Chapter 10

Trade and Illicit Flows: A Case Involving the United States, China and Mexico

Nikos Passas

Introduction

Despite several major US domestic and international initiatives since 9/11, there remain significant opportunities for criminals and terrorists to evade efforts to detect and intercept their illicit activities within the global flows of money, people and goods. Financial controls, in particular, have been stepped up to try to address serious crime and security challenges. These controls are embedded within a national and international legal and institutional infrastructure that has been developed to combat proliferation activities, money laundering, terrorism finance, corruption, tax evasion and sanctions violations. Nonetheless, even if all countries and jurisdictions were to fully embrace and effectively apply the measures that are now in place, there would still be a general lack of transparency and traceability in the commercial transactions associated with the movement of goods (Passas, 2012, 2011, 2006). There also remain significant shortcomings with the current US and international cargo security programmes that rely on rudimentary intelligence-based targeting tools and an extremely limited number of non-intrusive inspections and even fewer physical examinations of cargo containers (Cassara, 2016; Flynn, 2008; Flynn 2012; Bakshi *et al.*, 2011; Young, 2017). Consequently, criminals and terrorist groups have been able to hide very high levels of illicit money flows by exploiting the limited monitoring of commercial trade through false invoicing, diversion and other fraudulent practices (Baker *et al.*, 2014; Bindner, 2016; DeKieffer, 2005; Passas, 1994; Passas and Nelken, 1993; Zdanowicz, 2009; Zdanowicz *et al.*, 1995). Additionally, currency, narcotics, weapons and other contraband continue to be smuggled within international cargo shipments (Erickson 2015; OECD, 2018).

National and international security, as well as private sector profitability, increasingly depend on making not just financial global flows visible and traceable, but the

The Handbook of Global Trade Policy, First Edition. Edited by Andreas Klasen.

flows of trade as well. Inter alia, this requires enhancing the analytical capabilities to support the work of inspectors and investigators as well as the deployment of new technological tools that can validate the legitimacy of goods moving through the global transportation system. The goal should be to develop the means to reliably verify the contents of trade flows, thereby deterring trade-based money laundering and supporting efforts to detect and interdict contraband. Unfortunately, the current practices by law enforcement and regulatory agencies including Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE) and the Financial Crimes Enforcement Center (FinCEN) fall well short of this goal. While improvements have been made on integrating various databases and enhancements have been made to the software that supports data-mining, there remain large data gaps that preclude assembling a detailed picture against which the detection of irregularities can be done efficiently and effectively. Since many analysts and investigators have limited confidence in the efficacy of new data-mining and decision-support tools, they end up relying on time-honoured methods for identifying suspicious transactions. While these methods may work for catching common criminals, they are no match for the latest tactics of sophisticated offenders and terrorist groups.

Despite well-documented shortcomings of data- and intelligence-based targeting tools, most cargo moves through the international trade system and across US borders without being subjected to inspection. This is true even though a 2007 US law mandates that 100% of US-bound cargo be subjected to non-intrusive scanning at the overseas port of loading. According to testimony by Kevin McAleenan, the then Assistant Commissioner for CBP's Office of Field Operations, before the House Subcommittee of Border and Maritime Security on 6 February 2012, the total number of containers inspected overseas in 2011 prior to shipment to the United States was just 45,500. This represents 0.5% of the 9.5 million manifests that CBP stated that the agency reviewed overseas in advance of loading. If the 45,500 number is divided by 365 days and the 58 Container Security Initiative (CSI) ports where US inspectors have been deployed overseas, the result is that these inspectors are examining with their foreign counterparts, on average, 2.15 containers per day per port before they are loaded on carriers bound for the United States (Flynn, 2012). Upon arrival in the United States, only 1–3% of containers are being subjected to some form of non-intrusive scanning to confirm if the contents match the declared cargo manifests. As the continuing occurrence of smuggling, trade fraud and cargo theft makes clear, there remains a long way to go in securing global supply chains against illicit trade (Oxford Economics, 2018). This includes preventing the scenario of transportation conveyances being used as a weapon of mass destruction (WMD) delivery device (Bakshi *et al.*, 2011).

With sobering implications for North American security, Mexican criminal groups have been particularly adroit at capitalising on the myriad shortcomings of US efforts to monitor and police global trade flows. The power of these organisations is undermining governance in Mexico through corruption and violence. Drugs and arms are big business, and Mexican traffickers have had little trouble in laundering their ill-gotten gains in ways that damage the Mexican economy. Their schemes include variations on what is known as black market peso exchange (BMPE), which was first developed by Colombian traders in the 1960s and then used by drug traffickers for money laundering (Dellinger, 2008; US Congress, 1999).

As early as 2000, law enforcement officials found evidence that Mexican drug traffickers were using non-bank financial institutions to send dirty money to China to purchase goods such as clothing items. These goods were exported to Mexico through the US in-bond system. After the goods arrived in the United States for trans-shipment to Mexico, the process was manipulated at the border to falsely declare the cargo to be US-manufactured goods, thus avoiding the very high Mexican Customs duties applied to many Chinese imports. These goods were then sold within the Mexican economy at discounted rates, providing traffickers with "clean" pesos for their illicit proceeds. These schemes have benefited from the nominal oversight by US authorities of outbound commercial trade flows into Mexico as well as the limited effort by Customs authorities on both sides of the border to fully exploit proven technological tools and applications for better detecting fraudulent shipments (Wilkinson and Ellingwood, 2011).

This study illustrates the fragmented, unsystematic and wasteful way in which trade integrity is approached not only in Mexico and the United States but also globally. It is consistent with the view that efforts to counter illicit trade are inadequate even though data exists, software for big data analytics is available and expertise can be found to make optimal use of these resources (Passas, 2016). The study uncovered preliminary evidence, gathered from active and retired law enforcement officials, of substantial outflows of US dollars to China through money service businesses (MSBs) that suggest remitters and agents engaged in purposeful actions to reduce the risk their transactions would be identified as suspicious by government authorities. The study also identifies ways that existing data and technologies could be improved upon to help reveal ongoing conspiracies, identify likely offenders and support the seizure of criminal assets to the extent that strong investigative clues, hints and leads can be produced by the suggested approach, so that both government and private sector leaders will be able to undertake a more comprehensive and systematic approach to preventing criminal and terrorist groups from exploiting global trade flows for nefarious purposes. This study also finds that, given the significant limitations of current intelligence-based analytical tools, efforts to improve those tools should be made in parallel with more widely deploying technologies that can support the monitoring and non-intrusive scanning of cargo and conveyances.

The chapter proceeds as follows. It first outlines the methods and data used for the study. It then provides some information about the processes that have been developed by US Customs authorities for detecting and intercepting criminal activities within trade movements. It then proceeds to examine the vulnerabilities of trade-based money laundering in cargo flows across the US–Mexican border. It then provides evidence of transaction irregularities revealed by this study that suggest that trade-based money laundering involving China, the United States and Mexico is ongoing, while also identifying additional problem areas that warrant close attention by US and Mexican authorities. The chapter concludes with some recommended next steps to address the serious issues highlighted by the study.

Methods and Data

The study began with a review of open-source materials and interviews with enforcement officials in Washington, DC, and Arizona. Data for financial flows from and to the southwest US states via non-bank financial institutions were collected by the

Arizona Attorney General's office and shared with Northeastern University according to terms governed by a Memorandum of Understanding. Specifically, the focus was on fund transfers from three US states (Arizona, California and Texas) to China. The objective was to identify irregularities in US–China flows outside the banking sector where trade finance and related transactions are normally done. Finally, a sample of private sector data on import/export activities was collected from the commercially available Port Import/Export Reporting Service (PIERS) database that tracks information on US imports and exports to assess the likelihood that goods exported from China to Mexico were moving through the US in-bond system to Texas where they could potentially be compromised before they were sent on to Mexico.

Detecting and Intercepting Criminal Activities within Legitimate Trade Movements

After 9/11, the two groups of officials that made up the then-US Customs Service inspectors and agents were split into separate agencies that were incorporated into the new Department of Homeland Security. The inspectors were placed within CBP, where they were assigned oversight of the arrival and payment of duty on cargo. The agents were placed in ICE. While the responsibilities of inspectors and investigators remained relatively unchanged, their activities ended up becoming more isolated from each other. Ironically, while the attacks of 9/11 resulted in efforts intended to strengthen collaboration and information-sharing across the intelligence community, the CBP/ICE split had just the opposite outcome, disrupting longstanding intra-agency collaborative arrangements between inspectors and agents.

For instance, once the US Customs Service was broken apart, agents in ICE lost their capacity to directly access the automated commercial data systems operated by CBP. CBP inspectors, in turn, do not have routine access to the Data Analysis & Research for Trade Transparency System (DARTTS), a proprietary system developed to create a common interface for a variety of entry-related documents including Automated Manifest System (AMS), Automated Commercial System (ACS), Custom and Border Protection Form 7501 (goods "Entry Summary"), Currency and Monetary Instrument Reports (CMIR), Currency Transaction Reports (CTR), Foreign Bank and Financial Accounts Reports (FBAR), Suspicious Activity Reports (SARs), Form 8300 (Reporting Domestic Currency Transactions) and a wide collection of import and export data provided to the United States by other countries. At present, DARTTS is mainly distributed to a select group of criminal investigators. Additionally, the division of data and tools ended up fragmenting established control systems, potentially raising the risk of abuse.

While post-9/11 organisational changes had the unintended effect of eroding the ability of inspectors and agents to closely collaborate, several new initiatives were launched to enhance the capacity of Customs authorities to better detect and intercept dangerous contraband. Of greatest concern was the risk that terrorists might smuggle a WMD or nuclear-related materials into the United States concealed within the legitimate trade system. To provide more time to evaluate the risk that a cargo shipment might be present within a shipment, CBP began requiring that manifest data be transmitted electronically 24 hours before the cargo was loaded on a ship destined for the United States from an overseas port. In 2009, CBP began requiring additional information pertaining to cargo brought to the United States by vessels under the Importer Security Filing "10+2" Program. These data were then transmitted to the US National Targeting Center-Cargo to decide on whether the cargo might pose a risk and therefore should be examined. A total of 58 ports from around the globe have agreed to participate in the CSI whereby US Customs inspectors are deployed overseas to work with their counterparts to inspect cargo identified as high risk.

The Vulnerability of the In-Bond System on the US–Mexican Border

Mexican crime thrives on the profits from sales of illicit narcotics in the United States. This brings with it the attendant challenge of repatriating these earnings into Mexico. Law enforcement and media reports (Coleman, 2006; Holmes, 2012) suggest that Mexican traffickers have devised sophisticated money-laundering operations that exploit trade transactions associated with the flows of legitimate commercial products. Indeed, it is likely that illicit flows first identified by US and Mexican authorities a decade ago continue largely unabated today. The most recent mutual evaluation of Mexico's anti-money-laundering efforts is insufficient and undermined by corruption (Financial Action Task Force [FATF] and Financial Action Task Force on Latin America [GAFILAT], 2018). Specifically, what is known as the black-market peso exchange (Dellinger, 2008; James *et al.*, 1997) or trade-based money laundering (FATF, 2006; Liao and Acharya, 2011) may be at the centre of the traffickers' money-laundering activities. These schemes involve the use of crime proceeds from across the United States to place orders for goods produced in China and other countries. These goods are then sent to Mexico or neighbouring countries and sold so as to generate pesos that appear to be derived from legitimate commercial activity. The basics of trade-based money laundering have been described in the following way.

"Instead of smuggling the money the old-fashioned way, by simply carrying it south in bags and trucks, teams of money launderers working for cartels use dollars to purchase a commodity and then export the commodity to Mexico or Colombia. Paperwork is generated that gives a patina of propriety. Drug money is given the appearance of legitimate proceeds from a trade transaction. By turning their mountain of proceeds into tomatoes, say, or bolts of Chinese fabric shipped and resold in Mexico, cartels accomplish two goals at once: They transfer earnings back home to pay bills and buy new drug supplies while converting dollars to pesos in a transaction relatively easy to explain to authorities. Long used by Colombian cartels, the scheme is becoming more popular with Mexican traffickers after new efforts to combat laundering by restricting the use of dollars. Those restrictions, plus proposed limits on cash purchases of big-ticket items such as houses and boats, make it less attractive for traffickers to hold trunks full of US cash. After many years of using dollars to buy luxury items and pay their suppliers and dealers, cartel capos have suddenly found themselves in need of pesos. Trade-based money laundering solves that problem" (Wilkinson and Ellingwood, 2011).

One way that drug traffickers have been able to get their cash into the financial system is to deposit it in multiple transactions via the non-bank financial sector in bundles under US$10,000. These smaller deposits are made to avoid triggering cash transaction reports that financial institutions are required to make to US authorities. Wire transfers can then be combined overseas to purchase textiles, toys, perfumes and other goods in Asia. A case involving the Angel Toy Corporation in Los Angeles illustrates this money-laundering scheme, which involved the collection and structured deposit of the proceeds of illegal drug sales to purchase goods from China. In this instance, the goods were shipped from China to South America, to be sold in retail outlets, from where the proceeds were passed on to the criminal entrepreneurs (Wilkinson and Ellingwood, 2011).

Mexican traffickers may also be exploiting the in-bond process that allows goods that originate outside of North America to move through the United States for delivery in Mexico. The normal routine for an in-bond shipment is for cargo to move unmolested through a trans-shipment country. However, along the Texas border with Mexico, in-bond shipping containers arriving by train from the US West Coast are offloaded on the Texas side of the border. Then, Customs bonded *cartmen* transfer them to local warehouses. *Cartmen* are subjected to a mandatory background screening by CBP and issued a licence. They are required to post a bond that will automatically be drawn upon to pay a penalty should CBP find that there has been a violation of any prescribed procedures and protocols when carrying transit cargo from one Customs location to another (e.g. from a railhead to a port). The risk of this penalty is to provide an incentive for *cartmen* to maintain constant custody and control over a shipment. However, at the common warehouse, the seal applied to the container door is broken, and the goods are then removed from the original container in which they were shipped and reloaded for movement across the border by truck.

According to interviewees, the rationale for this cumbersome repacking procedure is that it is supposed to facilitate the inspection and confirmation of the contents of the imported goods in order to ensure that they match what is described in the cargo documentation. This procedure has been advanced as a necessary contingency for lowering the risk of major delays and fines that Mexican importers face when the Mexican Customs inspection process identifies discrepancies between the shipment and the associated documentation.

The procedure of repacking in-bond container shipments on the US–Mexican border creates a significant opportunity for fraud. For one thing, the supporting paperwork provided to Mexican Customs officials could potentially be altered to declare the goods as originating in the United States instead of China. In this way, the shipment can take advantage of the terms of the North American Free Trade Agreement (NAFTA) that has fuelled a tremendous upsurge in trade between the United States and Mexico over the past quarter century. NAFTA allows for goods that originate in Mexico, Canada and the United States to be shipped within North America without incurring Customs duties. By fraudulently declaring overseas imports to be “Made in the USA”, traffickers can sell the goods in Mexico at a considerable discount. Beyond the laundering of illicit profits, this illicit activity causes two other negative effects. First, the Mexican government is deprived of revenue. Second, legitimate companies who produce similar products in Mexico, or import them and pay the required duties, are placed at a competitive disadvantage when their goods must go up against those merchants.

In short, Mexican traffickers are able to take advantage of the lax oversight of in-bond shipments by US authorities to relabel Asian imports as US goods and export them duty-free to Mexico. The scale of the opportunity is likely to be considerable since each year ocean containers with billions of dollars of in-bond shipments arrive by rail in Laredo, Texas, and other border areas. Once these goods are unloaded at common warehouses and then transported by the local truckers for the short trip across the border into Mexico, they are unlikely to receive any scrutiny by US Customs inspectors.

But it should be possible to reduce this vulnerability since illicit flows invariably leave traceable marks that should raise red flags for law enforcement. For example, shippers might be making different declarations about the contents of the same shipment to authorities in the originating, transiting and final jurisdictions. If those declarations are shared and compared among Mexican, US and Chinese authorities, irregularities and discrepancies will be revealed. It would be a simple matter of (i) checking that goods stamped as exported do indeed cross the border; (ii) cross-checking declarations/export documents presented to Mexican Customs authorities about US-origin fabrics and other goods; and (iii) reviewing the declared US exporters to ensure they are legitimate traders. Additionally, data held by private sector entities involved in shipping the goods can be analysed to assist in detecting anomalies; for example, Union Pacific Railroad maintains records showing the arrival time of the in-bond containers that it transports to Laredo from the West Coast and the recipient who assumed custody of the shipment.

This important vulnerability could also be addressed by ending the practice of unloading in-bond shipments from their original container at the US side of the border and reloading them for shipment by truck into Mexico. The contents of a sealed container can be confirmed as not having changed while in transit by subjecting the container to scanning via non-intrusive inspection technology.

More close monitoring of trade flows can be an important complement to other anti-money-laundering efforts. Indeed, any effort to combat the financial crimes that facilitate serious crimes or sophisticated terrorism requires a comprehensive approach that simultaneously takes on the "challenge of three global flows": financial, commercial and informational (Passas, 2017). While significant efforts have been made to better police financial flows and to bolster the transparency and accountability of informational flows, much work remains to be done toward strengthening the integrity of physical movement of commercial flows within the international trade system. This is especially the case with the in-bond system.

Our Approach

There are several sources of data that are being routinely incorporated into efforts to better manage the risk of misconduct through trade. These include Bank Secrecy Act (BSA) financial data, arrival and departure data as declared to CBP by traders, investigation reports, criminal records and foreign government data (including Mexico). With the development of DARTTS, Customs agents and inspectors are provided with access to all these databases. In addition, Customs officials have new means to evaluate financial data that support tracking commercial and financial transactions and the movements associated with imported goods using common identifiers, such as the importer number.

Nonetheless, our study has found that there are ordinary business data that are not being used by Customs authorities, even though these data could help them make more accurate predictions of what shipments arriving in the United States could be compromised and therefore should warrant an inspection. For instance, data routinely collected by ocean carriers used to manage their cargo-handling operations could support efforts to more closely monitor the movement of cargo and identify irregularities. These data can help to develop baseline patterns of “normal” cargo movement. Such baselines can make it relatively straightforward to identify trading anomalies in much the same way as an air traffic controller can spot flights that deviate from established flight patterns. This provides a way for an investigator to develop leads. It should be possible for a third party, such as a university, to develop a system to receive, securely store and analyse business data that could then be used by inspectors and agents to develop patterns and spot anomalies.

To test this hypothesis, we set out to gather data about trans-Pacific shipments of cargo destined for Mexico via the US in-bond systems. Specifically, we received private sector data from two sources. First, we partnered with the Arizona Attorney General’s office and obtained the complete dataset of financial flows collected by that office from six non-bank MSBs. Second, we obtained a small sample of commercial data provided by the PIERS. Analysis of this data appears to substantiate that trade-based money laundering is taking place using US MSBs to send funds to China to purchase Chinese low-cost goods that move through the US in-bond process so as to take advantage of the vulnerabilities in that system to enter Mexico while evading duties and tariffs.

Analysis of MSB Data and Findings

Several years ago, the southwest region of the United States organised a Southwest Border Anti-Money-Laundering Alliance that began collecting the complete set of remittances from and to the United States made through MSBs within Arizona, California and Texas. The Arizona Attorney General’s office provided us with data from 3 January 2005, to 29 June 2012 for analysis. These records included information from six companies that we have designated as C1, C2, C3, C4, C5 and C6. The records include information on the sender, payee, amount, date, recording agent and paying agent, country, sender identification number, occupation, address and phone, and payee occupation. In total, the data filled 70 fields.

The Arizona Attorney General’s Office relies on a consulting company to organise the MSB data it receives. An early challenge we faced in subjecting the data to analysis was that we found several problems with the reliability and accuracy of some of the fields, especially with respect to country codes, names of transaction parties, telephone numbers, sender identification numbers and addresses. We suspect (and interviewees agree) that some of these data inaccuracy problems may have arisen as a result of remitters and agents who showed little interest in ensuring transmitters provided complete and accurate information even though that information is central to the capacity for authorities to detect suspicious transactions.

One common problem was that first and family names were not in separate fields to allow proper sorting and retrieval of the information. For instance, the Arizona database listed within a single column the first name, the middle name, the last name and generational suffixes such as "senior" or "junior". It also included forms of salutation such as Mr, Mme, Miss etc. There were also problems of consistency when it came to ethnic names such as Spanish names that may include both the father's family name and the mother's family name. Some of the names were also entered in different versions (shorter and longer ones, different sequences and complete versus incomplete names). The fields were rife with typographical errors, or in some cases, fields were left totally blank.

We encountered similar problems with variations in the information provided in the address field. Many times, the telephone numbers were either empty or the entry contained random numbers, probably to avoid giving the correct information. For example, there was sometimes just the area code, or a series of zeros or simply sequential numbers such as 123, 123 – 456 – 7890, which limits the utility of the field.

There were also problems with the way country codes were entered to include inconsistencies both within and across the data provided by the six remitting companies. These included people's names added to country code field or strange combinations of numbers such as "Jesus", "Maria", "B1", "85586".

The identified problems affected the majority of the funds destined to China. We, therefore, had to create routines and clean up the data on a sample basis. Once this was done, it improved the usefulness of the data dramatically. For instance, we were able to identify when variations of the same name were used with the telephone number. We were also able to identify when multiple senders used the same telephone number. Ideally, similar routines and methods could be replicated by the Southwest Border Anti-Money Laundering Task Force to clean up the entire database.

One of our first steps was to do a financial volume analysis by examining total volumes and the destinations for the MSB companies. In doing this we found that the MSB designated as C5 dealt mainly with South America, and when aggregated, senders were below US$200,000 for the entire period. C4 dealt mostly in 16 countries in South America, with Mexico being the main destination. C3 dealt also with 16 countries, with Mexico again being the top declared destination or paying agent location. We found that the total amount sent to Mexico was over US$1 billion between 2005 and 2012. C1 was the largest operator, with a total of 23 million records. The top destination was again Mexico, where the total amount sent was US$7 billion during the period we examined.

C1 is the most interesting part of the database for our case study because it both illustrates problems with the data and has the largest volumes around the world. Most importantly, it is the only MSB in the database with financial flows to China. Therefore, for our purposes, it made sense to focus mostly on C1 data.

The total amount wired via C1 to China in the study period was US$1,156,566,352.61 in 597,517 transactions or an average just above US$1935 per transaction. In addition, US$421,231,818.71 went to "CN" (also China) in 228,923 transactions (average US$1840/ transaction), US$20,023,520.46 went to "Hong Kong" in 11,319 transactions (average of US$1769/transaction) and US$9,074,981.70 went to "HK" (also Hong Kong) in 5797 transactions (average of US$1565.46/transaction). Finally, US$408,648.91 was wired to Macau in 377 transactions (average of US$1083.94/ transaction). In short, the data demonstrated that a considerable amount of money is going to China in small transactions from the Southwest United States through C1.

Given that money going to China was our main interest, the next questions we wanted to answer were who has been placing funds into the financial system and sending them to China, how many of these transactions were made by the same people and what sort of irregularities could be spotted in the data. In trying to accomplish this task, one obstacle we faced was that the sender names were often missing. For instance, we found that there were nine transactions for a total of US$447,267.57 that did not list the sender names. Another obstacle was that there were clearly erroneous entries made in the records, such as "133100". Given the obligation of remitters and all MSBs to properly record identifiers for transacting parties, these practices reflect a heedless carelessness that suggests that transactions may have a suspicious origin. In some cases, there was a name but it was mistakenly placed in a different field in the database.

Once we identified the senders, we listed them by volume. This revealed that some senders were making hundreds of transactions over the period. The total value of each of these senders' transactions was often over half a million dollars. The individual transmissions averaged from more than US$1000 to just under US$7000 per transaction (amounts below the US$10,000 level avoid triggering a mandatory report by the MBS).

These patterns are irregular for businesses, both because legitimate importers would not use this payment vehicle and because the amounts are too structured in small pieces, which translates into the sender paying fees for making each of these many small transactions. If the funds were indeed legitimate, it does not seem likely the senders would be willing to incur these extra costs. This prompted an inquiry into the payees for these transactions, which showed lower amounts for each payee, showing that senders have been transferring funds to more than one payee over this period.

The next step was to see whether searching by the payee phone numbers would yield a better aggregator. This revealed that the phone data were extremely poor and problematic: in just one entry, for example, there were missing numbers for US$390 million and 203,543 transactions. When we narrowed the analysis to total amounts over US$500,000 in the study period, we found that hundreds of millions of dollars flow through the system to China (and other places as well) with the authorities never receiving proper information on the sender's telephone number. As we inquired more into the recipients of funds in China, our analysis revealed that the payee designated as AS25 had the highest total amount, with a value of US$1,319,943.00 and a count number of 272.

The next step was to see how much open access information we could gather on these recipients. We were able with simple online searches to track down several of them, who happened to have trading businesses. AS25 turned out to be located in Guangdong Province and has a website with company profile, contact (with the phone number we had in our data) and other details.

In another example, we found information on an individual who listed a Los Angeles, California, address and with a business listed as "China Manufacturer – T-Shirts – Apparel". In yet another example, we located information on multiple entities linked to an individual who was listed as operating a furniture company in Guangdong and Los Angeles as well as several technology companies in Shenzhen. In short, the data identified that the largest recipients of the funds appear to be traders in China, as hypothesised.

Going back to the top payee in China, AS25, we were able to link him with two senders from the United States, one of whom used two ways of entering the name field. Moreover, we found that AS25 had been using multiple telephone numbers entered in the data for different sets of transactions. Further analysis of several China payees showed that many of them were traders and used multiple telephones, multiple senders and numerous transactions in small amounts. This way of doing business makes no logical or commercial sense. The amounts and partners are too fragmented into a few thousand or hundred dollars per transaction with identifiers that are inconsistent, incomplete or missing altogether, and to reiterate, the very use of MSBs for trade purposes is unusual and costly.

To summarise, the Arizona database provided valuable insights that are suggestive that considerable funds are being moved by remitters to China to undertake trade-based money-laundering schemes. The data also point to numerous additional irregularities.

The first pattern noted was that tens of millions of dollars were going to stored value cards. In other instances warranting further inquiry, we found several senders using different telephone numbers. Some of them were Asian, but the practice goes beyond China. The extent of structuring that was going on by senders with no name entered was also found to be quite remarkable. Finally, even when a known commercial name was entered, questions can be raised with respect to the excessive number of transactions used at MSBs for very small sums, even when the total amount was in the millions.

PIERS Data

We requested PIERS data for Los Angeles in-bond shipments of goods originating in China. We received these data covering one month (January 2010), for which there were a total of 11,229 records in total. The main issue we wanted to confirm was the movement of textiles and similar goods from China through the in-bond process.

Small as the size of this sample is, the data confirm that clothing and other items do come to Los Angeles from China and go through the in-bond process, the majority of which then go to Texas, as hypothesised.

Several of the shipments go to Laredo, Texas, but much higher volume is going to Dallas, Houston and El Paso, with a smaller amount going to San Antonio and other cities.

We were not able to gain access to Customs declarations made to Mexican authorities. For this reason, we were not able to document that these in-bond fabric shipments were re-characterised as originating from the United States. A follow-on study that includes data from Mexican Customs officials could confirm this. It is important to note that the financing used in the trade-based money-laundering schemes identified in this study differs from the kinds of transactions that the banking sector normally uses in financing trade. In a legitimate trade transaction, the bank requires that contracts be signed overseas that specify the goods to be purchased, the destination of where they will be sold and the means that will be used to move the goods. These requirements are made because banks do not want to be duped into providing funds for "phantom shipments". In other words, the bank needs to be satisfied that the goods exist before it agrees to serve as the financial backer for the purchase of those goods. Further, the bank will not make payment until it is provided with the bills of lading and Customs entry documentation since it wants to be sure that the goods are not being held up by Customs authorities, but are available to be sold into the economy.

In short, for legitimate trade transactions, it is customary for importers and their bankers to be involved in the purchase of cargo from start to finish. The cargo would be picked up at the supplier site, transported to a port, loaded on a ship, moved by ship to the destination port, unloaded and delivered to the purchaser. In some instances, the goods might be put into the in-bond system for trans-shipment through the United States to the border region for importation into Canada or Mexico. All these transactions would be fully documented. For in-bond shipments, the banks would be waiting for the document showing the movement of the container across the border into Mexican territory and would likely require that Mexican Customs documents be submitted as well to verify that the goods were on their way to their intended destination. At that point, the banks would release the funds to support payment of the trade transaction. In short, when normal trade financing is involved, banks end up ensuring that there is a clean trail of documentation as a condition of underwriting the transaction.

However, when large trade purchases are being made by bundling small transactions transmitted by US-based MSBs to China, such purchases will not involve bankers looking over the importer's shoulder. Without this check in the system, a dishonest importer can more easily alter the documentation after it arrives in the United States. Normally goods moving as a part of the in-bond system would require a declaration to the Mexican authorities that the goods originated outside North America. But for the trade-based money-laundering scheme outlined in this study, the documentation can be changed to falsely declare that the goods originated from the United States without there being an auditable paper trail at a financial institution that could prove otherwise. Lacking such a basis to challenge the false declaration, Mexican Customs authorities are compelled under NAFTA rules to allow the goods into the Mexican economy without having to pay heavy Customs duties.

Next Steps

Even by drawing on a relatively small set of commercial data sources, limited in their quality, size and time duration, the study was able to uncover evidence of suspicious transactions that suggest trade-based money laundering is exploiting gaps within the US non-bank financial sector and shortcomings in the oversight of the import and in-bond system. This is taking place despite the stepped-up efforts since the attacks of 11 September 2001 to enhance the monitoring and analysis of trade data to identify anomalies that might point to supply chain security risks. Specifically, the study findings show that there are substantial flows of money moving out of the southwest region of the United States by way of MSBs. These money flows are being structured into small amounts that are well below levels that trigger a reporting requirement by the MSB. The aggregated transactions result in large amounts of money finding their way to recipients in China in ways that make no commercial sense given the fees involved. These recipients appear to include Chinese exporters who ship goods such as textiles to Mexico by way of Los Angeles and via the

US in-bond system. These shipments may not be showing up in Mexican statistics as Chinese imports. Instead, because banks are not providing financing and serving as intermediaries for these transactions, it is likely that dishonest importers are manipulating the importation process and falsely declaring to Mexican Customs authorities that the goods have originated from the United States and therefore are not subject to duties. The findings of this study also revealed additional irregularities that point to other possible fraudulent activities that warrant investigation by law enforcement authorities.

The implications of the above are threefold. First, Customs authorities have been overlooking important sources of business data that could support their efforts to more effectively detect and intercept illicit activities involving international trade flows. Second, national security officials should re-evaluate the extent to which they are relying on the current targeting capabilities of Customs authorities to identify cargo that may pose a threat. A system of controls that Mexican and US criminal organisations appear to be successfully working around to repatriate their illicit drug profits is hardly up to the task of detecting a sophisticated terrorist conspiracy intent on smuggling a WMD into the United States via the global supply chain. This leads to the third implication: a renewed effort should be made to identify and integrate new technologies that can more closely monitor and verify the contents of international trade flows.

A great deal can be accomplished towards making trade flows more transparent by simply ensuring that data are entered correctly by mandated reporters through closer monitoring of the data's quality. Also, existing data sources could be better organised and additional sources of business data could be used to provide a more comprehensive picture of all the transactions associated with a given trade flow. Collectively, these sources could be integrated into software-based analytical systems that are used by Customs inspectors and investigators looking for clues of illicit activities. The Document Archiving, Reporting, and Regulatory Tracking System (DARRTS) system can integrate all such data, as well as financial data, and enable comparisons and analysis indicating where manufacturers in the United States understate or overstate the quantity of goods they are exporting to Mexico. The DARRTS system could also be refined to support the analysis of other evidence of trade-based fraud, such as irregular pricing and the use of similar or other names to engage in nominee trade.

The goal should be to develop as detailed a picture of legitimate flows as possible, thereby creating a baseline for identifying anomalous behaviour that indicates the likelihood of illicit flows. When analysts who understand shadow financial and commercial activities evaluate anomalies, they can develop leads for investigations. These investigations are likely to result in significant asset seizures that, in turn, can help provide additional resources to fund advance training and the development of new applications to support the sustainable and long-term success of control efforts against serious crime and security threats.

Systematic comparisons should also be made between the documentation that US authorities possess for exportation of in-bond goods from the United States and the documentation that their Mexican counterparts received for the importation of goods in Mexico. Such routine reconciliation of data would allow for the detection of in-bond shipments from Asia that are fraudulently characterised as goods that originate from the United States. This study suggests that if US and Mexican enforcement agents perform this analysis, they will find, for instance, that textiles that are manufactured in China are being routinely imported into Mexico as having been "Made in the USA". Cross-border reconciliation would also detect blatant discrepancies in the reporting of quantity and value of goods.

Finally, there should be much closer monitoring of border warehouses and businesses repackaging in-bond shipments. These entities should be required to provide data on when they assume custody of in-bond goods and how and when they are loaded on "over-the-road-trucks" to move into Mexico. An even better solution would be to eliminate this procedure altogether. In-bond shipments could be scanned by using non-intrusive technology at the overseas port of loading and/or at the US port of arrival. When these goods arrive at the US–Mexican border, they could be scanned again so that US and Mexican authorities can compare the images. There should be no reason to break the seal of a bonded shipment at the US border if the images do not reveal evidence of tampering during trans-shipment.

Conclusion

Much can and should be done to improve the current efforts to detect and intercept criminal and security threats involving global supply chains. Too much commercial data is left unexamined, scattered among databases and subjected to fragmented analysis across different agency units. Adequate resources have not been allocated to harness new technologies that can make global trade flows far more visible and accountable. This reality should be a substantial cause for concern for policymakers, law enforcement agents, national security officials and civil society.

At the same time, this study points to the still largely untapped expertise that lies outside the US government that could and should be enlisted in enhancing global supply chain security. The private sector can be engaged to make their legitimate transactions more transparent so that they can be more closely monitored. Academic institutions such as Northeastern University can collect commercial and open-source data, and integrate and analyse that data to find anomalous behaviour that might point to criminal and security risks. Universities can serve as honest brokers by entering into agreements with the appropriate safeguards that allow them to undertake research by acquiring, developing, storing, updating and maintaining sensitive databases from both private and public sources across national boundaries. This research can support the development of information and control approaches that enhance private–public collaborations. Academic institutions can also assist by providing the kind of advanced training that government analysts increasingly need to do their jobs.

In a nutshell, the data needs to be systematically reviewed and analysed as follows: Most governments maintain online computer systems that are used to control the flow of goods into and leaving their respective countries. The control is typically designed to ensure the admissibility and classification of goods with the aim of accurate revenue collection and the denial of entry of goods deemed to be hazardous, unsafe or illegal. In addition, goods that can cause economic destruction of local industries require further review.

The documentation produced in the performance of these duties is usually processed (where personal and propriety information is stripped) and made available to the public.

This results in four classes of records:

1. *Inbound* manifest/movement transactions: Goods arriving by road, rail, sea and air; usually provided as manifest data detailing the who, what, where and when of goods shipped and received. These records are supplied by the carriers and shippers of such goods.
2. *Import* declarations: Goods declared to the government as entering the economy, becoming part of the goods and services of the country, where the importer performs his legal responsibilities. These documents are usually provided to the public in a form whereby individual transactions are treated to remove the particulars of individual transactions and grouped by some means that accurately reflects the totals of the import transactions.
3. *Outbound* manifest/movement transactions: Goods departing by road, rail, sea and air; usually provided as manifests detailing the who, what, where and when of goods shipped and departing. These records are supplied by the carriers and shippers of such goods.
4. *Export* declarations: Goods declared to the government as leaving the economy, becoming part of the goods and services of another country. These documents are usually provided to the public in a form where the individual transactions are treated to remove the particulars of individual transactions and grouped by some means that accurately reflects the totals of the export transactions. These types of export records are collected for and maintained for statistical purposes mainly because few countries collect duty and taxes on exportations.

The databases mentioned above are either released directly to the public by the concerned governments at their respective official websites (US import and export data can be found on websites maintained by the US Department of Commerce and International Trade Commission) or, for other countries, they may be available at the revenue producing or statistical agencies' websites.

In the case of manifest data, there are several large firms that specialise in collecting these public data. Each firm has its own niche market and processes the data offered by the governments to satisfy their customers. PIERS is available for a fee and was the source of the manifest data reviewed in this report. Similar data are collected, by PIERS and others, from other countries and are commercially available.

Other types of data are available, such as port and ship loading information. It should be noted, there are currently no commercial sources of such data, which is the heart and soul of the shipping companies' business.

In the past, the US government looked to industry to maintain documentation (supply chain correspondence) normally prepared in the course of business in lieu of providing entry documents. This approach assumed that government officials would need such data only to support investigations. Because the events of September 2011 highlighted the need to better assess the risk a cargo shipment might pose *prior* to arrival, US Customs officials began demanding that data be presented to them in advance.

Collection and analysis of these data files could provide a system, when processed by off-the-shelf computer programs, which could illuminate threats and trends deleterious to the welfare and security of the country.

This chapter attempted to review some of the above records and compare that information with records of the movement of money through a non-banking system under scrutiny. In the end, reducing the risk of global trade flows being exploited to cause harm is a mission we must all share. Hence, it is important to move beyond government-centric approaches to policing global supply chains. There is much that civil society, academia and the private sector can contribute towards enhancing cargo security. An important stepping-off point is for Customs authorities to acknowledge that significant gaps exist in their current capabilities to detect and intercept illicit and dangerous goods. They should also frankly declare that they would welcome this assistance and collaboration. As noted before the US Congress,

> 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 the necessary data is not in one place but does 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 is 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. (N. Passas written statement and testimony at the US Congress Committee on Financial Services, Task Force to Investigate Terrorism Financing, 2016)

References

Baker, R., Clough, C., Kar, D. *et al.* (2014) Hiding in Plain Sight: Trade Misinvoicing and the Impact of Revenue Loss in Ghana, Kenya, Mozambique, Tanzania, and Uganda: 2002–2011. Global Financial Integrity. Retrieved from: http://um.dk/en/danida-en/partners/research/other//~/media/UM/English-site/Documents/Danida/Partners/Research-Org/Research-studies/Hiding%20In%20Plain%20Sight.pdf (accessed 11 July 2019).

Bakshi, N., Gans, N. & Flynn, S. (2011) Estimating the Operational Impact of Container Inspections at International Ports. *Management Science*, 57(1), 1–20.

Bindner, L. (2016) Illicit Trade and Terrorism Financing. Center for the Analysis of Terrorism. Retrieved from: http://cat-int.org/wp-content/uploads/2017/03/Interim-note-Illicit-trade-and-terrorism-financing-Dec-2016.pdf (accessed 11 July 2019).

Cassara, J.A. (2016) *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*. Hoboken: John Wiley & Sons.

Coleman, R. (2006) US and Brazilian Stings Nab Trade-Based Laundering Ring. *Money Laundering Alert* (August).

DeKieffer, D. (2005) Trade Diversion as a Fund Raising and Money Laundering Technique of Terrorist Organizations. Unpublished paper.

Dellinger, L. (2008) From Dollars to Pesos: A Comparison of the US and Colombian Anti-Money Laundering Initiatives from an International Perspective. *California Western Law Journal*, 39, 419ff.

Erickson, J.L. (2015) *Dangerous Trade: Arms Exports, Human Rights, and International Reputation*. New York: Columbia University Press.

Financial Action Task Force (2006) Trade Based Money Laundering. Financial Action Task Force, OECD. Retrieved from: https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf (accessed 11 July 2019).

Financial Action Task Force & Financial Action Task Force on Latin America (El Grupo de Acción Financiera de Latinoamérica) (2018) Anti-Money Laundering and Counter-Terrorist Financing Measures: Mexico. Fourth Round Mutual Evaluation Report. FATF and GAFILAT. Retrieved from: https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Mexico-2018.pdf (accessed 11 July 2019).

Flynn, S. (2008) Overcoming the Flaws in the U.S. Government Efforts to Improve Container, Cargo, and Supply Chain Security. Hearing on Container, Cargo and Supply Chain Security: Challenges and Opportunities before the Homeland Security Appropriations Subcommittee, US House of Representatives, 2 April. Retrieved from: http://opim.wharton.upenn.edu/risk/library/2008-04-02_Flynn_ImprovingContainerSecurity.pdf (accessed 11 July 2019).

Flynn, S. (2012) The New Homeland Security Imperative: The Case for Building Greater Societal and Infrastructure Resilience. Hearing on The Future of Homeland Security: Evolving and Emerging Threats before the Committee on Homeland Security and Governmental Affairs, US Senate, 11 July, pp. 114–124. Retrieved from: https://www.hsdl.org/?view&did=729192 (accessed 11 July 2019).

Holmes, C. (2012) Mexico Threat Assessment: Strategy and Countermeasures. *Southwest Border Anti-Money Laundering Alliance*, August.

James, A.C., Doody, A.J. & Passic, G. (1997) The Colombian Black Market Peso Exchange. Statement before the Subcommittee on General Oversight and Investigations Committee on Banking and Financial Services, US House of Representatives, 22 October.

Liao, J. & Acharya, A. (2011) Transshipment and Trade-Based Money Laundering. *Journal of Money Laundering Control*, 14(1), 79–92.

OECD (2018) Illicit Financial Flows: The Economy of Illicit Trade in West Africa. OECD. Retrieved from: https://www.oecd.org/development/accountable-effective-institutions/Illicit-Flows-Economy-of-Illicit-Trade-in-West-Africa.pdf (accessed 11 July 2019).

Oxford Economics (2018) Combatting Illicit Trade. Retrieved from: http://www.oxfordeconomics.com/publication/download/300615?__hstc=30812896.2d3fcf2f99a265337744294b740e0787.1554076800139.1554076800140.1554076800141.1&__hssc=30812896.1.1554076800142&__hsfp=3733277192 (accessed 11 July 2019).

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

Passas, N. (2006) Setting Global CFT Standards: A Critique and Suggestions. *Journal of Money Laundering Control*, 9(3), 281–292.

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

Passas, N. (2012) Financial Controls and Counter-Proliferation of Weapons of Mass Destruction. *Case Western Reserve Journal of International Law*, 44(3), 747–763.

Passas, N. (2016) Collective Action for Trade Transparency against Financial Crime. *Translational Criminology*, (Spring), 16–18, 26.

Passas, N. (2017) Security Threats and Illicit Flows: What they Hide and How to Control Them. Paper presented at Dangerous Ties: How to Fight the New Networks of Terror and Crime, German Council on Foreign Relations (DGAP), Berlin.

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

United States Senate Caucus on International Narcotics Control (1999) The Black Market Peso Exchange: How US Companies Are Used to Launder Money: Hearing before the

Senate Caucus on International Narcotics Control, One Hundred Sixth Congress, First Session, 21 June 1999. Washington, DC: US Government Publishing Office. Retrieved from: https://www.govinfo.gov/content/pkg/CHRG-106shrg60125/html/CHRG-106shrg60125.htm (accessed 11 July 2019).

United States House of Representatives Committee on Financial Services, Task Force to Investigate Terrorism Financing (2016) Trading with the Enemy: Trade-Based Money Laundering Is the Growth Industry in Terror Finance: Hearing before the Task Force to Investigate Terrorism Financing of the Committee on Financial Services, US House of Representatives, One Hundred Fourteenth Congress, Second Session, 3 February 2016. Washington, DC: US Government Publishing Office. Retrieved from: https://www.hsdl.org/?abstract&did=806585 (accessed 11 July 2019).

Wilkinson, T. & Ellingwood, K. (2011) Cartels Use Legitimate Trade to Launder Money, US, Mexico Say. *Los Angeles Times* (19 December). Retrieved from: https://www.latimes.com/world/la-xpm-2011-dec-19-la-fg-mexico-money-laundering-trade-20111219-story.html (accessed 19 July 2019).

Young, A. (2017) *Trade-Based Money Laundering: Overview, Issues, Perspectives*. Hauppauge: Nova Science.

Zdanowicz, J.S. (2009) Trade-Based Money Laundering and Terrorist Financing. *Review Of Law & Economics*, 5(2), 855–878.

Zdanowicz, J.S., Welch, W.W. & Pak, S.J. (1995) Capital Flight from India to the United States Through Abnormal Pricing in International Trade. *Finance India*, IX(3), September.