



MONEY LAUNDERING AND TERRORIST FINANCING (ML/TF) TYPOLOGIES AND TRENDS FOR CANADIAN MONEY SERVICES BUSINESSES (MSBs)

FINTRAC Typologies and Trends Reports—July 2010



MONEY LAUNDERING AND TERRORIST FINANCING (ML/TF) TYPOLOGIES AND TRENDS FOR CANADIAN MONEY SERVICES BUSINESSES (MSBs)

© Her Majesty the Queen in Right of Canada, 2010

Catalogue No.: FD5-1/3-2010E-PDF

ISBN: 978-1-100-16310-9

FINTRAC Typologies and Trends Reports—July 2010

July 2010

MESSAGE FROM THE DIRECTOR

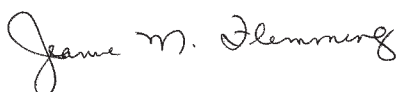
I am pleased to present **Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)**. This report is intended to provide targeted feedback for reporting entities within the MSB sector to assist them in strengthening their compliance regimes pursuant to obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. These obligations include the requirement for MSBs to register with FINTRAC, establish a compliance regime, and also include obligations related to record keeping, customer identification and reporting certain transactions to FINTRAC.

MSBs provide a range of unique, valuable, and competitive financial services for Canadians and international customers, and while the variety of MSB types and sizes can provide consumers with expanded choices, it also means that the sector has unique challenges and risks with respect to money laundering and terrorist financing. This report is part of FINTRAC's commitment to demonstrate the value of information submitted by reporting entities, in terms of helping to identify trends in ML and TF, and also to provide tangible feedback which assists the MSB sector with its own compliance regimes.

Canada's anti-money laundering (AML) / combating the financing of terrorism (CFT) regime is comprised of a variety of actors, including government, the private sector, the general public, and the international community. The strength of any AML/CFT regime is gauged by the seriousness with which ML/TF risks are taken by each component within that regime. As part of Canada's effort to deter, detect and prevent money laundering, MSBs play an important role in ensuring the integrity of Canada's financial system against financial crime, and doing what it can to mitigate possible threats to national security.

As FINTRAC's Director, it is my hope that this report will help reporting entities to better understand some of the vulnerabilities they face, and that it will highlight the importance of the role the private sector plays in assisting FINTRAC to produce timely and relevant financial intelligence for our law enforcement and national security partners.

I look forward to building on this report and working collaboratively on similar projects and I would encourage you to comment on its contents and to suggest issues for future exploration.



Jeanne M. Flemming
Director



CONTENTS

PART 1: INTRODUCTION	2
PART 2: ML/TF IN THE CANADIAN MSB SECTOR	4
(A) Common Designated Offence Types in FINTRAC Case Disclosures Involving the MSB Sector	4
(B) ML/TF Methods and Techniques Applied Through the MSB Sector	4
(C) Sanitized Case Examples and Red Flags	7
PART 3: OTHER ANTI-MONEY LAUNDERING (AML) / COMBATING THE FINANCING OF TERRORISM (CFT) CONCERNS	15
(A) Use of Registered MSBs by Unregistered Remittance Businesses	15
(B) Emerging Issues to Monitor in the Canadian MSB Sector: Merging of Traditional and New Payment Methods	16
PART 4: CONCLUSION	17
ANNEX 1 — FATF ML/TF Indicators Relevant to the MSB Sector	18
ANNEX 2 — Money Laundering and Terrorist Financing in Canada for All Sectors: Review of 2008-2009 FINTRAC Case Disclosures	19



1. INTRODUCTION

This report is one in a series of FINTRAC publications which are intended to provide targeted feedback to specific reporting entity sectors. This particular report is focused on the MSB sector in Canada, and was made possible through collaboration between FINTRAC and certain Canadian MSBs, including Western Union, Encaissement de Chèques Montréal Ltée, and AlertPay. The discussions between the MSB sector and FINTRAC have guided the subjects that are examined in this report.

This report is divided into three principal sections. The first highlights common money laundering (ML) / terrorist financing (TF) methods and techniques which were found through a review of FINTRAC cases for 2008-2009, and presents sanitized case examples, a selection of red flags which may be useful to the MSB sector. This section also provides information regarding criminal offence types linked to suspected ML and TF which were observed in relation to financial transactions conducted at MSBs. Wherever possible the report aims to provide illustrative examples that support more generalized findings. Publicly available indicators specific to the MSB sector, which were developed by the Financial Action Task Force (FATF), are also listed in Annex 1.

The second section deals with issues which are more future-oriented, and raises areas of possible concern or emerging trends or technologies that FINTRAC believes may warrant closer attention by the sector and AML/CFT authorities over time.

Contextual information on ML/TF trends in Canada, across all sectors, as observed in cases from 2008-2009 is also presented in Annex 2 which is the final section of this report.

The MSB Sector in Canada

Money services businesses (MSBs)¹ are non-bank entities which provide transfer and exchange mechanisms. People generally use MSBs to exchange or transfer value, or to purchase or redeem negotiable instruments. In Canada, an MSB is defined as an individual or an entity that is engaged in the business of any of the following activities:

- foreign exchange dealing;
- remitting or transmitting funds by any means or through any individual, entity or electronic funds transfer network; and/or
- issuing or redeeming money orders, traveler's cheques or other similar negotiable instruments.²

1 See money services businesses (MSBs) on FINTRAC's Web site: <http://www.fintrac-canafe.gc.ca/re-ed/msb-eng.asp>.

2 Note that this does not include redeeming cheques payable to a named individual or entity. In other words, cashing cheques made out to a particular individual or entity is not included.

MSBs are reporting entities and subject to the *Proceeds of Crime (Money Laundering and) Terrorist Financing Act (PCMLTFA)*. As such, MSBs are required to register with FINTRAC. Furthermore, MSBs must fulfill other legislative and regulatory obligations, which include establishing a compliance regime, filing reports, identifying clients, maintaining records. The legislative definition of MSBs also includes alternative money remittance systems such as hawala, hundi, chitti, and undiyal.

In terms of outlining the diversity of the MSB sector, the table on this page provides a general sense of how the sector is broken down by major service lines at the time of drafting. It should be noted that the total number of registered MSBs does not include the number of MSB agents. In the Canadian regime, MSB agents are often covered through the MSB which engages/contracts with the agents (depending on the other activities of the MSB agent)³.

FINTRAC recognizes that there is great diversity within the almost 1,000 registered MSBs which constitute the sector in Canada. This diversity is the result of a wide range of business sizes⁴ and business models, and also a result of the variety of services available at different MSBs and the communities they serve. The MSB sector includes everything from large multinational companies with thousands of employees, branches, and thousands of franchised agents, who collectively carry out hundreds of millions of dollars worth of transactions, to very small independent businesses, with no employees beyond the owner, and which are engaged in very low volumes of transactions.

Some MSB business models operate using an account-based approach, some with significant linkages to much larger financial institutions, including banks, while other MSBs operate almost exclusively on a “per transaction” basis (meaning there is no standing account or business relationship between the MSB and the person seeking to undertake a particular transaction). This report attempts to provide illustrations of some of the ML/TF risks facing MSBs, and highlight – where possible – how particular MSB services can be exploited by suspected criminals who have used MSBs as part of their financial activity.

MSB Service Focus	Description ⁵
Money remitters / transmitters	The MSB Registry includes 698 MSBs which reported that they were providing this type of service. This represents approximately 73% of the MSB sector.
Currency/foreign exchange	The MSB Registry includes 770 MSBs which reported that they were providing foreign exchange services. This represents approximately 80% of the MSB sector.
Issue or redeem negotiable instruments	The MSB Registry includes 276 MSBs which reported that they were providing this type of service. This represents approximately 29% of the MSB sector.

3 In the Canadian regime, persons or entities which are exclusively agents of an MSB are partially covered through the MSB that engages/contracts with them. MSB agents are, however, required to report suspicious transaction reports (STRs), attempted suspicious transaction report (STR-As), and terrorist property reports (TPRs). If agents carry out money services business outside of the activities considered in the contract, they are also required to register as an MSB, establish a compliance regime, and fulfill other PCMLTFA requirements.

4 As noted earlier in this report, there is a wide range of business sizes within the MSB sector, and providing a single report that fully reflects the variety of specific ML/TF risks to MSBs of different sizes and geographic distribution is a highly complex task. Efforts were made in this report to reflect a variety of MSB service lines and business sizes in the examples and sanitized cases provided where this was possible. However, because of the space limitations of this report it is not possible to provide exhaustive coverage. In this context, it should be noted that different business models, sizes, and business orientations create different and unique risks. Reporting entities are encouraged to consider specific ML/TF risks, including business size, when they conduct their own risk assessments.

5 It should be noted that there is significant overlaps in terms of MSBs offering these services and this is why the total of the three types does not equal 100%. In addition, some MSBs have indicated to FINTRAC that they intend to offer some of these services but have yet to start delivery.

2. ML/TF IN THE CANADIAN MSB SECTOR

In 2008-2009, FINTRAC disclosed 197 cases that involved transactions through the MSB sector, out of a total of 556 cases. The information below provides a general overview of trends in ML/TF in relation to the MSB sector, and also includes a basic review of the types of criminal offences associated with suspicions of ML or TF found in these cases.

While a review of cases covering all sectors was undertaken for 2008-2009 (and is included at Annex 2 of this report) this section focuses on the most common money laundering methods and techniques identified in cases where transactions were conducted at MSBs. Many of the methods and techniques described in this report may be known to MSB operators and agents as they have been employed for many years.

(A) Common Designated Offence Types in FINTRAC Case Disclosures Involving the MSB Sector

In examining cases where the services of an MSB were used by individuals suspected of criminal activity, a number of different offence types were observed and are listed in the table on the right.

It should be noted, as highlighted earlier, that case disclosures reviewed for this report were not solely connected to transactions conducted at MSBs, and that approximately one-third of the reviewed cases involved both MSBs and financial institutions (such as banks, credit unions, and cooperatives). The following table was derived from all 197 case disclosures involving the use of MSBs in 2008-2009, and provides a summary of the primary designated offence type that was suspected or alleged to be associated with each case. It is important to note that many cases involve multiple designated offences; this table only refers to the offence types which were most prominent in the reviewed cases.

Commonly Observed MONEY LAUNDERING (ML) Designated Offence Types ⁶	Proportion of Cases of This Type Involving Transactions at an MSB (%)
Substantive offence not identified ⁷	30%
Drug offences	25%
Fraud	20%
Terrorist financing (TF)	12%
ML (and/or TF) + Tax evasion ⁸	4%
Human smuggling / trafficking	2%

Other observations regarding “designated offences” and ML/TF in the MSB context include:

- In cases where drug-related activity was suspected, the majority of cases involved the trafficking of cocaine and/or marijuana; and
- In cases where fraud was suspected, investment/securities and telemarketing fraud (or other Mass Marketing Fraud (MMF)) were the most observed.

(B) ML/TF Methods and Techniques Applied Through the MSB Sector

Of the case disclosures involving the use of an MSB, FINTRAC identified and focused on 126 cases (from 2008-2009), which were the most illustrative of how MSBs could be exploited for money laundering and terrorist financing purposes.

⁶ A number of these criminal offence categories have been identified by the FATF as being common concerns across many jurisdictions in relation to the MSB sector.

⁷ As noted, this category reflects cases where the pattern of financial activity, or other information available to FINTRAC, suggested money laundering (including suspected laundering of proceeds of crime on behalf of a person/entity) and/or where the designated offence may not have been identified.

⁸ Tax evasion is currently not a money laundering designated offence under the Criminal Code of Canada, but is an offence under the *Income Tax Act*. Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, FINTRAC may disclose suspicions of tax evasion to the Canada Revenue Agency (CRA) where the Centre also has reasonable grounds to suspect money laundering or terrorist financing. Tax evasion has been placed in this table because it was observed more frequently in relation to ML and TF.

While some ML/TF risks are common across the MSB sector (and other sectors), FINTRAC also recognizes that different MSB types and MSB service lines are subject to different types of ML/TF risks. For that reason, FINTRAC has endeavoured to show how specific ML/TF techniques have been observed by using examples which focus on the different MSB service lines. In this context, the most commonly observed money laundering techniques are described below.

STRUCTURING OR ATTEMPTING TO CIRCUMVENT MSB RECORD-KEEPING REQUIREMENTS

“Structuring” can be defined as a pattern of financial transaction activity in which a single transaction is broken down into multiple/ sequential transactions below the threshold which would require mandatory reporting and/or the application of an MSB’s client ID and record-keeping obligations. As a more general (and more obvious) technique, some conductors simply ask that transactions not be recorded.

By carrying out transactions at levels below the mandatory reporting threshold (or attempting to) some conductors believe their transactions can effectively evade detection. Such conductors do not understand that MSBs are required to report suspicious transactions at any level, and/or believe that they have a greater chance of avoiding scrutiny by carrying out structured transactions. Structuring is by far the most prevalent ML technique observed in FINTRAC cases, and can be found in relation to all MSB types and service lines.

Examples of this technique being used at MSBs include:

- In a suspected mass marketing fraud (MMF) case, the organizers of the fraud repeatedly used the same location, in a very short period of time, to break down their transfers to criminal associates below the mandatory \$10,000 reporting threshold.

- In one suspected drug trafficking case, the disclosure subject made several dozen separate money order purchases, seeming to structure them below record-keeping thresholds. These money orders were made payable to an MSB, and were negotiated in a variety of cities across North America.

ATTEMPTING TO CIRCUMVENT MSB CLIENT IDENTIFICATION REQUIREMENTS

Attempts to avoid MSB client identification obligations are very common, and occur across all MSB types within the sector. They are often linked to efforts to mislead MSBs about the purpose of a transaction and may involve concealing the beneficial ownership or control of funds in an attempt to obscure a link between the money which is used to carry out a particular transaction and the criminal act from which the proceeds were gained.

This technique can also be used to create the false impression that a financial transaction is legitimate where it might be questioned if the conductor provided accurate information. This technique can include the use of fake identification/names/ addresses, and/or unverifiable information based on combinations of real or fake names and addresses.

Examples of this technique being used at MSBs include:

- In one case, the disclosure subject purchased dozens of money orders valued in the tens of thousands, in less than a year. Each transaction was structured below reporting requirements, with most of these funds being sent to individuals outside of Canada. The disclosure subject provided inaccurate job title information and misleading address information possibly to add apparent legitimacy to transactions which were not commensurate with the individual’s actual employment and income.

SMURFING, USING NOMINEES, AND/OR OTHER PROXIES

The use of nominees or other proxies is observed with some frequency in FINTRAC cases as part of an effort to conceal the beneficial ownership of the funds being moved or to obscure the coordinated nature of a series of financial transactions. The coordinated use of nominees for the purposes of breaking down what would be a large value transaction into several 'below threshold' amounts is a specific type of structuring which is often referred to as 'smurfing'.

Examples of this technique being used at MSBs include:

- In a suspected drug trafficking-related case involving 'smurfing', members of an organized crime group appeared to have used several individuals to send funds through an MSB to the same individual in the United States. In this particular case, the first 'smurf' was followed 20 minutes later by a second smurf (a different individual) at the same MSB, who proceeded to send an EFT to the same beneficiary in the United States.

EXPLOITING NEGOTIABLE INSTRUMENTS

The purchase of negotiable instruments can be a means of placing the proceeds of crime into the formal financial system, and the subsequent redemption of those instruments can be used in the layering stage of money laundering to help create gaps in the transaction audit trail (e.g. between reporting sectors). The types of negotiable instruments which were found to be relevant to various patterns of ML/TF activity within the MSB sector included the issuance of cheques by the MSB (in lieu of cash, etc.), the issuance of bank drafts made payable to an MSB, and money orders.

Examples of this technique being used at MSBs include:

- In a suspected terrorist financing case, FINTRAC observed transactions by an individual using an MSB to exchange thousands of Canadian dollars for US dollars and who often left the MSB with cheques.
- In a suspected drug case, an MSB filed STRs regarding an individual who purchased multiple, non-sequential money orders (payable to himself/herself) in a possible attempt to obscure the conductor's connection to a suspected drug trafficker.⁹

REFINING

Refining refers to the conversion of small denomination bank notes to large denomination bank notes. FINTRAC has observed this practice in conjunction with some currency exchange transactions. This ML technique is commonly associated with drug trafficking, as drug dealers accumulate a large amount of smaller denomination notes through the course of their illegal drug sales. Large quantities of cash, especially in small denomination bank notes can be difficult to transport, and may raise greater suspicion as criminals attempt to place these funds into the financial system. Money launderers will therefore seek to convert or "refine" small denomination bank notes (\$5, \$10, and \$20 notes) into larger denomination bank notes (such as \$50 and \$100 notes).

Examples of this technique being used at MSBs include:

- In a suspected human smuggling case, an individual with suspected ties to Eastern European Organized Crime (EEOC) simultaneously refined and exchanged foreign denominated cash.
- In one case involving suspicions of laundering drug proceeds, the disclosure subject exchanged a total of US\$8,000 in US\$20 bank notes. This individual used the MSB in a regular pattern of activity, including transactions on consecutive days, using US\$20 bank notes.

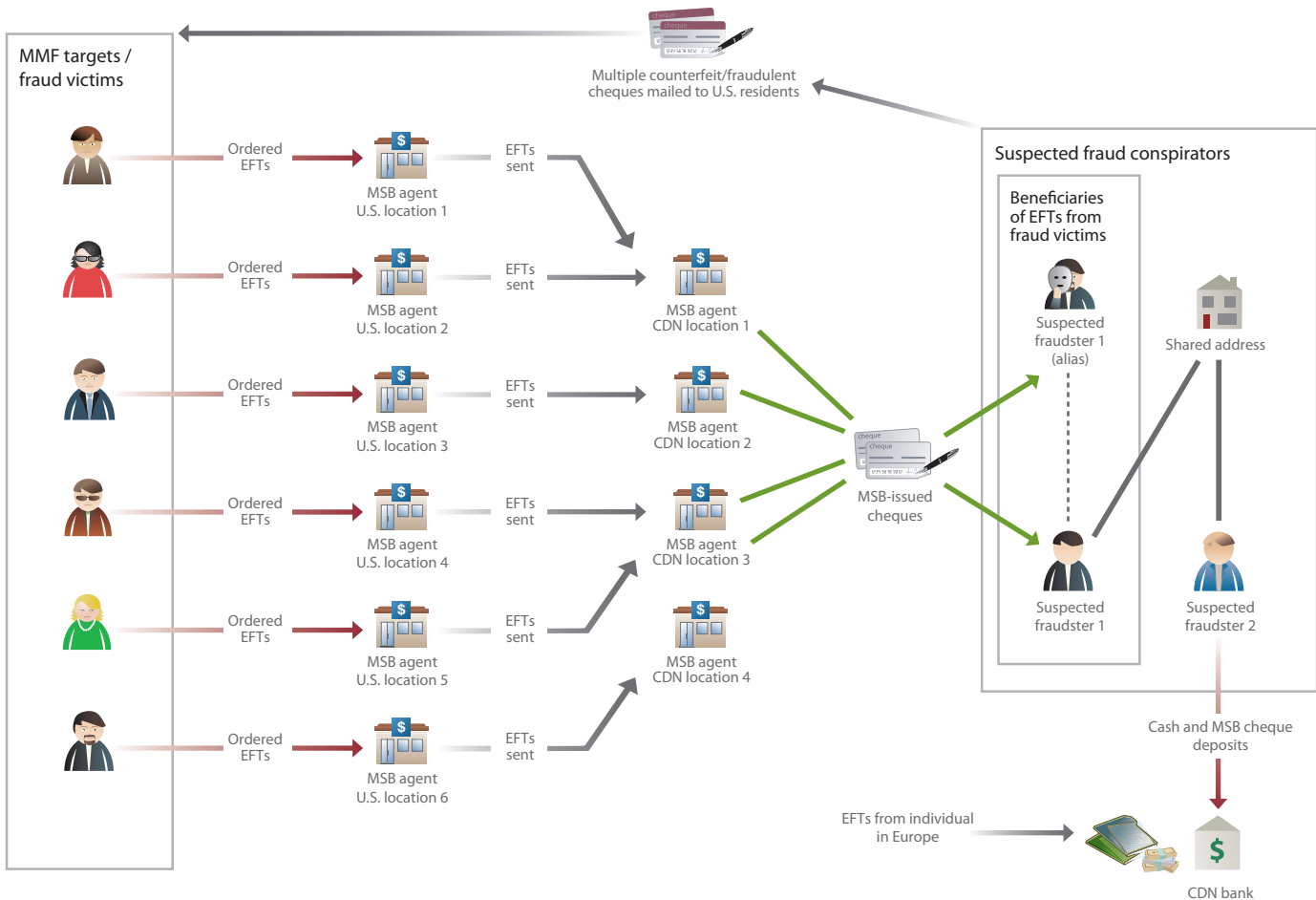
⁹ This particular example is drawn from sanitized case #3.

(C) Sanitized Cases and Red Flags

Case example # 1 Criminal dimension: Suspected laundering of mass marketing fraud (MMF) proceeds

MSB service highlighted: Use of electronic funds transfers (EFTs)¹⁰ by fraud victims to send funds to fraud perpetrators in Canada.

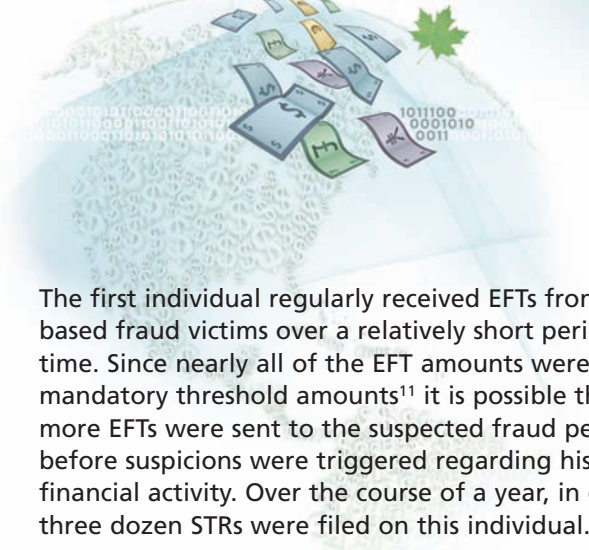
Sanitized case example: Suspected laundering of MMF proceeds



Law enforcement provided information on two individuals who were suspected of running a mass marketing fraud (MMF) scheme. In this scheme the perpetrators used MSBs to receive payments from fraud victims in the United States. Counterfeit cheques were sent to U.S. residents, who were then instructed to send a portion of these funds back to two individuals perpetrating the fraud.

One of the individuals, who appeared to use two different identities/aliases and various addresses, was the beneficiary of most of the EFTs sent through the MSBs. The other individual, sharing the same residential address (apparently never used when receiving the EFTs) with the first one, was suspected of being the mastermind of the scheme, as he/she had been convicted of a large number of fraud-related offences.

¹⁰ FINTRAC receives electronic funds transfers reports on orders of international wire transfers of CAD \$10,000 and more, which are referred to as "EFT's" in this report. It also receives information regarding domestic wire transfers, reported in suspicious transaction reports (STRs), which are referred to as "wire transfers" in this report.



The first individual regularly received EFTs from U.S.-based fraud victims over a relatively short period of time. Since nearly all of the EFT amounts were below mandatory threshold amounts¹¹ it is possible that many more EFTs were sent to the suspected fraud perpetrator before suspicions were triggered regarding his or her financial activity. Over the course of a year, in excess of three dozen STRs were filed on this individual.

The main EFT recipient (using two identities and eight different addresses) appeared to be using multiple MSB agents (close to twenty locations) in an attempt to conceal the fraudulent activity. Funds were paid out in cheques issued by the MSB. STRs filed by a bank indicate that this individual made a series of deposits into two different banks accounts, using cash and cheques.

The suspected mastermind of the scheme was also flagged in bank STRs for a series of multiple cash deposits and in relation to depositing MSB-issued cheques. The same individual also received Euro-denominated EFTs from Europe.

This case highlights how an MSB can be used as an important part of a mass marketing fraud scheme, where it was used to move funds from fraud victims to the suspected perpetrators. This case also underscores the importance of STRs filed by the MSB. Without the STRs the “below threshold” transactions would not have been captured by FINTRAC.

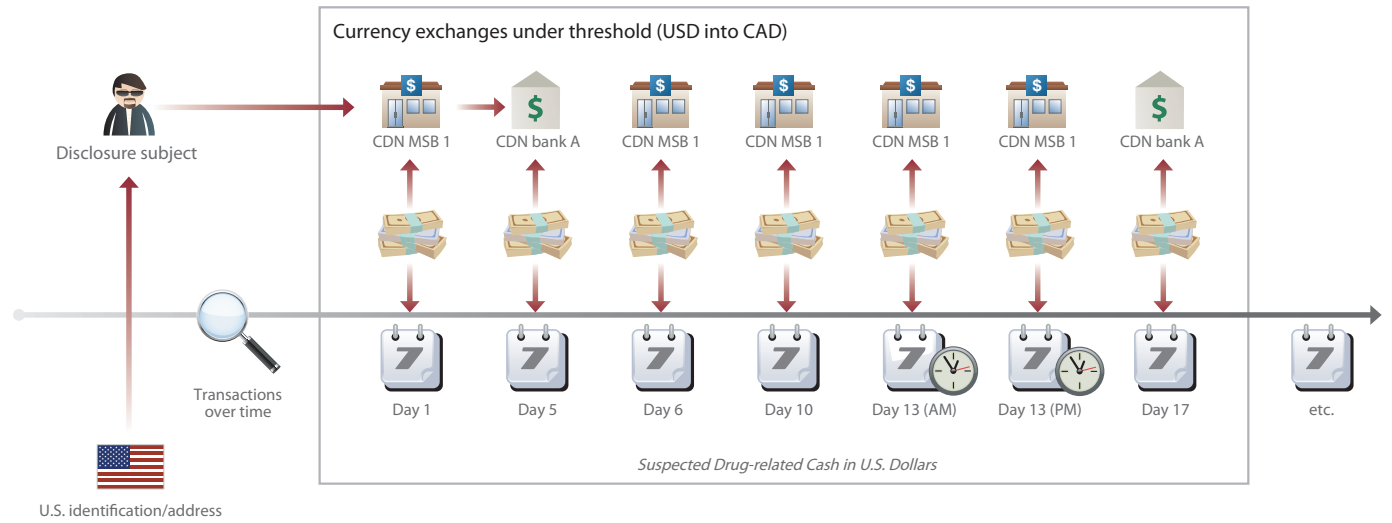
RED FLAGS associated with this case:

- Customer used multiple names/identities, in conjunction with providing multiple addresses, making it difficult to ascertain the true identity of the customer.
- The frequency of the customer’s visits was excessive, and also involved the use a wide range of MSB agent locations.
- The purpose of the transactions, and the relationship between the beneficiary and the ordering clients of the wires, does not appear to make business sense.

¹¹ Suspicious transaction reports (STRs) can be filed on any transaction regardless of the value of the transaction.

Case example # 2 Criminal dimension: Suspected laundering of drug proceeds
MSB service highlighted: Use of an MSB by a U.S. resident to exchange and refine suspected drug-related proceeds.

Sanitized case example: Suspected laundering of drug proceeds

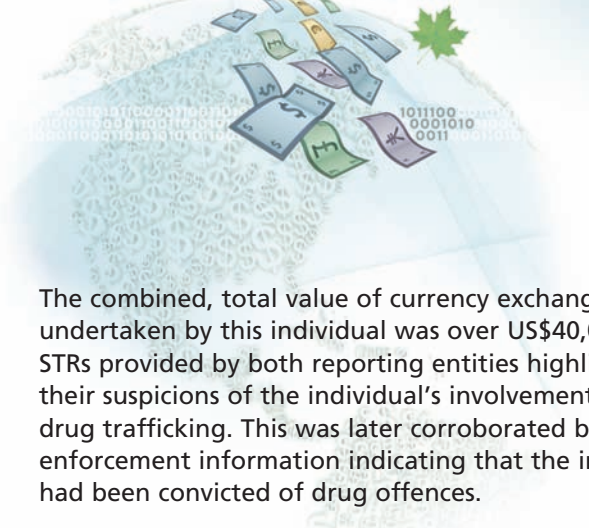


STR information provided by an MSB indicated that the disclosure subject used the currency exchange MSB as part of a regular pattern of financial activity consisting of converting and refining U.S.-denominated cash through a series of structured exchanges. In this particular case, covering a two month period, the disclosure subject regularly travelled over 70 miles from the U.S. to Canada to conduct the transactions. The individual concentrated his/her currency exchanges on one particular MSB, and a bank branch in the same Canadian town. Both the MSB and the bank filed STRs on the individual.

STRs filed by the MSB highlighted the high frequency of visits which occurred every two or three days and sometimes twice on the same day. The reports also

noted that the individual was a U.S. resident. In each case none of the disclosure subject's transactions exceeded \$10,000 which would have triggered a requirement to file a large cash transaction report (LCTR) with FINTRAC.

Bank STRs also flagged this individual as a U.S. resident, who had travelled to their branch to undertake several thousand dollars worth of U.S. to Canadian dollar exchanges in U.S. \$20 bills. The bank indicated that the individual did not have an account at the bank, that no explanation could be given for either the source of funds or for why the individual would travel from the United States to undertake these currency exchanges.



The combined, total value of currency exchanges undertaken by this individual was over US\$40,000. STRs provided by both reporting entities highlighted their suspicions of the individual's involvement in drug trafficking. This was later corroborated by law enforcement information indicating that the individual had been convicted of drug offences.

The STRs filed by the MSB provided information that allowed analysis of the disclosure subject's transaction activity over time which assisted FINTRAC's determination that there were reasonable grounds to suspect money laundering. This case highlights how an MSB can be used to facilitate the placement and layering of proceeds by converting suspected drug cash into a different currency. It also illustrates how an MSB can simultaneously be used to "refine" suspected drug proceeds.

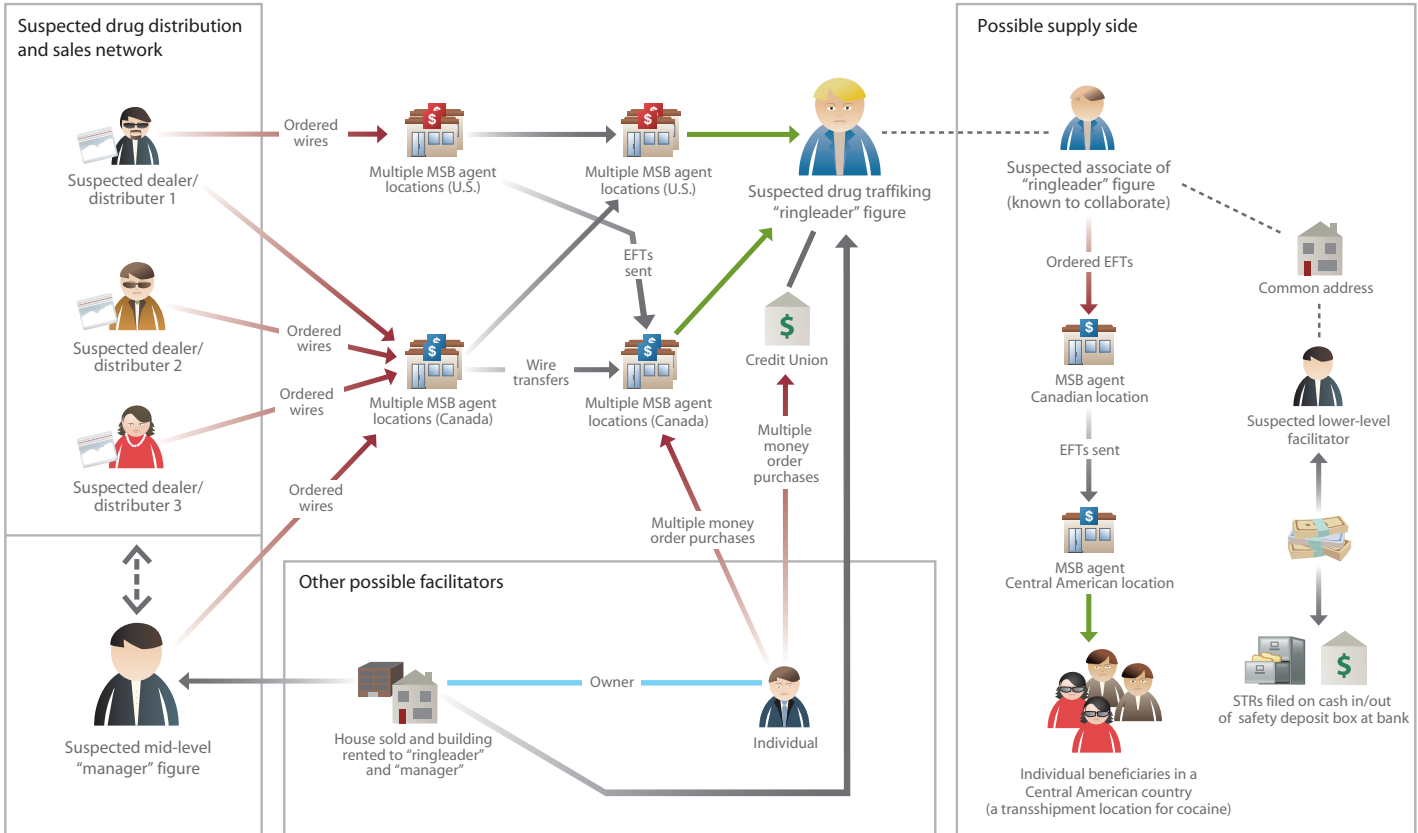
RED FLAGS associated with this case:

- The customer made frequent visits to conduct currency exchanges, sometimes two or three times in a given week, and sometimes in the same day.
- The client's ID indicated that the individual was a U.S. resident, but travelled a long distance to Canada to conduct transactions.
- The individual converted small denominations of U.S. cash into larger denominations of Canadian cash.
- All currency exchange transactions were below the \$10,000 threshold, presumably to avoid large cash transaction report (LCTR) requirements.

Case example # 3 Criminal dimension: Suspected laundering of drug proceeds

MSB service highlighted: Electronic funds transfer (EFT) services exploited by suspected drug dealers to send funds to the ringleader of a drug trafficking operation.

Sanitized case example: Suspected laundering of drug proceeds



This case was initiated following the receipt of law enforcement information about one senior suspected drug trafficking “ringleader” and three individual subordinates who acted as “middle-managers” between several drug suppliers, and also coordinated street-level drug sellers. According to law enforcement, the suspected ringleader, and his principal “middle-managers”, had long histories of criminal charges and convictions for drug trafficking and possession of the proceeds of crime.

Law enforcement suspected that the ringleader bought cocaine himself, or through his middle-managers. The “managers” then sold the cocaine themselves, and also dealt with other lower-level individuals as part of a “dial-a-dope” operation. Financial transactions for these individuals show that they used dozens of MSB locations/agents across a wide geographic area in North America, and sent over \$70,000 in drug proceeds to the suspected ringleader through hundreds of below threshold international EFTs and domestic wire transfers.

The ringleader also collected the proceeds at different agent locations, including one in a casino. Most of those involved in the trafficking operation reported employment at a restaurant or were on social assistance.

MSB STRs indicated that both the ringleader and the “middle-managers” were sending wires/EFTs at a very high frequency, were suspected of splitting transactions, were travelling across jurisdictions to different MSB agent locations to either send or receive wires/EFTs, and were consistently providing multiple names or different spelling to MSB agents.

Police information also identified an individual with suspected links to the ringleader. Financial transactions for this suspected associate showed that he/she sent thousands of dollars worth of international EFTs to a Central American country with a known history of being a transshipment point for cocaine trafficking – suggesting a possible connection to the supply side of the drug operations. Another individual who shared an address with the ringleader’s suspected associate was also flagged in bank STRs for suspicious financial activity related to the use of a safety deposit box, and to what appeared to be “refining” through small denomination cash deposits, followed by cash withdrawals.

STRs and law enforcement information also identified other suspected facilitators who were positioned to assist the ringleader with trafficking-related operations. One such suspected facilitator was reported in MSB and bank STRs as having purchased a number of non-sequential money orders, payable to himself/herself, and then deposited these into his/her account at a financial institution. This individual also apparently sold one property to the ringleader and a middle-manager figure, and also rented out another building to them as well.

This case highlights how MSBs can be used as a central part of the financial activity of a drug trafficking operation. In this case, MSB agents in a wide range of geographic locations were used by a group suspected drug traffickers to “repatriate” drug money back to an individual suspected to be the operation’s ringleader.

RED FLAGS associated with this case:

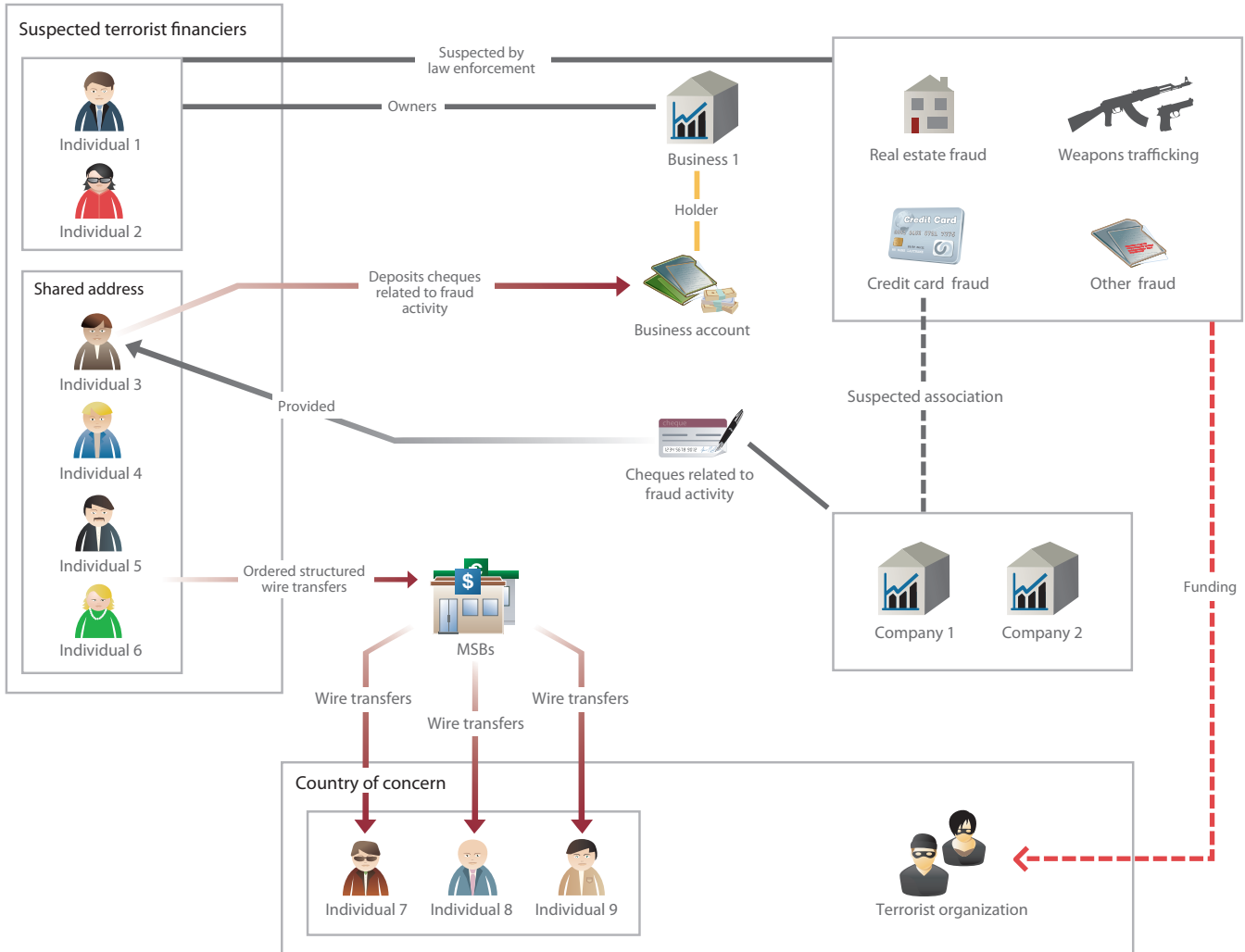
Some red flags in the case include:

- Clients appeared to split their transactions to avoid reporting requirements.
- The transaction frequency was high, combined with the use of multiple agent locations (sometimes on the same day).
- Subjects used various spellings of their names and/or misled reporting entities regarding their names.
- International electronic funds transfers (EFTs) were sent to a country which is frequently exploited by drug trafficking organizations (DTOs) for cocaine transshipment and money laundering purposes.
- The value of transactions did not appear to be commensurate with stated employment.

Case example # 4 Criminal dimension: Suspected terrorist financing

MSB service highlighted: MSB electronic funds transfer (EFT) services used by suspected terrorist financiers to send funds to a country of concern for terrorism.

Sanitized case example: Suspected terrorist financing



Law enforcement provided information on two individuals who were suspected of being involved in a variety of criminal activities such as weapons trafficking and various fraud schemes, including credit card and real estate fraud. It was also suspected that a portion of these criminal proceeds was for the benefit of a terrorist organization based overseas.

The two individuals owned a business which law enforcement suspected of being used as a vehicle for the proceeds of fraudulent activity. A financial institution advised FINTRAC of cheque deposits by a third individual to the business' account. The financial institution also reported that the cheques were issued by two companies suspected of being associated to the aforementioned credit card fraud scheme.

Based on STRs provided by MSBs, FINTRAC determined that the newly identified individual provided the same address as three other people. The STRs also revealed that wire transfers were ordered by all of these individuals for the benefit of individuals in the country where the terrorist organization is based. The wires were conducted in concentrated bursts over a two year period, with each burst consisting of a series of wires which were generally structured below mandatory reporting thresholds, and conducted within days of each other. FINTRAC also received STRs from another MSB describing the same pattern of activity and suggesting that some of these individuals were providing multiple dates of birth and address information, and similar sounding name variations.

This case highlights how individuals who were suspected of providing funds to a listed terrorist organization used an MSB to transfer funds, a portion of which was believed to be derived from fraud schemes. Given that the wire transfers in this case were below the mandatory reporting threshold, this case also underscores the importance of STRs filed by the MSBs.

RED FLAGS associated with this case:

- Multiple senders shared common address information.
- Multiple senders sent funds to the same beneficiary in a country of specific concern for terrorism.
- Senders conducted structured transactions within days of each other.
- At least one individual involved in this case used multiple dates of birth (DOB), ID, and addresses to MSBs.

THE IMPORTANCE OF SUSPICIOUS TRANSACTION REPORTING

Suspicious transactions are financial transactions that occur in the course of the activities of a reporting entity, and about which the reporting entity has reasonable grounds to suspect are related to the commission of a money laundering or terrorist financing offence. The filing of STRs by reporting entities links the private sector with broader governmental and law enforcement efforts to detect, deter, and disrupt criminal activities which threaten the integrity of Canada's financial system, and which also underpin threats to Canada's public safety and national security.

A suspicious transaction report (STR) or an attempted suspicious transaction report (STR-A) should be filed whenever a reporting entity has reasonable grounds to suspect that the person(s)/entity undertaking a transaction activity appears to have the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated criminal offence, including drug trafficking, fraud, terrorist financing, robbery, counterfeit money, stock manipulation, bribery, forgery, murder, etc. STR requirements include an obligation to take reasonable measures to identify the person(s) involved in the transaction, and apply not only when the financial transaction has been completed, but also to attempted suspicious transactions. Suspicious transaction reports (STRs) and attempted suspicious transaction reports (STR-A) are fundamentally important to Canada's anti-money laundering (AML) / countering terrorist financing (CTF) regime.

3. OTHER ANTI-MONEY LAUNDERING (AML) / COMBATING THE FINANCING OF TERRORISM (CFT) CONCERNS

(A) Risks to Registered MSBs from Unregistered Remittance Businesses

For the purposes of this section, an “unregistered remittance business” is any entity which is engaged in the business of a money services business but which is not registered with FINTRAC¹². The operators of unregistered remittance businesses may come in contact with the formal financial system through a number of ways, including through the banking sector and/or registered MSBs in order to meet the needs of their clients to get funds to a final beneficiary. The most common point of contact between an unregistered remittance business and formal sectors lies in the bilateral or multilateral process of financial settlement of debts with other dealers / operators incurred as a result of the trust-based transactions common to these remittance systems.

Reporting entities (REs), including registered MSBs, may be exposed to risks associated with unregistered remittance operators when (for example):

- The operator of an unregistered remittance business (outside of Canada) seeks to use a registered MSB or other RE to wire funds directly to their counterpart in the country/place where the beneficiary resides; or when

- Multiple operators of unregistered remittance businesses settle their transaction accounts by using multilateral financial settlements, possibly using a money transfer service to deliver funds to an intermediary country, and then further transferring the funds to the (recipient) country in order to settle the outstanding debt.

Examples of unregistered remittance business can include, *but are not limited to*, unregistered alternative remittance systems (ARS) such as hawala, hundi, undiyal, fei ch’ien, chitti, or other informal value transfer systems (IVTS).¹³ For a variety of socio-cultural and economic reasons, ARS are pervasive in many parts of the world. ARS provides a cost-effective means of moving money—particularly in those parts of the world which have little or no formal banking infrastructure. Because ARS usually operate on the basis of trust between remitters (and intermediaries acting on their behalf), they are able to persist outside of normal financial system regulatory controls, and may not record clients and transactions in the way that registered MSBs do (insofar as registered MSBs are required to submit certain categories of information to the government which might not be required in the ARS operation). As useful as ARS may be to a wide variety of financial services consumers, a number of jurisdictions and international bodies have identified ML/TF risks linked to the possibility of anonymity which ARS can provide, and in relation to risks associated with the lack of record-keeping and absence of report filing.^{14,15,16,17,18}

Canada’s AML/CFT regime relies on adequate and appropriate coverage of those financial sectors which may be used by money launderers and terrorists. In this context, unregistered remittance businesses continue to be a concern for FINTRAC because such businesses do not submit mandatory transaction reporting and create opportunities for anonymity within the financial system.

12 For additional information on MSB registration refer to the FINTRAC Web site at: <http://www.fintrac-canafe.gc.ca/publications/general/05-2010/1-eng.asp>

13 It is important to note that ARS is not “illegal” in Canada; the question of legality hinges on whether or not an ARS operator is registered with FINTRAC. In Canada it is illegal to engage in the business of remitting or transmitting funds, exchanging currency, or issuing or redeeming negotiable instruments without registering as a money services business (MSB) with FINTRAC. Nothing precludes an ARS from being a registered MSB; it would however need to adjust its business operations to satisfy the conditions of the PCMLTFA and associated regulations.

14 International Monetary Fund (IMF), *Approaches to a Regulatory Framework for Formal and Informal Remittance Systems: Experiences and Lessons*, 2005.

15 Financial Action Task Force (FATF), *Money Laundering and Terrorist Financing Typologies 2004-2005*, 2005.

16 INTERPOL, *Alternative remittance systems distinguishing sub-systems of ethnic money laundering in INTERPOL member countries on the Asian continent*, 2007.

17 A full list of ML/TF indicators relevant to the MSB sector is available through the FATF’s typology work. Refer to the *FATF Working Group on Typologies: Money Laundering through Money Services Businesses (MSBs)*.

18 World Bank, *Alternative Remittance Systems and Terrorist Financing: Issues in Risk Financing*, 2010.

These issues could create AML/CFT vulnerabilities and also create investigative obstacles. Unregistered remittance businesses should also be a concern for the MSB sector in that these operations can create reputational risks for registered MSBs and other financial institutions which may ultimately be used (knowingly or not) as settlement mechanisms for an unregistered remitter who could potentially be facilitating illicit financial activity.

(B) Emerging Issues to Monitor in the Canadian MSB Sector: Merging of Traditional and New Payment Methods

New payment methods (NPMs) such as prepaid cards¹⁹ and Internet payment services²⁰ started to emerge in the 1990s, while mobile payment services²¹ have been introduced more recently. In comparison to more traditional “online banking” or “phone banking” services, customers of NPM services generally do not access their individual bank accounts but instead keep an account with the (generally non-bank) NPM service provider.

Many NPMs are now well-established payment systems although their relative market success varies greatly. Some well-known service providers are operating successfully across the globe, while others are restricted to domestic business and yet others are still waiting for relevant market acceptance and success. Three types of NPMs, prepaid cards being the most common, are currently offered in Canada.

One of the newest developments is the convergence and combination of different types of NPMs (e.g. mobile payment services introducing prepaid cards for their customers) and/or the combination of NPMs with traditional payment methods (e.g. mobile payments that cooperate with MSBs).

To date, MSBs have offered prepaid cards and also, in some instances, Internet payment services. However, some MSBs have recently started to consider the possibility of providing their customers with the option of transferring and receiving funds to/from mobile payment services’ account holders. This development is significant since international funds transfers through mobile payment services will now be possible, while before they were mostly, if not only, offered domestically.

Because a number of MSBs provide NPM services, or are considering the possibility of offering such services, this report provides a high level overview of some of the risks associated with these NPMs which reporting entities should consider. Three main risks are common to all three types of NPMs:

- Many NPMs work on a prepaid basis. That is, the customer can never spend funds in excess of what has been previously paid into his/her account held by the NPM service provider. These accounts can sometimes be funded anonymously or by a third party, making ML/TF risks higher since appropriate customer due diligence (CDD) are not undertaken.
- The various business models used to support or deliver NPM services help people to withdraw and/or convert funds more quickly than through traditional channels, including international transactions in real-time. These factors can complicate monitoring as well as making it difficult for authorities to follow the money trail.
- All Internet payment services and many prepaid cards are distributed through the Internet, making the establishment of a customer relationship on a non-face-to-face basis difficult if not impossible. This poses additional challenges for the providers’ verification procedures, increasing the risk of customers remaining unidentified or using false/stolen identities.

¹⁹ These refer to open-loop prepaid cards that are issued by banks but sometimes distributed and managed by third parties such as MSBs. These cards are usually re-loadable and can be anonymous.

²⁰ Internet payment services (IPS) offered in Canada include 1) payment processing providers allowing merchants to authorize, settle and manage transactions from websites; and 2) account-based service providers allowing users to accept electronic payments and make person-to-person funds transfers. FATF has issued some guidance with respect to ML/TF vulnerabilities associated with IPS: <http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf>

²¹ This refers to mobile payment services offered by telecommunications companies and which involved the opening of an account with the latter and funding the account through various means (e.g. bank transfers, credit cards). Person-to-person funds transfers are then possible between account holders with the same telecommunications company and are usually conducted through text messaging (SMS technology).

In recent years, FINTRAC has observed the use of Internet payment services and prepaid cards in a limited number of case disclosures (e.g. 4% of all cases disclosed in 2008-2009 involved Internet payment services). The low number of cases may be due to the lack of awareness of the reporting entities, to the low usage to date of NPMs by money launderers and terrorist financiers, or to successful evasion of authorities. It may also be due to the fact that NPMs are still a new phenomenon and are not yet familiar to potential criminals and terrorist financiers.

MSBs may consider offering NPM services for a variety of reasons, including capitalizing on lower overhead costs, increased speed and efficiency of transactions, and in order to expand market coverage. While the business logic behind offering NPMs is sound, MSBs are reminded of their obligation under the PCMLTFA to take into account the associated money laundering and/or terrorist financing risks and put in place appropriate mitigation strategies when they deem these risks to be high. These measures should include taking reasonable measures with respect to keeping client identification up to date and to conducting ongoing monitoring to detect suspicious transactions.

FINTRAC is currently participating in a FATF typology project that focuses on the risks associated with NPMs and that will present a number of case studies highlighting how these payment methods have been used for ML/TF purposes. FINTRAC anticipates that the FATF will publish a public report on this work later in 2010.

4. CONCLUSION

Criminals will continue to employ many of the money laundering and terrorist financing methods and techniques described in this report for as long as they believe they can be successful in doing so, and FINTRAC is aware that many of these issues are already familiar challenges faced by MSB operators.

Although this report has focused on money laundering and terrorist financing activity in Canadian MSBs, often the overall money laundering process includes transactions in more than one sector. FINTRAC is aware that this issue is a challenge for every sector, and realizes that both small MSB operators and large corporate franchised MSBs are only privy to those transactions which they themselves process. It is in this context that the Centre believes that this Trends and Typologies Report supports a much larger need for greater AML/CFT focus across all sectors.

The Centre believes that Canadian MSBs can make a real difference in the fight against money laundering and terrorist financing, and looks forward to continued collaboration with the MSB sector and other financial entities in order to detect, deter, and disrupt money laundering and terrorist financing activities. Not only does money laundering and terrorist financing threaten the integrity of Canada's financial system, but these activities are fundamentally at odds with Canadian values and interests, and pose serious risks to the safety, security, and prosperity of all Canadians.

ANNEX 1

FATF ML/TF Indicators Relevant to the MSB Sector²²

In addition to the ML/TF techniques, red flags, and sanitized cases already provided in this report, FINTRAC has also included a summarized set of internationally recognized indicators of possible ML/TF through MSBs which FINTRAC has observed in cases and/or which the Centre believes are relevant to the Canadian context. These include:

INDICATORS FOR MSB MONEY REMITTERS / TRANSMISSION SERVICE LINES

- Unusually large cash purchase(s) of EFT(s) in circumstances where payment would normally be made by cheque, banker's draft, etc;
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings;
- High volume of transactions over a short period of time;
- The lack of apparent relationship between the sender and beneficiary, and/or personal remittances sent to jurisdictions that have no apparent family or business link to conductor, and/or the conductor has no relation to country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there;
- The customer only seems to know which amount is being transferred after the MSB employee has counted the cash and/or the customer shows no interest in the transfer costs;
- Large amounts are transferred to companies abroad with a service provider address;
- Multiple senders transferring funds to a single individual; and
- Money is received by the same individual from different money remittance companies or MSB agent locations.

INDICATORS FOR MSB FOREIGN EXCHANGE / BUREAUX DE CHANGE SERVICE LINES

- Exchange of large quantities of low denomination notes for higher denomination ones;
- Large or frequent exchanges that are not related to the customer's business;
- Fragmentation of large amounts and high frequency of currency exchange transactions over a short period of time;
- The same person uses multiple FOREX/bureau de changes;
- Repeated requests for foreign exchange purchasing/selling in amounts slightly less than the transaction limit for identification;
- The customer buys currency that does not fit with what is known about the customer's destination or the customer buys currency from an unusual location in comparison to his/her own location; and
- The customer apparently does not know the exact amount being exchanged, the customer does not watch the counting of money, and/or the customer is happy with a poor rate.

INDICATORS FOR MSBs REGARDING CASH TRANSACTION

- Unusually large cash payments in circumstances where payment would normally be made by cheque, banker's draft, etc;
- Cash is in "used notes" and/or small denominations ("used notes" may imply that notes are worn, dirty, stained, give off unusual smell, etc.);
- Customer refuses to disclose the source of cash;
- Customer has made an unusual request for collection or delivery;
- Significant discrepancy between customer's declaration of cash total and counted total;
- Presence of counterfeit banknotes in the bankroll; and
- Cash transactions followed closely by transfer of funds on the same or next day.

²² A full listing of ML/TF indicators relevant to the MSB sector is available through the FATF's typology work. Refer to the *FATF Working Group on Typologies: Money Laundering through Money Services Businesses (MSBs)*.

ANNEX 2

Money Laundering and Terrorist Financing in Canada for ALL Sectors: Review of 2008-2009 FINTRAC Case Disclosures

For this report, FINTRAC conducted an extensive review and analysis of all cases disclosed over the fiscal year 2008-2009 (April 2008 to March 2009).²³ The methodology for the case review involved a complete examination of all cases with a focus on key characteristics within each FINTRAC case disclosure.²⁴ For the purposes of this document, the general observations included in this report emphasize the following characteristics:

- types of case/activities;
- most common criminal offence types²⁵ associated with observed ML/TF;
- sectors and services used for various activities associated to ML/TF;
- most common ML/TF stages and techniques used; and
- the most common types of businesses used in ML/TF schemes.

(A) GENERAL OBSERVATIONS – ALL SECTORS

FINTRAC uses a wide variety of information inputs to initiate its case disclosures, including proactive disclosure based on a pattern of financial activity, information in a reported financial transaction, or

based on suspicious transaction reports (STRs)²⁶ sent to FINTRAC by a reporting entity. Cases may also be initiated based on information volunteered to FINTRAC by law enforcement, other government agencies, or the general public. In all instances FINTRAC must reach a legislated threshold of reasonable grounds to suspect ML/TF before it can disclose designated information to authorized recipients.

Types of Suspected Activities and Designated Offences:

In 2008-2009, FINTRAC disclosed a total of 556 cases, divided in the following ways:

- 474 cases associated with money laundering;
- 30 cases associated with money laundering, terrorist financing and threats to national security;
- 52 cases associated with terrorist financing and threats to national security;
- 197 of the total number of case disclosures involved transactions through the MSB sector;
- Where FINTRAC was able to link suspected ML/TF activity to a designated criminal offence, fraud and drug-related activity were the most frequently observed suspected offences;
- In cases where drug-related activity was suspected, the majority of cases involved the trafficking of cocaine and/or marijuana; and
- In cases where fraud was suspected, investment/securities and telemarketing fraud (or other mass marketing fraud [MMF]) were the most observed.

23 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.

24 For clarification, a FINTRAC case disclosure contains what is referred to as “designated information” that is prescribed by the PCMLTFA. Designated information includes key identifying information about each person or entity about whom FINTRAC has reasonable grounds to suspect ML or TF (e.g. name, address, bank account numbers, etc.). In the interests of space the full description of designated information is not included in this report. The full description of designated information can be found in subsection 55(7) and 55.1(3) of the PCMLTFA.

25 For the purposes of this report “common criminal offence types” refers to “designated offences” as that is defined under 462.3(1) of the Criminal Code of Canada.

26 Reporting entities listed under the PCMLTFA are required to file suspicious transaction reports (STRs) and suspicious attempted transaction reports (STR-As).

(B) COMMON PHASES AND TECHNIQUES OF MONEY LAUNDERING

Money Laundering	Terrorist Financing
<p>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.</p> <p>There are three widely recognized stages in the money laundering process:</p> <p>Placement involves placing the proceeds of crime in the financial system.</p> <p>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.</p> <p>Integration involves placing the laundered proceeds back in the economy to create the perception of legitimacy.</p>	<p>Terrorist financing refers to the direct or indirect furnishing of financial support to an individual, group, entity, state, or agents 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.</p> <p>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. Also constitutes a threat to the security of Canada as that is defined under section 2 of the <i>Canadian Security Intelligence Service Act (CSIS)</i>.</p>

The most common phases of ML/TF appearing in FINTRAC case disclosures for 2008-2009 were the “placement” and “layering” of the proceeds of crime, and the most common ML/TF techniques observed were “structuring” and “smurfing.”

“Structuring” normally involves multiple cash deposits at amounts below the reporting threshold and “smurfing” is defined as multiple deposits of cash, and/or low-value monetary instruments, typically purchased from banks or money services businesses, by various individuals.

Using “nominees” is also a feature of some ML/TF cases. A “nominee” is an individual or business that acts on the behalf of a third party in an attempt to conceal the third party’s involvement in a particular transaction or in relation to the

beneficial ownership of property. The use of nominees was found to be involved in 15% of all cases disclosed in 2008-2009, a significant increase in comparison to approximately 4% of cases disclosed in 2007-2008.

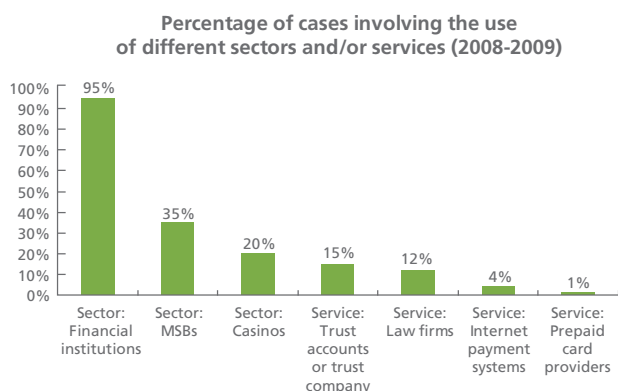
(C) SECTORS AND SERVICES USED

In 2008-2009, as with previous years, financial institutions (including banks, credit unions, cooperatives, and caisses populaires), were the major contributors of reports²⁷ received by FINTRAC. Consequently, the majority of financial transactions in cases disclosed to law enforcement and intelligence agencies were conducted through financial institutions.

27 The main report types submitted to FINTRAC by reporting entities (REs) include suspicious transaction reports (STRs), suspicious attempted transaction reports (STR-As), large cash transaction reports (LCTRs) and electronic funds transfer reports (EFTRs).

While financial institutions, MSBs, and casinos are considered to be reporting entity “sectors” by FINTRAC, a number of “services”²⁸ were also noted as having been used in disclosures for 2008-2009. These services included the use of trust accounts (offered by trust companies or law firms) where these services were used to conduct financial transactions, but to a much lesser extent than the services offered by the reporting entity sectors.²⁹ These transactions were mostly related to suspected drug offences and also to suspected fraud, organized crime activities and terrorist financing. Trust accounts or trust companies were involved in at least 80 FINTRAC case disclosures.

The following chart represents the use of various sectors for ML/TF purposes in 2008-2009, and also notes the instances where certain “services” were also observed in case disclosures:



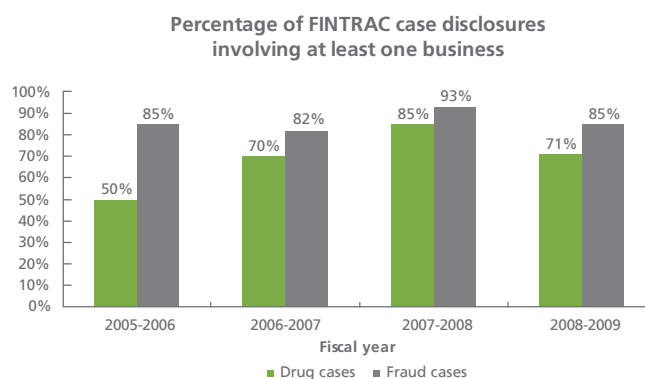
(N.B. “Services” should not be mistaken for “sectors”; A “sector” denotes a collection of reporting entities (REs) which are listed as such under the PCMLTFA.)

It should also be noted that certain ML/TF schemes can involve the use of multiple sectors and/or services at the same time. For example, in 33% of all 2008-2009 cases, financial transactions were conducted through both financial institutions and MSBs. Similarly, 17% of 2008-2009 cases contained financial transactions conducted through both financial institutions and casinos. Finally, 6% of all cases involved financial transactions conducted

through all three sectors (i.e. financial institutions, MSBs and casinos).

(D) TYPES OF BUSINESSES INVOLVED

Case disclosures often involved business entities in addition to transaction information for individuals. In 2008-2009, over 70% of cases suspected to be related to drugs or fraud involved at least one business in addition to individuals, and in many instances, involved multiple businesses.



Sixty percent (60%) of cases associated with terrorist financing were found to involve at least one business, and approximately 25% involved the use of non-profit organizations (NPOs).

The following types of businesses were found to be associated with all categories of cases³⁰, that is to say that they were suspected of being involved in ML/TF, or were used to facilitate such activities:

- import/export (e.g. food, clothing, medical supplies);
- financial services;
- real estate;
- transportation (e.g. trucking, air, taxi);
- car sales/rentals/repairs;
- convenience stores;
- electronics/computer sales;
- oil and gas (e.g. gas stations, petroleum providers); and
- non-profit organizations.

28 It is important to note that these “services” are distinct from “reporting entity sectors” and are not (under most circumstances) covered by the regime as such.

29 As noted in relation to reporting entity sectors, “services” (as they are described in this report) are not necessarily covered as such under existing legislation/regulation. Indications of the use of these “services” in cases may be related to third-party information provided to the Centre, and is the reason why a lower volume of reports would be expected. That being noted, these statistics are not necessarily an indication that these “services” are more or less vulnerable to money laundering or terrorist financing than reporting entity sectors.

30 Note that this does not mean these businesses were found in each individual case.

Other types of businesses were found to be associated with both fraud and drugs/organized crime cases. These were identified as (in no particular order):

- Investment/securities;
- Business management and marketing;
- Construction/renovation/landscaping;
- Precious metals;
- Mining development or exploration;
- Food and entertainment;
- Beauty salons;
- Retail;
- Internet payment systems; and
- Travel agencies.

The following table identifies additional types of businesses that were specifically associated to particular types of cases:

Drug cases/ organized crime	Fraud	Terrorist financing
Farms/ hydroponics/ indoor gardening	Life insurance	Long distance prepaid phone cards
Real estate/ land development	Technology (e.g. aviation)	
Jewellery	Medical supplies	
White-label ATMs		

