



# MONEY LAUNDERING AND TERRORIST FINANCING TYPOLOGIES AND TRENDS IN CANADIAN BANKING

MAY 2009

Big Five Bank Participants:

CIBC  
RBC  
BNS  
TD  
BMO

**MONEY LAUNDERING  
AND TERRORIST FINANCING  
TYPOLOGIES AND TRENDS  
IN CANADIAN BANKING**

**MAY 2009**



## MESSAGE FROM THE DIRECTOR

I am pleased to present the first report intended to address the interests of the Canadian banking sector and other financial entities, **Money Laundering and Terrorist Financing Typologies and Trends in Canadian Banking**.

The efforts to combat money laundering and terrorist activity financing are, by necessity, collaborative. The Canadian banking sector and other financial entities are uniquely positioned through their involvement in hundreds of millions of financial transactions to make a contribution to this effort. As Canada's financial intelligence unit, FINTRAC is able to aggregate and analyze the reported transactions from many different sectors in order to produce financial intelligence. Ultimately, the investigations and prosecutions that are assisted by this intelligence are carried out at yet another stage of the larger initiative.

As FINTRAC's Director, I am aware of the need for greater information sharing throughout this chain of activity. I hope that this report and the collaborative spirit within which it has been undertaken are a step in that direction. I look forward to building on this first report and working collaboratively on similar future projects.

As you take the time to read it, I would encourage you to comment on its contents and to suggest issues for future exploration and exposition.

Jeanne M. Flemming  
Director



# TABLE OF CONTENTS

INTRODUCTION .....	2
REVIEW OF CASES DISCLOSED BY FINTRAC IN 2007-2008 .....	3
<b>General observations</b> .....	3
Types of suspected activities and predicate offences .....	3
Common phases and techniques of money laundering .....	3
Sectors used .....	4
Types of businesses involved .....	4
<b>Suspicious financial transactions</b> .....	6
SANITIZED CASES .....	7
<b>Sanitized Case 1 – Fraud-related Money Laundering</b> .....	7
<b>Sanitized Case 2 – Drug-related Money Laundering</b> .....	7
<b>Sanitized Case 3 – Terrorist Financing</b> .....	8
TYOLOGIES .....	9
<b>Investment companies and trusts</b> .....	9
<b>Securities industry</b> .....	11
EMERGING VULNERABILITIES .....	14
<b>Prepaid cards</b> .....	14
Vulnerabilities associated with open-loop prepaid cards .....	14
Vulnerabilities associated with closed-loop prepaid cards .....	15
<b>Digital Precious Metals</b> .....	15
CONCLUSION .....	18



## INTRODUCTION

This report is the first of its kind. It has been made possible through the collaboration of five of Canada's largest banks and FINTRAC. The exchange between the banking sector and the financial intelligence unit has guided the subjects that are examined in this report.

Through this paper FINTRAC seeks to address questions about money laundering and terrorist financing that are unique to the Canadian banking sector and have been observed in our analysis of financial transactions. Through a better understanding of these patterns and trends, the banking sector will be better able to combat money laundering and terrorist financing and able to carry out their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

There are four key sections to the report. The first section highlights the observations of a review of all the cases FINTRAC disclosed to law enforcement or national securities agencies in 2007-2008. The second section presents sanitized cases and the third section presents typologies on money laundering and terrorist financing (ML/TF) related to the banking sector. The difference between a sanitized case and typology will be further explained in those sections. The final section identifies two emerging vulnerabilities that may be of interest to the banking sector.

It is important to note that statistics related to the prosecution or asset confiscation of a money laundering or terrorist financing case that may contain information that FINTRAC disclosed is not included in the report, as FINTRAC is not an investigative agency. The focus of this report is the intelligence that FINTRAC has been able to produce to assist investigations and the observed trends as they related to Canadian banking.

# REVIEW OF CASES DISCLOSED BY FINTRAC IN 2007-2008

For this report, FINTRAC conducted an extensive review and analysis of all cases disclosed to various recipients for the fiscal year 2007-2008 (April 2007 to March 2008). Annual case reviews provide a complete picture of the trends and activities related to ML/TF within that year. Every case review better positions FINTRAC to be able to identify Canadian trends in ML/TF and ultimately share this information with reporting entities.

The methodology for the case review involved a complete examination of all cases with a focus on some key characteristics within a FINTRAC case disclosure. For clarification, a FINTRAC case disclosure contains what is referred to as “designated information” that is prescribed by our enabling legislation. This designated information includes key identifying information from FINTRAC’s analysis (e.g. name, address, bank account numbers, etc.). For the purposes of this document, the general observations presented place emphasis on the following characteristics:

- types of case/activities;
- most common predicate offences<sup>1</sup>;
- sectors used for various activities associated to ML/TF;
- most common ML/TF stages and techniques used; and
- most common types of businesses used in ML/TF schemes.

In addition, the most common suspicious financial transactions that FINTRAC observed in money laundering (including cases related to drug and fraud) and terrorist financing cases are also presented. It should be noted that the examples of suspicious financial transactions included in the case review are not necessarily an indication of the frequency in which they were used but are included because they were representative and specific of different types of cases.

## General observations

### TYPES OF SUSPECTED ACTIVITIES AND PREDICATE OFFENCES

In 2007-2008, FINTRAC disclosed a total of 210 cases, divided in the following activities:

- 171 cases associated with money laundering
- 10 cases associated with money laundering and terrorist financing
- 29 cases associated with terrorist financing and threats to national security<sup>2</sup>.

FINTRAC may be informed of the suspected predicate offence through voluntary information received from law enforcement or it may be included in a suspicious transaction report. In instances where FINTRAC was able to link the suspected money laundering to a suspected predicate criminal offence, fraud and drug trafficking were the most frequently observed offences. For the cases where fraud was suspected, investment/securities and telemarketing fraud were the most observed. For cases where drug-related activities were suspected, marijuana grow operations and/or distribution, as well as the trafficking of cocaine were the most observed.

### COMMON PHASES AND TECHNIQUES OF MONEY LAUNDERING

In reviewing the most common phases and techniques of money laundering appearing in the cases, the results are similar to previous years. The most observed stages of money laundering were placement and layering and the most common techniques for money laundering were structuring and smurfing. Structuring normally involves multiple cash deposits or withdrawals at amounts below the reporting threshold and smurfing is defined as multiple deposits of cash, and/or low-value monetary instruments purchased from various banks or money services businesses by various individuals. Nominees (individuals and businesses) were also found to be involved in at least nine cases that related to drugs or organized crime.

<sup>1</sup> For FINTRAC’s purposes, a “predicate offence” is an offence under the *Criminal Code* or any other criminal law statutes under Parliament’s jurisdiction from which proceeds of crime may be derived (with the exception of offences under certain acts including the *Income Tax Act* and the *Excise Tax Act*.)

<sup>2</sup> FINTRAC’s role is to provide CSIS with financial intelligence to assist that agency in fulfilling its mandate of investigating threats to the security of Canada. There will be limited references to threats to national security in this document.

There are **three** widely recognized stages in the money laundering process:

**PLACEMENT** involves placing the proceeds of crime in the financial system.

**LAYERING** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.

**INTEGRATION** involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

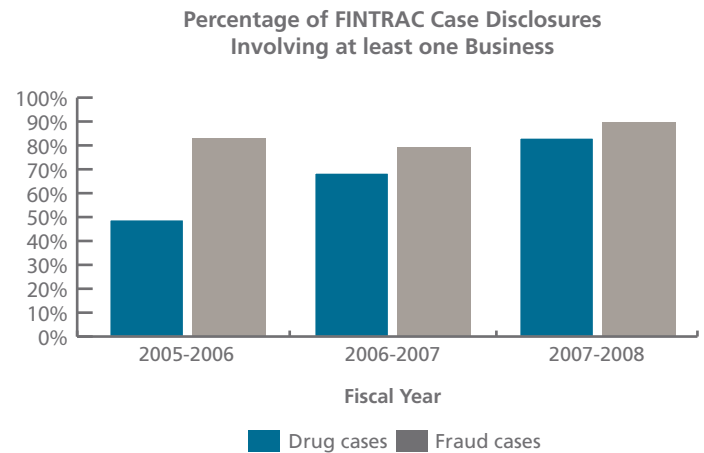
#### SECTORS USED

The reports submitted by the banking sector to FINTRAC, suspicious transactions reports (STRs), large cash transaction reports (LCTRs) and electronic funds transfer reports (EFTRs) played a major role in assisting FINTRAC in identifying individuals and entities suspected of being involved in activities associated with ML/TF. This role is attributed to the large volume of reports provided by banks and financial institutions to FINTRAC and also the implementation of strong compliance regimes to detect suspicious financial transactions. As observed in the previous years, the majority of suspicious financial transactions associated to cases disclosed to law enforcement and the intelligence community in 2007-2008 were conducted through banks and other financial institutions.

Casinos, money services businesses (MSBs), and some trust companies or accounts were also used to conduct suspicious financial transactions, but to a lesser extent. It was found that suspicious financial transactions were conducted at casinos in twenty-five cases and were mostly related to suspected drug offences but also to suspected fraud and terrorist financing. Trust companies or accounts were involved in at least twelve cases that were suspected to be related to drug, fraud, terrorist financing and organized crime activities. The use of Internet payment systems was observed in five cases.

#### TYPES OF BUSINESSES INVOLVED

In some instances, case disclosures only involve individuals, but often, they also involve businesses. In fact, the majority of 2007-2008 cases suspected to be related to drug or fraud involved individuals and at least one business and, in most instances, multiple businesses. The chart below provides an illustration of how the number of cases involving businesses has changed over the last few years:

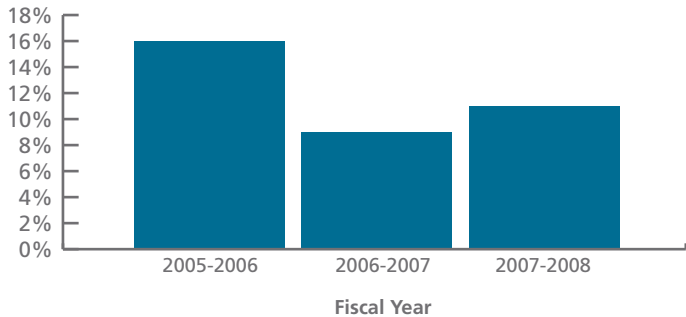


As observed on the chart, the number of drug-related cases involving businesses continued to increase for the third year in a row. A slight increase was also observed in the number of cases involving fraud.

On the other hand, 82% of cases related to terrorist financing and/or other threats to the security of Canada in 2007-2008 also involved businesses and/or non-profit organizations, and remained almost the same.

The chart on page 5 illustrates how the percentage of cases involving individuals and/or businesses believed or suspected to be associated to organized crime groups has remained fairly stable in the last two years, 11% in 2007-2008 and 9% in 2006-2007, after having decreased to almost half of what it was in 2005-2006 (16%):

Percentage of Case Disclosures Believed or Suspected to be Associated to Organized Crime



The following types of businesses were found to be associated to *all types of cases*, that is, suspected to be complicit in (or created for the purpose of) laundering illicit proceeds gained from various criminal activities (possibly related to drugs, fraud and organized crime), and suspected of acting as vehicles for terrorist financing:

- investment/trust companies;
- import/export businesses (e.g. food, clothing, medical supplies);
- money services businesses (MSB), including foreign currency exchange dealers;
- telecommunications businesses; and
- car sales/rentals.

The table on the right identifies additional types of businesses that were specifically associated to each type of case:

DRUG/ORGANIZED CRIME <sup>3</sup>
Hydroponics/indoor gardening
Construction renovation
Real estate
Travel agencies
Electronics
Pharmaceutical
Convenience/grocery stores
FRAUD
Holding companies
Real estate development
Consulting firms
Energy sector
Precious metals
Technology
TERRORIST FINANCING
Non-profit organizations
Convenience/grocery stores
Real estate

<sup>3</sup> Organized crime groups are often involved in various types of criminal activities which include drugs, fraud, prostitution, loan sharking, cigarette and tobacco contraband, and so on. However, because most of these cases involved drugs and similar types of businesses were used, organized crime activities have been included in this section dealing with drug offences.

## Suspicious financial transactions

The following identifies the most common types of suspicious financial transactions for ML/TF cases conducted through the banking sector in 2007-2008. In most instances, it is also indicated at what stage of ML/TF the suspicious financial transaction had likely occurred:

- Large cash deposits (\$20, \$50 or \$100 bills)/cheques/bank drafts (often under the reporting threshold – structuring) to personal/business bank accounts followed by either issuance of cheques (often payable to 3rd parties) or purchase of bank drafts or electronic funds transfers (EFTs) to Canadian or foreign entities/individuals (often associated) or cash withdrawals – **placement, layering and use of pass-through accounts to conceal source of funds**
- Deposits of \$20 bills (CAD) were sometimes followed by USD EFTs – **placement and layering**
- Deposits of cash or cheques were sometimes followed by transfers to accounts held by the same individual/entity in other Canadian or foreign financial institutions – **placement and layering**
- Multiple cash deposits were conducted in a short time frame and below the reporting threshold, as well as alternating between branches across the country (sometimes through automated teller machines), followed by cash withdrawals – **structuring and smurfing in an effort to place the funds**
- Receipt of EFTs followed by purchase of bank drafts or issuance of cheques payable to 3rd parties – **layering**

More specifically, for drug-related cases, the suspicious financial transactions represented **placement and layering** activities:

- Large cash deposits (structured and conducted by various individuals in different locations – i.e. **smurfing**) followed by EFTs sent to foreign countries (often to Asia)

- USD deposits in bank accounts held by one MSB (in larger amounts than normal for most MSBs as indicated in STR information) followed by purchase of USD bank drafts payable to an entity with similar name
- Numerous EFTs sent to one MSB and associated individuals from an individual in a country of concern

Of the identified drug cases, certain types of suspicious financial transactions were found to be particularly associated to grow operations:

- Bank drafts purchased at one bank and deposited at another bank, then followed by EFTs sent to foreign countries
- Numerous large rounded-sum cash deposits followed by payment of large hydro bills
- Cash payments (under threshold) to credit card accounts (sometimes multiple payments in one day and conducted by 3rd parties)

For fraud-related cases suspicious financial transactions represented mostly **layering** activities:

- Cheques or bank drafts drawn from a financial institution were deposited into business accounts held at other financial institutions then followed by cash withdrawals
- 3<sup>rd</sup> parties in the United States purchased, over a short period, large numbers of money orders (in \$500 and \$1000) payable to companies in Canada – these money orders were deposited in business accounts held in Canada, then EFTs were sent back to accounts in the United States – this scheme was repeated a number of times

Terrorist financing cases were found to include the following types of suspicious financial transactions:

- Large cash deposits (sometimes conducted by third parties) into accounts of non-profit organizations
- Large number of deposits (into personal accounts) of cheques drawn from legal trust accounts followed by withdrawals
- Deposits of U.S. postal money orders (\$500 and \$1000) or cash were followed by large cash withdrawals or issuance of cheques or purchase of bank drafts payable to foreign MSB

## SANITIZED CASES

In an effort to provide additional insight based on the review of the cases FINTRAC disclosed in 2007-2008, the following are actual cases that were disclosed to law enforcement or national security agencies. The cases included in this section are sanitized, all identifying information has been removed and were chosen for inclusion in this paper as they involve transactions associated with both retail (personal) and commercial (business) banking. The “red flags” associated with each case assisted FINTRAC to reach the threshold for reasonable grounds to suspect that the information would be relevant to a money laundering or terrorist financing investigation, and thus to disclose the case.

### Sanitized Case 1 – Fraud-Related Money Laundering

FINTRAC received one STR from a bank, which generated this case involving ten individuals and twelve businesses, located in the greater Toronto area, suspected of possible fraudulent and money laundering activities. An additional 22 STRs, provided by the same bank and two others, as well as one MSB, further contributed to this case.

FINTRAC’s analysis revealed that most businesses in this case appeared to be involved in the employment service industry and the associated individuals/officers conducted multiple cash deposits. Employees of the businesses were also paid in cash. These transactions were found to be unusual since this industry is not typically cash-driven. The businesses were linked through common directors/officers, financial transactions, and shared addresses/phone numbers. The individuals involved were also linked through similar addresses and joint signing authorities for various bank accounts.

One individual was the subject of a previous disclosure to law enforcement regarding fraud/extortion activities and was suspected to have links to Eastern European organized crime.

#### *RED FLAGS associated with this case:*

- Individuals made cash deposits (in \$100 and \$50 denominations) into the personal accounts of multiple associates who then issued cheques payable to other individuals (i.e. use of pass-through accounts)
- Numerous businesses paid their employees in cash and reporting entities indicated in the STR that this was not consistent with typical business operations
- Cheques were deposited into business accounts then immediately withdrawn in cash or through the issuance of cheques payable “to cash” or payable to the individual making the initial deposit
- Reporting entities also reported excessive cash flow in the business accounts

The transactions conducted in this case were mostly representative of the placement and layering stages of money laundering. The relevant designated information was disclosed to four different law enforcement agencies.

### Sanitized Case 2 – Drug-Related Money Laundering

FINTRAC received information from law enforcement regarding a number of individuals and businesses, located in the greater Vancouver area, under investigation for suspected involvement in the importation of drugs to Canada from an Asian country.

FINTRAC’s analysis revealed financial transactions associated to five of the individuals and three MSBs that were mentioned in the information provided by law enforcement. FINTRAC suspected that six additional individuals and five businesses specializing in telecommunications, construction, foreign exchange and interior renovation were also involved in the scheme.

Thirty-five STRs reported to FINTRAC by multiple branches of four different banks and three different credit unions were instrumental in allowing FINTRAC to find connections between the various players in this scheme, as well as

identifying ones that may not have been previously known to law enforcement. LCTRs and EFTRs also assisted FINTRAC in its analysis.

**RED FLAGS associated with this case:**

- Large cash deposits (in CAD and USD) into personal accounts were sometimes followed by the purchase of bank drafts payable to trust companies or money services/currency exchange businesses
- Domestic wire transfers between personal accounts were followed by the purchase of bank drafts payable to trust companies
- Bank drafts and cheques issued from other financial institutions were deposited into personal and business accounts and were sometimes followed by EFTs to a Middle Eastern country
- EFTs were also received from the same Middle Eastern country
- Multiple transactions were carried out on the same day at the same branch but with different tellers, hours apart
- Some cash deposits were structured to keep amounts under the reporting threshold and/or conducted at different branches
- Cash, cheques and bank drafts were deposited by third parties into the business accounts of MSBs and domestic wires were received into the same accounts; they were immediately followed by withdrawals to purchase bank drafts payable to other MSBs which then sent EFTs to various beneficiaries in foreign countries
- The same MSBs receiving deposits or wires also directly sent EFTs to beneficiaries in foreign countries

Individuals and entities involved in this case appear to have conducted a number of suspicious activities mostly representative of the placement and layering stages of money laundering in addition to furthering their drug trafficking activities. FINTRAC disclosed all relevant designated information to law enforcement to assist them in their investigation.

## Sanitized Case 3 – Terrorist Financing

FINTRAC received information from law enforcement and intelligence agencies regarding a non-profit organization (NPO), located in the greater Toronto area, which was suspected of acting as a front for a terrorist organization. The NPO and associated individuals were suspected of facilitating the acquisition and aggregation<sup>4</sup> of financial resources in Canada, as well as the transmission of resources ultimately for the benefit of the terrorist organization's operations overseas.

The NPO was the subject of several FINTRAC disclosures to law enforcement and intelligence agencies between 2002 and 2007. STRs, LCTRs and EFTRs from financial institutions were instrumental in assisting FINTRAC in its analysis.

**RED FLAGS associated with this case:**

- The NPO ordered many EFTs to the benefit of individuals and entities (including a foreign NPO also suspected of being a front for the terrorist organization) located overseas. The EFTs were ordered primarily through major financial institutions rather than through domestic MSBs
- Various officers of the NPO made large cash deposits to the various accounts of the suspect NPO, held at multiple financial institutions, for which the source of funds was unknown
- An individual also attempted to deposit a number of cheques, made payable to third parties, to the account of the suspect NPO
- Multiple, recurrent electronic credits were made to the accounts of the suspect NPO for which the original source of funds and remitters' identity were unknown
- The deposit of cash and monetary instruments (cheques, bank drafts etc.) to the account of the suspect NPO, were often followed by the purchase of bank drafts or offshore movement of funds

FINTRAC disclosed all relevant designated information to law enforcement and intelligence agencies to assist them in their investigation.

<sup>4</sup> Acquisition is the initial identifiable movement of funds or goods into the process of terrorist financing and includes activities such as voluntary donations by individuals/businesses to charitable organizations, loans by individuals and businesses to terrorist front organizations, and the use of proceeds (funds or goods) from criminal activities. Aggregation is the stage of terrorist financing involving the pooling of smaller amounts of funds or goods into larger ones, usually by moving them to financial institution accounts or to other locations.

# TYOLOGIES

When a series of money laundering or terrorist financing schemes appear to be constructed in a similar fashion or using the same methods, the similar schemes are generally classified as a typology. By reviewing its cases and conducting targeted environmental scanning, FINTRAC was able to identify a number of typologies associated to wealth management. In particular, this section discusses the use of investment companies/trusts and the securities industry for the purpose of money laundering. Case examples are also provided.

## Investment companies and trusts

The following typologies have been identified as a result of a comprehensive study conducted by FINTRAC of all cases disclosed between April 2005 and March 2007 that involved money laundering through the use of investment companies and trusts<sup>5</sup>. The review provided FINTRAC with better knowledge of how investment companies and trusts located in Canada or associated with Canadian individuals/entities could be used or controlled for suspected ML/TF activity. The use of professionals as intermediaries in the creation of such companies or accounts, and the facilitation of some financial transactions was also studied.

The results of this study indicated that investment companies and trusts may be used by individuals committing various crimes (drug, fraud and other organized criminal activities). While both can sometimes be used to commit fraud, they appeared to be mostly used in the layering stage of money laundering.

Three typologies were found to be associated, although not exclusively, with the use of investment companies and trusts for suspected money laundering and terrorist financing purposes:

1. multi-jurisdictional structures of corporate entities and trusts;
2. involvement of non-financial intermediaries/professionals; and
3. use of nominees (individuals and businesses, including shell companies).

## CASE EXAMPLE PROVIDING AN OVERVIEW OF THE THREE TYPOLOGIES

Information from law enforcement indicated that a large number of individuals and businesses, located in the greater Montreal area and with links to organized crime, were under investigation for money laundering and proceeds of crime related offences.

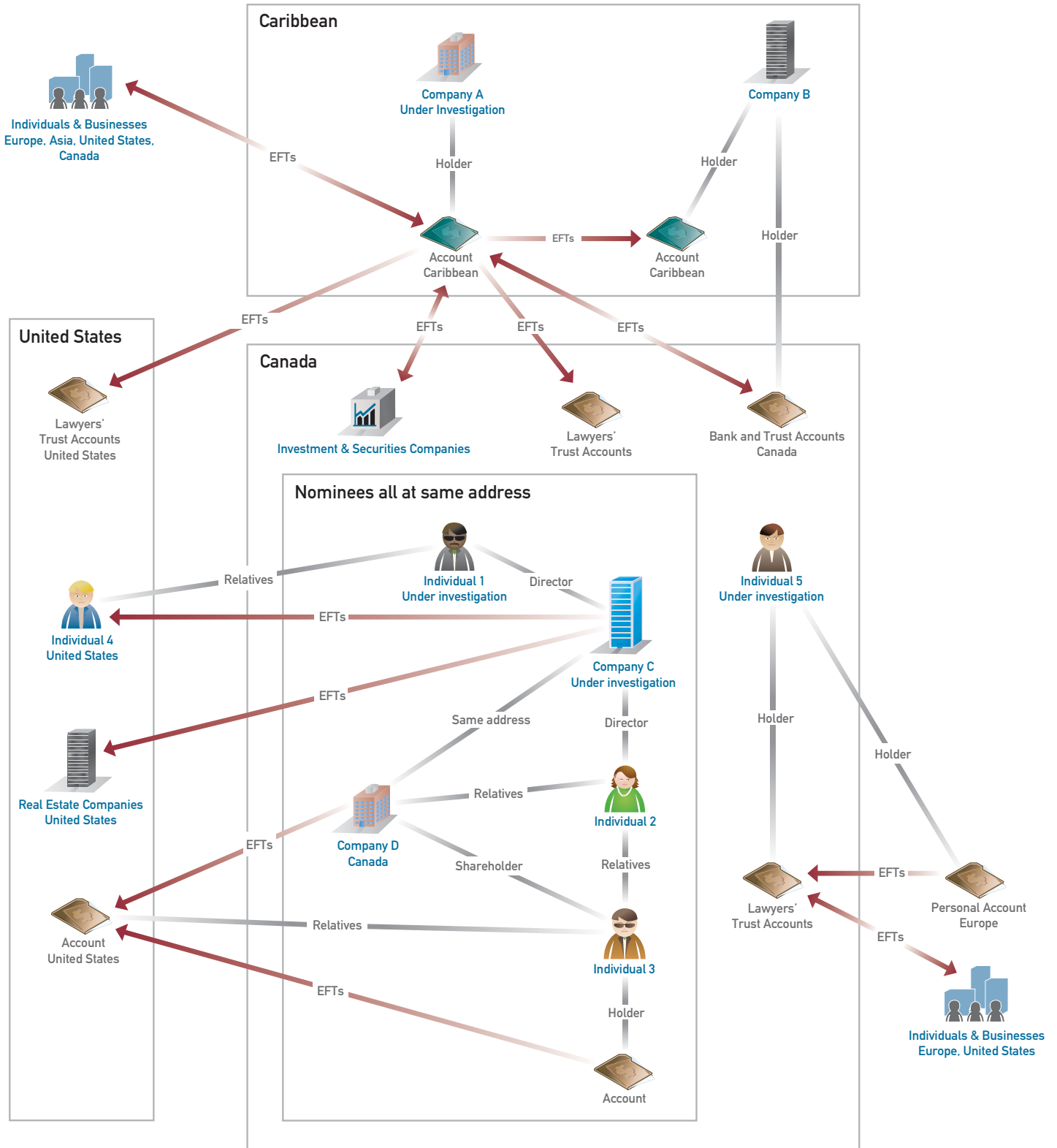
This Canadian organized crime group was believed to be generating illicit revenues and was suspected of investing these revenues in various businesses (including investment companies) that generated further profits. This was done with the assistance of nominees (family members and other associates) and through the use of trust accounts set up by lawyers and/or notaries, referred to as lawyers' trust accounts.

Many separately incorporated businesses were found to be located at the same address and their owners or directors were suspected to be nominees, sometimes with no apparent links to the organized crime group. Most of the companies were located in Canada but many financial transactions were conducted with offshore companies (**Company A** and **Company B**), some of them suspected of having been created for the sole purpose of concealing the criminal origins and ownership of the funds. As published on their Web sites, these two companies were reported to offer financial and investment services, which included the use of trusts, therefore allowing the clients to keep their own identity and that of beneficiaries completely confidential.

The chart on page 10 summarizes the case, but most importantly, illustrates the complexity of money laundering schemes.

<sup>5</sup> For the purpose of this document, "trusts" is used when referring to both trust companies and trust accounts that are set up by lawyers or notaries, and held within financial institutions.

**SUSPECTED LAUNDERING OF CRIMINAL PROCEEDS CONDUCTED THROUGH THE USE OF INVESTMENT COMPANIES AND TRUSTS.**



## HIGHLIGHTS OF THE CASE:

- EFTs were ordered by or for the benefit of **Company A**, located in the Caribbean, and individuals and businesses from Europe, Asia, and the United States. Furthermore, EFTs were ordered by or for the benefit of **Company A** and investment/securities companies, as well as trust accounts (including lawyers' trust accounts) located in Canada, some of them held by **Company B**. **Company A** also ordered EFTs to the benefit of a lawyer's trust account held in the United States.
- **Company C** and its Director, **Individual 1**, both under investigation and suspected of being nominees for the organized crime group, were found to be associated with another three investment companies (including **Company D**) and two other individuals (**Individual 2** and **Individual 3**). All of these entities were associated with the same specific address in Eastern Canada and were linked through their positions within each organization.
- **Company C** offered financial services and ordered EFTs to the benefit of **Individual 4**, a lawyer residing in the United States. **Individual 4** and **Individual 1** had the same last name and were suspected of being relatives. **Company C** also ordered EFTs to the benefit of real estate companies located in the United States.
- According to publicly available information, **Individual 2** held the position of Director for both **Company C** and **Company D**. In addition, **Individual 3**, a relative of **Individual 2**, was reported to be a major shareholder of **Company D**. A number of EFTs were ordered by or for the benefit of **Company D** to an account in the United States held by **Individual 3**, as well as to another personal account in Canada also held by **Individual 3**.
- **Individual 5**, a notary, was also under investigation and suspected of facilitating the laundering of illicit funds through a trust account and a personal account. **Individual 5** transferred funds from a personal account in Europe to the lawyers' trust account in Canada. **Individual 5** was also the beneficiary of EFTs ordered by individuals and businesses mainly located in Europe and the United States.

Nominees and trust accounts set up by lawyers and/or notaries were used in abundance in this case. Some of the companies, located in various jurisdictions, were suspected of being shell companies and used solely for laundering funds generated by the organized crime group.

## RED FLAGS associated with this case:

- Frequent movement of funds between same trust accounts and bank accounts held by businesses located in various jurisdictions and with accounts in different financial institutions also located in various jurisdictions
- Multiple and frequent transfers of funds between accounts held by businesses located at the same address and/or owned by the same individuals

## Securities industry

In order to gain a better understanding of how the global securities industry may be used or associated with suspected money laundering activities, a detailed review of open sources, FINTRAC's case disclosures, and large cash and suspicious transaction reports for the period of November 2001 to March 2007 was conducted. Focus was also placed on market manipulation and insider trading which are the most common crimes in the securities industry.

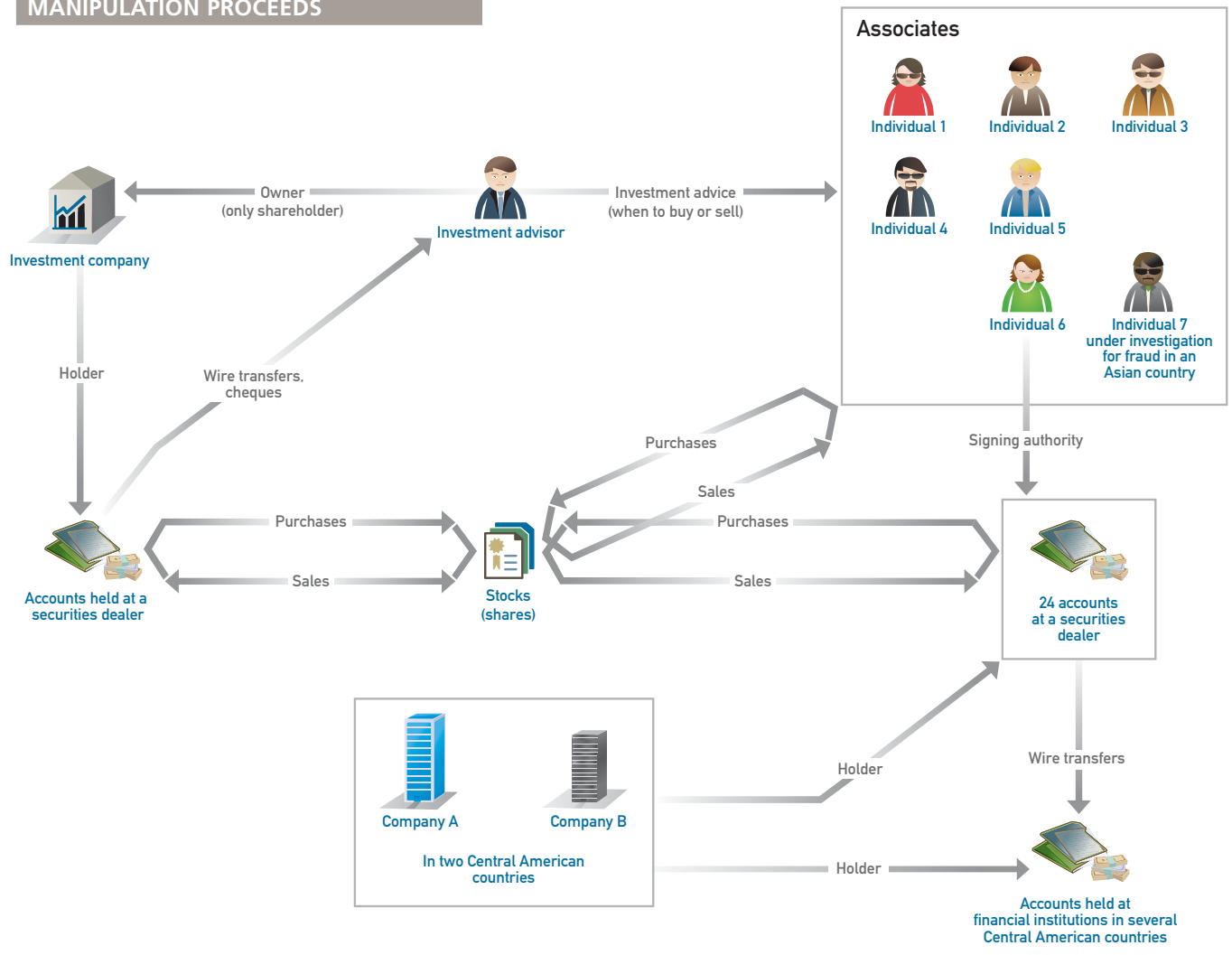
Based on the results of this study, FINTRAC believes that the securities industry has been used to launder proceeds generated by various crimes including drug trafficking, stock manipulation and fraud. The following typologies were found to be associated with the use of the securities industry for suspected money laundering:

1. use of front companies;
2. use of professionals to facilitate the introduction of proceeds;
3. use of margin trading accounts; and
4. use of money orders.

## CASE EXAMPLE ILLUSTRATING THE SUSPECTED LAUNDERING OF STOCK MANIPULATION PROCEEDS AND THE FIRST TWO TYPOLOGIES

This scheme involved the manipulation of stocks to make fraudulent profits which were laundered through a number of bank accounts in Central America and the Caribbean, as well as through the purchase of monetary instruments made payable to suspected nominees. The chart on page 12 provides an overview of the case.

**SUSPECTED LAUNDERING OF STOCK MANIPULATION PROCEEDS**



STR information received from the Canadian securities sector and financial institutions led to this case which involved eight individuals located in the greater Toronto area and two corporations located in Central America.

An investment advisor was found to be the main subject of a stock manipulation investigation, along with seven other individuals, suspected of being business associates. One of these individuals was under investigation for banking fraud in an Asian country, which cost investors close to \$100 million CAN.

**HIGHLIGHTS OF THE CASE:**

Under the present scheme, the investment advisor appeared to be providing information to the seven individuals as to when to purchase and sell stocks of certain firms:

- One financial institution reported that the investment advisor was receiving large wire transfers into a business account from a securities dealer. When questioned as to the reason for the transfers, the investment advisor became uncooperative; the financial institution suspected that the individual was dumping a large number of shares purchased earlier from the same securities dealer.
- STRs from other financial institutions confirmed that the individual was the investment advisor of at least two other members of the group.

Another member of the group was found to be associated to two corporations with addresses in two different Central American countries:

- This individual, **Individual 6** had signing authority over 24 accounts held by these corporations with the same securities dealer.

- STR information received from a securities dealer revealed that this individual sold shares of specific companies shortly after purchase.
- The sales were followed by wire transfers to various bank accounts held by the two corporations and the aforementioned investment advisor at financial institutions in Central America and the Caribbean.

The same type of activity appeared to be conducted by all of the individuals associated to this scheme:

- The purchase of securities (mostly penny stocks that were not regulated, and therefore easy to manipulate) would be quickly followed by a sale, which would then be followed by wire transfers or deposits to bank accounts. Bank drafts would then be purchased, or cheques would be issued and made payable to suspected nominees.

**RED FLAGS associated with this case:**

- Large number of accounts with (a) securities dealer(s)
- Large number of shares were traded shortly after being purchased
- Two companies (possibly front ones) were located in a jurisdiction where incorporation is easily obtained, or where business-related claims are difficult to confirm
- A significant number of wire transfers were made to offshore accounts, particularly following the sale of a substantial amount of shares
- Monetary instruments were made payable to a number of suspected nominees

**Additional red flags possibly related to market manipulation include:**

- Large percentage of securities dealers' commission revenue generated from limited number of clients
- Securities agent or advisor purchasing or selling stocks outside his or her jurisdiction of registration
- Financial statements of companies, including balance sheets, income statements, and statements of change in financial position are not publicly available
- Company's published statements of cash flow indicates the presence of capital, but no cash flow generated by the organization
- Company's executives reside in jurisdictions without extradition treaties with Canada
- Securities sales by insiders such as company executives, their relatives etc.
- Unrealistic increase in share prices without major announcements in terms of future projects, earnings etc.
- Unrealistic increase in share prices with an announcement that cannot be verified

Relevant designated information regarding this case was disclosed to law enforcement to assist in their investigation.



## EMERGING VULNERABILITIES

Payment system innovations are driven by a number of factors, including economic environment, technology, consumer preferences, costs, regulations, as well as private and government policies/practices. In this fast-paced environment, consumers are looking for quick and easy payment methods. In response to these needs, new payment technologies have been introduced and with them, new risks related to money laundering and terrorist financing have emerged for the banking sector, other reporting entities and FINTRAC.

In 2007-2008, FINTRAC's environmental scanning of various sources of information related to ML/TF, in combination with the review of cases disclosed during the same period, revealed that prepaid cards and digital precious metals were new payment methods that were becoming increasingly popular and possibly posing certain ML/TF risks. The ML/TF risks associated with prepaid cards and digital precious metals are discussed in this section.

### Prepaid cards

Prepaid cards provide access to funds that are paid in advance by the cardholder or a third party. These cards have the same characteristics that make cash so attractive to criminals: they are portable, valuable, exchangeable and anonymous.<sup>6</sup> In addition, they are not subject to cross-border reporting since they are not considered monetary instruments, making it easier to transfer wealth from one jurisdiction to another. The wide variety of funding mechanisms also means fund origins are difficult to trace and it is difficult to ascertain whether or not the money is from a legitimate source.

FINTRAC conducted a vulnerability assessment of prepaid cards after it was identified as an emerging issue throughout our ongoing environmental scanning. Within the Canadian market, there are two types of prepaid cards that are currently offered: open-system/loop and closed-system/loop. FINTRAC's assessment of the business models for the two types of prepaid cards that identify possible areas of vulnerabilities to ML and TF are provided in the following section.

### VULNERABILITIES ASSOCIATED WITH OPEN-LOOP PREPAID CARDS

Open-system/loop prepaid cards are always issued by financial institutions but can be distributed either by financial institutions or by MSBs, and are in most cases network-branded with Visa or MasterCard. These cards can be used to make purchases at any locations which have access to these networks and also to withdraw cash from ATMs. Open-loop cards can be obtained at the physical location of the banks or service providers, or online. These cards are not necessarily connected to a bank account and the verification of cardholder identity varies from one provider to another. Examples of open-loop cards include payroll cards and prepaid cards that can be used by the purchaser or by someone else.

Open-loop cards allow cardholders to move funds easily and anonymously worldwide because of potentially limited identity verification mechanisms and the possibility of multiple cardholders, around the world, using the same card. The online availability of cards means that there is no face-to-face contact between the customer and the service provider, hence increasing the risk that stolen information or nominees could be used to obtain cards. In addition, holders of cards of the same issuer but with different accounts can, in some cases, also transfer funds from one card to another through the Internet. Generally, transactions on the Internet allow a certain degree of anonymity that can potentially be exploited by money launderers or terrorist activity financiers.

In addition, cards can be anonymously loaded with funds. For example, some cards can be loaded with cash at a third party reseller location. The loader is not required to show identification, and the source of funds is not determined. The large variety of loading options makes it possible for a money launderer to fund a card with illicit proceeds.

High or no value limit open-loop prepaid cards significantly increase the risk of ML and TF.<sup>7</sup> For instance, many offshore financial institutions, sometimes located in countries with weak AML legislation, offer unlimited value prepaid cards and market the cards in a way that specifically

<sup>6</sup> <http://www.moneylaundering.com/Agent.aspx?Page=/NewsBriefDisplay.aspx?id=963>

<sup>7</sup> "Report on New Payment Methods", FATF Report, October 2006. Available at: <http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf>

promotes the movement of money in an anonymous fashion.<sup>8</sup> The high card limits allow for large amounts of funds to be moved around the world.

#### VULNERABILITIES ASSOCIATED WITH CLOSED-LOOP PREPAID CARDS

Closed-system/closed-loop prepaid cards can be obtained in many retail stores, online and in casinos. They can be used to make purchases or conduct gaming transactions within an internal network. Most closed-loop cards are not provided by financial institutions, and little or no identification is required to obtain them. Examples of closed-system prepaid cards include gift cards and prepaid long distance phone cards. These cards are either limited to the original value placed on the cards or can be reloaded, within limits determined by the company.

Since identification is not required when purchasing most closed-loop prepaid cards, they can be obtained and used anonymously to make purchases. The lack of customer identification blurs transaction trails, making it more difficult for law enforcement to track cardholders.<sup>9</sup> Closed-loop cards are also more easily traded, making them ideal for commodity trading or as an alternative for bulk cash smuggling, especially since these cards are not monetary instruments and are, therefore, not subject to cross-border reporting.

Gift cards have also been reported to be used in “cyber money laundering” or “e-fencing” in which criminals use stolen credit card numbers to buy gift cards online, and then sell them to the highest bidder at an online auction Web site or for a set discount at a gift-card exchange Web site.<sup>10</sup> Similarly, gift cards can be purchased with any illicit proceeds and then re-sold for the sole purpose of money laundering. This method has been found to be very lucrative for criminals since stolen or illegitimate gift cards can typically be re-sold for 80 per cent of their face value, compared to just 30 per cent for typical goods on the black market.<sup>11</sup> Since late 2002, gift cards have been increasingly turning up for resale at eBay, Craigslist and card-exchange sites such as cardavenue.com, plasticjungle.com and swapagift.com. In July 2007, eBay was listing

more than 3,400 gift cards for resale.<sup>12</sup>

The U.S. Drug Enforcement Agency has also indicated that prepaid cards are often being targeted by thieves normally stealing credit cards, drug rings and terrorist cells for terrorist financing.<sup>13</sup> For example, these cards could be used to purchase supplies necessary for terrorist activities or be smuggled cross-border in lieu of cash. In fact, the Singapore Internal Security Department has found that the Liberation Tigers of Tamil Eelam (LTTE)<sup>14</sup> has made extensive use of mobile phones loaded with prepaid cards.<sup>15</sup> The Singapore Government is therefore planning to regulate the sale of prepaid cards for mobile phones.

To date, a limited number of cases disclosed by FINTRAC have involved the use of prepaid cards. Businesses involved in the sales of prepaid phone cards (closed-loop) have been part of suspicious schemes possibly related to both ML and TF. On the other hand, FINTRAC suspects that open-loop cards have been used to conduct illegal online gambling activities, i.e. mainly to redeem gambling winnings/proceeds.

### Digital Precious Metals

Through environmental scanning of publicly available information and the review of 2006-2007 case disclosures, FINTRAC identified Internet payment systems (IPS) and their variants, including digital precious metals (DPMs), to be possibly exploited for money laundering and terrorist financing activities. Consequently, FINTRAC studied the various business models of IPS and of DPMs to identify the features/characteristics that would make them vulnerable to ML and/or TF.

The study was divided in two parts, the first part focused on *payment processing and debit-account* IPS, while the second one focused solely on DPMs. *Payment processing* IPS offer services only to online merchants, *debit-account* IPS allow person-to-person transfers across jurisdictions, and DPMs allow users to convert national currencies into electronic currencies via an exchange maker. *Payment processing* and *debit-account* variants of IPS are vulnerable in part because two of

<sup>8</sup> <http://www.usdoj.gov/ndic/pubs11/20777/20777p.pdf>

<sup>9</sup> “Report on New Payment Methods”, FATF Report, October 2006. Available at: <http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf>

<sup>10</sup> “Online Resale of Gift Cards Raises Fraud Alarms”, ABC News, July 23, 2007.

<sup>11</sup> “Scam may be tied to stolen TJX data”, The Boston Globe, March 24, 2007.

<sup>12</sup> “Online Resale of Gift Cards Raises Fraud Alarms”, ABC News, July 23, 2007.

<sup>13</sup> <http://moneycentral.msn.com/content/Banking/P137668.asp>

<sup>14</sup> The Canadian Government listed the Liberation Tigers of Tamil Eelam (LTTE) as a terrorist group on April 8, 2006, pursuant to the Criminal Code.

<sup>15</sup> <http://www.textually.org/textually/archives/2005/03/007377.htm>

their key attributes, *anonymity and payment disintermediation* (i.e. *untraceable transactions*), match those of physical cash, the ideal method of value transfer for criminal activity. Moreover, *debit-account IPS* offer a greater layering risk than *payment processing IPS* because their design features facilitate person-to-person (P2P) transfers across jurisdictions with relative speed and ease.<sup>16</sup>

Digital precious metals appear to be more vulnerable to ML/TF than the other two variants. Digital precious metals operators (DPMOs) are IPS providing users with “digital currencies” purportedly backed by precious metals that can be used for e-commerce, bill payments, person-to-person payments and other typical transactions. In contrast with payment processing and debit account type IPS, using a DPMO involves the use of two separate service providers. A user account first needs to be set up with the DPMO. Then to fund the account, the user needs to remit currency into “digital currencies” via a digital currency exchange service (DCES). Upon receipt of the remittance, the DCES funds the user’s account with the DPMO. DCES and DPMOs operate independently from one another.

FINTRAC’s analysis revealed that DPMOs and DCES have features that may be suitable for each phase of money laundering. It was found that exploitable weaknesses such as user anonymity and the existence of a network of exchange services—some accepting cash deposits to fund DPM accounts—may facilitate the placement phase. In the layering phase, a launderer can “cash in” and “cash out” his/her DPM account with multiple DCES, convert e-currencies into other e-currencies and transfer e-currencies to another user who can then redeem his/her account in currency. Finally, cash withdrawals with so-called “digital gold cards” may facilitate the integration phase of ML.

While there is a legitimate market demand for such alternative payment systems, FINTRAC believes that there is a real potential for DCES/ DPMOs to be exploited for ML/TF because of the two-layer transaction process. This results in:

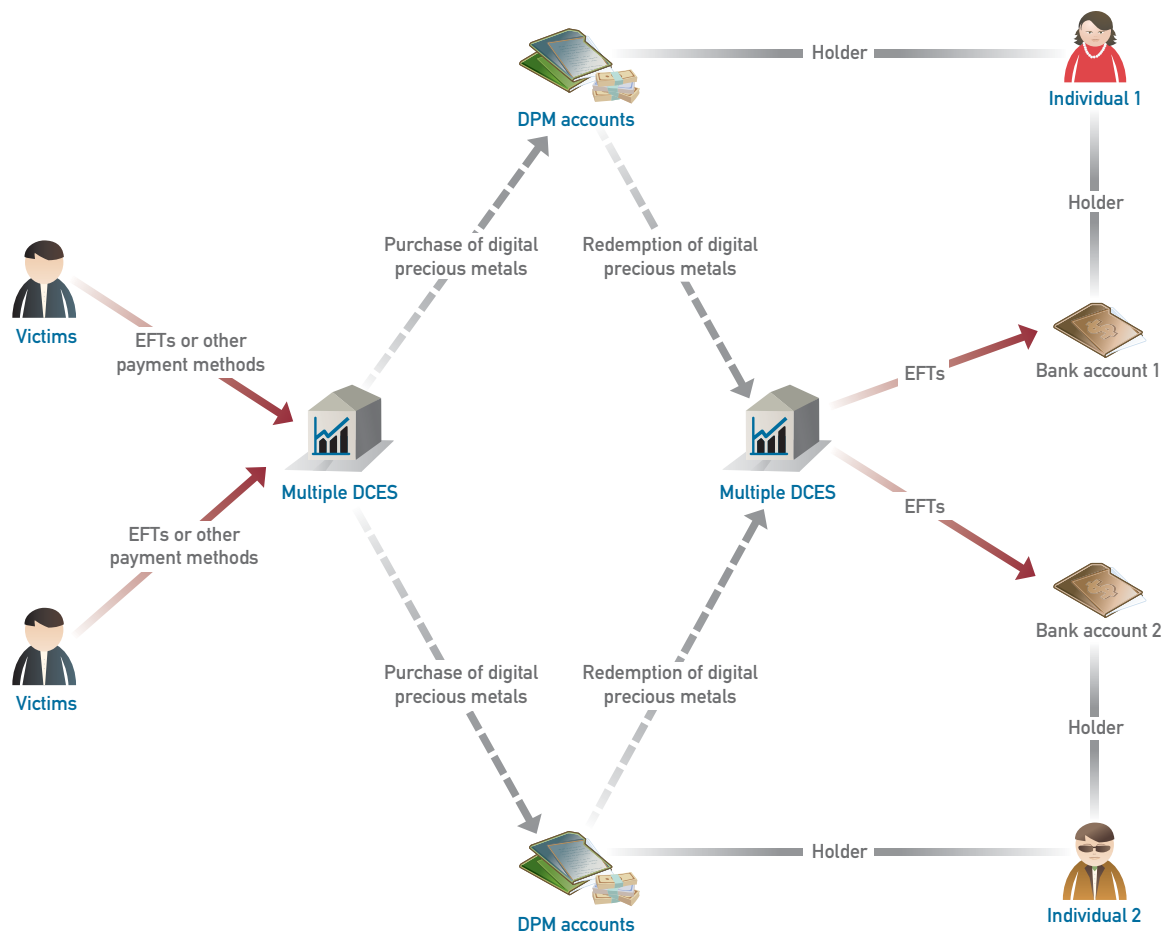
1. A higher degree of anonymity than with other IPS
  - DPM accounts are not tied to bank accounts that are subject to customer identification verifications. DCES are under no obligation to vet the source of funds they transfer to DPM accounts. Similarly, DPMOs cannot truly ascertain the origins of the funds they receive from DCES. The relationship between the DPMO and the DCES is almost entirely online, raising risk.
2. A greater potential to disguise the origin and destination of funds than with other IPS
  - The existence of a web of DCES offering different options for receiving and sending funds — some accepting cash, some allowing users to convert e-currencies into other e-currencies — can make it challenging to audit a user’s full transaction activity. Moreover, the recent introduction on the market of so called “digital gold ATM cards” offers the potential for launderers to re-integrate proceeds into the conventional financial system.

The following sanitized case example (see chart on page 17) illustrates how the user anonymity, the two-tier transaction process (i.e. DPMO and DCES) and the possible network of DCES involved in transactions associated to one DPM account can facilitate fraudulent and money laundering activities:

- According to voluntary information FINTRAC received from law enforcement, **Individuals 1 and 2** were suspected of being involved in an “online investment fraud” scam. Victims were told to send their payments to **Individuals 1 and 2’s** DPM accounts through multiple DCES. The latter then funded **Individuals 1 and 2’s** DPM accounts with digital precious metals. Upon receipt, the digital currencies were exchanged via different DCES and wired into **Individual 1’s and 2’s** bank accounts.

<sup>16</sup> While *debit-account and payment processing IPS* both offer payment disintermediation, the design features of the former potentially increase the money laundering risk. While it may be true that *debit-account IPS* users whose virtual accounts are tied to their bank accounts theoretically leave an audit trail, the most vulnerable type of transactions to money laundering, P2P ones, can only occur within a closed network of users. Thus, if there is no central vetting process to effectively trace and scrutinize all this P2P exchange of financial value over a certain monetary threshold, and therefore no reporting of such potentially suspicious information, there is a greater possibility for disintermediation and the money laundering risk increases accordingly.

## SUSPECTED FRAUD AND MONEY LAUNDERING ACTIVITIES USING DIGITAL PRECIOUS METALS ACCOUNTS



- STR information received from a financial institution further revealed that **Individual 1** had received numerous electronic funds transfers (EFTs) from different DCES over a period of six months. Funds were then withdrawn at various ATMs and drafts payable to **Individual 1** were purchased. Records indicated that **Individual 1**'s employment did not support activity in the account and the original source of funds was unknown.
- **Individual 2** followed the same pattern of financial activity as Individual 1. The latter received numerous EFTs from the DCES and transfers were offset by cash withdrawals. Again, the original source of funds was unknown.

Any suspicious purchases and redemptions of digital precious metals (shown with dotted lines in the diagram) between different DCES and the DPMO would not be reported unless the DCES was considered a reporting entity. Currently, only those suspicious financial transactions involving a reporting entity as defined in the PCMLTFA are subject to being reported.

This explains why, so far, FINTRAC has only disclosed a limited number of cases involving digital precious metals. However, FINTRAC will continue to monitor suspicious transactions that may involve them.



## CONCLUSION

FINTRAC continues to value the work and efforts of the Canadian banking sector and other reporting entities in the fight against money laundering and terrorist financing. The information provided in this document is intended to further assist the banking sector and other financial entities in detecting and deterring ML/TF activities. FINTRAC is committed to providing the banking sector with the necessary information to assist in the development of new and better tools/systems and also train staff.

