




Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des
opérations et déclarations
financières du Canada




MONEY LAUNDERING AND TERRORIST FINANCING TRENDS IN FINTRAC CASES DISCLOSED BETWEEN 2007 AND 2011

FINTRAC Typologies and Trends Reports – April 2012



Canada



MONEY LAUNDERING AND TERRORIST FINANCING TRENDS IN FINTRAC CASES DISCLOSED BETWEEN 2007 AND 2011

© Her Majesty the Queen in Right of Canada, 2012
Catalogue No.: FD5-1/5-2012E-PDF
ISBN: 978-1-100-20282-2

FINTRAC Typologies and Trends Reports – April 2012

April 2012

MESSAGE FROM THE DIRECTOR

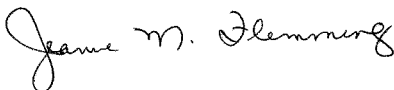
I am pleased to present the latest in FINTRAC's series of Trends and Typologies Reports, *Money Laundering and Terrorist Financing Trends in FINTRAC Cases Disclosed Between 2007 and 2011*. Previous reports in this series have addressed specific business sectors that have reporting obligations under Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. This report, however, boasts a greatly expanded scope, studying the 2,122 case disclosures that FINTRAC has provided to assist law enforcement and intelligence agencies in their investigations throughout the last four years. As such, it offers the public an unprecedented survey of FINTRAC's core product: its tactical intelligence. This report provides a bird's-eye view of how this intelligence tracks national and international trends in money laundering and terrorist financing.

FINTRAC's main tactical intelligence product, the case disclosure, is a vital tool to our partners in law enforcement and intelligence. Each case is built from thousands of transaction reports that FINTRAC receives from reporting entities such as banks, credit unions and casinos. These reports are analyzed for suspicious behaviour or patterns, and to identify key links between individuals, accounts and businesses - all of which assist law enforcement and intelligence agencies' investigations.

Case disclosures are instrumental for investigations of money laundering, terrorist financing and security threats in Canada and around the world. Because of the sensitive information they contain, individual case disclosures are only seen by selected members of FINTRAC and our partners. However, in this report, a wider audience can now see for the first time the larger trends that case disclosures reveal.

The cases FINTRAC compiles yield a wealth of details about potential money laundering, terrorist financing and other national security threats. Moreover, they contribute to an ever-more-precise profile of the suspected perpetrators. FINTRAC's intelligence contributes to the safety of Canadians, and this report offers the public greater insight into how this is achieved.

We at FINTRAC are proud of the work we do. I am equally proud to share this work with you.



Jeanne M. Flemming
Director





CONTENTS

INTRODUCTION	2
PART I: GENERAL OBSERVATIONS	2
(A) Types of cases	3
(B) Disclosure recipients	3
(C) Predicate offences related to cases	5
(D) Reporting sectors most commonly “used” in suspected ML and/or TF schemes	6
(E) Financial transaction reports included in case disclosures	8
PART II: ROLE OF FINTRAC WITHIN CANADA	9
(A) Money laundering methods and techniques related to suspected drug offences	11
(B) Money laundering methods and techniques related to suspected fraud offences	16
(C) Methods and techniques observed in cases related to suspected terrorist financing	20
(D) Country distribution of EFTs included in FINTRAC case disclosures	27
PART III: ROLE OF FINTRAC INTERNATIONALLY	31
CONCLUSIONS	33
ACRONYMS	34

INTRODUCTION

This report is one in a series of FINTRAC publications that are intended to provide strategic financial intelligence and feedback to specific reporting sectors and FINTRAC partners. Unlike previous reports, which focused on suspected money laundering and terrorist financing activities conducted through various sectors, this particular paper is focused on an overview of FINTRAC cases disclosed between April 1, 2007 and March 31, 2011.

While researching this paper, FINTRAC extracted relevant financial intelligence from cases previously disclosed to law enforcement and intelligence agencies. These cases involved money laundering (ML), terrorist financing (TF) and other threats (TH) to the security of Canada. The resulting report presents general observations related to case disclosures, and describes methods and trends in ML and TF¹. In doing so, this report seeks not only to demonstrate how FINTRAC contributes to the anti-money laundering/anti-terrorist financing (AML/ATF) regime, but also to illustrate how all the information received by reporting sectors is an essential component of investigations of money laundering and terrorist financing.

Part I of this report offers a general overview of issues related to case disclosures. Part II describes methods and trends in ML and TF, while Part III expands on FINTRAC's role in the international AML/ATF community.

Part I: General observations

At its most basic level, financial intelligence establishes identity and behaviour in relation to the financial activities of suspected money launderers or terrorist financiers; as such, it is an important source of information in the fight against unlawful activities, organized crime and terrorism. FINTRAC offers a unique

contribution to ML and TF investigations by assisting law enforcement and intelligence agencies in tracking and tracing the proceeds of crime across Canada and around the world.

FINTRAC must first ensure that reporting entities (REs) comply with their legislative obligations, which include the submission of the following reports to FINTRAC:

- Suspicious transaction reports (STRs) as well as reports of attempted suspicious transactions;
- Large cash transaction reports (LCTRs);
- Electronic funds transfer reports (EFTRs);
- Casino disbursement reports (CDRs); and
- Terrorist property reports (TPRs).

In addition to these, FINTRAC receives cross-border currency reports (CBCRs) and cross-border seizure reports (CBSRs) from the Canada Border Services Agency.

FINTRAC case disclosures can be generated from information provided by numerous sources, such as information provided by domestic law enforcement and intelligence agencies through voluntary information records (VIRs) and by foreign financial intelligence units (FIUs) through queries (FIUQs). STRs submitted by reporting entities, results of data mining techniques (known as pattern detection), and open source information also lead to case disclosures. Once these case instigators have been identified, the tactical analytical process begins.

FINTRAC's tactical analytical process involves the analysis of the reports and VIRs found in its databases in conjunction with information from other sources. These include law enforcement databases, commercially or publicly available databases, open source information and information from foreign financial intelligence units. When FINTRAC has reasonable grounds to suspect that the information provided in these reports would be relevant to an investigation or prosecution of ML

¹ The Proceeds of Crime (Money Laundering) and Terrorist Financing Act does not allow FINTRAC to publish trends related to threats to the security of Canada.



or TF, the designated information is shared with relevant recipients in the form of case disclosures. These case disclosures mainly include details about financial transactions, their conductors, the locations and dates where and when they were conducted, the relationships between various individuals and entities, and other information.

A) Types of cases

Between April 2007 and March 2011, FINTRAC disclosed a total of 2,122 cases to law enforcement, intelligence agencies and foreign financial intelligence units. These cases amounted to 72% of all cases disclosed since FINTRAC's inception in 2000. They can be broken down into three main disclosure type categories, as represented in Table 1. As noted in this table, ML cases continue to be the leading category, followed by TF/TH and the combination of ML/TF/TH. The hybrid nature of the last category highlights the connection between crime and terrorism.

B) Disclosure recipients

FINTRAC discloses cases generated by STRs, open source and pattern detection to relevant law enforcement or intelligence agencies; however, cases generated by VIRs are disclosed to the VIR originator only, unless the originator allows dissemination to other relevant disclosure recipients. FINTRAC's disclosure recipients include ML/TF investigative bodies, as well as foreign FIUs. In addition, FINTRAC can also disclose to the Canada Border Services Agency (CBSA), the Canada Revenue Agency (CRA) and the Communications Security Establishment Canada (CSEC) if the related financial transactions fall within their respective mandates and FINTRAC has already met its disclosure threshold relating to a suspected ML or TF offence. Table 2 and Figures 1 and 2 highlight the main recipients of disclosures, as well as the distribution of disclosure recipients in Canada.

TABLE 1: CASES DISCLOSED PER CATEGORY

DISCLOSURES BY TYPE	2007-08	2008-09	2009-10	2010-11	TOTAL
ML	171	474	470	626	1741
TF/TH	29	52	73	103	257
ML/TF/TH	10	30	36	48	124
Total	210	556	579	777	2122

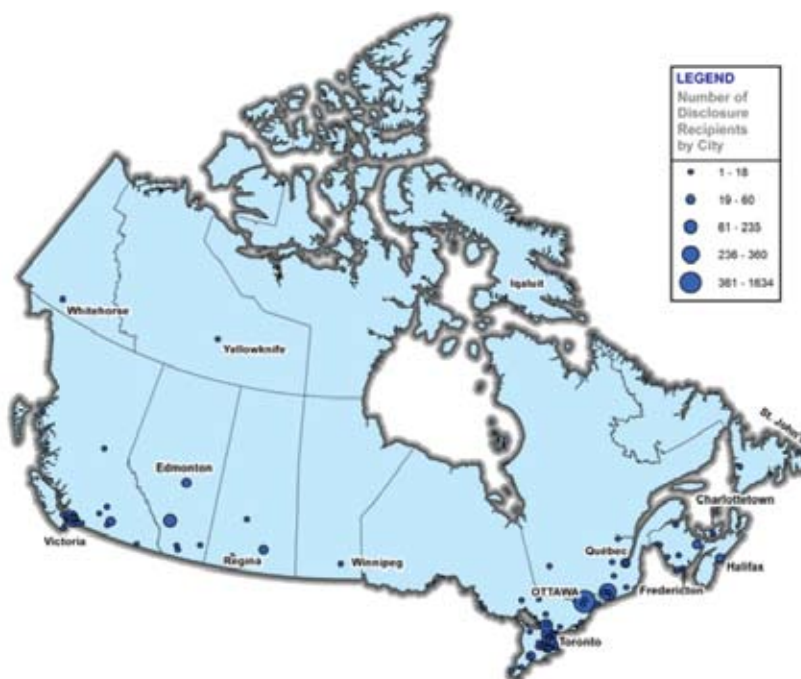
TABLE 2: MAIN DISCLOSURE RECIPIENTS²

RECIPIENTS	2007-08	2008-09	2009-10	2010-11
RCMP	61%	68%	63%	59%
Municipal Police Services	24%	27%	23%	18%
Foreign Financial Intelligence Units	24%	17%	22%	19%
Provincial Police Services	12%	10%	21%	21%
Canadian Security Intelligence Service	12%	10%	13%	15%
Canada Border Services Agency	5%	14%	7%	11%
Canada Revenue Agency	5%	27%	22%	18%

In 2010-11, more than half of FINTRAC's case disclosures were sent to the RCMP, a result similar to what was observed in previous years. Generally, the distribution of disclosure recipients has remained relatively stable over the last four years. As illustrated in Figures 1 and 2, disclosure recipients were concentrated in Canada's metropolitan areas, particularly in Vancouver, Montreal and the Greater Toronto Area. On a provincial scale, there

were a higher number of disclosure recipients in British Columbia, Alberta, Ontario and Quebec, as well as in major urban centres across Canada in close proximity to the border. Despite what appears to be a high distribution of disclosures focused in the national capital region, this is mainly attributed to the disclosure recipients' headquarters being located in that region, who often received copies of disclosures sent to provincial branches.

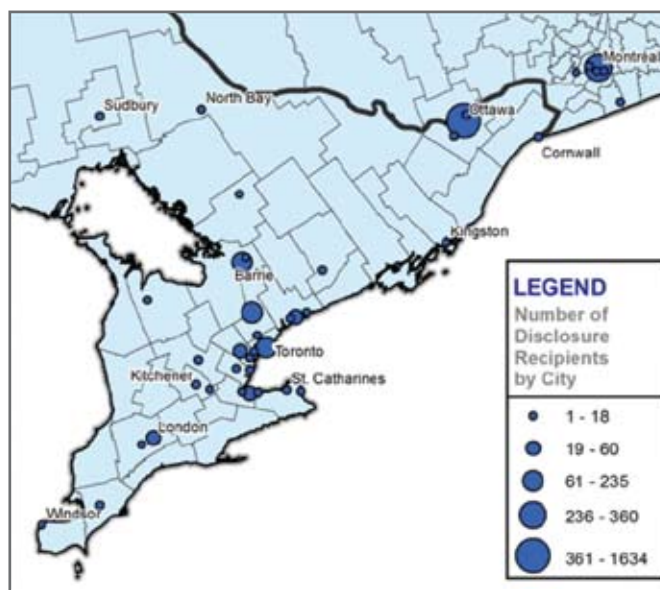
FIGURE 1: DISTRIBUTION OF DISCLOSURE RECIPIENTS IN CANADA (2007-11)



² The percentages in this report do not add up to 100% because FINTRAC disclosures are often sent to more than one recipient. A few cases were disclosed throughout the years to the CSEC; however, the percentages were not significant enough to be included in the report.



FIGURE 2: DISTRIBUTION OF DISCLOSURE RECIPIENTS IN SOUTHERN ONTARIO AND WESTERN QUEBEC (2007-11)



C) Predicate offences related to cases

FINTRAC may be informed of a suspected predicate offence³ either through information that is volunteered by law enforcement, intelligence agencies or other

partners such as CBSA, or through what is included in a suspicious transaction report and open source information. Table 3 highlights the most common types of predicate offences related to cases.

TABLE 3: TYPES OF PREDICATE OFFENCES RELATED TO CASES⁴

PREDICATE OFFENCE CATEGORY	2007-08	2008-09	2009-10	2010-11
Fraud	35%	27%	29%	33%
Drug	28%	31%	34%	26%
Unknown ⁵	16%	18%	13%	14%
Tax Evasion	4%	13%	6%	5%
Customs/Excise ⁶	8%	4%	3%	5%
Corruption	0%	4%	3%	5%
Human Smuggling	0.5%	2%	2%	4%
Theft	2%	4%	4%	3%
Illegal Gambling	1%	2%	2%	1%

³ The term "predicate offence" is used in this report in the same context as the term "designated offence," which is defined as an offence under Canada's *Criminal Code* or any other federal Act.

⁴ Figures included in the table do not total 100% given that cases can involve multiple predicate offences.

⁵ This category reflects cases where the pattern of financial activity, or other information available to FINTRAC, suggested money laundering for which the predicate offence was unknown or not identified.

⁶ The customs/excise category includes cigarette smuggling/contraband and illegal imports/exports.

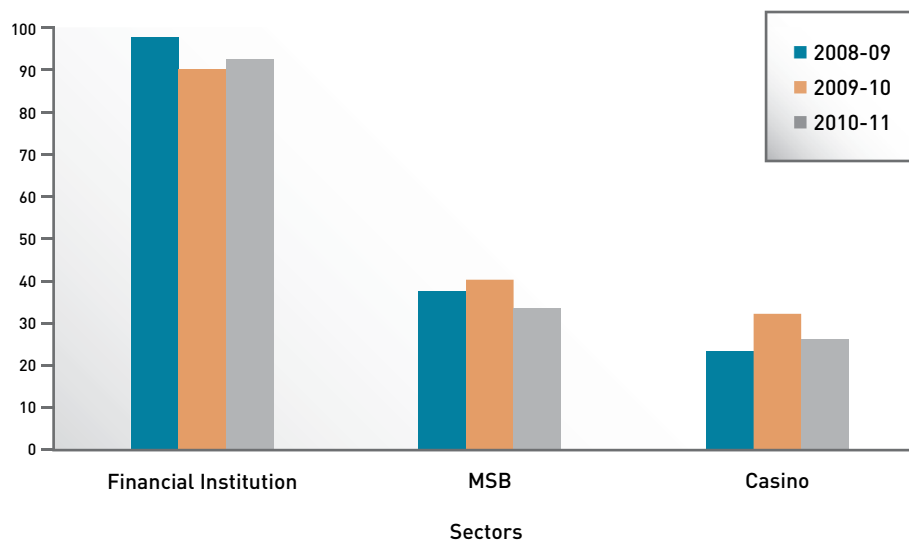
Throughout the past four years, the most frequently observed cases were those related to fraud and drugs. In general, the percentages of cases in each category have been relatively stable across offences. It is important to note, however, that since most FINTRAC case disclosures are generated from information received from partners (i.e. VIRs or FIUQs), the case disclosures may for the most part reflect trends in criminal activity, but may also be a reflection of law enforcement and intelligence agencies' investigative priorities.

D) Reporting sectors most commonly "used" in suspected ML and/or TF schemes

During the past three years⁷, financial institutions (e.g. banks, credit unions, caisses populaires, etc.) were the reporting entity sector whose financial transactions and

reports (i.e. STRs, LCTRs, EFTRs, etc.) constituted the majority of those associated with case disclosures. An average of 94% of cases involved the use of financial institutions, a statistic most likely attributable to the size of this sector and the volume of reports it produces. Money services businesses (MSBs) were involved in 36% of case disclosures (making them the second most used sector), while 15% of case disclosures involved the use of the casino sector. Figures 3 to 5 illustrate how the use of various reporting sectors in case disclosures where FINTRAC suspected the transactions were linked to ML and/or TF has changed over time.

FIGURE 3: PERCENTAGE OF SUSPECTED ML DRUG-RELATED CASES INVOLVING MAIN REPORTING SECTORS



⁷ Data for 2007-08 were not available at the time of publication and therefore Figures 3 to 5 only provide results for the last three years.



FIGURE 4: PERCENTAGE OF SUSPECTED ML FRAUD-RELATED CASES INVOLVING MAIN REPORTING SECTORS

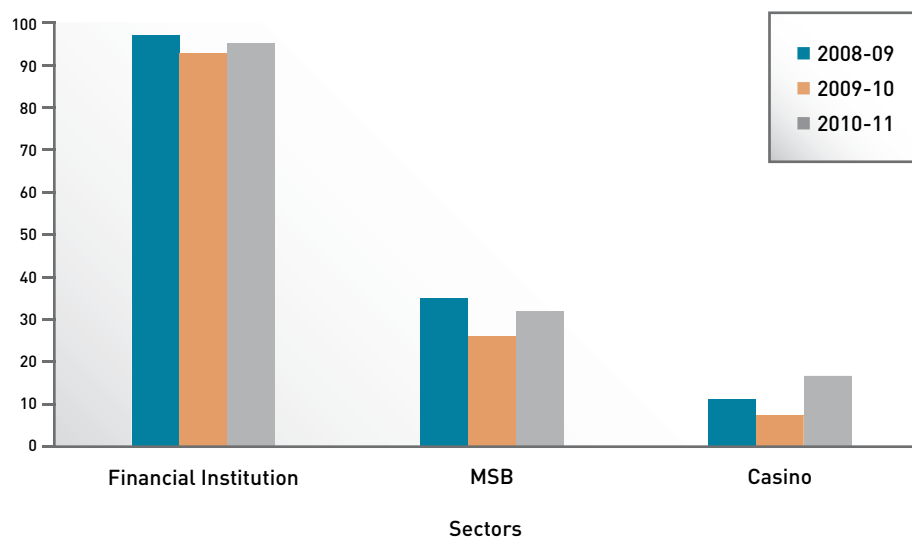
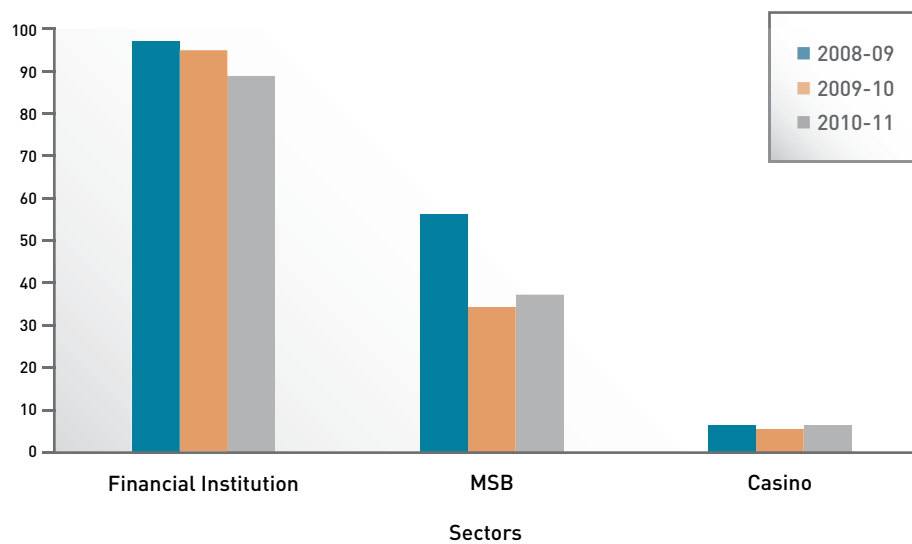


FIGURE 5: PERCENTAGE OF SUSPECTED CASES RELATED TO TERRORIST FINANCING INVOLVING MAIN REPORTING SECTORS



As shown in Figure 3, there was a slight increase in the use of casinos in drug-related cases observed from 2008-09 to 2009-10. Secondly, as illustrated in Figure 4, there was a slight increase in the use of casinos in fraud-related cases from 2009-10 to 2010-11. Lastly, the most significant change was the decrease in the use of MSBs for TF cases from 2008-09 to 2009-10, as shown in Figure 5.

E) Financial transaction reports included in case disclosures

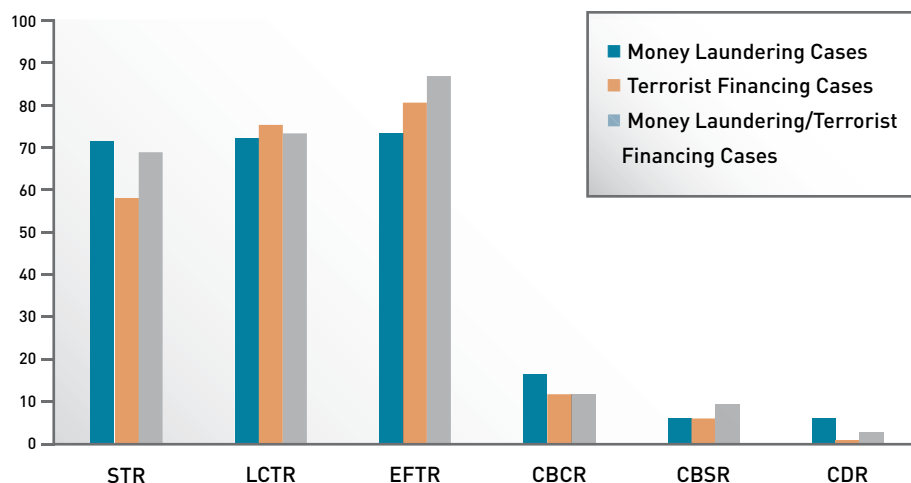
STRs, EFTRs, LCTRs, and other reports and information received by FINTRAC are an extremely valuable source of financial intelligence. A total of 407,835 of those reports were included in cases disclosed between 2007 and 2011. Of that number, 60% were EFTRs, followed by LCTRs at 36%, STRs at 33%, CBCRs at 0.6% and CDRs at 0.5%. Figure 6 shows the percentage of money laundering, terrorist financing and a combination of both types of cases disclosed between 2007 and 2011 containing at least one STR, LCTR, EFTR, or other type of report.

Interestingly, the percentage of cases containing at least one STR is similar to the percentage of cases including at least one EFTR or LCTR. This is significant, since STRs

are usually human-generated and therefore the volume of these reports submitted to FINTRAC is much lower than that of EFTRs and LCTRs. STRs are particularly useful for providing additional information related to individual behaviour and transactional activity. STRs and other reports are powerful tools in detecting suspected money laundering and terrorist financing activities. In some instances, STRs alone provide the necessary grounds to suspect ML and/or TF. While it is a challenge for compliance professionals and employees within the financial system to remain vigilant and report suspicions through STRs, FINTRAC and disclosure recipients depend on the experience and judgement of those on the front line in their efforts to detect and deter suspected ML and/or TF.

Results shown in Figure 6 further reveal that the percentages of ML cases containing at least one STR, LCTR or EFTR were about the same. However, for TF and ML/TF cases, the percentage of cases including at least one LCTR or EFTR was greater than that for cases with at least one STR. Although the percentages of cases containing at least one CBCR, CBSR or CDR are much lower, it is interesting to note that CDRs have been mostly included in ML cases.

FIGURE 6: PERCENTAGE OF ML, TF AND ML/TF CASE DISCLOSURES (2007-11) CONTAINING AT LEAST ONE OF EACH REPORT TYPE



Part II: Role of FINTRAC within Canada

A significant component of FINTRAC's mandate is to assist in the detection, deterrence and prevention of money laundering and terrorist financing. As part of its mandate, FINTRAC produces different types of tactical and strategic financial intelligence that assist investigations or prosecutions by law enforcement and intelligence agencies.

As indicated earlier, FINTRAC provides proactive disclosures (i.e. generated by STRs, pattern detection and/or open source), as well as other disclosures generated following the receipt of VIRs or FIUQs to law enforcement and intelligence agencies. It also provides regular tactical disclosures to specific ongoing investigations, in the form of case updates and/or new but related case disclosures. For example, in 2010, FINTRAC contributed to two related municipal police force investigations. The investigations focused on an organized crime group suspected of drug trafficking and other criminal activities. FINTRAC played an active analytical role in these investigations, and through numerous and ongoing disclosures, helped police target individuals who were later arrested. The financial intelligence produced by FINTRAC revealed to police that the suspects were involved in activity consistent with money laundering, and this information was important in leading to the arrests.

FINTRAC's greatest asset is its database of reports. In the world of analysis, one report is valuable, but thousands are invaluable. The accumulation of these reports (provided primarily by REs), pieced together with other sources of information, can ultimately allow FINTRAC to uncover networks of seemingly unconnected individuals and entities participating together in criminal activity. Case disclosures often identify additional aliases, associates, individuals and entities previously unknown by law enforcement or intelligence agencies, bank accounts, addresses and other identifiers, as well as businesses owned

or operated by individuals that are suspected to be involved in ML or TF activities. This additional information can be obtained, for example, through a combination of information reported in STRs, through transactional data linking personal identifiers, and through open source information and commercial databases, to name but a few methods. It identifies individuals or entities involved in possible schemes of collusion or those involved in common ML methods such as the use of nominees or front companies.

FINTRAC's strategic intelligence assessments and reports (such as the present report) are based on the macro analysis of a large number of tactical disclosures combined with other sources of information and attempt to explain trends in money laundering and terrorist financing. The goal of these reports is to assist partners and REs in their front line detection and deterrence. For example, FINTRAC recently produced a classified Financial Intelligence Brief which described and explained suspicious financial activity between a South American country and Canada. This activity was suspected to be linked to drug trafficking. The report identified the methods that individuals and entities used to transport the illicit cash into Canada, to deposit it in the financial system, then – through various layering techniques – to integrate it back into the regular economy. Such strategic intelligence reports can assist law enforcement and intelligence agencies in identifying individuals and entities conducting similar suspicious activities and can lead to new investigative approaches.

Further to the strategic intelligence produced for this report, FINTRAC assessed a number of case disclosures in an attempt to find common characteristics of money laundering and/or terrorist financing cases. For the purpose of this report, FINTRAC identified general characteristics much like the customer risk profile applied by many REs as part

of their compliance regime. The common characteristics, which are presented in the following sections of this report, are merely guidelines; they should not be assumed exclusive of other factors, since criminals and terrorists have consistently operated outside of a single profile and are each uniquely resourceful in the methods and techniques they employ.

MONEY LAUNDERING Money laundering is the process whereby “dirty money” – produced through criminal activity – is transformed into “clean money,” the criminal origin of which is difficult to trace. The money laundering process is continuous, with new dirty money constantly being introduced into the financial system.

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.

TERRORIST FINANCING Terrorist financing refers to direct or indirect financial support to an individual, group, entity, state, or agent thereof, which plans or carries out acts of organized violence against the Government of Canada, Canadians, or Canadian interests or allies, or against other sovereign states, for the purpose of weakening the state, influencing policy, communicating a perceived grievance, and/or to threaten or intimidate the public or portion thereof. Terrorist financing is a defined criminal offence under section 83 of the *Criminal Code* of Canada. In general terms, the criminal dimension of terrorist financing includes collecting property/money for terrorists, possessing property of or making property available to terrorists, and/or using terrorist property. It also constitutes a threat to the security of Canada as defined under section 2 of the *Canadian Security Intelligence Service Act (CSIS Act)*.

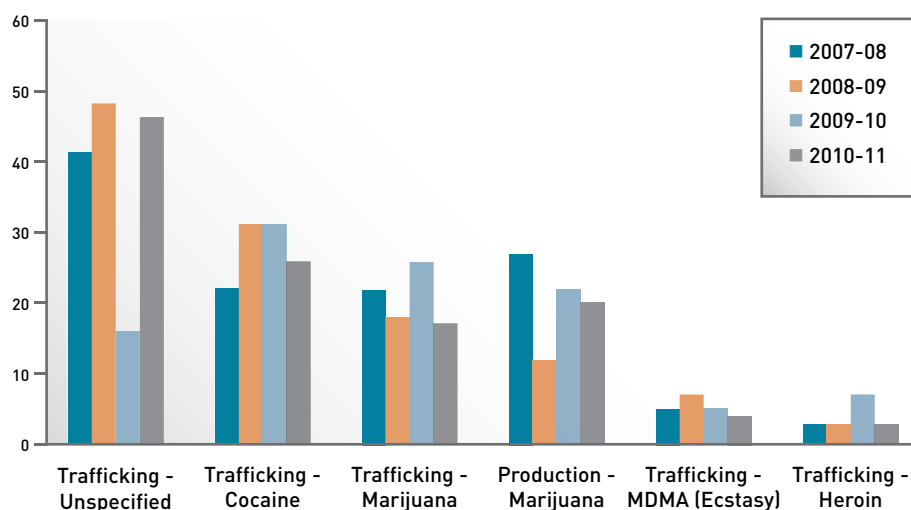


A) Money laundering methods and techniques related to suspected drug offences⁸

Investigations of drug trafficking and/or production were suspected in 30% (632/2122) of cases involving money laundering or terrorist financing. Of those cases, the most common drug offences were related to marijuana and/or cocaine. Figure 7 provides an additional breakdown of the more commonly observed drug-related offences per year.

It was also found that, during the same period, organized crime groups were involved in at least 28% of drug-related cases.

FIGURE 7: PERCENTAGE OF ALL CASES RELATED TO INVESTIGATIONS OF DIFFERENT DRUG OFFENCES⁹



⁸ Changes over time in the percentage of cases related to investigations of different drug offences are closely linked to law enforcement priorities.

⁹ Percentages included in the chart do not total 100% given that cases can involve multiple predicate offences.

The main findings related to suspected ML drug cases have been summarized in the following text box:

Common Characteristics of Suspected ML Drug Cases

1) Typical scheme:¹⁰

Tony, age 35, had worked at his family's car dealership (which his father owned) since he was young. After working there for several years, and having sold cars to numerous people, he also started to get to know members of the local organized crime group. They would often walk into the dealership with bags full of cash and purchase the latest flashy car. Tony was happy, as the commission he made was great. Then they started asking him for favours. They told him that they would give him a bag of cash which would "buy" a car, but the car would actually just sit there on the dealership lot. Six months later, they would return to "sell" the car back and pick up a cheque from the dealer – after paying Tony's commission. This is how Tony, unbeknownst to his father, became the "banker" of choice for this organized crime group.

The banks started to suspect something when Tony started to deposit large amounts of cash on a regular basis. He told them it was from the sale of vehicles; however, bank staff knew how unusual it was for someone working for a car dealership to walk in with a bag of cash (and for it to come from a legitimate source). Tony started to ask his wife to deposit cash in order to draw less suspicion to himself. He figured that if they split the deposits between themselves under the \$10,000 reporting threshold, the bank wouldn't be suspicious. However, the banks quickly picked up on this trend, linking Tony and his wife to the same address on file, and submitted multiple STRs to FINTRAC regarding the couple.

At some point, the police were tipped off that Tony was providing money laundering services for an organized crime group. In order to gather more intelligence, the police informed FINTRAC of their suspicions through a VIR and FINTRAC quickly made an ML disclosure to the police force. After finalizing their investigation, the police charged Tony, who was eventually sentenced to jail for money laundering.

2) Characteristics of individuals suspected of ML related to drug offences:

Based on a review of a sample of 2010-11 ML case disclosures related to suspected drug offences, the following characteristics were noted:

- The majority of suspected offenders are middle-aged males;
- While participation of females in ML activities is generally less frequent than that of males, females were mostly involved in ML cases related to drugs;
- Females are often linked in cases through familial relationships and they hold jobs in a variety of sectors, including food, retail and the services sector; otherwise, they are either homemakers or unemployed;
- It is not uncommon to find an entire family taking part in the suspected criminal activity;

¹⁰ The details of the scheme represented here are not taken from one particular case disclosure; rather, they are based on observations made in a number of similar cases.



- Business ownership is the most common “declared” occupation, second to individuals employed in the service sector, i.e. trades (e.g. carpenter, electrician, plumber, etc.), restaurants/bars, travel or the beauty industry;
- The businesses owned are also often classified as being part of the service sector, i.e. restaurant, real estate, financial, etc.

3) ML methods and techniques observed in suspected drug-related cases:

- Structuring and smurfing:
 - Cash purchases by one or many individuals of EFTs that fall under the reporting threshold;
 - Currency exchanges under \$10,000 from CAD to USD or vice versa;
 - Cash purchase of money orders or bank drafts under \$1,000 (which does not require identification) that are payable to third parties;
 - Depositing a large number of \$20 bills totaling under \$10,000.
- Refining:
 - Exchanging small-denomination bills for larger ones (e.g. \$20 bills for \$100 bills).
- Commingling:
 - Financial transactions suspected to be a mix of legitimate business revenue with criminal proceeds;
 - Businesses acting as fronts to make financial transactions appear more legitimate, indicated by multiple entities sharing a common address;
 - Holding numerous business bank accounts and conducting various transfers between accounts. Funds are then moved to one account and bank drafts are purchased.
- Casinos
 - Cash purchase of casino chips, with minimal play, followed by the redemption of chips for either cash or cheque.
- Electronic funds transfers
 - Large funds transfers from a business account to individuals located in countries of concern.
- Foreign exchange transactions
 - Currency exchanges from CAD to USD or vice versa;
 - Large cash deposits, converted to USD, then wired to a country related to drug trafficking;
 - Currency exchanges followed by purchases of EFTs.

4) Types of businesses used in suspected drug-related cases:

Over the past four years, 68% of drug-related cases consistently involved at least one business that was not necessarily a cash-based business. Examples of businesses and sectors observed in drug-related cases were:

- MSBs
- Construction/development industry
- Shipping/freight companies
- Import/export companies
- Travel agencies
- Real estate
- Electronics
- Pharmaceutical
- Convenience/grocery stores
- Food and entertainment
- Auto industry
- Hydroponics/indoor gardening
- Trucking companies
- Gas stations



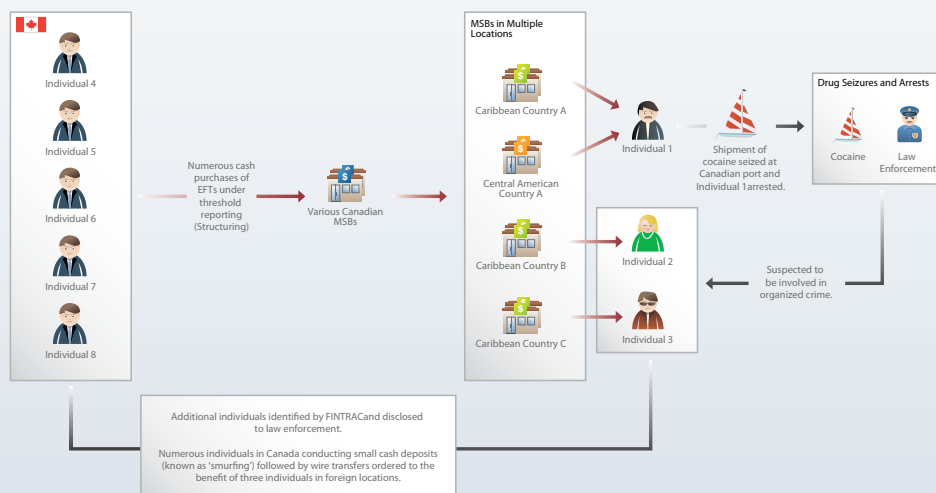
Case example 1: ML case related to a cocaine trafficking network

FINTRAC received a VIR from the police regarding a shipment of cocaine which originated in Central America and was seized in Canada. Individuals identified in the VIR were suspected to be connected to the shipment. Upon its analysis, FINTRAC quickly uncovered a money laundering network and identified five new individuals who were suspected of facilitating the laundering of funds relating to a cocaine trafficking syndicate.

Analysis of the flow of EFTs and information submitted by reporting entities, especially STRs, led FINTRAC to piece together a smurfing network consisting of EFTs conducted by various individuals under the \$10,000 threshold. The following money laundering scheme was identified:

- Law enforcement suspected that the imported cocaine was sold on the streets in Canada and cash was received as method of payment.
- Over time, the group of individuals took the money to MSBs and ordered EFTs below the \$10,000 threshold limit to avoid detection, to the benefit of three individuals operating in the same syndicate located in South American and Caribbean countries. According to STRs, these individuals in Canada were trying to avoid providing any ID, and when prompted, provided similar false address information. Analysis led FINTRAC to suspect that the cash was taken and divided into smaller amounts and distributed to a group of individuals.
- The three individuals in the Caribbean and South America received these funds at MSBs.
- The funds were then suspected to be ultimately distributed for payment where the cocaine was originally produced.

FINTRAC provided all relevant designated information to law enforcement to assist them in their investigation.



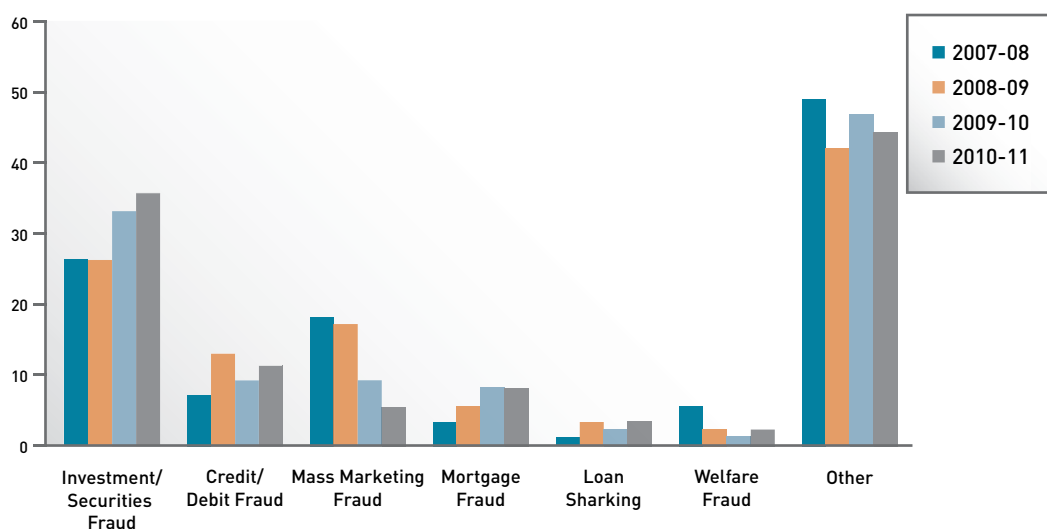
B) Money laundering methods and techniques related to suspected fraud offences¹¹

Fraud was suspected in 30% (644/2122) of all cases disclosed from 2007 to 2011 and 12% of these cases involved organized crime groups. Based on yearly statistics, investment/securities fraud was the most prevalent type of fraud observed in 2010-11, followed by credit/debit card fraud, which surpassed mass marketing fraud in comparison to previous years. Based on information received from law enforcement and intelligence agencies, specific fraud types were observed and are depicted in Figure 8.

As shown in Figure 8, mass marketing fraud (including popular schemes such as 419 scams, advanced fee schemes, telemarketing fraud, internet fraud, etc.) has declined significantly since 2007. Meanwhile, investment/securities fraud and mortgage fraud have continued to increase.

Drawing on the most recent data available (from April 2010 to March 2011), a sample of ML case disclosures related to all types of fraud was analyzed, but securities/investment fraud was assessed independently of the other types due to its unique characteristics. The main findings have been summarized in the following text box:

FIGURE 8: PERCENTAGE OF ALL CASES RELATED TO INVESTIGATIONS OF DIFFERENT FRAUD OFFENCES



¹¹ Changes over time in the percentage of cases related to investigations of different fraud offences are closely linked to law enforcement priorities.



Common Characteristics of Suspected ML Fraud Cases

1) Typical investment fraud scheme:¹²

Richard Jr., age 30, inherited his father's empire while Richard Sr., age 60, still had controlling interest. The two individuals approached elderly individuals in their Canadian community. They presented them with their business proposal to develop land nearby, for which they were seeking investment funding. They promised a 30% return on the initial investment once the development would be finished. The community trusted them as they were already established, successful businessmen and had strong ties to the greater community. Through the assistance of colluding investment advisors, a network of offshore shell companies was established. The two men, aided by their wives (who also held directorships in some of the companies), took the investors' money and used multiple business and personal bank accounts to order numerous EFTs for the benefit of individuals and entities located in the Caribbean as well as the newly established companies in offshore locations. Some of those offshore EFTs were used to purchase large luxury assets in those jurisdictions. EFTs worth millions of dollars were also sent to law firms in multiple countries through the company accounts.

Eventually, investors started asking questions; they demanded the return of their initial investments, but the family had already packed up and relocated to another country far away. Contrary to many other types of crimes, investment fraud funds were already in the financial system and transferred electronically by victims to the perpetrators of the scheme. There were no STRs reported on this family or their businesses, as the companies under them were so diverse that the number of EFTs and the beneficiaries to which they were sending them could all be justified as normal business activity. There were many EFTs involved and hardly any LCTRs reported.

2) Characteristics of individuals conducting ML activities related to fraud

Based on a review of a sample of 2010-11 ML case disclosures related to suspected fraud offences, the following characteristics were noted:

- Fraudsters are typically middle-aged males, but are on average 10 years older than individuals disclosed in drug and TF cases;
- Females are typically related through marriage or other familial ties and are suspected to work in partnership to facilitate the fraud;
- The involvement of an entire family is more commonly noted in investment/securities fraud cases than in other types of cases;
- Individuals perpetrating investment fraud often hold ownership or senior management positions within a number of private and/or public companies, sometimes holding up to a dozen positions at one time. These companies are commonly related to investment/financing/consulting services;

¹² The details of the scheme represented here are not taken from one particular case disclosure; rather, they are based on observations made in a number of similar cases.

- Individuals suspected of taking part in other types of fraud hold various employment positions which do not fit a single profile. In reviewed cases, the majority of individuals under suspicion owned their own business. Where this was not the case, individuals mainly held an office job or were employees of businesses under suspicion.

3) ML methods and techniques observed in suspected fraud-related schemes:

- Use of multiple institutions:
 - Individuals used the proceeds of fraud to purchase a bank draft, which was deposited in another financial institution, then followed by an EFT to another individual;
 - Individuals deposited cheques from a business account at one financial institution to a business account at another institution, then offset the money by depositing cheques into personal accounts, then purchased bank drafts and drew personal cheques payable to the first business account at a different institution.
- Use of credit cards:
 - Individuals purchased large amounts of goods on credit cards and paid it off with fraudulent funds on a regular basis.
- Use of shell/front companies:
 - Individuals registered shell companies in foreign jurisdictions and sent the proceeds of fraud to the foreign accounts of these companies;
 - Individuals used asset management and securities firms as a front to lure investors. Once the investors' money was acquired, bank drafts were issued to nominees or individuals;
 - Several investment companies located offshore were used in the process of moving money from one country to another to create a complex trail;
 - Individuals used multiple front companies which shared the same address.
- Use of electronic funds transfers:
 - Individuals frequently used EFTs (EFTs appear to be used four times more often in fraud cases than in drug cases);
 - Individuals moved proceeds of fraud to specific bank secrecy and tax haven countries, and took up residence there;
 - EFTs were received in a company account, then were immediately wired to a personal account;
 - Complicit investment advisors or lawyers established offshore accounts and businesses and used EFTs to send funds to multiple offshore locations. Money was moved between these accounts and new offshore companies were created;
 - EFTs were ordered to 10 or more countries, with the ordering business registered in a high-risk jurisdiction;
 - Individuals used foreign pass-through accounts: money sent by EFT from Canada to a secondary country, which was then immediately sent by EFT to a third country;
 - Some investor victims sent EFTs directly to offshore accounts held by the fraudsters.



- Personal bank accounts
 - Excessive activity was observed in a short period of time with multiple unrelated third parties depositing funds.
- Nominees
 - Owners of companies were only nominees, and financial transactions were really conducted by suspected criminals.
- Use of prepaid cards
 - Investors ultimately defrauded in a Ponzi scheme received untraditional payouts through prepaid cards.
- Use of MSBs
 - MSBs were used to send and receive funds to/from offshore companies and Canadian companies, where this would have normally been a direct payment at a financial institution between the company bank accounts. The use of MSBs redirected the money trail to avoid linking the two companies together.

4) Types of businesses used in suspected fraud-related cases:

Cases involving fraud are more commonly associated with businesses compared to other predicate offences, particularly when it involves investment/securities fraud. For example, businesses act as conduits to receive investments from victims which can then be easily transferred to accounts held in offshore banking centres. Other types of fraud, such as debit/credit card fraud, can utilize the services of collusive merchants to perpetrate the fraud. Throughout the last four years, 84% of fraud-related cases involved at least one business. Examples of businesses and sectors observed in fraud-related cases were:

- Holding companies
- Financial services companies
- Investment/securities companies
- Real estate development
- Consulting firms
- Energy sector
- Precious metals
- Life insurance
- Technology (e.g. aviation, computers, etc.)
- Medical supplies
- Food and entertainment
- Auto industry

C) Methods and techniques observed in cases related to suspected terrorist financing

FINTRAC disclosed 287 cases related to TF throughout the last four years. Of these TF case disclosures, 34% also involved suspected ML predicate offences. FINTRAC observed a higher occurrence of such TF cases when human smuggling, credit/debit card fraud, and visa/passport fraud were investigated. This could possibly relate to an increasing reliance of terrorist organizations

on revenue raised through criminal operations, which seems to support the growing concern in the international community regarding the crime-terrorism nexus.

Overall, 17% of TF case disclosures involved fraud offences, while 5% of cases involved drug offences. As observed in Figure 9, between 2007-08 and 2008-09, the percentage of fraud-related cases more than doubled, but was followed by a gradual decline. Figure 10 also illustrates how the percentage of cases involving drug offences has changed over time.

FIGURE 9: PERCENTAGE OF TF-RELATED CASES INVOLVING INVESTIGATIONS OF FRAUD

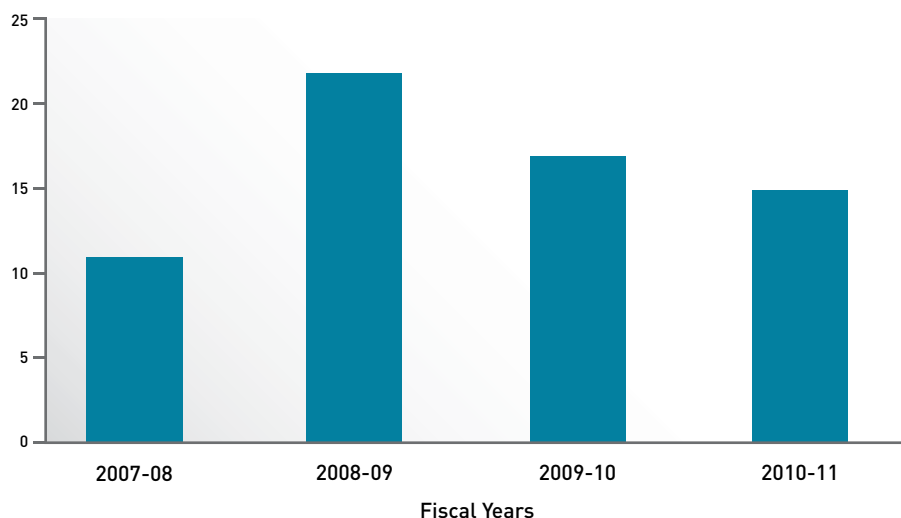
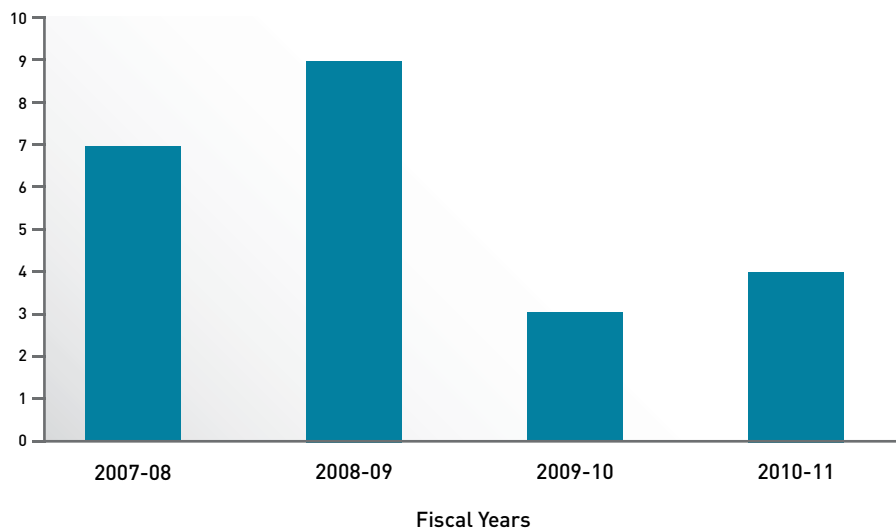


FIGURE 10: PERCENTAGE OF TF-RELATED CASES INVOLVING INVESTIGATIONS OF DRUGS





Drawing on the most recent data available, from April 2010 to March 2011, FINTRAC analyzed a sample of case disclosures related to suspected TF. The main findings have been summarized in the following text box:

Common Characteristics of Suspected Terrorist Financing-Related Cases

1) Typical scheme:¹³

For years, the Smith family had supported the liberation efforts in their home country. They had an especially deep attachment to the cause as some of their close family members continued to live in that country and were affected by the ongoing conflict. They had become close with a number of individuals in their community who felt the same way and through this friendship the Smith family employed them in their family business. Together, they conspired to raise funds for this cause and attempted to develop ways in which to transfer funds to their country of origin without being detected. The following methods and techniques were employed:

- *They took small amounts of cash under \$10,000 to MSBs and ordered numerous EFTs to individuals, including relatives, in their country of origin;*
- *Through business and personal accounts, they also ordered EFTs at banks in larger amounts which benefited individuals in their country of origin;*
- *They would also order EFTs to bank accounts they held abroad and indicated they were for purposes such as real estate. However, the frequency and amounts of the EFTs were excessive;*
- *They would deposit cash at banks and purchase multiple drafts payable to precious metal dealers, for the buying and selling of gold;*
- *They physically couriered the cash in large amounts when travelling, without declaring it at the border;*
- *Some of them were nervous when they came to the bank and appeared to be following instructions from someone who came into the branch with them.*

By the time each individual conducted his own transactions over a period of time, the group had managed to transfer a significant amount of money indirectly (through nominees and businesses) and directly to the country where the terrorist group was active. Law enforcement informed FINTRAC of its suspicions and FINTRAC was able to identify numerous types of reports on these individuals. A number of STRs were submitted by multiple institutions, providing detailed information on the actions and suspicions relating to the individuals. STRs also provided information, based on keen observations from bank staff, that certain individuals were linked. A number of cross-border seizure reports were also received when individuals failed to declare having \$10,000 or more when leaving Canada. Based on FINTRAC's analysis of the financial transactions and other information received, FINTRAC reached reasonable grounds to suspect that the information would be relevant to the ongoing terrorist financing investigation.

¹³ The details of the scheme represented here are not taken from one particular case disclosure; rather, they are based on observations made in a number of similar cases.

2) Characteristics of individuals suspected of terrorist financing activities:

Based on a review of a sample of suspected 2010-11 TF case disclosures, the following characteristics were noted:

- The majority of these individuals are middle-aged males. Individuals working in groups are within the same decade in age;
- Females are related through marriage and familial ties and are suspected of facilitating terrorist financing;
- Individuals are not generally connected through business relationships, in contrast to other crimes;
- However, where there is a business involved, there are often familial ties between the individuals;
- Individuals suspected of being involved in TF activity are more likely to own a small business;
- Other employment sectors include non-profit organizations; professions (such as accountant, doctor, dentist, engineer, etc); service industry, including retail; trades (such as painter, flooring professional, etc.); and the food industry. In some instances, individuals were students.

3) Methods and techniques observed in cases involving suspected terrorist financing and money laundering:

- Structuring and smurfing:
 - Individuals conducted large cash deposits into bank accounts, but split it up so that deposits were under the \$10,000 threshold to avoid reporting requirements;
 - Individuals ordered several EFTs on the same day, each under \$10,000, to the benefit of the same individual when it would have been more economical and logical to send a single EFT;
 - Multiple unrelated individuals ordered EFTs (through MSBs) to the benefit of the same beneficiaries located in a high-risk foreign jurisdiction.
- Precious metal dealers
 - A group of individuals used smurfing methods to deposit large amounts of cash into the financial system followed by purchases of multiple drafts payable to precious metal dealers.
- Use of nominees
 - Individuals conducted transactions at financial institutions while receiving instructions from unknown individuals over the phone;
 - Two individuals arrived at the bank and only one conducted transactions while receiving instructions from the unidentified individual.



- Commingling and the use of front companies
 - Business bank accounts were used to conceal illicit funds;
 - Bank accounts were opened for front companies. When compared to similar types of business bank accounts, transactional activity was not in keeping with that type of business.
- Use of credit cards to perpetrate “bust out schemes” in both TF and ML cases
 - A change in cardholder activity occurred with an increase in purchases, followed by out-of-pattern cheque payments. Large purchases at retail stores were made which were abnormal for that type of business, such as gas stations, fast food restaurants, etc. Eventually, the cheque payments were returned but the cardholder quickly used the available credit before a hold was placed on the account;
 - This scheme often used collusive merchants (according to STR information) to facilitate false credit transactions, where goods or services were never exchanged;
 - In the instance where illicit cash was laundered, both layering and integration phases were observed when payments were made to the credit card account with proceeds of crime and then using the credit card to conduct purchases.
- Use of electronic funds transfers
 - Individuals ordered numerous but low-value EFTs under \$1000 at MSBs to the same foreign beneficiary or various foreign individuals on a daily or weekly basis. Over time, the amounts increased to under \$5000.
- Lawyer’s trust account
 - Large bank drafts were purchased and large cheques were issued to lawyers’ trust accounts. At times, there were multiple law firms receiving deposits.
- Real estate
 - In the instance where terrorist financiers are laundering illicit cash, bank account funds were depleted for high value real estate purchases, which might have been part of the integration stage.
- MSBs
 - Suspected complicit MSBs ordered large EFTs to the benefit of foreign MSBs in countries of concern;
 - Individuals appeared to be operating an MSB through a personal account with rapid movement of funds and unknown source and destination of funds.
- Prepaid cards
 - Large cheques were issued to companies that distributed prepaid cards, including telephone cards.

4) Use of various businesses and NPOs in suspected terrorist financing cases

The last decade has seen an urgent commitment to developing anti-money laundering and terrorist financing compliance regimes; in response, terrorists have evolved and found ways to adapt to these restrictions. The use of non-profit organizations (NPOs) and legitimate businesses quickly became exploited by these groups. However, in reviewing cases of the past four years, a notable decline in the use of businesses to move funds was observed, as shown in Table 4.

Table 4: Percentage of suspected terrorist financing cases involving the use of at least one business

	2007-08	2008-09	2009-10	2010-11
% of cases involving businesses	82%	84%	56%	64%

Table 5: Percentage of suspected terrorist financing cases involving the use of NPOs

	2007-08	2008-09	2009-10	2010-11
% of cases involving NPOs	29%	25%	24%	20%

Throughout the past four years, the following businesses and sectors have been commonly implicated in suspected terrorist financing cases:

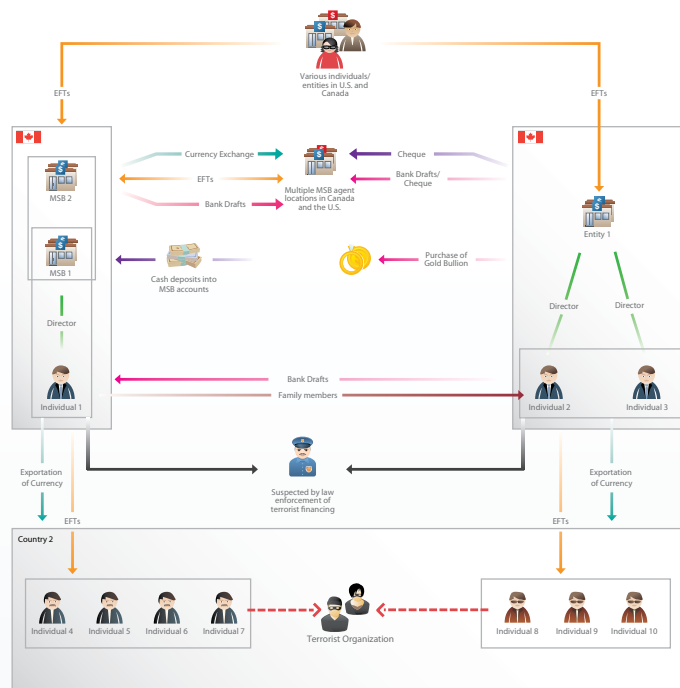
- Non-profit organizations
- Food industry (i.e. butcher, food distributor, grocery store, etc.)
- Real estate
- Auto industry
- Shipping/freight companies
- Import/export companies
- Trades (i.e. painter, flooring professional, carpenter, etc.)
- Textile and trading companies



Case example 2: Suspected Terrorist Financing

Law enforcement provided information on family members suspected of providing financial support for a terrorist organization (**Individuals 1 and 2**). Information was also provided on **MSB 1** owned by **Individual 1**. Upon further analysis, FINTRAC identified another MSB (**MSB 2**) registered to the same address, another company (**Entity 1**) owned by **Individual 2** and another family member (**Individual 3**). It was suspected that through these businesses, funds were deposited into accounts or moved through multiple MSB agent locations (by cheque and bank draft), then EFTs were ordered to numerous beneficiaries in the country where the terrorist organization was located. Some of the foreign beneficiaries were suspected to be related to the individuals in Canada. **MSB 1** sent and received numerous EFTs to and from two MSB agent locations in the United States. The purposes of these transactions were not known, but they could have been a way to potentially receive terrorist financing funds from anonymous individuals/entities in the United States and Canada. Millions of dollars worth of large cash deposits into accounts held at banks by **MSB 1 and 2** were reported by financial institutions to FINTRAC.

Currency exchanges were also conducted at MSBs to convert US dollars to Canadian dollars and vice versa, and **Individuals 1 and 2** were issued bank drafts and cheques which were then deposited into various accounts, including third party accounts. FINTRAC also received CBCRs relating to travel pertaining to **Individuals 1 and 2** and their declarations of currency being imported into the same country where the terrorist organization was located. According to an STR, large cash, cheque and bank drafts were deposited into bank accounts held by **Individuals 2 and 3**, which were then followed by the purchase of drafts payable to precious metal dealers, where they regularly bought and sold gold. All parties disclosed on also benefited from numerous EFTs ordered by various individuals and entities in the United States. This activity, pertaining to **Entity 1**, was described by the bank as being unusual for the nature of their business.



According to numerous STRs, the following red flags were identified:

- The individuals avoided the \$10,000 reporting threshold by breaking up large cash deposits;
- The individuals had multiple bank accounts at multiple financial institutions, and issued cheques from one financial institution to another;
- The individuals constantly moved money around between business and personal accounts;
- An individual withdrew funds from a personal account, then a few hours later deposited the amount plus a little extra into a business account, then proceeded to transfer the original amount back to the personal account;
- An individual deposited cheques and bank drafts for large amounts and then re-issued the drafts to third parties;
- The individuals issued cheques to an MSB in US dollars, then received drafts from the same MSB in Canadian dollars which were deposited back into the original issuing account;
- A third party made a cheque deposit into an individual's account drawn from the same MSB as above;
- When deposits and withdrawals were questioned by the bank, the individual was secretive and avoided providing an answer;
- Numerous third-party cash deposits were placed into accounts;
- Immediately after large cheque deposits were made, outgoing EFTs were purchased for foreign beneficiaries or bank drafts were purchased and made payable to MSBs;
- There was a rapid movement of funds inconsistent with personal banking;
- An account remained dormant for some time and then suddenly became very active.



D) Country distribution of EFTs included in FINTRAC case disclosures

Electronic funds transfers are used after money generated by criminal activities is placed in the financial system, or when terrorist financiers send or receive funds related to terrorism. Individuals use EFTs often to complicate the money trail, to conceal funding of terrorism, or to evade anti-money laundering authorities; they may send or receive EFTs in Canada or in foreign countries, offshore locations and tax haven countries with lax anti-money laundering laws.

Drug trafficking and the demand for drugs are fuelling global criminal operations. Drug traffickers are extremely diversified and their tentacles reach beyond our Canadian borders. In the drug trade, production and trafficking elements may take place in different countries, from the origin of precursor chemicals for production to countries of cultivation or drugs produced in one country, which may then be trafficked into a second country, and supplied to a third country. Similarly, the laundering of illicit drug proceeds can be done through various jurisdictions. FINTRAC is in a unique position to identify unusual patterns and emerging trends in EFT flows and, as a result, to recognize global financial routes related to those ML activities. Individuals involved in the drug trade normally introduce their illicit funds into the financial system through various methods (such as cash deposits and the use of front companies) to conduct financial transactions, which are followed by purchases of EFTs. In contrast to drug-related cases, fraudulent funds are normally already in the financial system, and so the placement stage of money laundering is not required. It is therefore more difficult to detect the layering and integration phases. One way to launder the proceeds of fraud is to send them to a foreign bank account, either in a bank secrecy country or offshore location, where the Canadian authorities cannot look for them. Overall, fraud-related cases have been observed to contain

four times the number of EFTs compared to drug-related cases, which indicates that this is a common method employed by these schemes.

Terrorist financing requirements are diverse and vary among groups. Typically, financing is required not only to fund specific terrorist operations, but also to meet the operational demands of the group, from recruitment to planning to training. At times, these groups are local, but most are part of a larger organization with an international footprint. The financial intelligence collected from EFT reports is especially significant when it comes to identifying suspicious transactions related to terrorist financing. Terrorist financing activity is unique in comparison to drugs and fraud cases, as money used to fund terrorist operations is sometimes derived through legitimate means; as such, concealing the source of funds is not required. However, in some terrorist financing cases, a crime may be committed and the proceeds may be sent by EFTs directly or indirectly to a foreign terrorist organization. Terrorist financiers may also attempt to send EFTs to individuals in unexpected locations, or through several countries, to further complicate the money trail.

Tables 6 to 9 list the jurisdictions where EFTs were most commonly sent or received in case disclosures between 2007 to 2011, and refer to specific case types. FINTRAC is not an investigative agency, and therefore cannot confirm the purpose and nature of all financial transactions included in disclosures. Consequently, relevant transactions disclosed in cases could, on further investigation by disclosure recipients, be found legitimate. Similarly, it is impossible for FINTRAC to differentiate between legitimate and illegitimate funds that are commingled by businesses or individual transactions. As a result, the identification of the top 15 countries provided in this section is more a general indication of geographic locations that may be more commonly linked to money laundering or terrorist financing. Regardless of the above caveats, the inclusion of these lists of jurisdictions may contribute to enhancing public awareness and understanding of matters related to money laundering and terrorist financing.

TABLE 6: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED MONEY LAUNDERING CASES INVOLVING DRUG OFFENCES

1. United States of America	6. Taiwan	11. Switzerland
2. India	7. Iran	12. Mexico
3. Vietnam	8. United Kingdom	13. Peru
4. Hong Kong	9. Belarus	14. Israel
5. China	10. Latvia	15. Thailand

TABLE 7: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED MONEY LAUNDERING CASES INVOLVING FRAUD OFFENCES (EXCEPT SECURITIES/INVESTMENT FRAUD)

1. United States of America	6. Israel	11. Austria
2. United Kingdom	7. Switzerland	12. France
3. Iran	8. China	13. Cyprus
4. Japan	9. Germany	14. Guernsey
5. Hong Kong	10. Italy	15. India

TABLE 8: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED MONEY LAUNDERING CASES INVOLVING SECURITIES/INVESTMENT FRAUD OFFENCES

1. United States of America	6. Bahamas	11. Panama
2. Netherlands Antilles	7. Antigua and Barbuda	12. Dominican Republic
3. United Kingdom	8. Netherlands	13. Turks and Caicos
4. China	9. Bermuda	14. Barbados
5. Mexico	10. Hong Kong	15. Luxembourg

TABLE 9: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED TERRORIST FINANCING CASES

1. United States of America	6. India	11. Sri Lanka
2. United Arab Emirates	7. Austria	12. Saudi Arabia
3. Lebanon	8. Netherlands	13. Switzerland
4. Pakistan	9. Iran	14. Hungary
5. United Kingdom	10. Hong Kong	15. Turkey



While many of the countries listed above are large financial hubs and trading partners with Canada, some of these jurisdictions are also known transits or entry points for drug traffickers. Some are also known for being tax havens and offshore financial centres, or locations of terrorist groups. The most frequently represented jurisdictions across the identified predicate offences were the USA, the UK and Hong Kong. Hong Kong is known as an offshore financial centre and for having strong bank secrecy laws. The prevalence of the USA and UK is mainly due to the strong financial ties between these jurisdictions and Canada.

Jurisdictions such as Vietnam, Taiwan, Belarus, Latvia, Peru and Thailand only appeared in the top 15 of drug-related cases (Table 6). Both Vietnam and Thailand have been previously identified by the Financial Action Task Force (FATF) as having deficient AML/ATF regimes, which have since improved. The Asia-Pacific region is known for its supply and smuggling routes. Latvia is a regional financial centre and is vulnerable to organized crime activity, which may explain its ranking in this category. Drug trafficking is a primary source of illicit proceeds in Belarus, which is also a drug transshipment point. Peru is known as a top producer of cocaine.

In terms of general fraud-related cases (Table 7), Japan, Germany, Italy, France, Cyprus and Guernsey were the jurisdictions identified uniquely. Europe had the greatest representation in this category, which included the UK, Switzerland, Germany, Italy, Austria, France, and Guernsey.

The securities/investment fraud category in Table 8 had the highest number of unique jurisdictions not found in other categories. These jurisdictions were the Netherlands Antilles, Bahamas, Antigua and Barbuda, Bermuda, Panama, Dominican Republic, Turks and Caicos Islands, Barbados and Luxembourg. With the exception of the Dominican Republic, all of these jurisdictions have strong bank

secrecy laws. Antigua and Barbuda and the northern part of Cyprus were previously identified by the FATF as having deficiencies in their AML/ATF regime; these have since improved.

Analysis of TF cases identified the following unique jurisdictions, not found in the other tables: United Arab Emirates (UAE), Lebanon, Pakistan, Sri Lanka, Saudi Arabia, Hungary and Turkey. Some of the jurisdictions identified in Table 9 have direct and indirect associations to terrorism, where they have been either a target of terrorism or a training/organizational base for terrorist activity. These jurisdictions include Lebanon, Pakistan, India, Iran, Sri Lanka, Saudi Arabia, and Turkey. The FATF has singled out Sri Lanka, Pakistan and Turkey as having deficient AML/ATF regimes. Pakistan has since improved, but as of June 2011, Sri Lanka and Turkey have yet to improve their deficiencies. India's geographic location makes it susceptible to drug trafficking via neighbouring countries and it is a significant target for terrorism. The UAE is a major financial centre in the Middle East region, as well as a leading trade and transportation hub. Due to its geographic location, the UAE is vulnerable to money laundering and terrorist financing. As well, many Canadian REs (such as MSBs) use the UAE as a hub for funds which are then distributed to other jurisdictions.

In summary, the main locations from which EFTs were ordered or where they were received, revealed that:

- Many of these jurisdictions had previously or currently been declared deficient in their AML/ATF regimes by the FATF;
- Many are known as offshore financial centres and have strong bank secrecy laws;
- Some are known for their drug supply and smuggling routes;
- Others are popular financial or transshipment hubs in Europe, Asia, and the Middle East; and
- Some have either been a target of terrorism or are a training/organizational base for terrorist activity.

Part III: Role of FINTRAC internationally

FINTRAC strives to be one of the leading financial intelligence units in the world and has endeavoured to take a strong leadership role in the international community. FINTRAC's work with international bodies, such as the FATF and the Egmont Group, contributes to the development of international anti-money laundering/anti-terrorist financing policies and standards. FINTRAC also strives to foster a greater cooperation among FIUs and to contribute to a better understanding of new trends and challenges.

Given that most money laundering activities involve transnational movements of funds, and that terrorist financing tends to transcend national borders, the effectiveness of FINTRAC's financial intelligence is reliant on information sharing, where appropriate, with our international counterparts. FINTRAC currently holds 76 Memoranda of Understanding (MOUs) with other FIUs around the world, and this number is constantly growing.

Case example 3: Assistance in international investigations

In one particular instance, FINTRAC received a query from a partner FIU regarding a criminal investigation of securities fraud relating to a Canadian citizen. As part of its investigation, the FIU was seeking to identify the perpetrators of the fraud and identify suspicious transactions, as this information could help identify where the funds had been placed in the financial system to prevent the further disposition of the proceeds of the fraud. FINTRAC's analysis identified suspicious transactions related to nine individuals/entities mentioned in the FIU query. Moreover, the analysis identified seven additional entities, some of which were affiliated to two previous criminal investigations in Canada relating to a large-scale marijuana grow operation and securities fraud. Many suspicious transactions were identified and a case disclosure was sent to the originating FIU, as well as to national and provincial law enforcement in Canada. Furthermore, FINTRAC granted permission for the FIU to share the information with a third FIU, as suspicious transactions were linked to the third identified jurisdiction. Therefore, although the query originated from one FIU, three countries became involved in a possible money laundering scheme.



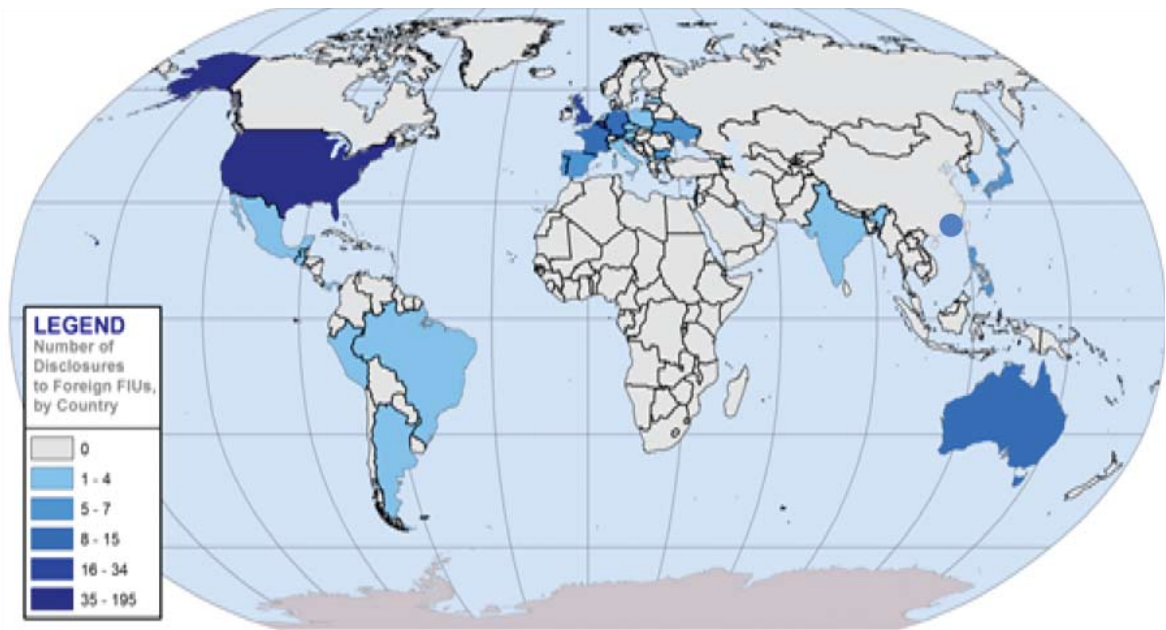
Throughout the past four years, foreign FIUs have consistently been within the top four leading recipients of case disclosures. FINTRAC provides case disclosures to FIUs either in response to a query originating from the receiving FIU where transactions are suspected of involving ML or TF, or when FINTRAC identifies suspicious transactions going to or from a FIU partner

country. By querying the foreign FIU, FINTRAC is able to obtain foreign transactional data and other information identified as suspicious by the foreign partner. This foreign information builds on the domestic information and can provide further leads in the case. The top 10 FIU country disclosure recipients from 2007 to 2011 are listed in Table 10 and the distribution for all FIU disclosures is illustrated in Figure 15.

TABLE 10: MAIN FIU DISCLOSURE RECIPIENTS

1. United States of America	6. France
2. United Kingdom	7. Australia
3. Bahamas	8. Luxembourg
4. Belgium	9. Singapore
5. Hong Kong	10. Germany

FIGURE 15: DISTRIBUTION OF ALL DISCLOSURES PROVIDED TO FOREIGN FIUS (2007-11)



CONCLUSIONS

As demonstrated in this report, money launderers and terrorist financiers continue to exploit Canada's financial system to launder the proceeds of crime or support terrorism. While some trends, typologies and methods may be new, many described in this report have been observed for several years, and will continue to be employed by criminals and terrorist supporters.

What we have observed over the past four years is that criminals and terrorist supporters are opportunistic; their activities evolve based on the AML/ATF community's pre-emptive response and preventative compliance measures. For example, debit/credit card fraud is gradually overtaking mass marketing fraud. Investment/securities fraud will likely persist due to the current unstable economic climate. It is more common to uncover fraudulent investment schemes in bad economic times. The promise of a huge return on one's investment administered by a trusted individual in the same community is more appealing than keeping money in a stagnant or declining investment fund. Unbeknownst to the investor, these funds will later disappear – along with the trusted friend.

The prevalence of transnational crime and the enhanced sophistication of international criminal and terrorist networks have highlighted the complexities of cross-border transactions. These trends, however, further entrench FINTRAC's role in the global

community by highlighting its important responsibility in detecting and deterring money laundering and terrorist financing activities. Financial intelligence is playing a heightened role in law enforcement and intelligence investigations as FINTRAC's analysis continues to provide useful leads and identify new players. The majority of case disclosures include international elements which would normally impede the investigative flow of information, but FINTRAC is uniquely placed at the heart of global financial communications with the international EFT reports it receives and its collaboration with counterparts abroad. Of course, without the valuable reports – particularly the suspicious transaction reports and EFTRs – provided by reporting entities, FINTRAC's analysis would not be as comprehensive. Reporting entities themselves play a pivotal role in the success of the AML/ATF regime, as they represent the first line of defence against financial crime; they question suspicious and unusual activity as it happens, and provide a concise account of their suspicions to FINTRAC.

FINTRAC's financial intelligence owes much to the outstanding effort and work that all reporting entities have made in the fight against money laundering and terrorist financing. Together, we ensure the continued integrity of Canada's financial system and deter individuals and organizations from using Canada as a criminal base.

ACRONYMS

AML	Anti-money laundering
ATF	Anti-terrorist financing
CAD	Canadian dollar
CBCR	Cross-border currency report
CBSA	Canada Border Services Agency
CBSR	Cross-border seizure report
CDR	Casino disbursement report
CRA	Canada Revenue Agency
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
EFT	Electronic financial transaction
EFTR	Electronic financial transaction report
FATF	Financial Action Task Force
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial intelligence unit
FIUQ	Financial intelligence unit query
ID	Identification document
LCTR	Large cash transaction report
MDMA	Methylenedioxymethamphetamine ("Ecstasy")
ML	Money laundering
MOU	Memorandum of understanding
MSB	Money services business
NPO	Non-profit organization
RCMP	Royal Canadian Mounted Police
RE	Reporting entity
STR	Suspicious transaction report
TF	Terrorist financing
TH	Threats (to the security of Canada)
TPR	Terrorist property report
UAE	United Arab Emirates
UK	United Kingdom
USA	United States of America
USD	United States dollar
VIR	Voluntary information record