



Audience: *Regional Operations, Regional Intelligence & Enforcement, International Region*  
Intelligence and Enforcement Priority: Trade Fraud

Issued: JUNE 2020  
Expiry: JUNE 2021

## Intelligence Collection, Analysis & Production Division



# Trade-Based Money Laundering Overview

ICAP 2020-JUNE-08

## HIGHLIGHTS

- Trade-based money laundering (TBML) is the process of concealing and moving illicit money through the legitimate international trade in goods; it is believed to be one of the largest money laundering methods in the world, but one of the least identified and understood.(U)
- The most common form of TBML involves the criminal mis-description of customs declarations, to, for example, artificially raise or lower the value of goods being declared on import or export to or from a country. The trade in goods is attractive to launderers, as it provides a pretext to wire money to accomplices abroad to pay for goods received.(U)
- While the true scale of TBML in Canada remains unknown, the CBSA assesses that at a minimum, hundreds of millions of dollars are likely being laundered through the trade in goods to and through Canada each year. Successful TBML harms Canada's national and economic security, its international reputation, and its revenue collection capabilities.(PA)
- The CBSA has a mandate to detect, deter and disrupt the customs fraud that underlies TBML, but refers suspected instances of TBML to the Royal Canadian Mounted Police for further investigation. (U)

## PURPOSE

1. The purpose of this paper is to provide introductory situational awareness on TBML in Canada. The information and judgements in this report are drawn from over a dozen active CBSA leads, a complex and ongoing RCMP money laundering investigation, several dozen Financial Transaction and Reports Analysis Centre of Canada (FINTRAC) disclosures, intelligence from international and domestic law enforcement partners, as well as TBML typology information from Canadian and U.S. financial intelligence units, the Financial Action Task Force, and several non-governmental organizations specializing in financial crime.(U)

PROTECTION • SERVICE • INTEGRITY

Canada



## CONTEXT

2. Proceeds of crime and other illicit financial flows fuel transnational criminal activity. These flows of funds need to be moved into legitimate economies in jurisdictions where they can be safely accessed and used by criminals.(U)
3. 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 place, disguise and integrate illicit flows into formal economies:
  - Through financial institutions;
  - Through the physical movement of cash and monetary instruments (i.e. bulk cash smuggling); and finally,
  - Through international trade. (U)
4. Money laundering through financial institutions and by bulk cash smuggling is well known, and AML/ATF controls to detect and prevent laundering through these channels have become progressively more robust. Awareness of trade-based threats, on the other hand, remains limited. Most national governments have done little to control laundering by these means, leaving international trade exposed to abuse. The process of disguising illicit financial flows and moving value through the use of trade transactions in an attempt to legitimize their illicit origins is known as TBML.(U)
5. TBML is easily concealed in enormous volumes of global trade, leading a panel of experts to proclaim it as the largest money laundering method in the world, but also the least known and understood<sup>1</sup>. No formal estimates exist on the scale of TBML in Canada; however, a sufficient body of intelligence exists to indicate that Canada is being routinely exploited for its relatively weak anti-money laundering controls, including the limited awareness of laundering through the international trade in goods in both the public and private sectors. CBSA assesses that TBML is believed to be emerging as a prevalent technique for professional money laundering networks in Canada, and illicit funds in the low hundreds of millions of dollars are being laundered each year via trade. The true extent of TBML is believed to be higher than these figures suggest.(PA)
6. By one estimate, created using comparisons of international trade datasets and balance-of-payment information, the fraud techniques that underlie most TBML schemes account for over 20% of all trade from developing nations<sup>2</sup>, at a cost of as much as \$8.7 trillion USD between 2008 and 2017<sup>3</sup>. Of this, the amount of TBML occurring through trade fraud around the world is believed to be substantial.(U)



## THREAT ENVIRONMENT

### Types of TBML Schemes

7. Most TBML occurs through the use of commercial trade fraud techniques, primarily through the mis-description of documents presented to customs services on the importation or exportation of goods from a national jurisdiction; however, there are a variety of TBML schemes ranging from simple to extremely complex, as follows.(U)
8. **Basic:** The most basic TBML schemes involve transferring goods to finance illicit activities or to procure supplies. In many of these schemes, a strong customs nexus does not exist. This could include the export and sale of vehicles to Africa in exchange for narcotics, or antiquities imports sold to finance the activities of a criminal or terrorist organization. (U)
9. **Moderate:** Circumvention of customs regulations is the basis for most TBML schemes. Criminals funnel proceeds of crime or other illicit financial flows into import/export companies and use these funds 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, quantity, or quality. The destination and the identity of the vendor and/or consignee of the goods may also be altered on both customs and shipping documentation to conceal the identities of those involved in the laundering from authorities.(U)
10. The primary purpose of importing and/or exporting goods is to create the pretext for criminals to send Electronic Funds Transfers (EFTs aka “wire transfers” or “wires”) to “pay” for said goods at source or destination, which will depend on the direction of the intended flow of illicit funds, as follows: (U)

To Move \$ OUT	Import Goods	At above value prices
	Export Goods	At below value prices
To Move \$ IN	Import Goods	At below value prices
	Export Goods	At above value prices

11. **Complex:** These schemes build on basic and moderate techniques. Third party goods payments, webs of freight forwarding companies, and international Free Trade Zones (de-regulated areas around the world that are intended to enhance trade) are often introduced to layer trade transactions and create a highly complex illicit international trade chain. These techniques can be complemented with other forms of money laundering (e.g. in the real estate and casino sectors) and related tradecraft to further reduce detection, including the use of shell companies, offshore accounts, nominees, legal trusts, and

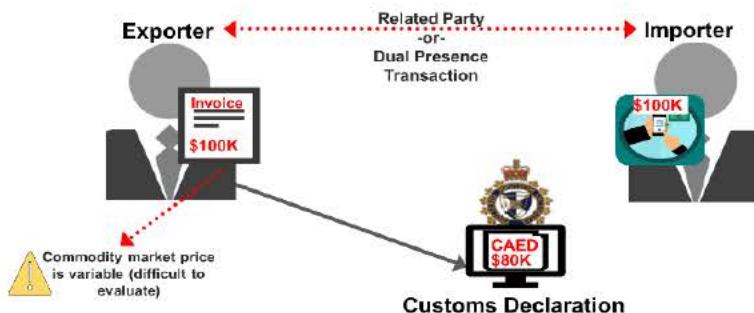


crypto-currencies. The most extreme example of customs-based TBML are “phantom shipments”, where customs declarations are presented for goods that are never shipped.(U)

12. Not all TBML involves the abuse of customs processes. Some schemes rely on the trade in services across borders (e.g. international consulting, research fees, fraudulent construction costs), which, while unsophisticated, is extremely difficult to detect, but could be relevant in the context of determining criminal inadmissibility to Canada under the *Immigration and Refugee Protection Act*. In addition, some “phantom shipment” schemes are purely financial: wire transfers are sent between banks under the pretext of trade payments, but neither shipments nor customs documents are ever declared in support of these transactions<sup>i</sup>. (U)

## Key Features

13. Criminals engaged in TBML are generally not interested in committing duty and tax evasion, which has been the traditional focus of the CBSA’s border enforcement efforts. Rather, launderers use customs paperwork to justify the wiring of illicit financial flows across borders. The costs involved in converting cash to goods and the payment of duties and taxes, if required, are viewed by launderers as the cost of doing business.(U)
14. All TBML schemes require a complicit buyer and seller. The risk for TBML increases in related party transactions, when the two parties of a trade transaction either have a linked corporate structure, or both ends of the trade transaction are controlled by the same entities.(U)



This scenario presents an instance of “suspected” over-valuation. \$100,000 in goods are being exported from Canada. The goods are invoiced at their presumed true value, however, only \$80,000 worth of goods are declared on export to the CBSA. The scheme allows for an excess of \$20,000 in value to be laundered into Canada. (graphic source: RCMP Financial Crime, Toronto North)

<sup>i</sup> These cases would only involve the CBSA mandate insofar as confirming for law enforcement the existence of any supporting import or export activity.



## Goods Used

15. While almost any product or commodity can be used to carry out TBML, certain goods are ideal. These include: high-demand, easy to sell goods; goods that are difficult for customs services to examine; and/or goods with variable price ranges (or are difficult to price). Goods exhibiting these characteristics feature repeatedly in TBML schemes in Canada and other countries. These include:

- Smartphones, tablets and electronics (see sidebar)
- Vehicles and vehicle parts
- Agri-foods (e.g. fresh and frozen meats, dairy, seafood, produce)
- Used clothing and textiles
- Lumber and paper products
- Scrap metal and plastic
- Precious metals and stones
- Perfumes and cosmetics

(U)

### Snapshot – TBML and Mobile Phones

**Mobile phones feature frequently in Canadian and international TBML schemes, and are well-known to both law enforcement and financial institutions. They are emblematic of the ease with which TBML can be conducted, and the difficulty in identifying suspicious shipments.(PA)**

**The devices are easy to acquire with proceeds of crime through networks of straw buyers (illicit funds are typically used to reimburse buyer's personal credit cards). Logistically, the devices are portable and can be shipped in bulk with ease. At the same time, the wide variety of models, features and price points facilitates mis-description (used models can be sold as new, memory sizes can be altered on declarations, etc). In extreme cases, entire shipments of phones have been known to be recycled from one country to the next, documented as new shipments each time. Demand, particularly for higher-end brand name devices, make phones easy to liquidate in destination markets in order to recover now "clean" funds.(U)**

## Geographic Concentrations

16. CBSA assesses that TBML activity is occurring on a daily basis in Canada, particularly in the financial and industry hubs of Toronto, Montreal and Vancouver. These locations are where the majority of import/export businesses are domiciled, and where most professional money laundering



activity is concentrated in Canada. Additionally, dozens of Canadian trading companies across the country have the capability and the suspected intent to engage in the placement and layering stages of TBML activities through the trade in goods.(PA)

17. TBML can occur anywhere, but, 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:

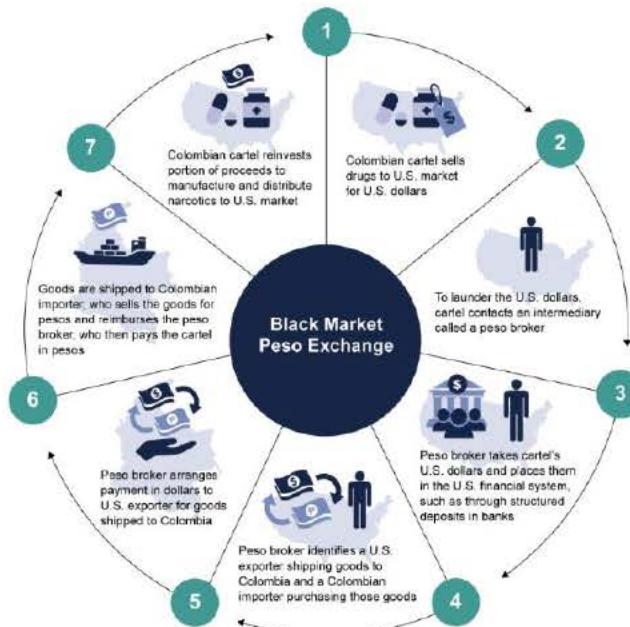
- United Arab Emirates
- Hong Kong
- China
- Pakistan
- United States:
  - Greater New York area
  - South Florida
  - Southern California
- Latin America, in particular:
  - Mexico
  - Colombia
  - Paraguay / Tri-Border Area (Ciudad del Este)

(PA)

## TBML Enablers

18. **The Black Market Peso Exchange:** Black Market Peso Exchanges (BMPEs) are a fundamental TBML typology. BMPEs are an “informal value transfer system” created by Colombian traders in the 1970’s seeking methods to evade domestic currency controls in order to access US dollars to pay for imported goods. These methods were quickly adopted by drug trafficking cartels as a method of swapping US drug dollars for Colombian pesos, and the technique remains closely associated with drug trafficking proceeds to date. While there are dozens of variants to the technique, BMPEs help criminal networks solve a key logistical dilemma: how to repatriate illicit finances, usually earned in foreign currency, with minimal risk of exposure, and convert it to local currency where it can be freely used to sustain criminal operations.(U)

19. BMPEs are, effectively, an illegal foreign currency exchange that avoids the large-scale currency transactions which are reportable to Canada’s financial intelligence unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). A typical BMPE, using the example of laundering US drug proceeds back to Colombia, works as follows (see accompanying graphic).(U)



Source: US Government Accountability Office

20. Not all BMPE schemes use fraudulent customs documentation. In some schemes, the prices, quality, quantities and descriptions of goods can be reported accurately for customs purposes. The money laundering in these instances occurs at the initial, or “placement” stage of the laundering cycle, by using illicit financial flows to purchase goods that are subsequently exported. Proving the complicity of the merchants who accepted illicit funds as payment for exports in these circumstances can be difficult for investigators and prosecutors.(U)
21. **Free Trade Zones (FTZs):** FTZs are de-regulated areas, typically located near ports of entry, that are created by governments to stimulate investment, economic growth, manufacturing and international trade through reduced regulatory controls (e.g. duties and tax collection, examinations) and enforcement. FTZs can also be used to create corporations and other legal entities necessary to access the global financial systems. These features make FTZs attractive for both licit and illicit economic activity, and generally enhance criminal opportunities to engage in money laundering. There are over 3000 FTZs around the world processing billions of dollars' worth of global trade each year. Many are located in major regional financial and trade centres, while others operate in drug trafficking and money laundering corridors (see “Geographic Concentrations” section above).(U)

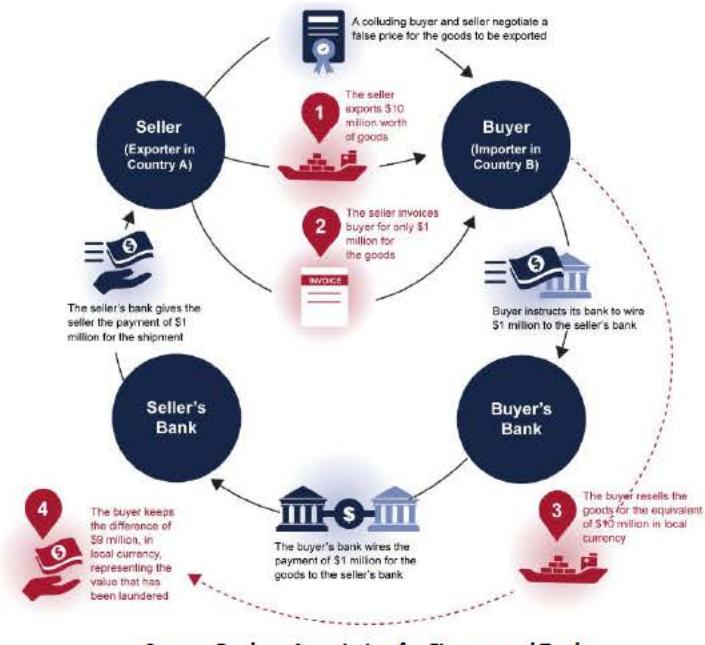


22. TBML schemes identified in Canada are frequently linked to FTZs through goods transshipments, particularly in suspected BMPE schemes. Goods effectively “disappear” into FTZs as they may be re-manifested and further mis-described before being transshipped onwards, which makes it extremely difficult to determine the ultimate destination (and consignees) of goods.(PA)

**23. Open-Account Settlements:** In open-account transactions, the role of financial institutions are to process the payments for a transaction negotiated between a buyer and seller (typically via a sales invoice) for a fee. Banks generally do no request any documents to support the legitimacy of the transaction, such as an invoice, bill of lading, or customs declaration. 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 CBSA.

Conversely, the CBSA has limited ability to reconcile financial transactions with customs records. This information gap increases the risk of goods mis-description or, in the most severe cases, entirely fictitious phantom shipments of goods. (PA)

**24. Trade Finance:** Information from a complex, ongoing TBML investigation suggests that trade financing mechanisms may be exploited to perpetrate TBML to a greater degree than the Government of Canada (GOC) may be aware. FINTRAC does not have the legislative authority to collect transaction information linked to documentary credit information, which creates a gaps in the CBSA and law enforcement’s ability to identify suspicious financing link to trade transactions. While financial institution anti-money laundering departments have submitted Suspicious Transaction Reports 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 the trade finance 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.(U)



Source: Bankers Association for Finance and Trade



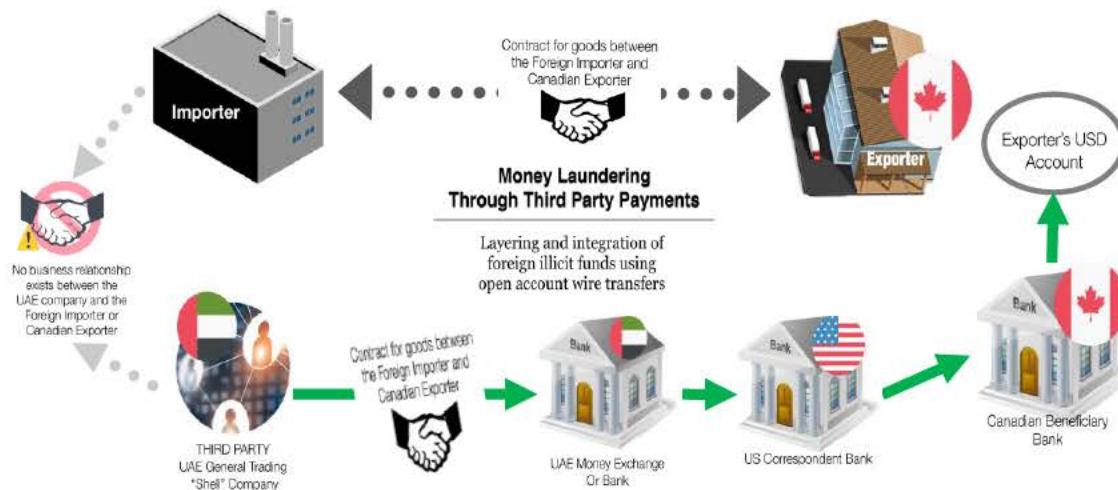
## Threat Actors

25. **Cartels:** Cartel drug trafficking accounts for much of the illicit financial flows being laundered, based on partner intelligence and through investigative leads currently under review. Most of the funds related to these schemes enter Canada from the United States, China, Hong Kong, and the United Arab Emirates for goods shipments to a wide variety of third countries, primarily using BMPE variations. Canada likely remains an attractive distribution link in the international flow of cartel narcotics proceeds back to producers, rather than as a key source or destination for the proceeds themselves through TBML techniques. This judgement derives from evidence of significant financial “flow through”<sup>ii</sup> in bank accounts linked to trade transactions in cases examined thus far.(PA)
26. While the CBSA has established linkages between suspected TBML and Mexican cartels, the majority of the suspected cases of TBML that the CBSA are currently examining are suspected 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 professional money launderers operating adjacent to the US financial system in Canada.(PA)
27. **Professional Money Launderers:** A significant amount of laundering continues to be carried out by low level currency smuggling “mules” who are paid or coerced to physically move cash between jurisdictions. Logistical difficulties plus the risk of theft or interdiction have led many sophisticated criminal networks to adopt less risk-prone and more efficient methods of money laundering, including the increasing use of PML networks in order to reduce their exposure to law enforcement.(PA)
28. PMLs are not involved in the generation of the proceeds of crime. Instead, they charge commissions to launder criminal proceeds, ranging from one to as much as 25 percent in Canada based on the level of laundering difficulty<sup>4</sup>. Many PMLs hold professional designations or own businesses conducive to laundering, including lawyers, accountants and trade chain professionals. CBSA and Government of Canada (GOC) intelligence holdings indicate that the use of TBML techniques via import/export shell and front companies (where beneficial ownership can be difficult to determine) in Canada is prevalent, and appears to be a key money laundering method employed by Mexican and Colombian drug trafficking cartels. R3
29. The identities of the international and domestic money controllers/remitters who broker laundering deals between organized crime groups and PMLs across borders remains a key intelligence gap, although indicators of their involvement have been identified in several CBSA files.(PA)

<sup>ii</sup> Deposits that are withdrawn or wired onwards from an account within 1-2 days of the initial deposit.



**30. Third-parties:** The use of third-parties, often located in third countries, who have no apparent connection to a trade transaction to pay goods invoices is one of the most commonly observed methods of facilitating TBML. It is a tactic frequently used in PML-controlled BMPE schemes, and the third party is often linked to an International Controller Network. These global networks of PMLs broker and reconcile laundering deals, and receive and transfer vast sums of illicit money on behalf of various criminal and terrorist enterprises for a fee, notable examples of controller networks with a global footprint and the capability and intent to launder billions of dollars per year include the KHANANI Money Laundering Organization and D-COMPANY, both of which have been sanctioned by the US Treasury and barred from transacting in the US financial system.(PA)



Source: RCMP Financial Crime, Toronto North

**31.** Payments are typically made by wire transfers between financial institutions with cross-border correspondent banking relationships. These transactions are rarely scrutinized by financial institutions and only come to the attention of the CBSA by way of FINTRAC once the suspicion of TBML has 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.(PA)

**32. Informal Value Transfer System (IVTS) Networks:** These trust-based, informal networks exist in parallel to the formal banking sector and serve as a way to transfer funds without money leaving physical borders (sometimes known as *mirror transfers*). IVTS networks receive money from clients seeking to transfer funds to a different geographic location; equivalent values are then paid out at the



opposite end of the network to the intended recipient. IVTS are often used by expatriates to remit money back to family in their countries of origin to avoid high transaction fees and exchange rates, or to transfer funds to hard-to-reach locations. IVTS include “alternative remittance systems” and underground banking that precede western banking by thousands of years (known variously as *hawala*, *hundi*, and *fei chien*). IVTS are secure, anonymous and mostly legal, making them highly attractive to PMLs. TBML is typically used by IVTS networks to balance their ledgers.(U)

33. Financial and other intelligence sources also provides emerging indicators of IVTS networks operating across Canada that are facilitating illicit financial flows to and from Canada and China, Hong Kong and the UAE are, possibly linked to proceeds of crime, capital flight from China and Iranian sanctions evasion (Venezuelan sanctions evasion is also possible, but has not yet been identified in Canada). 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 is not known. Unlike narco-proceeds cases, CBSA has 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.(PA)
34. **Freight Forwarders:** Freight forwarders can be a powerful facilitator of global TBML. The freight forwarding sector occupies a pivotal place in trade chains. They are neither the seller nor the buyer of goods; rather, they expedite goods shipments by helping buyers and sellers navigate often complex customs and shipping routes and processes. Unlike financial institutions, freight forwarders have no AML reporting obligations in situations where they suspect that certain trade transactions may be TBML-related. Taken together, these factors create ideal conditions for maintaining willful blindness to TBML: freight forwarders can use their knowledge of trade logistics and their lack of AML reporting obligations to control and direct TBML schemes, while disguising their role from law enforcement by acting as a facilitator, rather than the driver of suspect trade transactions.(U)
35. For example, in one ongoing TBML investigation, the Canadian and overseas freight forwarders are believed to be manipulating the exporter and consignee information on both Canadian export and overseas import declarations, likely in order to conceal the true identities of both the originator and the recipients of the goods from customs services and law enforcement on both sides of the transaction. In the same case, the Canadian exporter appears to be conspiring with the Canadian freight forwarding companies to use the freight forwarder’s name and business number information in place of their own.(PA)

## RED FLAGS

36. The following indicators of TBML activity are based on ‘red flags’ that have been identified by FinCEN<sup>6</sup> and the Asia/Pacific Group (APG) in their 2012 report *APG Typology Report on Trade Based Money Laundering*<sup>7</sup>. The APG report notes that no one activity by itself is a clear indication of



TBML. Indicators only identify possible signs of illicit activity and need to be evaluated in conjunction with other ‘red flags’ and the normal transaction activity expected.(U)

## A. RED FLAGS WITH REGARD TO CORPORATE STRUCTURES

<b>Use of front or shell companies</b>	<p>The transaction involves the use of front or shell companies.</p> <p>A shell company has no real operating activity and is used to hide ML activity, and the identities of individuals involved so as to obscure the money trail. Shell companies enable illicit actors to create a network of legal entities around the world, and distance themselves from the illicit proceeds.</p> <p>By contrast, a front company has real business whose legitimate operations are used as a cover for ML and other criminal activity.</p>
<b>Numerous sole proprietorship businesses / private limited companies</b>	Numerous sole proprietorship businesses / private limited companies set up by seemingly unrelated people (proxies) are found to be controlled by the same group of people. For the setting up of such businesses, false addresses are registered.
<b>Related party transactions</b>	<p>Trade transaction reveals links between representatives of companies exchanging goods (e.g.: same owners or management).</p> <p>Related-party transactions (i.e. transactions between entities that are part of the same corporate or business group), rely on mutual agreements between the parties. Over or under-invoicing of goods and services requires collusion between the exporter and importer.</p> <p>Note: Although there is a higher risk of related party transactions being used for fraud and for TBML, dealings between related parties are not necessarily illegal.</p>

**B. RED FLAGS RELATING TO FINANCIAL & BANKING PRODUCTS<sup>iii</sup>**

<b>Letters of Credit<sup>iv</sup></b>	<p>Use of letters of credit to move money between those countries where such trade would not normally occur or is not consistent with the customer's usual business activity.</p>
	<p>Repeatedly amended or frequently extended letters of credit without reasonable justification, or that includes changes in regard to the beneficiary or location of payment without any apparent reason.</p>
<b>Method of payment</b>	<p>The method of payment requested by the client appears inconsistent with the risk characteristics of the transaction. For example, receipt of an advance payment for a shipment from a new seller in a high-risk jurisdiction.</p>
<b>Use of unrelated third-party entities</b>	<p>Transactions that involve payment from third-party entities that have no apparent connection with the transaction (unrelated to the seller or purchaser of goods).</p>
	<p>Transactions that involve front or shell companies or wire instructions/payment from parties which were not identified in the original letter of credit or other documentation.</p>
	<p>Transactions that involve payments for goods through cheques, bank drafts or money orders not drawn on the account of the entity that purchased the items.</p>
<b>Unusual deposits</b>	<p>Unusual deposits, e.g.: use of cash or negotiable instruments (such as traveler's cheques, cashier's cheques and money orders) in round denominations to fund bank accounts and to pay for goods and services.</p>
	<p>The negotiable instruments sequentially numbered or purchased at multiple locations, frequently lacking payee information. Cash payments for high-value orders are also indication of TBML activity.</p>

<sup>iii</sup> These indicators are helpful when reviewing FINTRAC disclosures.

<sup>iv</sup> An important payment method that facilitates international trade as a bank guarantees a buyer's payment to a seller. Sometimes referred to as documentary credit.



<b>Sudden onset and sudden cessation of transactions</b>	Sudden onset and equally sudden cessation of payments - typically wire transfers - within a short duration. This could be an indication that the account is temporarily being used to launder illicit proceeds.
<b>Use of multiple accounts without explanation</b>	Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity.
<b>Merchanting Trade</b>	The trade finance mechanism should be in place for both export leg, as well as import leg, of transaction. If the trade finance mechanism, for example Letters of Credit, have been provided for only the import leg of the transaction and not for export leg, this indicates the possibility of TBML.

### C. RED FLAGS WITH REGARD TO JURISDICTION

<b>Use of high risk shipment or transshipment points</b>	The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities, or sensitive / non co-operative jurisdictions.
	The commodity is transshipped through one or more such high-risk or sensitive jurisdictions for no apparent economic reason.
<b>Free Trade Zones / Special Economic Zones</b>	<p>Free Trade Zones (FTZs) are emerging as being especially vulnerable to TBML. Shipments of high value merchandise (such as electronics, auto parts and precious metals and gems) to duty-free trade zones, seen in conjunction with the following red flags, could be an indication of a trade-based money laundering activity:</p> <ol style="list-style-type: none"><li>1) Third-party payments for goods or services made by an intermediary (either an individual or an entity) apparently unrelated to the seller or purchaser of goods.</li><li>2) Amended letters of credit without reasonable justification.</li><li>3) Significant discrepancies between the descriptions of the goods on the transport document (e.g.: bill of lading), the invoice, or other documents (e.g.: certificate of origin, packing list).</li></ol> <p>Payment destinations that include Hong Kong, China, South Korea, Taiwan, Spain, Panama, Curacao, as they relate to free-trade zones.</p>



<b>Unusual or circuitous routing</b>	Circuitous route of shipment or circuitous route of financial or trade transaction.  Order for the goods is placed by firms or individuals from foreign countries other than the jurisdiction of the stated end-user.
<b>Transactions inconsistent with geographic trade patterns</b>	Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction (e.g.: trade in goods which are not normally exported or imported by a jurisdiction, or which does not make any economic sense). For example, semiconductor manufacturing equipment being shipped to a jurisdiction with no electronics industry.

#### D. RED FLAGS WITH REGARD TO GOODS

<b>Misrepresentation of description, quality or quantity of goods</b>	Significant discrepancies between the description, quality and quantity of the goods on the documents, such as bills of lading, invoices, and the actual goods shipped.  Misrepresentation may also be in relation to or type or grade of goods. For example, a relatively inexpensive good is supplied, but is invoiced as being more expensive, of different quality or even as an entirely different item so that the documentation does not accurately record what is actually supplied (mis-declaration).
<b>Discrepancies between reported value of commodity and fair market value</b>	Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value. This is done either in conjunction with mis-declaration of the description / quality / grade of goods or without it. This is also often associated with mis-declaration of the jurisdiction of origin.
<b>Irregularities with consignment size or type</b>	Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the importer / exporter or in relation to their regular business activities, or the shipment does not make economic sense (i.e. there is no reasonable explanation for the client's financial investment into the shipment).



<b>Vulnerable commodity</b>	<p>All trade transactions are vulnerable for TBML; however, some commodities provide greater opportunity for ML. Goods involved in TBML will usually be those where it is difficult to identify true value, due to the nature of these goods. For example, anomalies in value are less apparent and more difficult to substantiate in commodities that exhibit a wide range in their valuation. The following goods have been identified as vulnerable for TBML:</p> <ul style="list-style-type: none"><li>• electronics</li><li>• agricultural products (meats/meat products, dairy)</li><li>• garments (e.g. used clothes) and textiles</li><li>• vehicles/vehicle parts</li><li>• precious metals and stones</li><li>• pulp and paper</li></ul> <p><u>Note:</u> This is not an exhaustive list.</p>
-----------------------------	--

## IMPLICATIONS FOR THE CBSA AND CANADA

### Enforcement Mandate

37. As Canada's trade gatekeeper, the CBSA supports public safety and national security priorities by ensuring that all goods imported or exported comply with border-related program legislation. Traders seeking to convey goods to and from Canada have the obligation under the *Customs Act* to provide "true, accurate and complete" reporting of goods imported or exported<sup>v</sup>. Launderers who willfully make false statements to the CBSA by mis-describing customs documentation to evade their reporting obligations may be subject to investigation by the CBSA's Criminal Investigations Division; however, when customs offences appear to be facilitating money laundering, the CBSA is obligated to refer these instances to the RCMP for investigative consideration<sup>vi</sup>, and *Customs Act* offences may form the basis of subsequent laundering investigations by the RCMP.(U)
38. There is no criminal offence under Canadian law called "trade-based money laundering". Responsibility for enforcing financial crimes, including fraud and 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*).<sup>vii</sup> The

<sup>v</sup> Further to *Customs Act* subsections 7.1, 12 and 95(3)

<sup>vi</sup> According to the *CBSA Act*, the Agency has a legislated responsibility to provide cooperation, support, information and advice to other federal departments to assist them in carrying out their mandated responsibilities.

<sup>vii</sup> *Criminal Code* subsection 463 31(1). Proceeds of crime and money laundering offences fall under Part XII.2 of the Code.



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. 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.(U)

## Harms

39. There are four broad categories of consequences for Canada and Canadians when TBML is successful:

- **National Security:** TBML provides criminals and terrorists with a relatively risk-free mechanism to repatriate narcotics, corruption and terrorist financing proceeds, to evade international sanctions, and to finance proliferation activities.
- **Reputation:** TBML has the potential to further entrench the perception of Canada being "soft" on money laundering. For example, the United States has identified Canada as a "major" money laundering "jurisdiction of primary concern" in each iteration of its Department of State *International Narcotics Control Strategy Report* since at least 2009.
- **Economic Security:** Moreover, the trade distortions that TBML creates can undermine legitimate competition and macro-economic decision-making. Finally, TBML damage the reputation of the financial institutions within a country, as well as that of the country itself.
- **Revenue:** When dutiable goods are targeted, TBML deprives countries of revenues that may otherwise be collected.(U)

## Trade Fraud and Trade Based Money Laundering Centre of Expertise

40. In recognition of the threat posed by TBML in Canada, and the critical role played by CBSA in addressing the issue, the GoC authorized the creation of the Trade Fraud and Trade Based Money Laundering Centre of Expertise within the Agency. The Centre is operational as of April 2020 and is mandated to enhance the Agency's capacity to identify, interdict, and investigate complex trade fraud, and refer TBML files to the RCMP. Establishing a multi-disciplinary team comprised of intelligence analysts, trade specialists, and criminal investigators will better position the Agency to identify and investigate anomalous trade transactions indicative of TBML, and fill in knowledge gaps on threat actors and modus operandi.(U)

**Prepared by:** J.G. , Trade Fraud and Trade-Based Money Laundering Centre of Expertise



<sup>1</sup> John A. Cassara. Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance. Written testimony before the US House Financial Services Committee. 2016-02-03.

<sup>2</sup> Global Financial Integrity. Illicit Financial Flows to and from 148 Developing Countries: 2006- 2015. January, 2019.  
<https://www.gfinintegrity.org/wp-content/uploads/2019/01/GFI-2019-IFF-Update-Report-1.29.18.pdf>

<sup>3</sup> Global Financial Integrity. Trade-Related Illicit Financial Flows in 135 Developing Countries: 2008-2017. 2020-03-03.  
<https://secureservercdn.net/45.40.149.159/34n.8bd.myftpupload.com/wp-content/uploads/2020/03/GFI-Trade-IFF-Report-2020-Final.pdf?time=1588394966>

<sup>4</sup> R3 [REDACTED]

<sup>5</sup> Ibid.

<sup>6</sup> Financial Crimes Enforcement Network (FinCEN). Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering. FIN 2010-A001. 2010-02-18.

<sup>7</sup> Asia Pacific Ground on Money Laundering. Trade-Based Money Laundering Typologies. 2012-07-20. <http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaunderingttypologies.html>