

CBSA Knowledge Pool on Trade-Based Money Laundering ¹

Background

Laws in place to enforce TBML and other illicit financial crimes

There is no criminal offence under Canadian law called “trade-based money laundering”. Rather, most TBML involves laundering the proceeds of crime using customs trade fraud techniques.

Responsibility for enforcing financial crimes, including fraud, proceeds of crime/money laundering offences in Canada fall largely under the domain of the federal, provincial and municipal law enforcement authorities who enforce the *Criminal Code of Canada (Criminal Code)*. The Royal Canadian Mounted Police (RCMP), Canada’s national police force, is responsible for enforcing federal financial crimes in the *Criminal Code* or those with a national or transnational dimension. Proceeds of Crime offences fall under Part XII.2 of the Code [S. 463.31(1) refers].

The RCMP also has criminal investigative authority for offences under Canada’s *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* This legislation establishes specific record keeping and reporting measures designed to detect and deter money laundering and the financing of terrorist activities and to facilitate the investigation or prosecution of money laundering and terrorist financing offences.

The Canada Revenue Agency has criminal investigation authorities to enforce tax evasion, a criminal predicate for money laundering, under the *Income Tax Act*. Fraudulent goods declarations often have bearing on the declared income of the front and shell import/export companies favoured in many TBML schemes. Similarly, income tax offences in the form of import/export tax credit fraud may also be vertically integrated into TBML schemes.

CBSA Mandate for Trade Fraud and TBML

The Canada Border Services Agency does not have the mandate to enforce financial or money laundering-oriented crimes. The Canada Border Services Agency has criminal investigation authorities to enforce trade fraud under the Customs Act. Trade fraud is unique in that it is both a criminal predicate for TBML, as well as the primary technique used to perpetrate the activity itself.

All importers and exporters seeking to convey goods to and from Canada have a legislative obligation under the *Customs Act* to provide “true, accurate and complete” reporting of goods imported or exported [further to subsections 7.1, 12 and 95(3)]. Most TBML schemes rely on the intentional misdescription of various elements on customs documentation (including the price, quantity, tariff classification, and physical description of the goods) in order to be successful.

CBSA officers at ports of entry, Intelligence Officers, CBSA foreign Liaison Officers, as well as CBSA Trade Compliance officers inland may develop grounds to suspect money laundering activity in the course of their mandated responsibilities related to the import or export of goods, and may refer these instances to CBSA’s Trade Fraud and TBML Centre of Expertise. The Centre will continue to build on these grounds

¹ This paper provides an overview of key insights CBSA has gained to date on TBML. Note that the TF/TBML Centre of Expertise only became operational as of April 1st and minimal work on TBML was done before that time.

which may yield referrals to CBSA Criminal Investigators for trade fraud offences, as well as the RCMP for suspected TBML.

Overview of Insights Gained To-Date

According to the Financial Action Task Force (FATF), the international body responsible for establishing global anti-money laundering and anti-terrorist financing (AML/ATF) norms and best practices, there are three main methods to disguise illicit proceeds and integrate them into the formal economy:

- o Via the financial system;
- o Through the physical movement of cash and monetary instruments; and finally,
- o Through the physical movement of goods through the trade system.

The risk of money laundering through financial institutions and bulk cash smuggling is well known, and corresponding anti-money laundering and anti-terrorist financing controls are robust. However, abuse of the international trade system has received relatively little attention by most national governments and awareness of trade-based threats is generally limited.

TBML is easily concealed in enormous volumes of global trade, leading some experts to proclaim it as the largest money laundering method in the world, but also the least known and understood. By some estimates, the trade fraud that underlies TBML accounts for over 80% of illicit financial flows from developing nations, and may cost the global economy as much as 1 to 7 percent of annual Gross Domestic Product (GDP) each year.

Scale of TBML in Canada: While the full scope and scale of TBML in Canada remains a gap, a sufficient body of knowledge exists to indicate that Canada is being routinely exploited due to key vulnerabilities, including limited awareness of laundering through the international trade in goods in both the public and private sectors. Canada has not yet developed a methodology to assess the scope and scale of TBML in Canada. However, it is assessed that TBML activity is occurring on a daily basis in Canada, particularly in large metropolitan cities.

How does this threat manifest itself in Canada

Tactics and Schemes

Trade Fraud Remains a Key Driver: Most suspected instances of TBML in Canada occur through the use of commercial trade fraud techniques, primarily involving the mis-description of the price, quantity or quality of goods on documents presented to Customs Services on the importation or exportation of goods from a national jurisdiction. In Canada, most TBML identified to date involves goods exported from Canada, primarily through marine containerized shipping, likely as a result of reduced controls for exports in comparison to imported goods (which have the potential for revenue generation depending on the tariff).

There are a range of TBML methods; however, a typical scheme will involve the use of proceeds of crime by complicit import/export companies to purchase goods destined to or from Canada. Goods will be fraudulently over- or under-valued (weights and goods descriptions can also be manipulated) on customs documents in order to inflate or deflate their value, depending on the direction of the intended flow of proceeds. The import or export of goods creates the necessary pretext for criminal syndicates to wire funds to “pay” for said goods at source or destination. The sale of said goods thus completes the

money laundering cycle, even if no physical goods are ever shipped (i.e. phantom shipments, which have been identified in one significant case). Circumvention of customs requirements is thus the basis for most TBML schemes.

BMPE Variants: In terms of newer TBML methodologies, Canada has identified the abuse of money or value transfer service providers or informal/illicit value transfer systems, as well as continued adaptations of the Black Market Peso Exchange (BMPE), allowing for cash settlement across multiple jurisdictions. BMPE-like schemes account for a significant part of TBML schemes observed in the Americas.

3rd Party Payments: The use of third-party invoice settlement is often used in the context of BMPE-like schemes which are linked to professional money laundering networks. Third-party invoice settlement for goods exported to/from Canada from entities located in high-risk money laundering jurisdictions, generally via open account payments through wires through correspondent banking relationships, remains one of the most commonly observed methods of facilitating TBML.

These transactions are rarely scrutinized by financial institutions and only come to the attention of the CBSA by way of FINTRAC once grounds to suspect TBML have already been established. Moreover, customs authorities are only able to physically examine a small percentage of corresponding goods shipments to validate the wire transfers. Detecting this behaviour would require the mandatory inclusion of some form of customs reference embedded within wire transfer remittance information. Canada, like many countries, does not mandate the inclusion of any form of cross-referencing identifier to link wire transfers with corresponding import or export activity.

Open Account Settlements: In addition, financial institutions have no means to verify whether goods that are either financed or settled through open account have indeed been physically imported/exported as there are no requirements to present confirmation of the submission of customs documents to the appropriate customs authority, the Canada Border Services Agency (CBSA). This information gap increases the risk of goods mis-description or, in the most severe cases, entirely fictitious phantom shipments of goods.

Trade Finance: Trade financing mechanisms may also be exploited to perpetrate TBML. Currently, FINTRAC does not have the legislative authority to collect transaction information linked to trade financing (SWIFT 700 series messages). While Financial Institution anti-money laundering departments have submitted Suspicious Transaction Report (STR) information pertaining to trade finance in some instances, it remains possible that money laundering threats to trade finance remain hidden through lack of access to related information coupled with a low degree of awareness of TBML within capital markets divisions of these institutions. In addition, lawyers who negotiate trade finance contracts are also exempt from Canadian AML reporting requirements due to solicitor-client privilege.

Misrepresentation of the counterparty in a trade transaction: Canada has observed the use of fraudulent customs declarations on both ends of a TBML transaction, likely in order to conceal the true identities of both the originator and the recipients of the goods from the customs administrations on both sides of the transaction.

Typically, a Canadian exporter or freight forwarder will declare a specific foreign entity as the consignee for the goods in question on their export declaration, while the complicit foreign counterparty to the

transaction will provide a different consignee name on the foreign import declaration. In some instances, the Canadian exporter appears to be conspiring with Canadian freight forwarding companies to use the freight forwarder's name and business number information in place of their own, again, likely to conceal the extent of the suspected laundering activity. These behaviours are only detected through access to open trade data, typically provided by for-profit data service providers.

Surrogate Shoppers: Another TBML scheme relates to the abuse of Chinese *daigou* ("buying on behalf of") personal shopping/surrogate shopping networks. This is an unregulated, cash intensive, but legitimate international commerce activity where Canada-based shoppers receive a commission for purchasing high-end luxury goods for customers in China (and possibly the Middle East) often to take advantage of lower Canadian prices. The trade in these goods creates opportunities for TBML when proceeds of crime are used to fund the purchase of inventories of goods for export. Misdescription of these goods creates further opportunity to inflate the value of wire transfers from China used to pay for these goods. This scheme allows launderers and criminal networks to move value between countries without resorting to the international financial system.

Locations

TBML can occur anywhere. However, while specific routings have not been analyzed in detail, imports or exports (and corresponding wire transfers) originating or transiting via the following jurisdictions are often an indicator for TBML:

- United Arab Emirates
- Hong Kong
- China
- Pakistan
- United States:
 - Greater New York area
 - South Florida
 - Southern California
- Latin America, in particular:
 - Mexico
 - Colombia
 - Paraguay / TBA: Ciudad del Este
- Russia related
 - Baltics (banking, now likely less prevalent)
 - Cyprus (professional services)
 - BVI and other offshore jurisdictions (shell company formation)

TBML schemes sometimes include transshipment via global Free Trade Zones (FTZs), particularly in Black Market Peso Exchange schemes. Goods effectively "disappear" into FTZs as they may be re-manifested and further mis-described before being transhipped onwards, which makes it extremely difficult to determine the ultimate destination (and consignees) of goods in these schemes.

Threat Actors

Cartel drug trafficking accounts for much of the proceeds being laundered based on information reviewed/assessed to date. Most of the funds related to these schemes enter Canada from the United States, China, Hong Kong, and the United Arab Emirates (UAE) for goods shipments to a wide variety of third countries, primarily using variations of the Black Market Peso Exchange.

While the CBSA has established linkages between suspected TBML and cartels, the majority of the suspected cases of TBML are believed to be conducted by Professional Money Launderers (PMLs) likely operating at arms-length under contract to the cartels. As the US Treasury continues to expand its Transnational Organized Crime and “Kingpin” sanctions lists, there is a risk that Cartels may come to increasingly favour PMLs operating adjacent to the US financial system in Canada. PMLs are not involved in the generation of the proceeds of crime. Instead, they charge commissions to launder criminal proceeds. Many PMLs hold professional designations or own businesses conducive to laundering, including lawyers, accountants and trade chain professionals (importer/exporters, freight forwarders).

There are also emerging indicators of a series of thriving informal value transfer networks operating across Canada that are facilitating illicit financial flows to and from Canada and a variety of international jurisdictions. It is unclear of the degree to which the money remitters operating these informal networks are aware of the source of the funds they are transmitting through the international movement of goods. Unlike narco-proceeds cases, we have not observed the same degree of financial flow-through activity, suggesting that these funds may be destined to remain within Canadian financial institutions. The mis-description of customs and trade chain documents remains the primary assessed method for facilitating this laundering activity.

Indicators, patterns, or anomalies do you use to highlight a potential TBML threat

The CBSA uses a variety of red flag indicators articulated in the following established TBML typologies to build grounds to suspect TBML:

- Trade Based Money Laundering. Financial Action Task Force. 23 June 2006.
- Asia/Pacific Group on Money Laundering. APG Typology Report on Trade Based Money Laundering. 2012-07-20
- Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering. FinCEN Advisory #FIN-2010-A001.
- FinCEN Advisory #FIN-2019-A006, August 21, 2019.
- FINTRAC – Professional money laundering through trade and money services businesses, July 18, 2018. Ref # 18/19-SIDEL-025
- FAFT Report: Professional Money Laundering. Financial Action Task Force. July 2018.

Conducting Analysis on TF/TBML Threats

The key to combating TBML lies in the ability to access and layering customs, shipping, tax, financial transaction, intelligence, and entity data. TBML often reveals itself in the layering of these datasets as it allows investigators and analysts to both “follow the goods” as well as “follow the money” and determine the narrative of the laundering activity.

The following traditional methods of conducting financial crime probes/investigations have also proven effective:

- Joint intelligence probes and investigations between the CBSA and the RCMP.
- Analysis of Suspicious Transaction Reports (STRs) and underlying financial transaction information originating from Financial Institutions and Designated Non-Financial Business and Professions to FINTRAC that are shared with the CBSA through a disclosure process. In Canada, financial transaction information can be obtained through FINTRAC without a subpoena.
- Suspicious Activity Reports and other financial intelligence obtained on request from foreign financial intelligence units by FINTRAC, based on Egmont Group Memoranda of Understanding.
- Requests/disclosures from foreign customs counterparts
- Intelligence provided from border, customs, law enforcement agencies and other intelligence services.

Common enablers of TBML

Lack of Awareness: Many TBML threats are perpetrated by networks of professional money launderers, who do not commit money laundering predicate crimes. As a result, enforcement responses tend to favour “traditional” threat actors (e.g. drug traffickers), rather than those cutting across the mandates of multiple agencies, such as with TBML, leading to intelligence blind spots and gaps in coverage.

Limited Examination and Data Analytics Capacity: The CBSA can only physically examine a very small percentage of the huge volumes of goods imported and exported from Canada. There is limited ability to leverage the Agency’s customs data holdings through advanced analytic techniques to identify anomalous transactions indicative of TBML behaviour that may warrant examinations to validate the anomalies in question.

Import Focus / Export Reporting Gaps: In the border domain, most CBSA controls focus on protecting Canadian industry and assuring high rates of compliance for duties and taxes paid on imported goods. However, TBML actors frequently exploit lax Canadian export reporting requirements (owing to significant export control weakness, such as limited review of export declarations and very low examination rates) under which no duties or taxes are levied. Investigations and intelligence probes regarding trade fraud (including those with possible TBML dimensions) in the export domain remain low.

Canada and the US also have a unique gap with respect to export data. Both countries do not require their exporters to file export declarations for goods destined to each other, which makes identifying TBML extremely difficult when only import records exist in either country to try to substantiate trade fraud. This also significantly complicates the ability to automate the detection of export anomalies through initiatives such as the US Trade Transparency Unit concept.

Limited Reporting by Trade Chains: Trade chain stakeholders do not currently have a mandated reporting role in Canada’s Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime in detecting TBML in Canada and the CBSA does not have systematic access to shipment information (bills of lading, shipping invoices, etc.). However, data provided from these stakeholders on request, particularly shipping invoices and bills of lading, coupled with their inside knowledge of complex transnational trade chains are crucial in substantiating the suspicion of TBML.

While some trade chain stakeholders have been forthcoming with information in support of anti-TBML efforts, others have insisted upon judicial authorization (production orders) to produce necessary data.

These authorizations require higher legal grounds (equivalent to a search warrant) which complicates and delays investigative activities.

Limited Information Availability: TBML exploits the trade and financial system, but the data required to identify schemes (customs data, bills of lading, shipping invoices, STR/SAR and financial transaction data) are often held by different authorities and private sector entities, and are not systematically available to the competent authorities to cross-check, or to proactively identify suspected TBML through analytics.

Goods identified as part of TBML schemes

The below noted goods are most frequently observed in TBML schemes, however, **any** high-demand, difficult-to-examine good featuring wide pricing margins (or difficult to price) is highly susceptible to TBML.

- Construction materials and plant machinery
- Agriculture products (e.g., fruits, vegetables, grains)
- Auto parts and vehicles
- Clothing (e.g., new, used and recycled textiles)
- Cosmetics and toiletries
- Gold or other precious stones and metals
- Forestry
- Scrap metals
- Electronics (e.g. smart phones, iphones, tablets).

Precious metals and stones do not fall under the definition of currency or monetary instruments (with associated reporting obligations therein) under the PCMLTFA in Canada. From a border perspective these goods are treated no differently from any other good in the Canadian Customs Tariff. This gap increases the likelihood of these high-value commodities as ML vectors.