for the HSI TTU initiative so as to promote its expansion. Our TTU has been raided of funds and personnel. Without resources, its functional existence is in jeopardy.

I also believe the concept of trade transparency should be built into the US trade agenda. For example, the new Trans-Pacific Partnership (TPP) is set to lower or eliminate tariffs on everything from imported Japanese cars to New Zealand lamb, while opening two-fifths of the global economy to easier trade in services and electronic commerce.[12] I don't have a position on the pros and cons of the TPP. But the volume of increased trade will provide additional opportunities for trade-based value transfer and money laundering. I suggest we help protect abuse by insuring that every TPP signatory country establish a TTU and share appropriate targeted trade data to spot anomalies that could be indicative of trade fraud at best and TBML at worst.

4. The misuse of trade is a law enforcement issue – not just a customs issue. Unfortunately, I have first-hand experience that there is almost a total lack of knowledge at the federal, state, and local law enforcement levels regarding TBML and the importance of following the value transfer trail. Even though I can demonstrate how TBML affects state and local law enforcement,

most often the consensus opinion is, "Trade is a customs issue. It doesn't concern me or my department."

Yet it is precisely because law enforcement officers are on the front lines in their communities and know their operating environment well, they should notice if a local business or commercial activity does not make market or economic sense. For example, a normal business should not remain in operation for long with sporadic commercial activity or when consistently selling goods far above or below market norms. Numerous businesses in the U.S. and elsewhere are involved at the local level in TBML schemes and deal with goods that are frequently manipulated to transfer value. Businesses involved with the black market peso exchange (BMPE) – large and small - are found throughout the United States. Underground financial networks such as hawala and fei-chien are found in local communities and they often depend on trade and local business networks.

Accordingly, I urge my state and local law enforcement colleagues to become more familiar with issues surrounding TBML schemes and how they affect the local community. Where appropriate, trade fraud and associated crimes should be part of their financial investigations education. The State and Local Anti-Terrorism Training (SLATT) program funded by the U.S. Department of Justice, Bureau of Justice Assistance (BJA) is an excellent starting point. The SLATT program is dedicated to providing specialized multiagency antiterrorism detection, investigation, and interdiction training and related services at no cost to our nation's law enforcement officers, who face the challenges presented by the terrorist and violent criminal extremist threat – including the detection of opaque underground financial systems sometimes employed by terrorists.[13]

With an expanded TTU, there should be more sharing of targeted trade data with local law enforcement. In addition, appropriate U.S. import and export trade data should be made available by the Department of Homeland Security and the Department of Commerce to Treasury's Financial Crimes Enforcement Network (FinCEN). Combined with commercially available data, criminal investigators and analysts should be able to conduct both reactive and pro-active queries into suspicious trade transactions.

We have plenty of laws, rules, and regulations on the books that enable law enforcement to combat financial crimes including TBML. In my opinion, what we need is awareness, consensus to make this a priority, and an emphasis on enforcement.

Other recommendations on combatting TBML and value transfer are included in my new book on trade-based money laundering.

I appreciate the opportunity to appear before you today and I'm happy to answer any questions you may have.

Much of the material in this statement comes from:

John Cassara, Trade-Based Money Laundering: the Next Frontier in International Money Laundering Enforcement; Wiley, Hoboken, New Jersey, 2015.

End Notes

[1] FATF; Trade Based Money Laundering (Paris: FATF, June 23, 2006), p. 1; available online: (http://www.fatfgafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf).

[2] Ibid.

[3] Analysis given to the author by Dr. John Zdanowicz via June 30, 2015 email.

[4] "The Economist Highlights the Scourge of Trade Misinvoicing," Global Financial Integrity, May 2, 2014; available online: (http://www.financialtransparency.org/2014/05/02/the-economist-highlights-the-scourge-of-trademisinvoicing/).

[5] "New Study: Illicit Financial Flows Hit US$1.1 Trillion in 2013," Global Financial Integrity, December 8, 2015; available online: http://www.gfintegrity.org/press-release/new-study-illicit-financial-flows-hit-us1-1-trillion-in2013/.

[6] Brett Wolf, "The Hide and Hair of Terrorist Finance in Pakistan," Complinet, January 17, 2007.

[7] Dilip Ratha, "Remittances, Funds for the Folks Back Home," International Monetary Fund; available online: (http://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm).

[8] Raymond W. Baker, Capitalism's Achilles Heel, John Wiley and Sons, Hoboken, New Jersey, p. 134.

[9] Source: John Cassara, "Fighting Terror with Analytics," SAS.com Magazine, (available online http://www.sas.com/news/sascom/terrorist-financing.html).

[10] Dr. John Zdanowicz, Trade-Based Money Laundering and Terrorist Financing; available online: https://datapro.fiu.edu/campusedge/files/articles/zdanowiczj3008.pdf.

[11] March 26, 2015, email exchange between the author and Hector X. Colon, he unit chief/director of the TTU.

[12] William Mauldin, "Details of Pacific Trade Pact Fuel Debate," Wall Street Journal, November 5, 2015; available online: http://www.wsj.com/articles/pacific-trade-agreement-terms-herald-public-battle-1446712646.

[13] The Institute for Intergovernmental Research (IIR) serves as the technical service provider for ongoing training, research, and analysis services to the SLATT Program through the support of grant awards received from the Bureau of Justice Assistance. IIR supports the SLATT Program by providing project coordination activities, training assessment, and meeting coordination. See the IIR/SLATT website for additional information; (https://www.iir.com/WhatWeDo/Criminal_Justice_Training/SLATT/).

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 5

TESTIMONY OF LOU BOCK, FORMER SENIOR SPECIAL AGENT, U.S. CUSTOMS AND BORDER PROTECTION. HEARING ON "TRADING WITH THE ENEMY: TRADE-BASED MONEY LAUNDERING IS THE GROWTH INDUSTRY IN TERROR FINANCE"*

I'm a retired Senior Special Agent who worked as a criminal investigator at the DEA, USDA, and fraud, financial and intel at Customs/Treasury and, later, ICE/DHS. For much of my career I generated and worked large, complicated criminal cases involving trade fraud and money laundering worth billions of dollars. I did so with a team of import and tax specialists, agents, and analysts by detecting patterns of criminal behavior that stretched across large amounts of diverse trade and financial data including import/export, manifest, Bank Secrecy Act, and other data sources. The software and methodologies that my team and I pioneered were successfully deployed in over three dozen countries which led, with the insight and vision of John Cassara, to Trade Transparency Units or TTU's.

To give you some sense of my history targeting crime, I would like to provide you with some background on myself and on some of the cases I've

* This is an edited, reformatted and augmented version of testimony presented February 3, 2016 before the House Committee on Financial Services.

been involved with, along with the methodologies I've developed and used to identify financial and trade fraud. I want you to understand that I know what I'm talking about: I've been doing this for 25 years and I know that trade-based money laundering (TBML) and associated crimes are solvable problems. We already know how to do this--we just need to have the will to implement the proven methodologies and assign a team with the appropriate mission.

Originally, I was assigned to the Customs Service headquarters Fraud Division, to develop a system whereby non-technical individuals such as criminal investigators or intelligence analysts could access core Customs databases. Specifically, we were to look at Customs import documents and look for problems or anomalies that would be indicative of over or under invoicing / valuation of goods. Once we found these indications, we could investigate the activities for fraud against the revenue of the United States Customs Service.

Specific data that we were looking at was maintained by the main United States Customs data center in Newington, Virginia. Newington housed one of the largest computer centers in the United States, consisting of a number of mainframe computers. Their core database was updated by a system that was approximately 40 years old at the time and was accessible to the user by way of a special application that queried the data by essentially asking one question at a time.

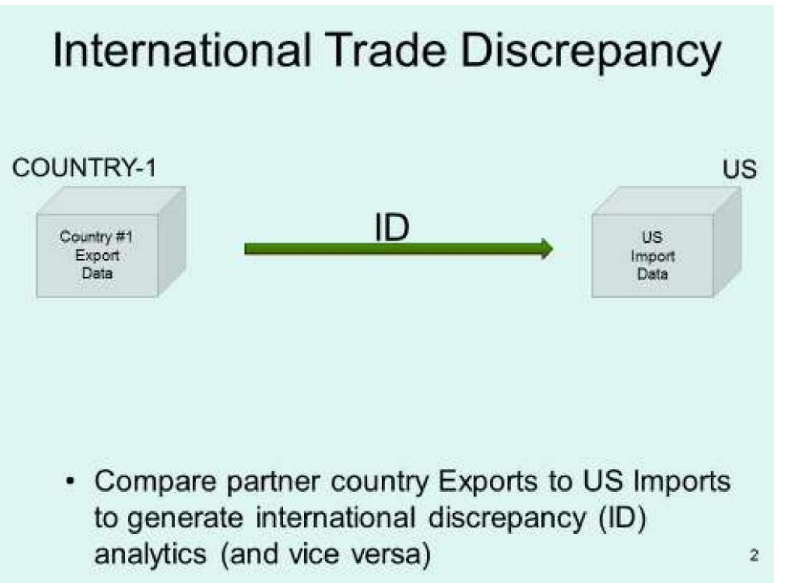
You could search by product, port, importer or document number. It worked fairly well if you knew exactly the items you were searching for; with the specific importer or document number, you could find out all the details of a given transaction. The system had little flexibility and there was no possibility of examining the bulk of the data as a way to identify trends.

It was decided that the best way forward was to leave this archaic system as it was, in order to prevent disruption of the entry process. We then proceeded to develop an approach with which we downloaded chunks of data from the mainframe and analyzed it separately.

The first document that we applied this treatment to was the Customs entry form known as the CF 7501. This document is used to describe the goods being brought into the United States and entered for consumption. You can think of it as is short form tax return. The importer usually through a Customs broker would file the CF 7501 when he or she was required to settle the account as to duty and taxes owed on the goods brought into United States from another country.

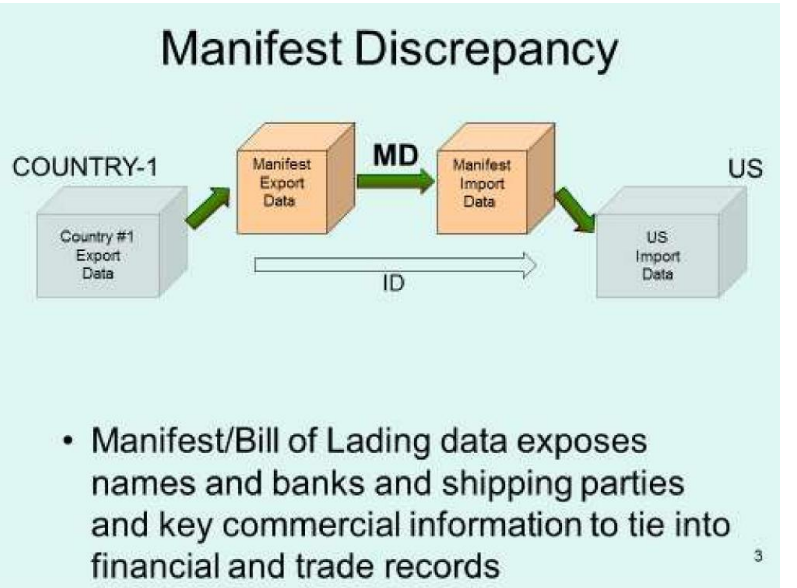
The system we started to develop simply took a copy of some of the data fields from the CF 7501 that would be relevant to the detection of fraud. The first attempt at this was named the Numerically Integrated Profiling System (NIPS). Our method of distributing NIPS to the field was to send the NIPS program and required 7501 data to the field.

The success of this initiative led to many different types of data being added into the analytical process over time. One type of data which proved enormously useful, particularly to identify trade discrepancies with other countries, was the addition of other countries' trade data. One outgrowth of this way of looking at trade data was the definition of an analytical methodology now known as the International Discrepancy Analysis. This is the core analytical approach invented, implemented, and successfully deployed by me and my team to understand trade fraud.



The dramatic success of this endeavor led to requests for more types of data from the field. These included data showing the movement of goods from the foreign country known as the manifest or the bills of lading. These transportation documents included such information as who shipped the goods to the United States, who was to receive them in the United States, what ship they arrived on, when they arrived, what ports were involved, as well as commercial description of the goods.

When you combine manifest with CF 7501 data you can find discrepancies. Some of these discrepancies may show that the route or the port of lading does not agree with the country of origin supplied on the Customs form 7501. This is useful to determine if the government has been furnished with a false country of origin. Violations of sanctions and of various treaties, as well as quota regimens, were detected in this manner. This led to the creation of the analytical approach known as Manifest Discrepancy.



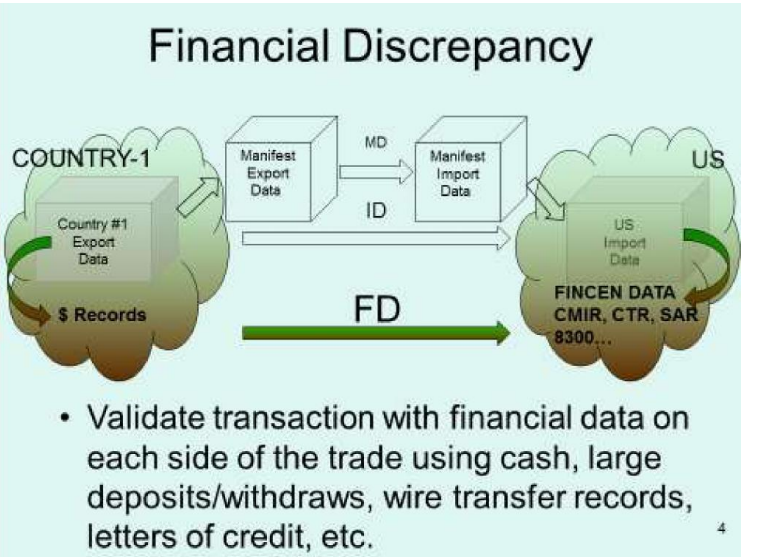
Once we had taken steps to address trade data discrepancies, the next data element that we sought to include in our analysis were the financial data sets, primarily drawn from the Bank Secrecy Act (BSA) data. Financial documents include:

- Currency Monetary Instrument Report (CMIR)--this document details the importation and exportation of money and financial instruments equal to or greater than $10,000. CMIR data fields include: owner of the money, the transporter of the money, parties to the transactions (complete with names and addresses), the from and to countries, and the dollar value of the instrument. Includes passport numbers.
- Currency Transaction Report (CTR). Reports banks and financial institution transactions equal to or greater than $10,000. Includes bank

info, account number, owner of the money, party making the transaction, dollar value. Also includes names and social security numbers.

- 8300. Cash transactions to purchase items equal to or greater than $10,000. Includes name of seller and buyer parties, addresses, social security numbers and other identifying data, and dollar value.
- Wire transfer data
- Suspicious Activity Reports (SAR). Derived from banks, casinos, and money service bureaus. Contains written reports identifying transactions that the banks feel are suspicious.
- Many additional financial data sources

The addition of these financial data sources opens up an entire new world of analytic possibilities as we begin the search for Financial Discrepancies:



The documents listed above are often located on mainframe computers found at various USG agencies. Each document's data required normalization, which we learned how to do, before effective targeting could be accomplished. The methodology requires that each document's fields to be used by the advanced TBML targeting system is formatted in specific ways. We integrated these various types of documents in order to supply the user/analyst with

answers to their law enforcement-related questions: *who, what, when, and where*.

Using this overall analytic idea, we approached the Treasury Department of the country Colombia (DIAN), under Plan Colombia, and set up a joint effort using both countries' imports and exports to one another. Money was allocated to allow our team to normalize the Colombian detailed import and export data. At this point, we were looking at all detailed U.S. import and export transactions, and Colombian data to match, for several years. The project immediately led to the discovery of major discrepancies between each country's imports and exports. Some discrepancies were in the dollar value, and in other situations it was the quantities that were seriously misaligned. Examination of the data showed that in many cases, the imports and exports between the two countries matched nearly perfectly, which indicated to our team that the significant problems we were uncovering were not data quality issues.

In the case of Colombia, the differences in value were mainly higher when the goods arrived in the United States. This is commonly called over-invoicing or overvaluing goods. This would usually have the effect of raising the amount of duty and taxes paid on imports. It is fairly common to see undervaluation because that would reduce the money owed in taxes. The overvaluation was, therefore, perplexing. The explanation supplied by financial investigators was that overvaluation was an illegal means of moving money out of the United States. Simply put, if you pay more for an item, money leaves the higher priced country to the lower priced country.

One might say this is counter intuitive. Why pay more US taxes and duties by overstating the amount of a given transaction? The answer is the overvaluation had involved items where there was no taxes or duties.

More was learned from that early experiment. We discovered that in the case of missing goods--where more left the United States than arrived in Colombia--it was simply smuggling that was occurring. We identified ways in which Colombia was losing significant revenue sources, which without our analysis would have been very difficult to detect. More importantly, the analysis identifies goods financed by the Black Market Peso Exchange (BMPE).

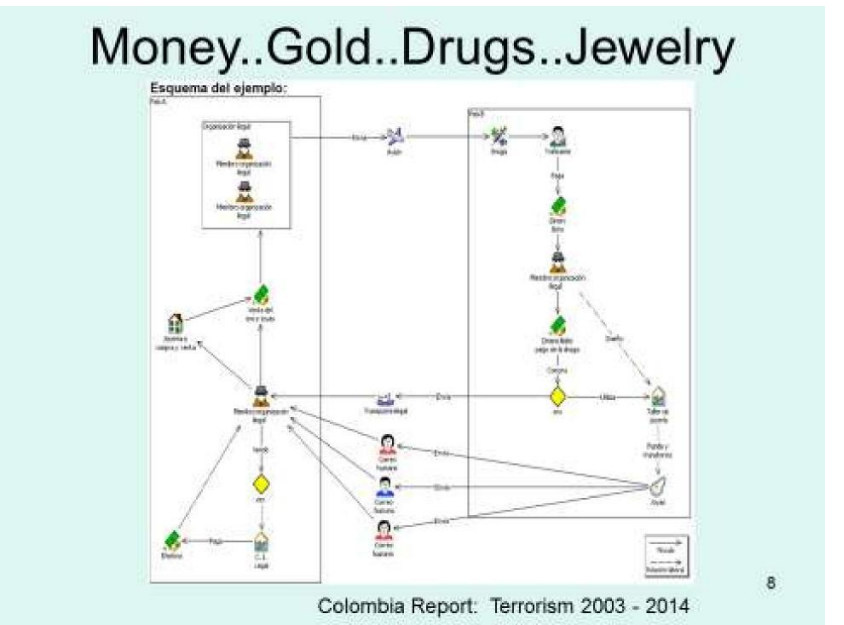
Because of oddities in the Colombian system of checks and balances, which is different than the system in the U.S., Colombia required that all dollar transactions have to originate through a Colombian bank. These banks were required to notify DIAN of goods they finance before the goods actually arrive in-country. By being financed outside the bank (by way of the illegal BMPE),

DIAN was unable to watch for or otherwise control these importations. Based on our pioneering efforts, many criminals and schemes in both Colombia and in the U.S. were identified and stopped.

Based on our string of successes working with Colombia, John Cassara and I proposed that the State Department fund the creation of Trade Transparency Units (TTUs). Once the funding was obtained, we set out and added six additional countries to the TTU project. This took place while I was still managing the TTU's at U.S. Customs.

I'm here today because I greatly believe in the mission of trade transparency and financial controls but I'm also frustrated that we have not made enough progress, or given enough focus, to the critical importance of the financial side of the trade transparency issue. Even our partners, including Colombia, are moving beyond us and are taking the idea of our initiative further and more effectively than we have. Colombia has effectively unified the financial and trade analytic components and leveraged into their equivalent of FinCEN an analytical unit looking at financial and trade data.

As an example, here is a chart from a Colombia report on the fraudulent movement of money, gold, drugs, and jewelry. I would love to explain to this committee how the chart below depicts the illicit movement of money and the role the U.S. should be playing to address these issues.



We need a new initiative, a new focus, which leverages the learnings from our previous efforts, learns from partner countries, but focuses on the critical financial and trade fraud issues facing the United States.

Within the United States and around the world, I have worked on a great variety of different cases involving trade fraud and money laundering. Below are a few examples.

Historical geographic focus:

- Colombia
- Panama
- Guyana
- Peru
- Argentina
- Brazil
- Canada
- Mexico / NAFTA
- China
- US/Laredo
- Many more...

Additional commodities and areas of fraud:

- Gold
- Chicken
- Licorice
- Tobacco
- Freon
- Coins
- Watermelons
- Garlic
- Tax credits
- Jewelry
- In-Bond
- T Shirts
- Many more...

For example, perhaps you wouldn't think licorice (listed above) would hold a great deal of interest but the following graph shows how we were able to identify over $100 million in fraud:

As I look at the current situation in the U.S., I see the data necessary to do the correct investigations is scattered, partially gathered in a few place, but nobody is looking at it with the right perspective. There is not, to my knowledge, a financial focused initiative within a financially knowledgeable entity such as FinCEN, nor is there any significantly funded effort to apply the things we already know to the current problems of trade based money laundering.

In conclusion, I hope this committee understands the following:

- Trade based money laundering (TBML) has been around for a very long time but it is of exponentially growing importance to the U.S.
- The financial nexus of trade is key.
- Addressed appropriately we can help the U.S. and partner governments increase revenue collection dramatically while cutting

down on illicit financing of many activities including terrorist financing.

- There is significant synergy between TBML and the existing FinCEN mission.

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 6

STATEMENT OF FARLEY M. MESKO, CO-FOUNDER AND CEO, SAYARI ANALYTICS. HEARING ON "TRADING WITH THE ENEMY: TRADE-BASED MONEY LAUNDERING IS THE GROWTH INDUSTRY IN TERROR FINANCE"*

Chairman Fitzpatrick, Ranking Member Lynch, and members of the Task Force, thank you for the opportunity to testify here today.

Detecting and preventing trade-based money-laundering (or TBML) schemes is a notoriously difficult task, because such schemes are by necessity deeply embedded in overt and legal trade flows. However, this dependency also presents an opportunity: in order to embed within overt systems of finance and commerce, TBML schemes require seemingly legitimate companies, which require paperwork, disclosures, sometimes even marketing and a web presence. This means the networks that perpetrate TBML schemes tend to leave a broad and publicly discoverable footprint, both digital and physical. Despite the many layers of obfuscation that may be built into a scheme, this footprint often leads directly back to an already-identified threat actor or network, particularly in the context of a sophisticated and persistent terror financing scheme.

* This is an edited, reformatted and augmented version of a statement presented February 3, 2016 before the House Committee on Financial Services.

TBML typologies evolve and change over time, but the key actors in the networks tend not to. This implies that even as public and private sector entities focus on identifying and screening for *typologies* of TBML, they also need to focus on identifying the *networks*.

I am going to use a case example to illustrate this point.

CASE STUDY

In 2011, as part of a larger sanctions package targeting a Hizballah terror financing TBML scheme, the United States Treasury identified a Cotonou, Benin-based group of companies known as the "Elissa Group." In addition to its alleged participation in this terror financing scheme, the Elissa Group was deeply integrated into seemingly legal streams of international trade and commerce, acting as shipping agent for several large international freight forwarders who specialized in maritime transport of new and used automobiles. By all accounts, this coordinated US government effort, which also included the designation of a Lebanese bank as a primary money laundering concern, was a success. However, patterns of economic activity subsequent to the designation, and patterns of later US government actions, suggest that this network continued to operate even in the face of exposure.

Treasury data from the original 2011 action indicate that at least six of the sanctioned companies shared an address in Cotonou, Benin, and further open source research revealed that several also shared the same phone number. Subsequent to the designation, a new company, Abou Merhi Lines, began to appear on maritime commercial listings linked to this same address and phone number, operating in the same industry segment as the Elissa Group. Reexamining publicly available bills of lading from prior to 2011 shows that this company owned and managed vessels used by the Elissa Group companies for hundreds of used vehicle shipments. Four years after the original Elissa designation, in October 2015, Treasury sanctioned Abou Merhi Lines for its alleged participation in the same TBML scheme identified in 2011. This suggests that the TBML network likely operated post-designation, through both new and old actors, for at least four years.

Even further, online trade data and public records from the Littoral Department Chamber of Commerce in Benin indicate that at the time of the original 2011 designation, at least six other companies and two individuals were active at the shared Cotonou, Benin address. One of these companies, Rmaiti SRL, was later identified in the 2013 FinCEN 311 designation of

Kassem Rmeiti and Co For Exchange. Another company, never publicly identified, was actually listed "care of Elissa Group." These and others were active in used vehicle imports, the same industry used to disguise illicit financial flows in the scheme targeted by Treasury.

In sum, 13 companies and two individuals shared identifiers and selectors in Cotonou, Benin; between 2011 and 2015, eight of these 15 companies and individuals were either sanctioned by OFAC or identified in a FinCEN 311 action, in several cases operating openly for years after the initial identification of the scheme; of the remaining seven co-located companies and individuals, five were overtly involved in the used vehicle trade, and may be operating today.

I chose this example because it illustrates several key points about targeting TBML networks.

First, sanctions, 311 actions, and indictments are a starting point and not an endpoint in the government's efforts to target money launderers (particularly those involved in complex networks and sophisticated schemes like TBML). Networks change over time in response to interventions from law enforcement and regulators, but they rarely go away.

Second, in addition to focusing on *typologies* of TBML, both public and private sector stakeholders need to focus on the *networks*. Proxies, shell companies, vessels, and other actors may change over time, but more often than not, there is a trail leading back to the same key players, whether it's a common director, shareholder, address, phone number, or otherwise. Further, many thousands of these key players have already been identified by governments worldwide, essentially providing the first level of lead generation for investigators and analysts in both the public and private sector.

Third, there is a tremendous amount of data available publicly to help detect and deter these schemes. Availability of course varies by jurisdiction, and most of these records are non-indexed, non-searchable, in local languages, and sometimes offline, but the information is there if you know where and how to look.

Finally, there are many stakeholders in this fight, from law enforcement and regulators to the transportation industry and the financial sector. Each of them holds some unique data, but nobody has the whole picture, and nobody is making full use of the range of data available to them in the public domain. The key to detecting and preventing increasingly complex TBML schemes is data integration, within government, within the private sector, between the two, and, for all the stakeholders, between proprietary and open data streams.

Thank you again for the opportunity to be here today, and I look forward to questions.

In: Trade-Based Money Laundering
Editor: Ashleigh Young
ISBN: 978-1-53610-543-8

Chapter 7

STATEMENT OF NIKOS PASSAS, PROFESSOR OF CRIMINOLOGY AND CRIMINAL JUSTICE, NORTHEASTERN UNIVERSITY. HEARING ON "TRADING WITH THE ENEMY: TRADE-BASED MONEY LAUNDERING IS THE GROWTH INDUSTRY IN TERROR FINANCE"*

INTRODUCTION

Terrorism is a persistent threat with no quick and easy solution. Anticipating the moves of terrorists and preventing their actions has become a top priority. In order to do so, the U.S. and the international community have introduced financial controls, along with military action and law enforcement techniques, to predict, restrict, and prevent terrorist activities. Countering terrorism finance (CFT) is not only about cutting off funds or mere displacement of sources and methods. Rather, the point is to undermine the finances and support networks of target groups. Conceived as financial vigilance, CFT helps focus on both fund raising and expenditure, as well as on partners, associates, facilitators, support networks, methods of operation and distribution of labor. Key nodes of information, intelligence and support can be identified and targeted as appropriate for more effective and sustainable results. The aim is to understand what they do, how they do it and how to

* This is an edited, reformatted and augmented version of a statement presented February 3, 2016 before the House Committee on Financial Services.

identify the key nodes of critical networks, partners and facilitators, blind eyes and corrupt enablers, so that we can more effectively disrupt their activities and achieve sustainable and long-term success (Passas, 2007).

Trade is not only a critical support system for numerous terror groups, but also the weakest link in the anti-money laundering (AML) infrastructure built since the 1980s. Despite substantial efforts, laws, measures and resources devoted to AML/CFT, there has been no systematic review or consistent action with respect to trade, which constitutes the biggest security and crime vulnerability, a black hole undermining the entire control framework. Even if all current rules were ever to be fully and consistently enforced throughout the world, billions of dollars could still be moved illicitly without detection and sanction. When CFT is not based on the best evidence and analysis the result is missed targets, false positives, false negatives and security weaknesses.

Imports and exports can hide illegal or controlled commodities trade, but they often shield significant illicit financial transactions. This can be accomplished by misdeclaring the quality, quantity, value, origin, destination, and final use of goods. Misinvoicing, trade diversion, counterfeiting and cargo theft are some of the most common methods (deKieffer, 2008; Passas, 1994; Passas and Nelken, 1993). Multiple terrorist groups are involved in these, so a focus on trade and terrorism is long overdue.

In this statement, I am summarizing some of the most important lessons learned through work I have been doing since 1989 on illicit financial and trade flows, including money laundering, the abuse of hawala and other informal remittance systems, terrorism and proliferation finance and the interface between legal and illegal actors. In a nutshell, the threats are serious but the good news is that effective responses are feasible and within reach. First I will review the challenges we face and then will outline available practical approaches and solutions.

The Challenges

Three global flows need monitoring and analysis for a clear picture of illicit flows: financial, information and trade. Ideally, these flows must become traceable and analyzed in parallel, so that discrepancies and anomalies can be revealed and studied. Most of our attention so far focuses on finance and information, but even there the work is imperfect and sources not cross-checked. Trade, on the other hand, is for the most part non-transparent, neglected and extremely vulnerable to abuse.

Abuses do occur routinely, not only for money laundering, but also for tax evasion, bribery and corruption, subsidy and other types of fraud, sanctions violations, embargo and quota violations, capital flight, as well as the financing of terrorism and WMD proliferation. The amounts involved are not known with precision but they are certainly staggering and likely exceed $1 trillion per annum. Many terror groups have used commodities in the modus operandi: from the Islamic State and al Qaeda in Iraq to the Kosovo Liberation Army (KLA), Jemaah al Islamiya, Tamil Tigers (LTTE), Hamas, Hizballah, the Partiya Karkerên Kurdistan (PKK) the Northern Alliance, al Qaeda, Groupe Islamique Armé (GIA), the Irish Republic Army, as well as Armenian, Chechen and Georgian paramilitary groups (Cassara, 2015; Freeman, 2012; Passas, 2011a, 2011b; Passas and Jones, 2006; Shelley, 2015).

When it comes to the trillions of dollars in trade volume annually, our vision is blurred for several reasons. First of all, relevant information is not collected in one place for consolidated analysis at the national and international level. Relevant information is collected by Customs, FinCEN, Department of Commerce, port authorities and their counterparts in other countries. Other data are in the hands of banks, insurance companies, brokers, shippers and logistics companies, importers and exporters. No one is getting the full picture because no one collects all of the information in one place.

Secondly, financial institutions are expected to focus on transactions monitoring working with large data that would presumably cover everything but end up identifying much less actionable intelligence than desired. A good deal of compliance work has become an automated tick-the box exercise that yields millions of SARs and massive false positives. These in turn tend to waste the time of personnel that must deal with them, rather than centering on the highest risks, analytical work for typologies or new algorithms, the identification of offenders and closer collaboration with controllers. After all, financial institutions have incentives to avoid heavy fines and reputational damage rather than to discover and chase away bad clients. In addition, financial institutions can only review data about their clients and have no way of accessing either government or other banks' clients and analysis. This leads to costly duplication of work and an incomplete view of the problem.

Thirdly, while some government work has been done on commerce-connected informal remittance and payment networks, such as hawala and black market peso exchange (BMPE), there has been no systematic assessment of trade threats and vulnerabilities in different economic sectors. Even when it comes to Informal Value Transfer Systems (IVTS), a term I coined in a study for the Dutch Ministry of Justice (Passas, 1999), no threat assessment has been

done since the studies commissioned by FinCEN right after 9/11 (Passas, 2003a, 2003c). The problem is that these informal networks evolve constantly and adapt to regulatory and law enforcement practices in different countries and environments in many of which they are outlawed (FATF, 2013). It is essential to keep an eye on these changes and also realize that hawala is not only a challenge for controllers, but can also be an invaluable intelligence asset (Passas, 2008) that can be leveraged in many places including Afghanistan, India and Somalia for both control purposes and assistance to fragile communities. This could address at once and synergistically terrorism finance, crime control, development and humanitarian policy objectives (Passas, 2015a, 2015b, 2016; SIGAR, 2013).

Finally, the value of open source information is under-estimated and underutilized. Reviewing and working only with classified and private data excludes information on the internet, in the press, public reports and research literature from NGOs and academics. Yet, these sources point to knowledge gaps, misunderstandings, contextual information, insights and items unavailable elsewhere that might contradict conventional wisdom or non-public data and discredit sources we should not rely too much on. This is all particularly relevant to the analysis of illicit networks, identification of true beneficial ownership, adverse media news in local or foreign publications, terrorism finance, sanctions violations, corruption, illicit enrichment and other issues of interest to those in charge of due diligence and investigative tasks.

The Solution

The answer to all of these challenges can be found by simply addressing the opportunities we have been missing up to now. As noted, all of the necessary data are not in one place but do exist. Hawala is not only a problem but also an intelligence asset and resource, if properly handled. Agencies that gather useful information can be encouraged to share it. Open source data are available for analysis. The private sector and academia can assist with additional data, collection in a secure environment, analysis and feedback to both government and business with red flags and guidance. Our view is blurred thus unnecessarily. It is like having a 4K TV that we use for analog programs instead of creating the feed for a high-definition picture of the global illegal trade and finance. The means are there to create it.

There are several data categories that can be collected systematically.

- Inbound Manifest/Movement data are provided to governments by carriers and shippers on goods arriving in a country by road, rail, sea, and air. These records offer details on what goods are received where, when and who is involved.
- Outbound Manifest/Movement Transactions are equivalent data on goods leaving a country.
- Import Declarations to governments when goods enter the economy. These are usually public in aggregate form.
- Export Declarations for goods leaving the economy.

Some of these data are published online, but there are also companies that collect and provide such information for a fee (e.g., Port Import Export Reporting Service - PIERS). U.S. import and export data can be obtained from U.S. Department of Commerce and International Trade Commission websites. Other countries publish theirs in revenue collection and official statistics agencies' websites. The United Nations also publishes trade information.

Port and ship-loading information, Electronic Data Interchange (EDI) records, which are standardized computer-to-computer documents between businesses can be used for the analysis for shipments, invoices and container movements. Trade finance, insurance, storage, satellite imaging, cash handling and movements data can be added to the database too. In the U.S., for example, Geographic Targeting Orders have been used in different states and yield complete records of Money Service Business (MSB) transactions.

By adding crime statistics, criminal records, reports of investigations, open source literature in multiple languages and qualitative on-the-ground sources, such as interviews from different jurisdictions, we can make case studies, pattern analysis and the mapping of criminal networks much easier, richer in details and policy useful. Oil, trade finance, antiquities, food and agriculture, medical and arms-related data can be tracked and added to the database especially for action against terrorist groups like the Islamic State that control territory, have access to natural resources, engage in trade and perform quasi government functions that leave traces.

A Promising Way Forward

Concrete steps the U.S. Government should consider include the following:

- Ensure that all government data are gathered and analyzed in one place that can liaise also with law enforcement agencies for swift action. FinCEN, for example could be ideal for this purpose.
- With appropriate legal pathways, bring all available private sector trade data and open source data together through a trusted third party, such as a university, that can develop a system to receive, securely store and analyze them in a consolidated way. A university can generate new data and collaborate with government agencies (e.g., FinCEN) to develop patterns, identify irregularities, generate typologies and red flags, issue guidance, and produce evidence-based investigative clues. Many of the problems cited with respect to financial institutions could be resolved with this type of collective action and synergies among business and the government. The university would also help obviate the reluctance of businesses to share information for competitive reasons.

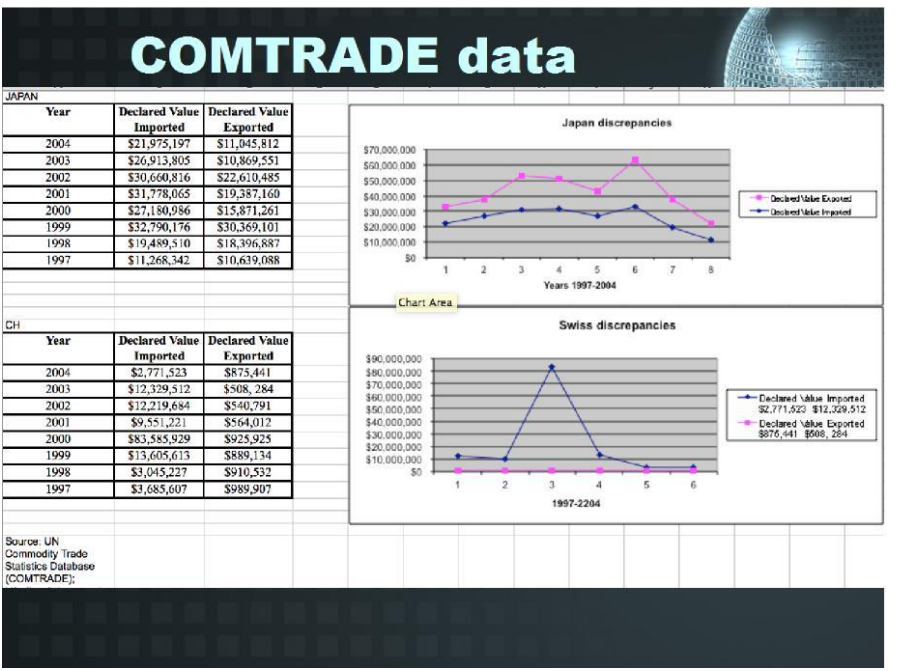
Below are some illustrations of how such analysis has been done in the past in Northeastern's NIJ-sponsored collaborations with FinCEN, DHS and the Department of Justice. It should be emphasized that the examples below do not constitute evidence of serious misconduct and crimes. Disparities may reflect errors, honest mistakes or some special commercial practices, such as inventory management and returned goods. These are clues for follow-up and investigations that can produce the necessary evidence.

The simplest first step is to compare import and export official records to see where these do not match. Items declared as exported from country A to country B, should be about the same the items declared as imported in country B from country A. This is often not the case as shown in tobacco trade statistics between the United States and Japan or Switzerland in the past.

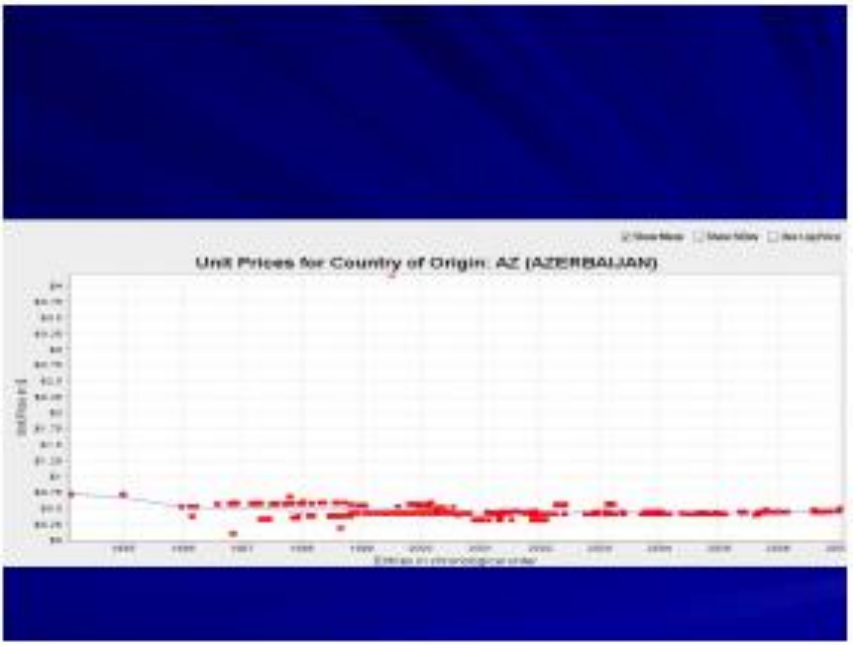
Another type of analysis is comparing declared value per unit for the same commodity in a given time period in different countries. When looking at world market prices for licorice for example, we see that these ranged roughly between $.50 and $.75 in the period between 1994 and 2007. This is what we see by looking at imports from Azerbaijan below. However, when we examine the figures for imports from Turkmenistan during exactly the same time span, we can identify substantial outliers worthy of investigation, as some values go up to $5.00. The numbers go through the roof, when we do the same analysis for Syria during the same period. In fact, the whole pattern of value is completely lost with transactions showing values in the teens and the twenties reaching all the way up to $26.00. It is certainly important for someone to

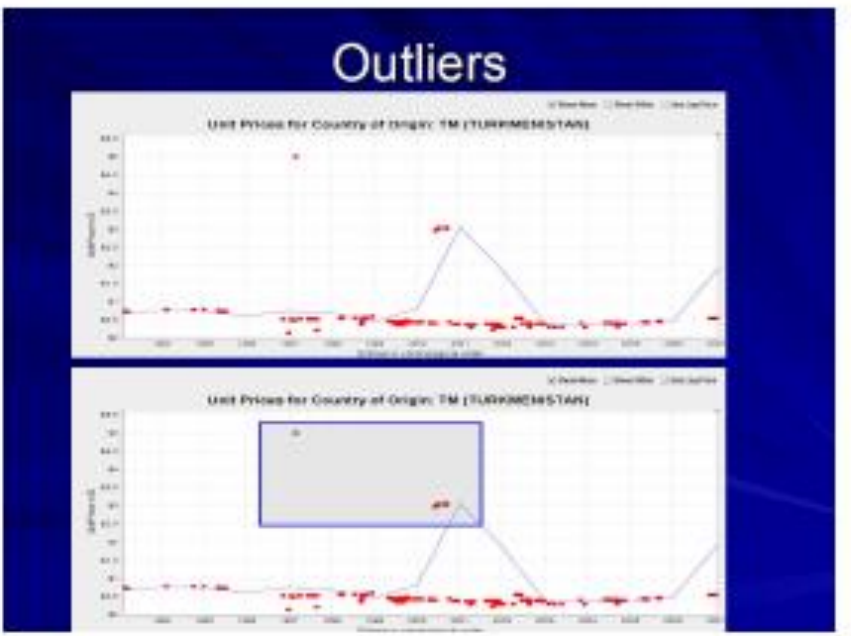
routinely and regularly monitor for such discrepancies and irregularities to find out what explains them and what action must be taken.

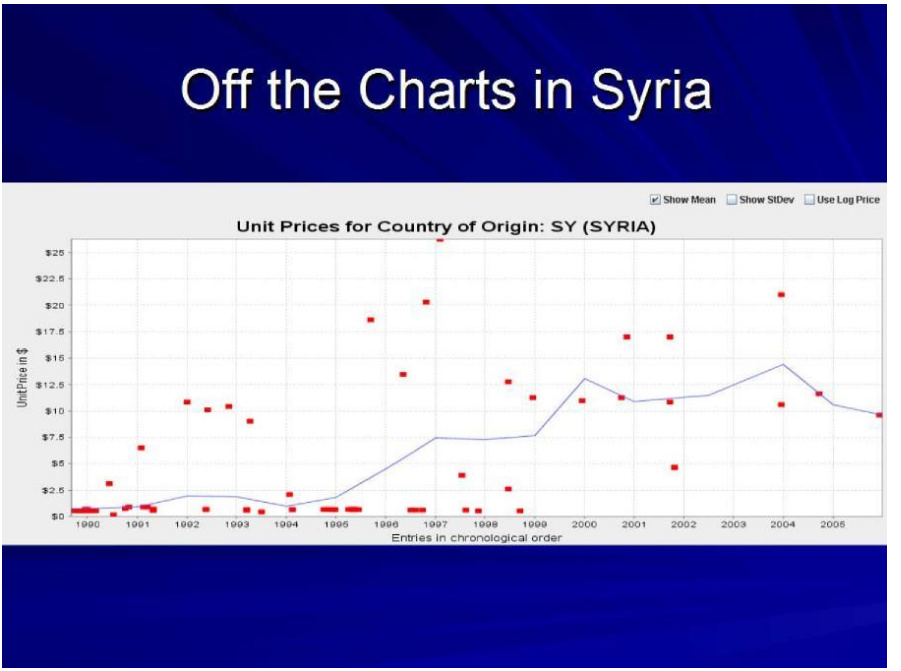
Pricing irregularities that make no commercial sense includes instances where obviously cheaper goods are imported for too high values. Scrap gold (in blue in the figure below), for example, must be much cheaper than pure gold (in red). This is the pattern observed in U.S. imports of gold from Mexico. Scrap and pure gold U.S. imports from Colombia however are all over the place. Some must ask the question who in the U.S. is buying scrap gold for double the price of pure gold and why.

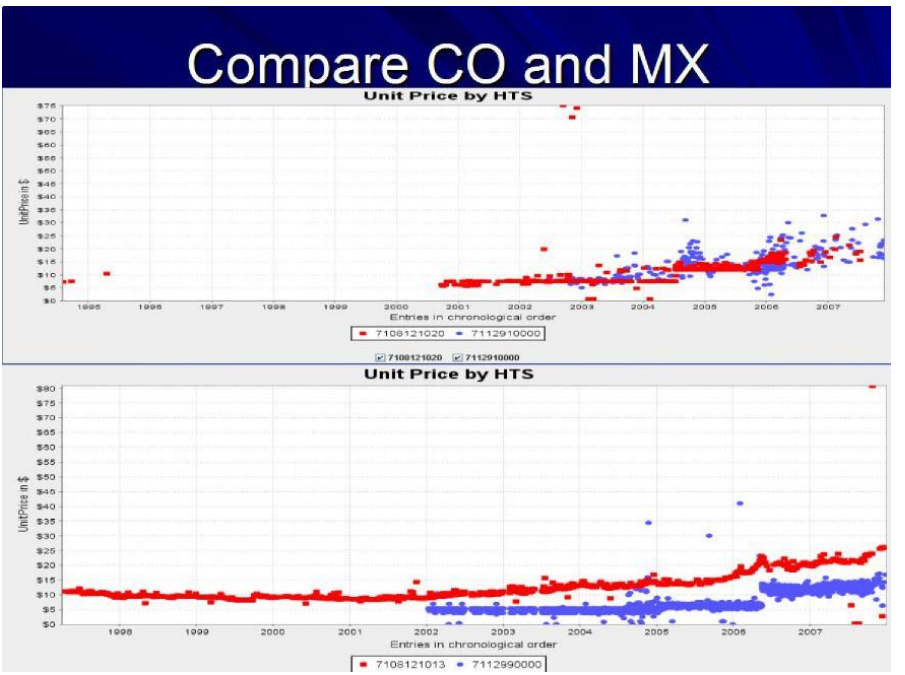


A review of diamond imports into the U.S. show how we sometimes do not know where things are coming from, where they are going and what values are moved: over a period of many years, brokers did not declare to Customs the identity of the real importers of record, but gave instead their own tax ID or someone else's. G. Britain has been declared as the place of origin and provenance of rough diamonds, even though G. Britain has no diamond mines. The declared price of polished diamonds imported from G. Britain ranged between a few dollars to $100,000 showing how diverse the value of stones is and how vulnerable this market is to mis-invoicing.


Unit Prices for Country of Origin: AZ (AZERBAIJAN)

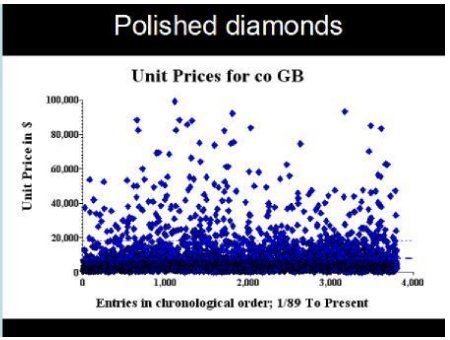

Outliers
Unit Prices for Country of Origin: TM (TURKMENISTAN)
Unit Prices for Country of Origin: TM (TURKMENISTAN)


Off the Charts in Syria
Show Mean
Show StDev
Use Log Price
Unit Prices for Country of Origin: SY (SYRIA)
UnitPrice in $
Entries in chronological order


Compare CO and MX
Unit Price by HTS
UnitPrice in $
Entries in chronological order
7108121020
7112910000
Unit Price by HTS
UnitPrice in $
Entries in chronological order
7108121013
7112990000

DATE	CO. OF ORIGIN	CO. OF EXPORT
20030709	GB	GB
20030711	GB	GB
20030715	GB	GB
20030722	GB	GB
20030725	GB	GB
20030821	GB	GB
20030822	GB	GB
20030823	GB	GB
20030827	GB	GB
20030830	GB	GB
20030910	GB	DE
20030925	GB	GB
20030929	GB	GB
20031002	GB	GB
20031007	GB	GB

Rough diamond import declarations



- Such clues and associated red flags can be communicated to banks and all relevant private sector entities for focused action and for their feedback with what information they find on such targets from their end. This can generate valuable new insights into specific targets and help control terrorist finance more effectively. A happy circle will be set off with the private sector making tangible contributions at a much lower cost.
- Update information on hawala and related IVTS methods of operation in the US and other geographic areas of concern. Methods keep changing and adapting to regulatory and law enforcement practices around the world. A new hawala review will be instrumental to more effective AML/CFT as well as control of illegal migration and smuggling. When hawala intermediaries want to help, they can. The Islamic State blackmails and steals a great deal from them too. Victims of extortion, including individuals and hawaladars can be extraordinary intelligence sources. Suspecting that this Committee may examine more in depth remittances, de-risking practices and hawala in the future, I leave a review of this issue and how hawala can be leveraged for CFT and crime control in the appendix to this statement.
- None of this is new. The feasibility of these proposals is demonstrated by the results of work on hawala, IVTS (Appendix) and trade of commodities like gold, diamonds and tobacco (above) at Northeastern in collaboration with U.S. government agencies right after 9/11 (Passas, 2004a, 2004c, 2004d; Passas and Jones, 2007). Other studies have been conducted in partnership with the Caribbean FATF to (free trade zones and financial crime in 6 jurisdictions) and with the Arizona Attorney General's office, when we combined

MSB, official and PIERS trade data to analyze a Trade-BasedMoney-Laundering case involving the U.S., Mexico and China (Passas, forthcoming). Ongoing work with Europe and M. East-based research organizations furnishes several partners ready to be enlisted in a collective action (offering data, adding resources, facilitating interviews, etc.), for instance targeting the Islamic State. This would be an excellent pilot of the general approach as the Islamic State has enemies in virtually all state and non-state actors in and around the territory they control. Similar universal condemnation and collective action took place in the financial against coalition against child pornography (see http://www.missingkids.com/FCACP), so there is good precedent for acting against serious and specific targets with consensus. Moreover, legal hurdles with data protection in Europe might be lowered as security, refugee and illicit flows have become a top priority there.

- Once positive outcomes are produced, this can be scaled up for other groups and financial crimes to include consolidated and low-cost risk analysis, regularly updated and focused guidance, training and capacity building for business and government officials.

With all this, instead of shooting in the dark, we can shed light on shadowy economic activities and go after well-defined targets. The data, the networks to produce new data, the technology for analysis, the analytical capacity, the previous experience and willingness to collaborate are all there. You have in your hands the switch to turn the lights onto what is now shadowy economic activities supporting the Islamic State, Boko Haram, al Shabab and other terror groups. I urge you to do it.

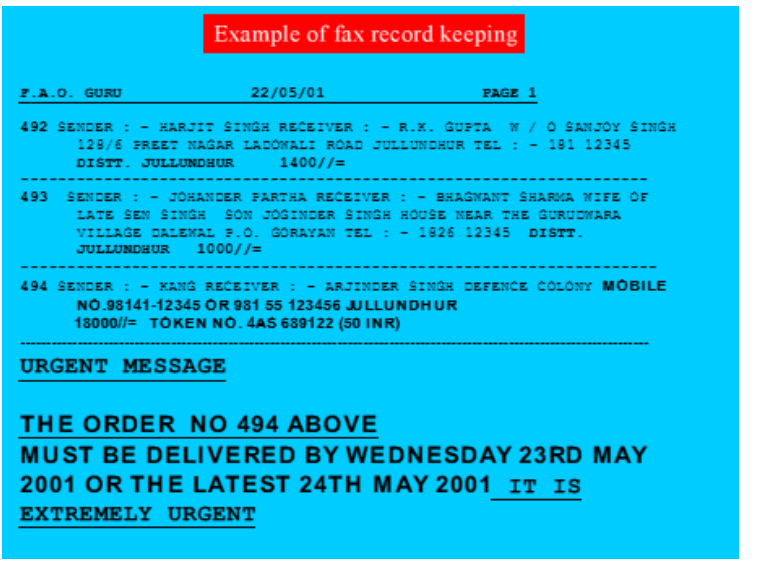
APPENDIX TO STATEMENT BY DR. NIKOS PASSAS
HAWALA MECHANICS AND CONTROL OPPORTUNITIES

Contrary to conventional wisdom, hawala and similar informal remittance channels could be a blessing in disguise. Although informal value transfer systems bring in risks and uncertainties, they also create practical and useful opportunities that could be leveraged in parallel with the international community's efforts to gradually build regulatory and governance capacity in

fragile environments. In order to appreciate these opportunities, it is helpful to take a closer look at hawala and its modus operandi.

1. The mechanics and operations of informal financial intermediaries (hawala) The word "hawala" refers to money transfer in Arabic. The operations of informal value and fund transfer systems, including hawala, have been described in works freely available online (Passas, 1999, 2003c, 2004b). More recent details on hawala routes and transactions of Pakistani and Indian networks (Passas, 2006; Razavy, 2005) apply to Somali and Afghani hawala as well (Maimbo, 2003; Orozco and Yansura, 2013; Thompson, 2011).

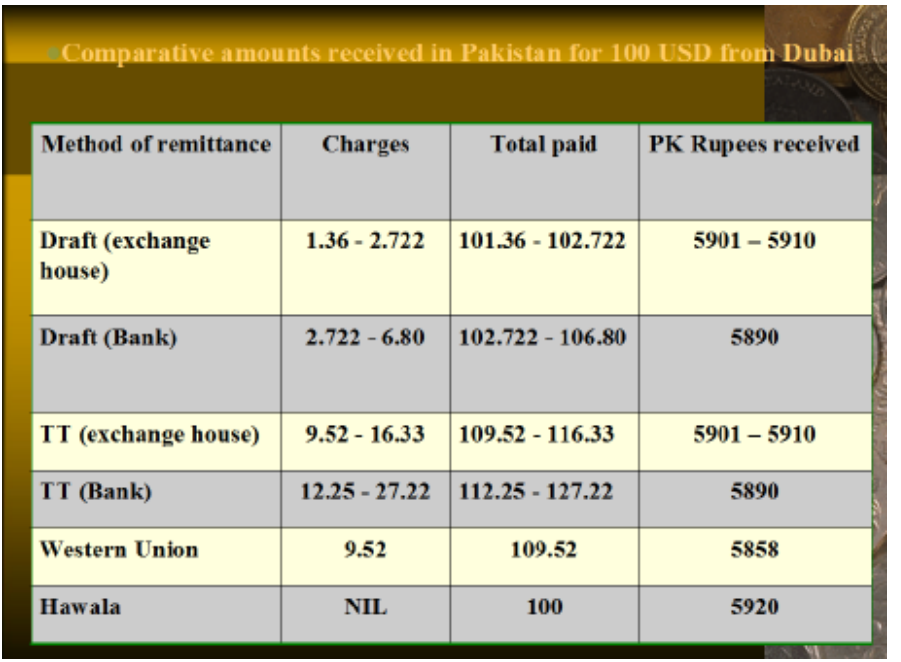
Hawala is a hierarchical network and market in which funds transfers for retail clients are tangential. The intermediaries (hawaladars) – active in different occupations and economic sectors - trade and speculate in currency in parallel to their main business. The basic way it works is as follows: migrants or donor organizations wish to send money from point A (e.g., the UK) to point B (e.g., Afghanistan). Importers and other customers want to send money from B to A. Intermediaries collect the money, organize and send payment instructions from each end and execute payment instructions received on a daily basis. Payment instructions contain a reference point for each transaction, as well as data on amount, payer, beneficiary, so if there is a delay or error, hawaladars go back to their records and sort it out.



Source: a case of South Asian hawala (names and numbers have been altered).

Figure 1. Payment Instructions.

Delivery can be made at the hawaladar's office, in a bank account or at the beneficiary's doorstep in local or foreign currency. The exchange rate they offer is much better than that of banks, Western Union or money changers.



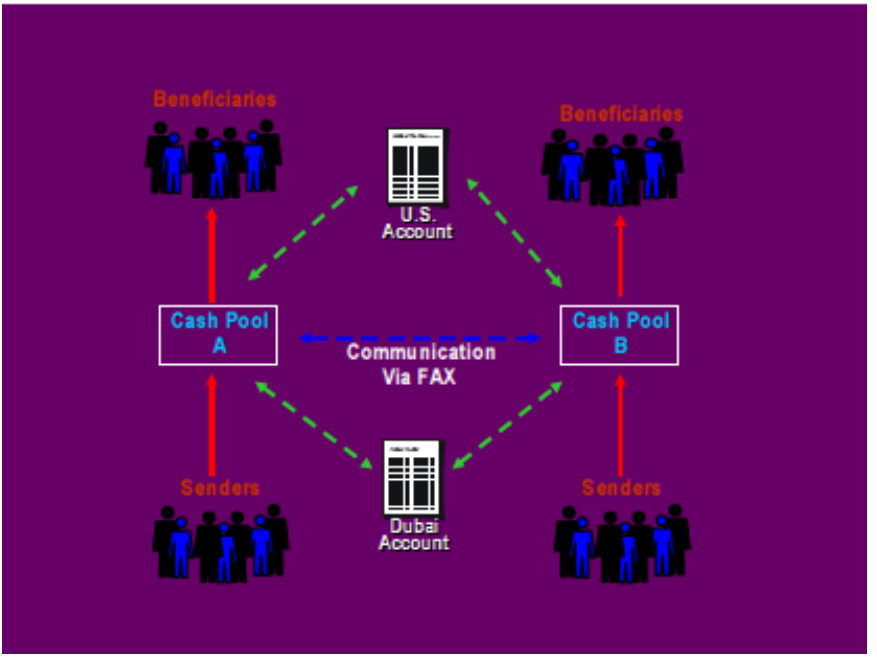
Method of remittance	Charges	Total paid	PK Rupees received
Draft (exchange house)	1.36 - 2.722	101.36 - 102.722	5901 – 5910
Draft (Bank)	2.722 - 6.80	102.722 - 106.80	5890
TT (exchange house)	9.52 - 16.33	109.52 - 116.33	5901 – 5910
TT (Bank)	12.25 - 27.22	112.25 - 127.22	5890
Western Union	9.52	109.52	5858
Hawala	NIL	100	5920

Source: Nikos Passas field research in 2005.

Figure 2. Exchanges Rates and Fees.

Efficient hawala operates with pools of funds on both ends of transactions: one cash pool in a labor-importing country like the USA on one side (pool A) and another cash pool in a remittance-receiving country such as India on the other (pool B). Each hawaladar makes payments for the counterpart's clients and minimizes the need to move money. Asymmetric flows are balanced through transfers to and from accounts held in large financial centers.

If the amounts pooled together in each jurisdiction were the same, there would be no need for either physical or other cross-border funds transfers or currency conversions. The British pounds of expatriates would cover exporters to Afghanistan, for example, while the afghanis of importers could be distributed to family recipients in Afghanistan. However, these pools are asymmetrical because people may remit in multiple directions or wish to receive funds in a third country (sometimes on behalf of another client).



Source: Passas (2003c).

Figure 3.

Account reconciliation between hawaladars occurs at regular intervals and depends on their relationship. If they are family, this may happen on an irregular basis. If they do not know each other well, they may balance accounts weekly. US dollar accounts in big financial centers (e.g., New York, London, Dubai, Hong Kong, or Singapore)[1] are typically used for this purpose.

So, the generic hawala modus operandi involves three components: (i) sending funds, (ii) delivering funds, and (iii) account consolidation and balancing. As networks evolve and grow, hawaladars engage in arbitrage and shop around for the best dollar, pound, rupee, or other currency exchange rates. Consequently, multiple intermediaries become involved adding to the complexity of hawala networks of operators, agents, subagents, clients, and clients of clients. These counterparties and clients may be traders or service providers. Travel agencies, money changers, corner shops, delicatessen shops, music stores, and import/export businesses are all often involved in hawala.

The service is fast, reliable, convenient, cheap and, in some locations, the only option. Recipients can get their money at the speed of a fax and receive their funds even when police confiscate hawala assets. Delivery at the

recipient's home benefits women who in some parts of the world do not leave their house unaccompanied. Illiteracy and lack of formal ID cards do not block access to this service, which yields more cash to the recipient than any alternative. Even small savings on the transaction cost represent significant amounts to those dependent on these flows for survival and basic expenses.

The more intermediaries join in, the less transparent transactions become to outsiders or government authorities, even in countries where hawala is authorized. *On the other hand, traceability is not lost.* On the contrary, because each node of these networks maintains records and knows its immediate counterparts, it is feasible and possibly easier to follow transactions and the money in these networks than in Western financial institutional systems[2]. Despite the mythology of paperlessness in hawala, operators create and keep records (Passas, 2006). The reason is simple: as retail, payment instruction, delivery and reconciliation transactions take place constantly, there is no other way they can keep track of what they are doing and with whom. It is a commonsense, necessary business routine. At least for the legitimate side of their business, they maintain their records for some time. Illegitimate deals may be entered in a different way or records destroyed after reconciliation is done, but this would create a red flag (Passas, 2004a).

For this reason, we need to *stress the distinction between transparency (that is, easy access to comparatively mechanized data) and traceability (the ability to find answers to investigative questions by contacting the information-rich nodes of these networks).* To the extent these nodes are open to collaboration, this is a great opportunity and low-tech tool for investigators and intelligence collectors, who can trace funds and intermediaries (Cockayne and Shetret, 2012; SIGAR, 2013) and solve important money laundering and terrorism cases.

If hawaladars do not wish to collaborate, they can obscure transactions or information about their clients. Blanket prohibitions of hawala for decades in South Asia and the Middle East (indeed, in any country with capital controls) have strengthened these networks and made them remarkably resilient and adaptable. The state neither can nor should try to abolish hawala – the question is rather how to handle and regulate it (Passas, 2003b). This is why it is helpful to engage in outreach and build communication and collaboration bridges in networks not overseen by government authorities. Such outreach can take place both in countries where hawala is legal (e.g., UAE) and where it is not (e.g., India). A FATF study reported that hawala is per se illegal in 18 out of 33 reviewed countries – 12 of the countries outlawing hawala are in the developing world (FATF, 2013). The outreach and handling of hawala players

in different cash societies will necessarily vary and would need to be based on an assessment of risk, capacity and local practices.

Absence of formal oversight does not mean that hawala is not regulated for integrity (Ballard, 2005). While trust may no longer be the most salient feature and condition sine qua non for hawala networks (Joint Narcotics Analysis Centre, 2008), there are in-built self-regulatory processes and mechanisms for dispute resolution and compliance with their own set of rules. One cannot over-estimate the significance of potential loss of reputation, honor and economic viability, as well as collective shame or ostracism suffered by dishonest participants. Violence is very rare, but has occurred in some instances in the past (Passas, 1999, 2004b).

When disputes arise, hawaladars from different locations meet and consult with each other. In some instances, there are also special bodies, such as a commission of elders in Afghanistan who assist with conflict resolution. Costs resulting from fraud or law enforcement action are usually absorbed in a shared and fair way, so individual remitters do not run a risk in established ("mature") hawala networks, esp. in S. Asia.

RECOMMENDATIONS

The first and most basic step is to establish the facts and the particular problems to be addressed in a given country, a thorough risk assessment for money laundering and related serious crimes. Well-designed research, solid data and thoughtful analysis will help produce a proper diagnosis and uncover the most serious vulnerabilities, risks and top priorities.

This is not a one-off process. Risks and vulnerabilities identified for each country need to be monitored and updated regularly with the active participation of all shareholders whose insights on irregularities and changes in the socio-political, economic and business environment are invaluable.

Attention thus should be paid to specific sectors, including remittance services and intermediaries. An open mind and shunning of misperceptions will lead to effective measures. Studies indicate that remittances are equally or less vulnerable to abuse than other institutions, contrary to regulator and bank assumptions (Orozco and Yansura, 2013; Passas, 1999; Todoroki, Noor, Celik and Kulathunga, 2014). Informal remitters may even provide an advantage in fighting terrorism and other crimes. This becomes even clearer when we distinguish between *transparency* and *traceability* of transactions.

Risk assessments may show that in some areas we are exaggerating the problem or over-shooting with controls. For instance, there is no need for enhanced customer due diligence for de minimis amounts. According to a recent survey, Somali expatriates remit an average $2,040 per annum (FSNAU, 2013). The average Somali remittance is £25 in the UK and $170 in the USA (Thompson et al., 2013). Minimal verification is appropriate for trivial amounts, which appear to be the overwhelming majority of remittances to cash societies (Shehu, 2012).

If a risk-based approach is applied to transactions lower than $200, a threshold informally discussed in FATF and regulatory circles, it could be that most transactions to Somalia, Afghanistan and other societies worry authorities and banks needlessly, while adding unnecessary compliance costs. The risk assessment should determine how much of the volume falls into this category. Enhanced due diligence efforts can then focus on large transactions, which may be a comparatively small and more manageable number.

This does not mean that low transaction flows would be left unchecked. A systematic effort could be made to connect sending and delivery actors and to compare their respective data (on clients and amounts). Inconsistencies between the two sides would be investigated and followed up. If no irregularities appear in the volumes of small transactions (i.e., no signs of structuring, nominee arrangements, amount discrepancies, etc.), then the bulk of attention would center on larger transactions. Congress should consider sponsoring and supporting the creation of a clearinghouse that allows the consolidation and analysis of sending and delivery data. Given the current Somali remitter willingness to collaborate, there is a window of opportunity to introduce a tool for the collection and analysis of data in order to detect suspicious activities.

At the same time, it is worth considering ways to leverage hawala information nodes and willingness of participants to collaborate with authorities. Hawala is a headache for controllers and bank compliance officers, but it is also a resource for risk analysis, monitoring, intelligence gathering and investigations. Outreach and good connections within hawala networks provide unique and valuable insights into otherwise non-observable shady networks and operations. It is a problem but also a solution.

The international community can help leverage the local agents' good knowledge of their clients, the ability to "smell a rat" and willingness to collaborate. Despite some arguments that informals in the UAE and Afghanistan resist state regulation, most participants desire to collaborate and contribute to AML/CFT (Todoroki et al., 2014; Vaccani, 2010). Hawala is the

only reliable means to investigate AML assets in Afghanistan, for example (SIGAR, 2013). We can raise awareness on this and promote a data linkage with the sending and settlement parts of the hawala process.

This suggests that there might be advantages to informality or at least that money laundering and terror finance risks in cash economies can be managed better. As pointed out elsewhere, "Informal remittance providers are not riskier than other financial intermediaries, while they may extend a helping hand with better governance and control in financial sectors especially in challenging environments. Hawala is a very good business model that helps communities and can foster development and humanitarian support. When traceability is possible, authorities and banks should take advantage of it rather than squander the opportunity to use such a strategic and operational tool" (Passas, 2016).

REFERENCES

Ballard, Roger. (2005). Coalitions of reciprocity and the maintenance of financial integrity within informal value transmission systems: the operational dynamics of contemporary Hawala networks. *Journal of Banking Regulation, 6*(4), 319-.

Cassara, John A. (2015). *Trade-based money laundering: the next frontier in international money laundering enforcement*. New York: Wiley.

Cockayne, James and Shetret, Liat. (2012). Capitalizing on Trust: Harnessing Somali Remittances for Counterterrorism, Human Rights and State Building. Goshen, IN: Center on Global Counterterrorism Cooperation.

deKieffer, Donald E. (2008). Trade Diversion as a Fund Raising and Money Laundering Technique of Terrorist Organizations. In T. J. Biersteker and S. E. Eckert (Eds.), *Countering the Financing of Terrorism* (pp. 150-). New York: Routledge.

FATF. (2013). The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing. Paris: Financial Action Task Force.

Freeman, Michael. (2012). *Financing terrorism: case studies*. Farnham; Burlington, VT: Ashgate.

FSNAU. (2013). Family Ties: Remittances and Livelihoods Support in Puntland and Somaliland. Food Security and Nutrition Analysis Unit - Somalia.

Joint Narcotics Analysis Centre. (2008). Hawala - Myths and Reality. London: Joint Narcotics Analysis Centre.

Maimbo, Samuel Munzele. (2003). *The Money Exchange Dealers of Kabul* (Vol. World Bank Working Paper No. 13). Washington, DC: The World Bank.

Orozco, Manuel and Yansura, Julia. (2013). Keeping the Lifeline Open: Remittances and Markets in Somalia. Washington, DC.

Passas, Nikos. (1994). European Integration, Protectionism and Criminogenesis: A Study on Farm Subsidy Frauds. *Mediterranean Quarterly*, *5*(4), 66-84.

Passas, Nikos. (1999). *Informal Value Transfer Systems and Criminal Organizations: A Study into So-Called Underground Banking Networks*. The Hague: Ministry of Justice (The Netherlands).

Passas, Nikos. (2003a). Financial Controls of Terrorism and Informal Value Transfer Methods. In H. van de Bunt, D. Siegel and D. Zaitch (Eds.), *Transnational Organized Crime. Current Developments* (pp. 149-158). Dordrecht: Kluwer.

Passas, Nikos. (2003b). Hawala and Other Informal Value Transfer Systems: How to Regulate Them? *Journal of Risk Management*, *5*(2), 39-49.

Passas, Nikos. (2003c). *Informal Value Transfer Systems, Money Laundering and Terrorism*. Washington D.C.: Report to the National Institute of Justice (NIJ) and Financial Crimes Enforcement Network (FINCEN).

Passas, Nikos. (2004a). Indicators of Hawala Operations and Criminal Abuse. *Journal of Money Laundering Control*, *8*(2), 168-172.

Passas, Nikos. (2004b). *Informal Value Transfer Systems and Criminal Activities*. The Hague: WODC. Ministry of Justice, The Netherlands.

Passas, Nikos. (2004c). Third-Party Checks and Indicators of Abuse in Cash Letter Activity. *SAR Activity Review* (7), 11-14.

Passas, Nikos. (2004d). The Trade in Diamonds: Vulnerabilities for Financial Crime and Terrorist Finance. Vienna, VA: FinCEN, US Treasury Department.

Passas, Nikos. (2006). Demystifying Hawala: A Look into its Social Organisation and Mechanics. *Journal of Scandinavian Studies in Criminology and Crime Prevention 7(suppl. 1): 46-62*(7(suppl. 1)), 46-62.

Passas, Nikos. (2007). Terrorism Financing Mechanisms and Policy Dilemmas. In J. K. Giraldo and H. A. Trinkunas (Eds.), *Terrorism Financing and State Responses: A Comparative Perspective* (pp. 21-38). Stanford, CA: Stanford University Press.

Passas, Nikos. (2008). Dirty Money: Tracing the Misuse of Hawala Networks. *Jane's Intelligence Review* (13 February), http://jir.janes.com/public/jir/index.shtml.

Passas, Nikos. (2011a). Lessons from the Countering of Terrorist Finance: The Need for Trade Transparency. In A. Chalkia (Ed.), *The Contemporary Criminality, it's Confrontation and the Science of Criminology* (Vol. II, pp. 1497-1511). Athens: Nomiki Bibliothiki.

Passas, Nikos. (2011b). Terrorist Finance, Informal Markets, Trade and Regulation: Challenges of Evidence in International Efforts. In C. Lum and L. W. Kennedy (Eds.), *Evidence-Based Counterterrorism Policy* (pp. 255-280). New York: Springer.

Passas, Nikos. (2015a). *Financial intermediaries – Anti-money laundering allies in cash-based societies?* Bergen: http://www.u4.no/publications/financial-intermediariesanti-money-laundering-allies-in-cash-based-societies/: U4 Issue 2015:10. Chr. Michelsen Institute,

Passas, Nikos. (2015b). Improving African Remittance Operations. In D. Rodima-Taylor (Ed.), *African Diaspora and Remittances* (pp. 7-8). Boston: Boston University, Center for Finance, Law and Policy.

Passas, Nikos. (2016). Informal payments, crime control and fragile communities. In SUERF (Ed.), *Cash on Trial*. Zurich: Société Universitaire Européenne de Recherches Financières (SUERF) - The European Money and Finance Forum.

Passas, Nikos. (forthcoming). *Trade-Based Financial Crime and Illicit Flows*. New York: Springer.

Passas, Nikos and Jones, Kimberly. (2006). The Trade in Commodities and Terrorist

Financing: Focus on Diamonds. *European Journal of Criminal Policy and Research, 12*, 1-33.

Passas, Nikos and Jones, Kimberly. (2007). The regulation of Non-Vessel-Operating Common Carriers (NVOCC) and Customs Brokers: Loopholes Big Enough to Fit Container Ships. *Journal of Financial Crime, 14*(1), 84-93.

Passas, Nikos and Nelken, David. (1993). The Thin Line Between Legitimate and Criminal Enterprises: Subsidy Frauds in the European Community. *Crime, Law and Social Change, 19*(3), 223-243.

Razavy, Maryam. (2005). Hawala: An underground haven for terrorists or social phenomenon? *Crime, Law and Social Change, 44*, 277-299.

Shehu, Abdullahi Y. (2012). Promoting financial inclusion for effective anti-money laundering and counter financing of terrorism (AML/CFT). *Crime, Law and Social Change, 57*, 305–323.

Shelley, Louise I. (2015). *Dirty entanglements: corruption, crime, and terrorism*. Cambridge: Cambridge University Press.

SIGAR. (2013). Quarterly Report to the United States Congress - Oct. 30. Arlington, VA: Special Inspector General for Afghanistan Reconstruction.

Thompson, Edwina. (2011). *Trust is the Coin of the Realm: Lessons from the Money Men in Afghanistan*. Oxford: Oxford University Press.

Thompson, Edwina, Plummer, Robin, Sentis, Keith, Catalano, Michael, Thompson, John and Keatinge, Tom. (2013). Safer Corridors Rapid Assessment. Case Study: Somalia and UK Banking. London: Beechwood International.

Todoroki, Emiko, Noor, Wameek, Celik, Kuntay and Kulathunga, Anoma. (2014). Making Remittances Work: Balancing Financial Integrity and Inclusion. Washington, DC: World Bank.

Vaccani, Matteo. (2010). *Alternative remittance systems and terrorism financing: issues in risk mitigation*. Washington, D.C.: World Bank.

End Notes

[1] Dubai's role is vital, because it is a commercial and financial hub for Asian, Middle Eastern, and African businesses connected with the West.

[2] For example, someone in the back office can abuse their position of trust and mix individual transactions with correspondent accounts. In such a scenario, even if the bank and its compliance office genuinely want to collaborate with authorities, it is not able to do so (interviews on an actual case in a big financial center).

INDEX

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y

Z