Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

OPERATIONAL BRIEF

Risks and indicators for

Dealers in precious metals and stones

July 2019

Canada

INTRODUCTION

This operational brief provides information and guidance about the factors that expose individuals and entities (both retailers and wholesalers/suppliers) that are dealers in precious metals and stones to money laundering and terrorist financing risks. The brief also includes indicators to help such dealers determine when they should report a suspicious transaction to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

BACKGROUND

Dealers in precious metals and stones (DPMS) have a unique risk profile with regard to money laundering and terrorist financing because they trade in transferable items of value. This risk is heightened because these items could be one or more of the following:

- the proceeds of crime
- purchased with the proceeds of crime
- used to launder the proceeds of crime.

This brief aims to identify possible money laundering and terrorist financing activities and assess the risks DPMS face.

As part of Canada's anti-money laundering and anti-terrorist financing efforts, DPMS must understand their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations.

When DPMS carry out purchases or sales, and the value of a single transaction is $10,000 or more, they become what are known as "designated reporting entities" under the Act. This means they have to file a report with FINTRAC in the following circumstances:

- they receive CAN$10,000 or more in cash, or they receive two or more cash amounts of less than $10,000 each that total $10,000 or more within 24 consecutive hours, from or on behalf of the same individual or entity
- they know that property in their possession or under their control is owned by, or is controlled by or on behalf of, a terrorist or a terrorist group
- they have reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering or terrorist financing offence.

In addition, all DPMS must have policies and procedures in place to determine when transactions pose a high-risk for money laundering or terrorist financing. This is accomplished by creating an effective compliance program and a documented risk assessment approach, including mitigation measures and strategies. To ensure DPMS are meeting the requirements of the Act and associated Regulations, FINTRAC conducts on-site and office examinations, measuring DPMS's compliance and risk assessment activities against the requirements set out in operational briefs and other sources of information.

FINTRAC's website contains detailed guidance on the legal obligations of DPMS under the Act.

IDENTIFYING MONEY LAUNDERING AND TERRORIST FINANCING RISKS

There are five areas that DPMS should be aware of when assessing their risk of being exploited for money laundering or terrorist financing:

- their products, services and delivery channels
- their clients and business relationships, including clients' activity patterns and geographic locations
- the geographic location where they do business
- new technologies
- other relevant factors affecting their business.

Products, services and delivery channels

DPMS offer unique products and services to the marketplace. In turn, each product and service involves unique money laundering and terrorist financing risks.

Gold, for instance, can be of considerable value and have considerable liquidity—that is, it can be converted to cash relatively easily at near-purchase value. As another example, individuals can purchase, transfer or store some types of jewellery, diamonds, gold bars and other precious metals and stones more easily than bulk cash.

Accordingly, dealers are at risk for being exploited for money laundering or terrorist financing due to the following attributes associated with precious metals and stones:

- **Liquidity**: This is the degree to which a product can be sold for near-purchase price. Higher liquidity means a higher risk for money laundering or terrorist financing. For example, gold has very high liquidity, while most finished jewellery does not.
- **Market size**: A larger market makes it easier to convert a product into cash or other financial instruments, and thus presents a higher risk for money laundering or terrorist financing.
- **Product value**: The higher the value of the product, the more attractive it is to criminals; therefore, the risk of money laundering or terrorist financing increases.
- **Product size/mass**: The larger the product, the harder it is to transport and/or store, which reduces the risk of money laundering or terrorist financing. For example, lower quality or unrefined stones, which are larger or heavier than their value would suggest, present less risk for money laundering or terrorist financing than do higher quality stones.
- **Ability to store/transfer**: The easier it is to store or transport a product, the higher risk it presents for money laundering or terrorist financing. Some contributing characteristics are the durability of the product, the ease of detecting the product and the changeability of the product.

When conducting transactions, DPMS must consider these attributes in conjunction with the other money laundering risks described in this brief.

DPMS must also consider their service delivery channels. Transactions not conducted face to face present greater money laundering or terrorist financing risk, particularly when products are shipped to post office boxes or international addresses.

Clients and business relationships, including activity patterns and geographic locations

When assessing the money laundering and terrorist financing risks transactions pose, DPMS must consider how clients present themselves and conduct transactions.

Dealing in large amounts of cash brings significant money laundering and terrorist financing risks with it, and these risks can extend beyond receiving cash as payment in a single transaction. For example, clients can make cash payments against layaway plans in an attempt to structure transactions and avoid reporting requirements. This makes DPMS vulnerable to exploitation over the life of the plans.

Transaction activity related to layaway plans may be subject to the large cash reporting requirement under the Act. When DPMS receive $10,000 or more in cash within a 24-hour period from or on behalf of the same person or entity, they must file a large cash transaction report with FINTRAC. When it appears that cash payments are being split up to avoid this type of reporting, DPMS should file a suspicious transaction report with FINTRAC.

At the same time, dealers should not assume that non-cash transactions are “clean,” since illicit funds could have been placed into the financial system prior to the transactions taking place. Other financial instruments may present lower money laundering or terrorist financing risk than cash, but the risk nevertheless exists and varies between instruments. For example, bank drafts present more risk than cheques because they are not linked to an account and its associated customer due diligence, while cheques are linked to an account.

When customers use other payment methods, such as wire transfers, credit cards or cheques, DPMS should consider whether transactions are in line with what is known about the customer and whether they are normal in the context of their dealings with those customers. For example, individuals who have made arrangements to ensure their anonymity, such as purchasing through shell companies, present a risk for money laundering or terrorist financing, since this is not a normal business practice. A purchase or a series of purchases outside of the apparent means of a client should be considered when assessing the money laundering or terrorist financing risk the client presents.

Geographic locations where dealers do business

DPMS must consider the location of their business, and how that affects their money laundering and terrorist financing risks. In particular, DPMS must evaluate the following characteristics:

- **Where the business is located**
  - whether they are located in a high-crime area or low-crime area
  - whether they are located in a rural area, where clients may be known to them, or do business in a large city, where new clients and anonymity are more likely
  - whether they see very-high-volume sales relative to the apparent financial standing of their surroundings
  - whether the business is close to a border crossing, since this could increase risk (businesses so located may be the first point of entry into Canada’s financial system).

- **Where the business is conducting transactions**
  - whether the business operates with a storefront only, online only or through a mix of locations and platforms
  - whether the business conducts transactions with foreign clients based in countries subject to sanctions, embargoes or other measures (these transactions should be considered high-risk).
- **Where the business's inventory is sourced from**
  - whether sellers are well known to the business, or the business works with a variety of providers
  - whether the business has inventory or works with sellers in jurisdictions of concern.

New technologies

DPMS must also consider whether their business is exposed to incremental money laundering and terrorist financing risks as a result of new technologies that their customers are using to pay for products or that they themselves are using to sell them. New technologies differ from product to product; however, some offer benefits to potential money launderers and terrorist financiers, including enhanced anonymity, quicker transactions and transactions outside of the financial system covered by anti-money laundering and anti-terrorist financing regulations.

Over the past several years, FINTRAC has noted an increased prevalence of new technologies in its suspicious transaction reports and disclosures of money laundering and terrorist financing activities to law enforcement. Virtual currencies, email money transfers and payment processors in particular have increased in prominence in FINTRAC's reporting.

Other relevant factors affecting the business

Finally, DPMS must consider other potentially relevant risk factors that may be affecting their risk level, and the risk level of customers, for money laundering and terrorist financing:

- **Elements of the DPMS's structure**: Entities with a high turnover of staff may present greater risks for money laundering and terrorist financing, since their staff may be less likely to be able to recognize potential red flags. Additionally, entities that operate solely in one location have significantly different risks than entities that are part of a chain with many locations.
- **Use of intermediary agents**: The use of intermediary agents to conduct transactions may present a higher risk. Entities should consider the transactions' appropriateness, necessity and normalcy.
- **Barriers to entry**: For parts of the industry with higher barriers to entry, such as specialized licences to sell, the money laundering and terrorist financing risks may be lower, since criminals may have a harder time infiltrating these markets.
- **Trends, typologies and potential threats of money laundering and terrorist financing**: When DPMS are dealing with clients for whom there are observable trends and/or typologies of money laundering and terrorist financing, they should review FINTRAC's Suspicious Transaction Guidance and Strategic Intelligence to determine whether these clients present a higher risk for money laundering or terrorist financing.

RISK MITIGATION: RISK-BASED APPROACH AND EFFECTIVE COMPLIANCE PROGRAM

FINTRAC published a comprehensive risk-based approach workbook on how DPMS can mitigate their risk of exploitation for money laundering or terrorist financing. This workbook is structured to help dealers identify the risks associated with products, services and delivery channels; clients and business relationships; and geography, as it relates to both clients and the location of their own business.

In addition to taking a risk-based approach, DPMS must put a comprehensive and effective compliance program in place to meet all their reporting and other obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (e.g. client identification and record-keeping).

INDICATORS OF SUSPICIOUS TRANSACTIONS

FINTRAC has developed indicators of suspicious transactions based on key factors related to retail and wholesale/supplier DPMS. These indicators detail situations and/or transactions in which DPMS are at an increased risk to be exploited for money laundering or terrorist financing, such that further assessment of these transactions may be required to appropriately mitigate the risk.

The indicators that follow are intended to help DPMS assess whether there may be reasonable grounds to suspect that a transaction, or attempted transaction, is related to the commission of a money laundering or terrorist financing offence. DPMS should use these indicators in conjunction with other published indicators, such as those contained in FINTRAC's Money Laundering and Terrorist Financing Indicators Guidance for DPMS. In addition, FINTRAC's Suspicious Transaction Guidance provides key considerations for determining whether DPMS should submit a suspicious transaction report to FINTRAC.

Retail indicators

INDICATOR (T for transactional indicators and B for behavioural indicators)	
T	The individual appears to be structuring amounts to avoid customer identification or reporting thresholds.
T	The individual frequently uses layaway plans in an apparent attempt to avoid reporting requirements (also known as structuring).
T	The individual uses a payment card that appears to be altered or stolen.
T	The individual buys high-value goods using small-denomination bills ($5, $10, $20).
T	The individual sells gold in non-standard bricks or similar shapes with no distinct markings or value.
T	The individual will only trade items for cash or other precious metals and stones.
T	The individual attempts to buy precious metals or stones with a company credit card or a credit card not in their name.
T	The individual trades items for similar items of near-equal value.
T	The individual uses negotiable instruments or credit cards issued in a country other than Canada to make purchases.
T	The individual frequently crosses the Canada–U.S. border to buy jewellery or precious metals, in particular where there is not a strong economic incentive to do so.
T	The customer or supplier attempts to maintain a high degree of secrecy with respect to the transaction, such as requesting that normal business records not be kept.
T	The individual makes large or frequent purchases in funds other than Canadian dollars.
B	The individual appears to be living beyond their means.
B	The transactional activity (level or volume) is inconsistent with the individual's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance).
B	The individual cannot explain the origin of the precious metals and stones.
B	The individual is willing to sell items at rates significantly lower than their typical sale value.
B	The individual appears to be uninterested in the details of the sale or purchase of goods, which would normally be material information for a client.
B	The individual indiscriminately purchases merchandise without regard for value, size or colour.
B	The individual is vague or refuses to provide details about why they are selling or buying items, or about the origin of the items.
B	The individual uses alternative addresses for deliveries, uses post office boxes or uses third parties to receive purchases.
B	Multiple individuals are involved in retrieving, transporting or purchasing items.
B	The individual does not wish to buy or sell face to face and is nervous about information related to their identification.
B	The individual attempts to purchase abnormally large quantities of precious metals or loose jewels in non-wearable form.

Wholesale/supplier indicators

INDICATOR (T for transactional indicators and B for behavioural indicators)	
T	The individual or entity appears to be structuring amounts to avoid customer identification or reporting thresholds.
T	The individual or entity pays for high-priced jewellery or precious metals with cash only.
T	The individual or entity pays for purchases through a lawyer's trust account.
T	The individual or entity pays for expensive purchases exclusively with cryptocurrency, especially when buying gold stored by a wholesaler or supplier.
T	The individual or entity uses financial instruments from a foreign bank and/or that are not in Canadian dollars.
B	The individual or entity amasses a large amount of stored bullion or precious stones over time, in an apparent attempt to avoid reporting requirements (known as structuring).
B	The individual's or entity's listed address is in a high-risk jurisdiction known for corruption or smuggling relating to precious metals or stones.
B	The individual or entity sells a large amount of precious metals and stones that originate or are known to be traded from areas not known for their production (i.e. trading centres).
B	The individual or entity amasses a large amount of precious metals or stones in a wholesaler's or supplier's storage facility or pool over time.
B	The entity's ownership structure appears invalid or altered, or the entity refuses to provide additional information when requested.
B	The individual benefiting from the purchase cannot be identified.
B	The location to which bullion or stones are moved directly to or from storage is different from the individual's or entity's listed address.
B	The individual or entity continually moves large volumes of bullion directly into and out of storage.
B	The individual provides only a non-civic address such as a post office box, or disguises a post office box as a civic address for the purpose of concealing their physical residence.
B	The individual or entity does not appear to understand the precious metals and stones industry, or lacks the appropriate equipment or finances to engage in activity in that industry.
B	The individual appears to be uninterested in or uninformed about the structure or transactions of their business.
B	The size or type of transactions is atypical for the individual or entity.
B	The customer or supplier attempts to maintain a high degree of secrecy with respect to the transaction, such as requesting that normal business records not be kept.

Contact FINTRAC

Email: guidelines-lignesdirectrices@fintrac-canafe.gc.ca

Telephone: 1-866-346-8722 (toll free)

Facsimile: 613-943-7931

Mail: FINTRAC
24th Floor, 234 Laurier Avenue West
Ottawa, ON K1P 1H7
Canada

Cat. No. FD4-21/2019E-PDF
ISBN 978-0-660-31641-3