Anti-Money Laundering in the Financial Services Industry
Anti-Money Laundering in the
Financial Services Industry

Contents

Chapter 1 Common Acronyms of Money Laundering............................................................. 1
Chapter 2 Background ............................................................................................................. 3
Chapter 3 The Hidden Costs of Money Laundering ............................................................... 7
Chapter 4 The Historical and Cultural Perspective ............................................................... 9
  Case Study: BCCI.................................................................................................................. 10
Chapter 5 Stages of Money Laundering................................................................................ 11
  Placement ....................................................................................................................... 12
  Layering ....................................................................................................................... 12
  Integration ................................................................................................................... 13
  Tax Havens of the World ............................................................................................. 13
Chapter 6 Methods of Money Laundering .......................................................................... 15
  Underground Banking ................................................................................................... 15
  Commodities and the Futures Market ............................................................................ 16
  Black Market Peso Exchange (BMPE) ............................................................................ 16
  Structuring of Funds (also Called Smurfing) ................................................................... 17
  Nominees .................................................................................................................... 17
  Securities ..................................................................................................................... 17
  Insiders ....................................................................................................................... 17
  Credit, Charge, and Debit Cards ................................................................................... 18
    Institutional Use ....................................................................................................... 18
    Personal Use .......................................................................................................... 18
  Real Estate .................................................................................................................. 18
  Life Insurance ............................................................................................................ 18
  Gambling ..................................................................................................................... 19
  Currency Smuggling .................................................................................................... 19
  Exchange Transactions ............................................................................................... 19
  Large Cash Purchase .................................................................................................. 19
Chapter 7 The Effects of Money Laundering ...................................................................... 21

Chapter 8 Terrorist Financing ............................................................................................. 23
  How Funds Are Raised ............................................................................................... 23
  Financial Operations ................................................................................................. 23
  Reactions and Responses to Terrorist Financing ......................................................... 24
  Recognizing Terrorist Activity .................................................................................... 25

Chapter 9 Catching the Crooks: The Macro Approach (International) ......................... 27
  International Efforts ................................................................................................... 28
  United States ............................................................................................................. 30
  United Kingdom ....................................................................................................... 30
## Chapter 10 Catching the Crooks: The Macro Approach (Canada) ........................................... 33
- Legislated Requirements ...................................................................................................................... 36
- Reporting ............................................................................................................................................... 36
- Ascertaining Identity ................................................................................................................................. 44
- Record-Keeping Requirements .............................................................................................................. 47
- The Compliance Regime ......................................................................................................................... 47
- Penalties for Non-Compliance ................................................................................................................. 51

## Chapter 11 Reporting Requirements and PIPEDA ............................................................................. 55

## Chapter 12 Catching the Crooks: The Micro Approach (Taking Personal Responsibility) ............. 57
- Education .................................................................................................................................................. 57
- Volunteering Information .......................................................................................................................... 58
- “Know” Directives .................................................................................................................................... 58
- Whistleblowing ......................................................................................................................................... 58
  - Whistleblowing and the Employee ............................................................................................................ 59
  - Whistleblowing and the Employer ........................................................................................................... 59
  - When to Blow the Whistle ....................................................................................................................... 60
  - Whistleblowing and Money Laundering .................................................................................................... 60

## Chapter 13 Keeping Paranoia in Check ............................................................................................... 61
- Common Sense Steps to Deter Money Laundering .................................................................................. 61

## Chapter 14 Money-Laundering Red Flags ....................................................................................... 63

## Appendix A ............................................................................................................................................ 65
- References ............................................................................................................................................... 65
Chapter 1
Common Acronyms of Money Laundering

CSIS—Canadian Security Intelligence Service
CRA—Canada Revenue Agency
EFT—Electronic funds transfer
FATF—Financial Action Task Force
FINTRAC—Financial Transactions and Reports Analysis Centre of Canada
FIUs—Financial Intelligence Units
FRPS—FINTRAC’s Report Preparation Software
LCTR—Large Cash Transaction report
OSFI—Office of the Superintendent of Financial Institutions
PATRIOT Act—Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.)
PCMLTFA—Proceeds of Crime (Money Laundering) and Terrorist Financing Act (Canada)
PIPEDA—Personal Information Protection and Electronic Documents Act (Canada)
SWIFT—Society for Worldwide Interbank Financial Telecommunication
Anti-Money Laundering in the Financial Services Industry
Chapter 2
Background

- Money laundering is said to the third-largest business in the world; it was estimated that, in 1996, between US$590 billion and US$1.5 trillion of funds were laundered annually.
- The International Monetary Fund estimates that laundered funds account for between 2 and 5% of the gross domestic product of the world.
- The true scale of the activity is not known and cannot be accurately measured, by virtue of the fact that no one can estimate the amount of money generated illegally.
- However, it is certain that money laundering is proliferating, not just as a result of an ever-increasing amount of criminal activity, but because the Internet and electronic banking have provided a more sophisticated and circuitous means to convert laundered funds into legal tender and assets.
- There is widespread knowledge of money laundering occurring throughout the financial services industry, including banking, securities, money service businesses, and life insurance. But the activity is far more pervasive than in financial services; money laundering has an impact on the global economy through many sectors of business activity, including the travel industry, automobile retailers, boat and yacht retailers, dealers in luxury goods, art, and antiques, and the real-estate industry.
- In Canada and the United States, legislation addresses money laundering and terrorist activities jointly; in this book, the focus will be on money-laundering activities since it is frequently money laundering that provides terrorists with the funding to undertake terrorist attacks.
- Money laundering can also be defined in different ways: it can mean the actual process of moving the proceeds of crime into the financial system or, more broadly, as almost any use of criminal profits.
- The actual transactions used to legalize the proceeds of crime are both legal and commonplace; they include making bank deposits, wiring funds, and exchanging currency.
There are four classes of money launderer:
- the criminal whose activity produces the dirty money;
- those who assist in the legitimization of the money;
- those who enjoy assets derived from the proceeds of crime;
- those who help to create the money-laundering schemes.

Money that is laundered is considered “dirty,” because it is the product of criminal conduct, and hence is identified as the proceeds of crime. Most crime is economic crime, that is a crime committed in order to make money.

It is criminals who create the need for money laundering, because a large quantity of cash, in and of itself, is worthless. It has value only when it appears to be legitimate and becomes an asset of the criminal who “earned” the funds in the first place.

Money made from criminal activity is used either to invest in another crime, to hide for use at a later time, or to be spent now.

The criminal activity most responsible for generating dirty money is the drug trade. Street sales of drugs typically produce cash in small-denomination bills.

The amount of cash retained by the person selling the drugs will not be significant, but the amount of cash funnelled up the chain of command becomes increasingly larger.

Those at the top of the business have been known to have so much cash that they will bury it in caches in an effort to hide it.

Such cash must be integrated into the economy to become legitimate. The numerous $50, $20, and $10 bills from “the street,” or produced by counterfeiting must be converted into cheques, money orders, or wire transfers in larger sums from legitimate sources – banks, financial services companies such as brokers and life insurers – that represent the sum totals of the bills. Thus, “dirty” money is laundered, becomes “clean,” and is above suspicion.

Money launderers expect that some portion of their proceeds will be lost to them in the process of laundering; this is their cost of business. Thus, for instance, they will sacrifice an insurance policy for less than its cost of acquisition in order to obtain the cheque from the insurance company that can be deposited elsewhere without raising suspicion.

Not all proceeds of crime are laundered. Much is retained as cash by the criminal or held in bank accounts, with no attempt made to disguise the origin of the funds.

Anyone who helps a person launder money – despite the fact that they may not be directly involved in the underlying criminal activity – is a money launderer.

Therefore, bankers, lawyers, accountants, car dealers, and life agents are money launderers if they either use their business to help someone legitimize money earned as proceeds of a crime or provide expertise to such a person.

Professionals may claim that they were unaware of their laundering activities and that their money laundering was inadvertent. However, in a trial, this defence requires that a negative event be proven (“I did not launder money”), which can be highly prejudicial in front of a jury.
Those who enjoy the assets of the proceeds of crime are often the wives or girlfriends of the criminals, who know or suspect that proceeds of crime are used to fund their lifestyle, including homes, cars, and jewellery.

Finally, the person who creates the money-laundering process – such as an accountant versed in audit trails and international finance – is also guilty of money laundering.

Drugs are not the only source of dirty money. Other criminal activities that will generate funds for money laundering include:
  o prostitution;
  o fraud;
  o counterfeit goods;
  o tax evasion;
  o financial crime, such as cheque fraud, internet crime, and credit card fraud;
  o extortion;
  o theft, including auto theft;
  o smuggling.

It is also alleged that some countries, such as Russia and other Eastern European nations, are heavily engaged in laundering money that has been stolen from aid money donated by First World countries and from International Monetary Fund loans.

Such funds diverted from Russia have totalled as much as US$15 billion in an 18-month period.

Money laundering is not concerned solely with the conversion of cash (bills and coins) into legitimate channels; often, criminal financial activity does not result in actual cash because there is no physical representation of the crime. The money exists in virtual space as bits and bytes of computer memory.

The advent of online finance has meant that criminal laws that once addressed the physical holding of stolen goods no longer apply and that laws must be restated to make virtual financial crime just as risky as the actual possession of stolen goods.
Chapter 3
The Hidden Costs of Money Laundering

- In addition to the societal costs of criminal activity, financial crime affects everyone.
- It increases the cost of living by:
  - increasing taxes for those who do not evade their tax responsibilities;
  - increasing the cost of doing business, because businesses must cover the cost of fraud and theft, which in turn is passed along as higher prices to consumers;
  - increasing insurance-policy premiums because of fraudulent claims and valid claims by victims of terrorist attacks;
  - increasing security costs for governments and companies that must institute measures to prevent money laundering and terrorism. These costs are also passed along to citizens and consumers in the form of taxes (e.g., the airport security tax) and higher costs for goods and services.
- Honest businesses are impeded, because they cannot compete fairly against those that derive some of their income from money laundering.
- Further, the risk of shopping in person or on the Internet is increased, because the shopper may be buying from a vendor engaged in criminal activity via credit card, bank card, or cheque fraud.
- Money that has inadvertently been paid to criminals may be used for trading in arms, nuclear weapons, human organs, or people, in addition to funding crimes of terrorism.
- Efforts to stop money laundering are hampered by the fact that money laundering appears to be a victimless crime. However, every robbery or break-and-enter or theft is one link in the money laundering chain, because these assets that were legitimately owned become money in the hands of criminals.
- There is a general lack of understanding about money laundering, its costs, and its consequences that has made it a difficult problem to address.
Chapter 4
The Historical and Cultural Perspective

- Evidence supports the existence of money laundering as far back as 2000 BC in China when merchants hid their wealth from the rulers of the day. As with today’s money launderers, they would move around and invest their wealth to disguise its origins.

- Money laundering was traditionally used by those who wanted to hide their wealth to avoid taxation and, in despotic regimes, to prevent seizure by those without a claim to the funds.

- Gold has always been a popular means of holding wealth; diamonds are also favoured. To this day, both products are used in money laundering.

- It is believed that the term money “laundering” was coined during Prohibition in the United States, when large amounts of cash were circulating among criminals as a result of the illegal sale of liquor. Just as now, the money had to be integrated into the legitimate economy, and one way of doing so was through the purchase of businesses that operated on a cash basis. Since laundries fit that description, it is rumoured that this is how money came to be described as “laundered.”

- It is also believed that slot machines were invented as a way to legitimize coins.

- Tax evasion is a driving force of the “underground economy” – of which money laundering is one aspect.

- The underground economy in Canada was strengthened by implementation of the Canadian Goods and Services Tax (GST). The GST has increased the number of tax evaders who pay for services in cash, and thereby do not pay GST, and hence avoid tax liability.

- Anti-money laundering legislation has existed in many countries since the 1970s. However, it was widely ignored until the scope of money laundering had become so pervasive in the 1990s that action was needed – and taken – to combat the problem.

- The events of September 11, 2001, revitalized global efforts to try and stop money laundering, since laundered money has been widely used to fund terrorist activities.
Case Study: BCCI

The Bank of Commerce and Credit International (BCCI), also known as the Bank of Crooks and Criminals International, operated in 62 countries before regulators stepped in to close down all operations in June 1991.

In its time, BCCI was described as “the most pervasive money-laundering operation and financial supermarket ever created for the likes of Ferdinand Marcos, Saddam Hussein and the Colombian drug lords.” (Time magazine, July 29, 1991)

BCCI was founded in 1972 and capitalized with $2.5 million; when it was folded, its “assets” stood at $23 billion, the bulk of which were unaccounted for and never found.

Headquartered in London, UK and with prominent international connections to individuals such as George H.W. Bush, Jesse Jackson, and Manuel Noriega, BCCI’s criminal activity constituted an accounting and legal nightmare. Investigation of the company has proven it was designed to obfuscate the audit trail by operating from a multiplicity of locations through a layered corporate structure, front companies and front men, by falsifying information from the top down, and by a pervasive disregard for the national laws of each country in which it operated. BCCI was not just suited to money-laundering practices, it actually sought out dirty money in its bid to build its asset base.

In 1988, BCCI was indicted on charges of laundering drug money in Florida and found guilty in 1990. BCCI’s money-laundering expertise was based on the bank having an international presence, sophistication with wire transfers, branches in parts of the world where dirty money originates, and flows into, and systems that permitted the quick retrieval of funds. Since the closing of the Bank in 1991, this expertise has found its way into numerous financial institutions around the world through the people who were not indicted.

BCCI’s money laundering was based on a corporate strategy of increasing deposits generated by the proceeds of drug sales and providing a full array of banking services to those customers by disregarding currency regulations, tax laws, and anti-drug laws. Their methods included:

- using certificates of deposits held at foreign branches to offset cash deposits made in the United States;
- crediting “counter-balancing loan proceeds” to foreign bank accounts designated by drug traffickers;
- using false names, codes, and counter-surveillance techniques against law enforcement.

The BCCI case illustrates the need for vigilance regardless of the apparent credibility of an organization, and of the people – including senior officers – within that organization. It also shows that wire transfers coming from countries in which criminal activity is prevalent should be suspect.
Chapter 5
Stages of Money Laundering

It takes three stages of money laundering to satisfy the objectives of the money launderers:

<table>
<thead>
<tr>
<th>Placement</th>
<th>Objectives</th>
<th>How Money Is Laundered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to disguise the origins of the dirty money</td>
<td>deposited into accounts at financial institutions (sometimes with staff complicity)</td>
</tr>
<tr>
<td></td>
<td>to avoid detection</td>
<td>mixed with funds earned legally</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>used to buy high-value goods, property, or business assets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layering</th>
<th>Objectives</th>
<th>How Money Is Laundered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to disguise the origins of the dirty money</td>
<td>wire transfers</td>
</tr>
<tr>
<td></td>
<td>to maintain control of the funds</td>
<td>cash deposited in foreign banks or financial institutions</td>
</tr>
<tr>
<td></td>
<td>to move the funds where they will attract less attention</td>
<td>the sale of goods acquired during placement</td>
</tr>
<tr>
<td></td>
<td>to conceal the audit trail</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Integration</th>
<th>Objectives</th>
<th>How Money Is Laundered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to make the money appear legitimate</td>
<td>false loan payments</td>
</tr>
<tr>
<td></td>
<td>to commingle legitimate with illegitimate funds</td>
<td>forged invoices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>income from property or assets appears clean</td>
</tr>
</tbody>
</table>
Anti-Money Laundering in the Financial Services Industry

Placement

- Disguising the origins of the dirty money is accomplished through the processes of placement and layering.
- Placement is the act of inserting the funds into the financial system or smuggling them out of the country in which they have been received.
- This stage is where the launderer is most vulnerable to detection, because it is very difficult to deposit the funds into the financial system.
- The criminal will be able to transform some of the funds into legitimate assets – which is the reason that luxury-goods retailers are a link in the money-laundering chain.
- Retailers are not required to question the source of funds used to pay for an expensive car, yacht, antiques, designer goods, or jewellery, whereas all financial institutions in Canada are required to report any suspicious transaction.
- Financial reporting requirements vary significantly between countries – in India, the amount considered a large cash transaction is the equivalent of US$800.
- High-value goods are highly appealing to money launderers, because they are portable and are often used as an alternative to cash.
- Also, during placement, funds will be split into smaller sums for deposit in a number of financial institutions, thus avoiding the suspicion that would be aroused by a large single deposit.
- Foreign banks favoured in the placement process include those that:
  - are located in jurisdictions identified as lacking basic anti-money-laundering controls;
  - are foreign shell banks (that is, banks with no physical presence in any jurisdiction); and
  - operate under an offshore banking licence.
- Casinos are also efficient for placement of funds. Cash is used to acquire chips or tokens. After a few turns at the table, the player cashes in the remaining chips or tokens for a cashier’s cheque that can be deposited anywhere.
- Casinos are effective for occasional placement; ongoing placement of funds requires the use of cash-based businesses, such as car washes, video-game arcades, video rentals, bars and restaurants, and vending-machine companies.
- During the placement process, money launderers often rely on “insiders” to make deposits, which prevents suspicions being raised.

Layering

- Layering consolidates funds once they have been placed. Layering uses a complex series of financial transactions to conceal an audit trail, so that the source and ownership of the funds remains anonymous.
- In legitimate business transactions, an audit trail sequentially demonstrates who has created or modified a document, transaction, or accounting entry, what was done, and when. An audit
trail maintains security, validates entries, tracks computer activity, and permits transactions to be recovered.

- Money launderers create a complicated web of financial transactions so that the audit trail is virtually impossible to discern.
- Money launderers also rely on bank and corporate secrecy and solicitor-client privilege for protection.
- Typically, money is moved in and out of the offshore bank accounts of bearer shell companies through electronic funds transfer.
- Throughout the world, over 500,000 electronic wire transfers, representing more than US$1 trillion, are sent daily, making the disclosure of clean versus dirty money impossible to detect. It is estimated that one out of every 2,000 transfers is laundered money. This sheer volume increases the probability that the money launderers will not be detected.
- Money launderers also perform complex transactions with stock, commodity, or futures brokers.

**Integration**
- Legitimizing the funds is part of the money-laundering process, and is called integration.
- The money launderers establish companies in countries in which their secrecy is protected or they buy banks. The banks they buy are not necessarily in countries that are tax havens, or in those with lax tax laws; even countries such as the United States have banks owned by people for the purpose of money laundering.
- If laundered funds can be commingled with legitimate funds, it is almost impossible to trace their origin.
- When that is done, the funds can be deposited into financial institutions, from which cheques can be written without questions being asked.
- Money laundering succeeds when legal transactions are mimicked using laundered funds, and thus the legal transaction and the illegal transaction appear identical.

**Tax Havens of the World**
Tax havens are a perfect place to launder money due to the minimal controls imposed by their governments on their financial services industry. Their bank secrecy laws mean that requests for financial information from governments abroad are often rejected. When information on a company is revealed, it is typically found that the company has been set up and registered without disclosing shareholders, directors, or owners.

Tax havens also do not normally tax interest on the bank accounts of non-residents; it is the account holders who are on the “honour system” to declare interest earned in these accounts for tax purposes in the country in which they are resident. Tax evasion may or may not be considered a money laundering offence within a jurisdiction.

In 1998, it was estimated that there were 4,000 offshore banks worldwide, licensed by nearly 60 offshore jurisdictions, controlling an estimated US$5 trillion in assets.
The Cayman Islands, listed below, is now the fifth-largest financial centre in the world, after London, New York, Tokyo, and Zurich. In the island of Nauru in the South Pacific, also listed, a person can set up his or her own bank (note: not a bank account, but an actual bank) with as little as US$25,000; 400 banks in that country operate from one mailbox. In 1998, it was estimated US$70 billion was moved into Nauru. In 2003 the U.S. Treasury issued a notice of proposed rule-making requiring all U.S. financial institutions to terminate correspondent accounts with banks from Nauru. However the subsequent introduction of AML (anti-money-laundering) legislation and its reduction of offshore companies from more than 2,000 to 66 (in 2005) meant that it was no longer considered non-cooperative by the Financial Action Task Force.

<table>
<thead>
<tr>
<th>Andorra</th>
<th>Indonesia</th>
<th>Singapore*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anguilla</td>
<td>Irish Republic</td>
<td>St. Vincent and the Grenadines</td>
</tr>
<tr>
<td>Antigua</td>
<td>Isle of Man</td>
<td>Switzerland*</td>
</tr>
<tr>
<td>Antilles</td>
<td>Jersey</td>
<td>Thailand</td>
</tr>
<tr>
<td>Aruba</td>
<td>Labuan</td>
<td>Turks &amp; Caicos</td>
</tr>
<tr>
<td>Australia*</td>
<td>Lichtenstein</td>
<td>Ukraine</td>
</tr>
<tr>
<td>Bahamas</td>
<td>Luxembourg*</td>
<td>United Kingdom*</td>
</tr>
<tr>
<td>Barbados</td>
<td>Madeira</td>
<td>Vanuatu</td>
</tr>
<tr>
<td>Belize</td>
<td>Malta</td>
<td></td>
</tr>
<tr>
<td>Bermuda</td>
<td>Mauritius</td>
<td></td>
</tr>
<tr>
<td>British Virgin Islands</td>
<td>Monaco</td>
<td></td>
</tr>
<tr>
<td>Canada*</td>
<td>Myanmar</td>
<td></td>
</tr>
<tr>
<td>Cayman Islands</td>
<td>Nauru</td>
<td></td>
</tr>
<tr>
<td>Cook Islands</td>
<td>Netherlands*</td>
<td></td>
</tr>
<tr>
<td>Costa Rica</td>
<td>Netherlands</td>
<td></td>
</tr>
<tr>
<td>Cyprus</td>
<td>Antilles</td>
<td></td>
</tr>
<tr>
<td>Dominica</td>
<td>Nevis &amp; St. Kitts</td>
<td></td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>Nigeria</td>
<td></td>
</tr>
<tr>
<td>Egypt</td>
<td>Niue</td>
<td></td>
</tr>
<tr>
<td>Gibraltar</td>
<td>Panama</td>
<td></td>
</tr>
<tr>
<td>Guatemala</td>
<td>Philippines</td>
<td></td>
</tr>
<tr>
<td>Guernsey</td>
<td>Sark</td>
<td></td>
</tr>
<tr>
<td>Hong Kong*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*A member of the Financial Action Task Force (FATF) on Money Laundering, a body of the Organization for Economic Cooperation and Development (OECD). As discussed elsewhere, the role of the FATF is to combat money laundering.

Sources: [www.fatf-gafi.org](http://www.fatf-gafi.org); www.Just1World.org
Chapter 6
Methods of Money Laundering

- Money launderers are renowned for their creativity and, of course, their secrecy. Thus, this list is only a partial listing of the ways in which money is laundered.

Underground banking
- Underground banking, also called parallel banking and alternative remittance systems, has existed for centuries. It has proven itself to be one of the safest methods for money launderers to transfer large sums of money without a trace.
- Underground banking exists outside laws and regulation.
- The systems of underground banking are known by different names, depending upon the community being served. They include: the Chop (Chinese); Hundi (Indian, Pakistani, and Afghani); Hawallah (Arab); Poey Kuan (Thai).
- Significant amounts of money are moved through the underground system; estimates indicate $2 billion move through the Hundi system alone annually.
- Hawallah is the best known form of underground banking, though the same techniques are used in the Chop and Hundi.
- Hawallah is the transfer of money between two persons by use of a third person. It requires trust among users, but its appeal lies in its simplicity.
- Hawallah bankers operate, often, within a very tight-knit community, using lines of communication that may be centuries old. Relationships may exist between the bankers and their clients; failure to meet obligations can result in reprisals on family members.
- The basic concept underlying all forms of parallel banking is that the movement of value is facilitated without the movement of money.
- Record-keeping procedures are nearly non-existent, making it difficult to apprehend those working within the parallel banking system. Coded messages, chits, and telephone calls effectively transfer money from one country to another.
- For instance, the chit system will be employed when the money launderer deposits funds with the underground bank, and the receipt issued may be a playing card or a postcard, torn in half.
- The other half of the card is forwarded to the Hawallah banker in the country of the money launderer’s choosing. When the money launderer presents his receipt, he receives the amount of his deposit (less fees charged by the banker).
Use of this system eliminates the need for carrying cash over borders.

Parallel banking may be suspected in shops that specialize in gold and precious jewels, money exchanges, and import/export businesses.

Internet banking and finance is the modern-day equivalent of Hawallah and other methods of parallel banking. Funds can be moved electronically (the movement of value) without the movement of money.

In addition to its effectiveness laundering proceeds of crime, the underground banking system also efficiently transfers money into Third World countries with monetary import restrictions. For instance, the underground banking system has been proved to be used by Vietnamese in the United States to send money to their families still living in villages in Vietnam. In this case, the money was not the proceeds of crime.

Commodities and the Futures Market

- In the futures market, the opportunity for transgression exists, because the brokers do not trade in the names of their clients, and thus the names of the beneficial owners are not known.
- Because commodities can only sell if there is a market, the money launderer will buy and then sell the same commodity.
- The contract will be paid from dirty money, a commission paid to the broker, and profits or proceeds of selling the contract paid by the broker to the money launderer.
- The money launderer then has a legitimate cheque for integration purposes.

Black-Market Peso Exchange (BMPE)

- This system of money laundering is used to swap dollars in the United States for pesos in Colombia, and is considered to be the largest single avenue for laundering drug proceeds in the U.S.
- In 2000, the BMPE laundered an estimated $5 billion of drug money for Colombian traffickers.
- There are three parties to the BMPE: the drug cartels, brokers, and Colombian businessmen.
- The drug cartels generate U.S. dollars by the importing and selling of drugs.
- The cartels sell their U.S. cash to brokers who launder the cash into the financial system. The brokers have two avenues for dispersal of the laundered money.
- One, the dollars are sold by the brokers to Colombian importers for pesos. An exchange rate is negotiated that is less than the official exchange rate. The importers need dollars to buy legitimate U.S. household goods, such as appliances, to import to Colombia.
- The brokers deposit the pesos from the Colombian importers into the accounts of the cartel members in Colombia. Thus, the drug-cartel members have been paid for the drugs they smuggle into the United States.
- Through this method, the drug-cartel members are paid in their currency of choice (pesos), Colombian importers circumvent the tight currency restrictions of their country and are able to buy more U.S. goods, because they are buying with cheap dollars, and the brokers take the risk.
The second way the brokers use the cash they have received is to pay for the household goods in the United States on behalf of the importer. The importers deposit pesos into the Colombian accounts of the drug-cartel members or the brokers.

Well-known companies, such as General Electric, Whirlpool, Phillip Morris, and Intel have been unwittingly implicated in the black-market peso exchange.

**Structuring of Funds (also Called Smurfing)**

- Structuring of funds occurs when a series of deposits is made that is just under the amount that must be reported to authorities as a suspicious transaction. In Canada, this amount is $10,000 or more.
- The deposits may be made by third parties, scattered widely over a geographic area, to a single “consolidation” account.
- Structuring can be used:
  - in the travel industry to buy airline tickets that are later returned for a refund;
  - with pawnbrokers that issue cheques written for cash on their accounts;
  - in money-services businesses that provide money orders or foreign exchange;
  - in the securities industry;
  - to acquire luxury goods that are later resold.

**Nominees**

- Nominees are friends, family, or business associates of the criminals, who are used as third parties to deposit funds.
- The nominees are usually well-known in their own right in their communities, and so do not attract attention for their activities. Thereby, suspicions are not likely to be aroused by their financial transactions.
- When nominees are used, the source and ownership of the funds are concealed, thus making it difficult for financial intelligence to identify the funds as laundered money.

**Securities**

- Securities are popular with money launderers, since once they have been successful in placing the funds in the system, pursuant cheques or wire transfers appear clean.
- Firms must be vigilant in regards to the suspicious movement of funds through wire transfers and cheques, cash deposits, and withdrawals.

**Insiders**

- Insiders in a financial institution can be one of the most effective aids to money launderers. Their complicity, and silence, is assured by bribery.
- While compliance officers often focus on young or inexperienced employees, it is often the more experienced and senior employees that will be targeted by money launderers.
Anti-Money Laundering in the Financial Services Industry

- Those in the retail branches of securities firms are under constant pressure from management to expand their client base and increase assets; unfortunately, laundering money fulfils these requirements too easily.

Credit, Charge, and Debit Cards
- Credit, charge, and debits cards can be misused by money launderers on both an institutional basis and a personal basis.

Institutional Use
- If a foreign bank that lacks anti-money-laundering controls issues a credit card that can be used in other countries, the risk exists that illicit funds located in the foreign bank may be accessed by account holders using that credit card to obtain cash advances – or if it is a dual card, they may use the card as a debit card.
- A primary concern by those who monitor the institutions that issue credit cards is that it is not clear that money laundering can be easily identified with the current technology that evaluates transactions passing through the operator’s system.
- Thus, the operator of the credit-card system within each country must conduct sufficient due diligence on the banks issuing the credit cards to ensure the bank has anti-money-laundering procedures in place.

Personal Use
- Credit cards are effective in the placement stage of the money-laundering process.
- Cash advances from credit cards can be used to purchase a cashier’s cheque or to wire funds.
- Cash payments are made on the outstanding balance of the credit card.

Real Estate
- The real-estate industry has traditionally been vulnerable to money laundering at all three stages of the money-laundering process:
  - placement: property is acquired for cash;
  - layering: multiple properties may be resold or exchanged, thus making the original property and its funding difficult to detect;
  - integration: when the property is sold to a legitimate customer whose financial institution gives the launderer a cheque, creating the proceeds of a legitimate transaction.
- Evidence of possible money laundering will include a buyer who knows little about the property being acquired, a property being acquired in the name of a third person, a property that is bought and sold again quickly, or a customer who buys multiple properties at one time.

Life Insurance
- The widespread use of life insurance products for money laundering has come to light only since 2002, when “Operation Capstone” revealed a scheme that involved the United States, the Isle of Man, Panama, and Colombia.
- It is believed that as much as US $80 million has been laundered via this means.
Colombian drug cartels purchased “investment grade” life insurance policies (i.e., policies with a cash surrender value) in the United States, the Isle of Man, and other locations through a small number of insurance brokers. The policies named cartel members as beneficiaries.

The policies were prepaid with millions of dollars sent in the form of cheques and wire transfers to the brokers by third parties using illegitimate funds.

The policies were then surrendered for their cash value after short periods of time, and, despite the penalties involved for early surrender, the beneficiaries would receive a cheque or wire transfer from the insurer.

Thus, the dirty money was laundered and the cheque or wire transfer appeared “clean.”

New legislation in the United States is being directed to the life-insurance industry.

Only policies with a cash value – universal life and individual variable investment contracts (segregated funds) – and annuities pose an opportunity for money laundering; term policies and health policies have no relevance.

When investment policies are overfunded, they are particularly indicative of money-laundering activity.

Life insurance policies can also be useful for the purpose of loan fraud: a borrower pledges a policy as loan security and he or she then cashes out the policy and defaults on the loan.

Gambling

Cash is used to buy gambling chips, which, after just a few bets, are then redeemed for a casino cheque. The cheque can be legitimately deposited into the banking system.

Currency Smuggling

Currency is exported from a country via mail, courier, and body-packing to a country with banking secrecy laws. It is then deposited to an account and legitimimized.

Exchange Transactions

Dirty money is exchanged for foreign currency that can then be transferred to accounts anywhere within the world.

Large Cash Purchases

Large, high-ticket items, such as jewellery, art, and expensive cars or boats, are bought with cash and are then resold. Even though a loss is incurred by the vendor, the money has been turned into a legitimate source of funds.
Chapter 7
The Effects of Money Laundering

- The financial services industry depends on the perception that it operates in a framework of high legal, professional, and ethical standards.
- If an institution turns a blind eye to suspicious activities, or its employees or directors have been bribed, that institution becomes a money launderer.
- The institution will not only face regulatory action and loss of its customers and reputation but, by association, all companies within the industry become tarnished.
- Thus, there are three risks assumed by an institution that launders money:
  o risk to reputation;
  o risk of censure;
  o risk of regulatory intervention.
- There are also macro-economic consequences of money laundering. Those cited by the International Monetary Fund include:
  o inexplicable changes in money demand;
  o risks to the soundness of banks;
  o contamination of legal financial transactions;
  o increased volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers;
  o a dampening effect on foreign direct investment when a country is perceived to be controlled or influenced by organized crime.
- Left unchecked, money launderers can control large sectors of a national economy through investment or bribery of public officials.
Chapter 8
Terrorist Financing

- Money laundering and terrorist financing are closely related, though much money-laundering activity occurs that is not linked to terrorists.
- Suppression of terrorist financing requires the coordination of diplomatic, law-enforcement, intelligence, regulatory, and policy measures on an international scale.

How Funds Are Raised
- Terrorists often operate under a cloak of legitimacy. Organizations or companies that fund terrorist activity appear to be legitimate, such as the honey traders in Yemen that have been identified as being part of the al-Qaeda financial network.
- Terrorists also procure financial support from criminal activity. Large-scale criminal activity is evident in the Afghan heroin trade; small-scale efforts include petty theft and smuggling.
- Muslims are bound by a religious duty, the Zakat, to contribute 2.5% of their income to humanitarian causes.
- An enormous amount of funds raised via the Zakat are inadvertently contributed to charities whose purpose is fund terrorism.

Financial Operations
- Terrorists are, for obvious reasons, attracted to operating in under-regulated jurisdictions. If bank supervision is limited, anti-money laundering laws are non-existent, or banks operate in a secretive manner, terrorists face little or no resistance to their financial dealings.
- In the past, many regional banking centres in the Middle East, such as Dubai, Kuwait, and Bahrain, have functioned outside the rules generally adopted by the international community.
- It is also known that money has entered legitimate financial institutions in under-regulated jurisdictions and is channelled through countries, such as Liechtenstein and the Bahamas, where bank secrecy prevails.
- Muslim terrorists are known to abuse the legitimate Islamic banking system that abides by the rules of Islamic law. Further, they are more likely to find collaborators sympathetic to their cause and willing to provide services within the Islamic banking system.
- The hawala system, previously discussed in this document, is also an effective means of moving cash between jurisdictions.
Reactions and Responses to Terrorist Financing

- Responses to terrorist financing are categorized as being tactical – in which individual nodes of the network are disrupted – or strategic, in which the environment in which terrorists raise and move funds is not supportive, or tolerant, of terrorists and their causes.

- The most visible aspect of the tactical response has been the public designations of people, businesses, and financial institutions associated with terrorist organizations. These designations have been commonly referred to as the “name and shame” lists.

- The United States led the way with such designations and were promptly followed by the UN, and many foreign governments.

- The UN called on all its member states to:
  - immediately freeze the assets of those who commit or attempt to commit terrorist acts or facilitate the commission of terrorist acts;
  - prohibit the provision and collection of funds for terrorist activities.

- These designations have resulted in the blocking of terrorist-related assets in banks and the barring of certain persons from doing business with designated organizations and individuals.

- Canadian measures, introduced in October 2001, further to the UN resolution include:
  - a listing provision, in which the list now published by the Office of the Superintendent of Financial Institutions identifies any person or organization that has committed, attempted to commit, or participated in a terrorist act or facilitated the commission of a terrorist act;
  - freezing of assets, so that no person in Canada or Canadian outside Canada will be permitted to knowingly deal directly or indirectly with any asset owned or controlled by a listed person;
  - prohibition of terrorist financing, so that funds cannot be collected for or provided to listed persons;
  - a new reporting requirement, detailed later in this document;
  - new compliance by financial institutions to determine if they have assets that belong to a listed person; federally regulated institutions report to OSFI and provincially-regulated institutions report to their provincial regulator or supervisor.

- Strategic initiatives have been less successful, due to inadequate money-laundering regulations in many countries, and poor implementation among some countries in which regulations do exist.

- No country in the world can regulate Islamic charities or the hawala system.

- The response to terrorism and terrorist financing will require a long-term sustained effort by the international community to bring about meaningful results.
Recognizing Terrorist Activity

- Suspicions of terrorist involvement will be raised if an individual tries to act on behalf of any one of the “Consolidated List of Names Subject to Regulations Establishing a List of Entities Made under UN Suppression of Terrorism Regulations.” This list can be acquired at www.osfi-bsif.gc.ca as an advisory to all federally regulated financial institutions.

- Particular caution must also be exercised whenever third-party transactions are being made and the third party (person or entity) is not known by the reporting person or entity.
Chapter 9
Catching the Crooks: The Macro Approach (International)

- Countering money laundering effectively requires not only knowledge of laws and regulations, investigation, and analysis, but also of banking, finance, accounting and other related economic activities.

- An effective system to combat money laundering, both on a national basis and internationally, requires:
  - mandatory reporting of suspicious and certain other financial transactions;
  - analysis of such reports;
  - dispersal of the analysis to relevant intelligence and law-enforcement agencies, when appropriate;
  - a multi-disciplinary approach

- The crime of money laundering may not become obvious until many or all of the pieces are put together. Since money may transfer hands in a matter of seconds or be relocated to the other side of the world instantaneously by an electronic wire transfer, law enforcement and agencies that investigate money laundering must be able to count on a virtually immediate exchange of information.

- This information exchange must also be at an early point after possible detection of a crime.

- Unfortunately, many barriers to the exchange of information exist, both within jurisdictions and between foreign governments and foreign counterparts. They include:
  - lack of resources;
  - the number of law enforcement agencies that may be involved within any one jurisdiction;
  - the reluctance of financial institutions to provide reports;
  - the unwillingness to share information;
  - technical obstacles to the rapid exchange of information.

- Despite the importance of apprehending those who are laundering money, privacy laws at home and abroad must be respected.
International Efforts

- The Financial Action Task Force (FATF) on Money Laundering, an agency that works closely with the Organisation for Economic Cooperation and Development, was established in 1989 to develop a coordinated international response to concerns about money laundering. There were 37 member countries as of 2007.

- The FATF developed 40 Recommendations on money laundering + 9 Special Recommendations on terrorist financing as a complete set of counter-measures against money laundering and terrorist financing to guide national governments. They address:
  - the scope of the criminal offence of money laundering, which includes identifying corporations themselves, and not just their employees, as subject to criminal liability and suggests measures for confiscation and criminal sanctions;
  - increased diligence of financial institutions, noting requirements for reporting and suggesting protection for “whistleblowers”;
  - measures to cope with the problems of countries with no or insufficient anti-money-laundering measures;
  - the strengthening of international cooperation, including the exchange of general information and the exchange of information relating to suspicious transactions;
  - other forms of cooperation, including the basis and means for cooperation in confiscation, mutual assistance, and extradition.

- The Recommendations established basic measures for all countries to implement, that:
  - make money laundering a crime;
  - ensure that financial institutions identify their clients, maintain client and account records, and report suspicious transactions;
  - monitor the flow of money over borders;
  - require international cooperation to strengthen efforts.

- Financial institutions were defined to be banks and non-bank financial institutions. The FATF list of financial activities of concern to the organization, whether undertaken by businesses or professions which are not financial institutions, includes:
  - acceptance of deposits and other repayable funds from the public;
  - lending;
  - financial leasing;
  - money transmission services;
  - issuing and managing means of payment (i.e., credit cards, cheques, traveller’s cheques, bankers’ drafts, etc.);
  - financial guarantees and commitments;
o trading for accounts of customers (spot, forward, swaps, futures, options) in:
  ▪ money-market instruments (cheques, Certificates of Deposit);
  ▪ foreign exchange;
  ▪ exchange, interest rate, and index instruments;
  ▪ transferable securities;
  ▪ commodity futures trading;
  ▪ participation in securities issues and the provision of financial services related to such issues;
  ▪ individual and collective portfolio management;
  ▪ safekeeping and administration of cash or liquid securities on behalf of clients;
  ▪ life insurance and other investment-related insurance;
  ▪ money changing.

• Implementation of effective anti-money-laundering controls requires international and domestic financial intelligence. Many nations have created internal agencies called financial intelligence units (FIUs) to gather the necessary information on individuals, institutions, and suspicious transactions.

• The Egmont Group of FIUs is an informal international group, established in 1995 to provide a forum for FIUs to improve support to their respective national anti-money-laundering programs. This support includes:
  o expanding and systematizing the exchange of financial intelligence;
  o improving expertise and capabilities of the personnel of such organizations; and
  o fostering better communication among FIUs through the application of new technologies.

• As of July 2007, there were 106 member nations of the Egmont Group, including Canada (FINTRAC) and, ironically, many nations deemed to be tax havens and possible prime targets for money launderers, such as the Bahamas, the Cayman Islands, Colombia, Lichtenstein, and Vanuatu.

• There are also a number of United Nations conventions and geographically-based initiatives from Europe, the Caribbean, and Asia Pacific that address anti-money–laundering concerns.

• In 2008, the headquarters of the secretariat of the Egmont Group was opened in Toronto.
United States

- Money-laundering legislation in the United States was strengthened in October 2001 through the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act.
- The act is written to deter and punish terrorist acts in the United States and around the world, to enhance law-enforcement investigatory tools, and for other purposes; money laundering is not the focus of the act, per se, but it is deterred by the act because of the link between money laundering and terrorist activities.
- The act requires every financial institution to establish an anti-money-laundering program that includes, at a minimum:
  a. the development of internal policies, procedures, and controls;
  b. the designation of a compliance officer;
  c. an ongoing employee training program; and
  d. an independent audit function to test programs.
- If convicted, one may be found guilty of a felony, imprisoned up to 20 years, and fined up to $500,000, or twice the value of the property involved, whichever is greater.
- A defendant may be charged not only with money laundering, but also with bank fraud, securities fraud, wire fraud, mail fraud, public corruption, RICO (Racketeer Influenced and Corrupt Organizations Act) crimes, and/or conspiracy to commit the aforementioned crimes.
- Since 1987, parole has been abolished in the federal system.
- Expungement (removal of conviction from public records) is also not available.

United Kingdom

- Existing U.K. law is contained within a number of acts and regulations, including the Proceeds of Crime Act 2002, the Terrorism Act 2000, and the Money Laundering Regulations 2007.
- The Joint Money Laundering and Steering Group (JMLSG) is the U.K. agency driving anti-money-laundering efforts.
- The Money Laundering Regulations specify customer-due-diligence steps to be taken when a business relationship is established with a customer or transactions are carried out that have a risk of money laundering attached. For some customers or situations where there is a higher risk of money laundering or terrorist financing, there is a requirement for enhanced due diligence. Ongoing monitoring (OM) of the customer’s activities must be undertaken when there is a continuing business relationship with a customer.
- When a transaction, or a pattern of transactions, is unusual and must be looked into as potentially suspicious activity, that activity must be reported to the Serious Organised Crime Agency (SOCA).
A major revision of JMLSG’s Guidance was published in January 2006, based on a number of fundamental principles, including that of senior-management accountability and the adoption of a risk-based approach. The latter allows firms to focus their AML/CTF resources on areas where the risk of money laundering/terrorist financing is higher, and therefore embodies proportionate and cost-effective approaches to managing these risks.

The risk-based approach – in which a firm establishes its own regime and safeguards specific to its business model – has also been adopted in Canada in 2008; please refer to the section titled “The Compliance Regime” later in this chapter.

More changes are expected in the United Kingdom as the JMLSG is currently in the process of amending its Guidance to reflect the provisions of draft Money Laundering Regulations 2007, which implement the EU’s Third Money Laundering Directive.
Chapter 10
Catching the Crooks: The Macro Approach (Canada)

- Under Canadian law, a money-laundering offence encompasses various acts committed with the intention to conceal or convert property or the proceeds of property (e.g., money), knowing or believing that it was derived from the commission of a designated offence.

- In this context, a designated offence means most serious offences under the *Criminal Code* or any other federal Act. It includes those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, etc.

- Canada’s strategy to combat money laundering is fourfold:
  a. enforce the laws;
  b. protect personal information;
  c. keep down the cost of compliance;
  d. support international efforts.

- In Canada, there are a number of agencies and federal departments with responsibility for implementing anti-money-laundering procedures.

- Foremost among them is the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), an agency created by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTF)*. As the central clearing-house for information related to money laundering in Canada FINTRAC:
  o receives, analyzes, and assesses transaction reports and other information relevant to money laundering, terrorist financing, and threats to Canadian security;
  o receives reports on the cross-border movement of large amounts of currency or monetary instruments;
  o provides intelligence about financial transactions to law enforcement agencies and to CSIS;
  o ensures that personal information under its control is protected from unauthorized disclosure;
  o monitors and ensures compliance in the business sector and by financial institutions with obligations under the Act;
  o enhances public awareness and understanding of matters related to money laundering and terrorist financing.
• Other agencies involved in anti-money-laundering efforts include:
  o Canada Revenue Agency (CRA):
    ▪ receives declarations of import and export of large amounts of cash or money in other forms and transmits them to FINTRAC;
    ▪ enforces reporting when large amounts of money are taken across borders;
    ▪ investigates the evasion of taxes or duties related to money laundering or terrorist activities.
  o Canada Border Services Agency (formerly known as Canada Customs and Revenue Agency)
    ▪ requires declaration of the import or export of currency or monetary instruments of or over $10,000.
  o The Office of the Superintendent of Financial Institutions Canada (OSFI):
    ▪ reviews policies and procedures to combat money laundering as part of its program of supervision of financial institutions and life insurance companies;
    ▪ suppresses terrorism by providing lists of names of entities and names of individuals subject to the Regulations Establishing a List of Entities made under subsection 83.05(1) of the Criminal Code or the United Nations Suppression of Terrorism Regulations.
  o The Royal Canadian Mounted Police (RCMP):
    ▪ investigates money-laundering offences and enforces laws;
    ▪ requires that Canadians inside Canada and abroad report the existence of any property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group. This includes information about any transaction or proposed transaction relating to that property.
  o The Canadian Security Intelligence Service (CSIS):
    ▪ investigates threats to national security linked to money laundering;
    ▪ also requires the same report of transactions or proposed transactions relating to terrorist property as provided to the RCMP.
  o Citizenship and Immigration Canada:
    ▪ prevents entry of foreign nationals engaged in money laundering and arranges their removal.
  o The Department of Finance:
    ▪ develops and evaluates policy and rules;
    ▪ leads international discussions on money laundering (although not through the Egmont Group).
  o The Department of Justice:
    ▪ prosecutes money laundering offences.
• Canada has also beefed up its Criminal Code, and the *Immigration and Refugee Protection Act* to strengthen its anti-money laundering efforts.

• An important objective of all those involved in the prevention of money laundering is to make financial organizations and the public aware of the rules, and to ensure their compliance with those rules.

• The core of Canada’s anti-money laundering efforts is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).*

• The objectives of the Act are:
  o To detect and deter money laundering;
  o To detect and deter the financing of terrorist activities;
  o To investigate and prosecute money laundering and terrorist activity financing offences.

• The *PCMLTFA* applies to almost 180,000 entities in Canada including:
  o accountants and accounting firms;
  o agents of the Crown for money orders;
  o banks;
  o caisses populaires;
  o Canada Post;
  o casinos (some charity exemptions);
  o co-op credit societies;
  o credit unions;
  o dealers in precious metals and stones (Dec. 30, 2008);
  o foreign exchange dealers;
  o government-owned deposit-taking institutions;
  o investment counsellors;
  o life brokers and agents;
  o life insurers;
  o money-services businesses;
  o portfolio managers;
  o public notaries and notary corporations in British Columbia (Dec. 30, 2008)
  o real-estate brokers or sales representatives;
  o real-estate developers (Feb. 20, 2009);
  o securities dealers;
  o employees of all these entities.
Legislated Requirements

- To meet the objectives of the Act, persons or entities covered by the Act must meet FINTRAC requirements for:
  - reporting;
  - ascertaining identity;
  - record-keeping;
  - a compliance regime

- Lawyers have been exempted from the requirement to report suspicious and large cash transactions and to implement a compliance regime based on the infringement that such requirements bring to the client-solicitor relationship. This places lawyers outside anti-money-laundering efforts, a situation that duplicates the position of lawyers in the United States.

- This course will focus on the requirements for financial entities, life insurers, and securities dealers.
  - Financial entities include banks, savings and credit unions, caisses populaires, cooperative credit societies, trust and loan companies, and agents of the Crown that accept deposit liabilities.
  - Life insurers include life insurance companies, brokers, or independent agents. Career agents (employees of insurers) are exempt from all requirements, except that they are responsible for reports of suspicious transactions and terrorist property. Reinsurers are exempt from reporting, client identification, and record-keeping requirements.
  - A securities dealer is defined as an individual or entity that is authorized under provincial legislation to deal in securities or other financial instruments or to provide portfolio management or investment advisory services.

Reporting

- Reports are required from financial entities, insurers, and securities dealers for:
  - large cash transactions (LCTs);
  - suspicious transactions;
  - terrorist property.

- In addition, financial entities alone must also report:
  - electronic funds transfers.

Large Cash Transactions (LCTs)

- A Large Cash Transaction report must be filed when an amount of C$10,000 or more is received in cash in a single transaction, or when two or more transactions are made that total $10,000 in cash within 24 hours of each other by or on behalf of the same individual or entity.

- This report must be filed by an individual with knowledge of such a transaction and if an employee or senior official has such knowledge.
- Cash means currency, either Canadian or foreign. It does not cover cheques, money orders, or other money instruments. Foreign currency must be the equivalent of C$10,000; the exchange rate to be used is the last noon rate of the Bank of Canada at the time of the transaction. This rate can be obtained at [www.bankofcanada.ca/rates/exchange/](http://www.bankofcanada.ca/rates/exchange/).

- If a large cash transaction results in an electronic funds transfer, then an Electronic Funds Transfer report is required, in addition to the Large Cash Transaction report by a financial entity.

- If there is a suspicion that the cash may be laundered money, then a Suspicious Transaction report is required, in addition to the Large Cash Transaction report.

- If a transaction involves property owned or controlled by a terrorist or a terrorist group, it must be frozen; the transaction cannot be completed, and a Terrorism Property report must be filed.
  - A consolidated anti-terrorism list for use by anyone in Canada and by Canadians outside Canada is published and maintained by the Office of the Superintendent of Financial Institutions (OSFI). See “Terrorism Financing” on OSFI’s website ([http://www.osfinbsif.gc.ca](http://www.osfinbsif.gc.ca)).
  - If you determine that you are in control or possession of property that is owned by or on behalf of anyone on this list, you must report its existence, as well as any transactions or proposed transactions related to the property, to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service.

- The Large Cash Transaction report must be filed with FINTRAC within 15 calendar days of the transaction.

- It is the responsibility of the employer of a reporting person or entity to file the report on behalf of employees and company agents. A life insurance broker or independent agent is responsible for his or her own filings.

- A report is not required when funds have been received from a financial entity, a government department or Crown agency, an incorporated municipal body, or a hospital.

- An LCT report is also not required for the operations of foreign subsidiaries or foreign branches of Canadian financial entities, life insurers, or securities dealers.

- Finally, some exemptions apply when an employee is depositing cash to his or her employer’s business account.

- Financial entities may be able to choose an alternative to Large Cash Transaction reports for some corporate clients. More details on this can be acquired from FINTRAC.

- The Large Cash Transaction report can be submitted electronically or in paper. All reports must be filed electronically if the technical capability to do so exists.

- The minimum technical requirements are a personal computer with:
  - 32 MB memory;
  - 640 x 480 VGA display (800 x 600 is preferable);
  - any operating system with a web browser;
  - an Internet connection.
Electronic reporting can be done on FINTRAC’s website (F2R) and by batch file transfer.

To access F2R, an entity must be enrolled for electronic reporting with FINTRAC.

F2R provides the Large Cash Transaction report with instructions for completion.

Batch file transfer requires a public key infrastructure certificate and software from FINTRAC.

There are seven parts to the Large Cash Transaction report; some parts are completed only if applicable.

To file a paper report, you can print a form from [http://www.fintrac.gc.ca/publications/LCTR-2008-eng.pdf](http://www.fintrac.gc.ca/publications/LCTR-2008-eng.pdf) or call 1-866-346-8722 to request a form be faxed or mailed.

When the form is completed, it can be faxed to 1-866-226-2346 or mailed to:

FINTRAC
Section A
234 Laurier Avenue West, 24th Floor
Ottawa, ON K1P 1H7

FINTRAC will acknowledge receipt of the electronic LCT report, but does not acknowledge the paper report.

Failure to report a large cash transaction can lead to a fine of $500,000 for a first offence, and $1 million for each subsequent offence.

When these reports are received by FINTRAC, they are assessed according to information contained in external government and commercial databases including the Canadian Police Information Centre’s database, voluntary information received, and with foreign financial-intelligence units.

FINTRAC analysts establish identification of those behind the financial transaction and, when money laundering is suspected, inform relevant intelligence and enforcement agencies.

**Suspicious Transaction Reports**

As with a Large Cash Transaction report, financial entities, insurers, and securities dealers are not required to file suspicious transaction reports for their foreign subsidiaries or operations outside Canada.

A suspicious transaction is a financial transaction in which there are reasonable grounds to suspect money laundering or an attempt to launder money or commission of a terrorist-activity financing offence or an attempted commission of such an offence. There is no dollar-limit threshold.

The identity of the person performing the transaction must be confirmed except:

- when the identity of the individual had been proved and there are no doubts about that previous identification information;
- if doing so would inform the individual that a Suspicious Transaction report is being considered or submitted.
• The suspicious transaction reports and attempted transaction reports must be retained by the reporting body.

• If an individual knows a financial transaction is related to terrorist groups or individuals, he or she cannot proceed with the transaction. The funds must be frozen. A Suspicious Transaction report would be required because of the attempted transaction, in addition to a Terrorist Property report.

• Suspicious transactions are more easily defined by what does not occur, than by what does. If a transaction does not fall within normal business practice, or does not feel “right,” because it give rises to feelings of discomfort, apprehension, or mistrust, then the transaction becomes suspicious.

• A transaction may also appear suspicious if the person who requested the transaction exhibited suspicious behaviour, or if he or she has suspicious associates.

• A suspicious transaction must be reported when the financial transaction has occurred or been attempted. For example, a life insurance agent who deposits a cheque on behalf of a client has made a financial transaction. If the cheque is refunded, that would also be a financial transaction. If a cheque was received and returned to the client before it had been deposited, then an attempted financial transaction has occurred.

• A suspicious transaction report must be submitted electronically by F2R or batch-file transfer if the technical capability to do so exists; computer requirements are the same as those described for Large Cash Transaction reports. FINTRAC will acknowledge receipt of the form.

• A report may be submitted in paper only when the electronic option is not feasible; forms may be accessed at www.fintrac.gc.ca/publications/TPR-2008-eng.pdf www.fintrac.gc.ca/publications/STR-2008-eng.pdf and mailed or faxed to the FINTRAC address previously provided. FINTRAC will not acknowledge receipt of the form.

• A suspicious transaction report must be submitted within 30 calendar days of the transaction.

• When preparing a report, it is essential not to alert the suspect by asking for information outside the norm.

• An employee or reporting entity cannot disclose that a Suspicious Transaction report has been made, or disclose the contents of a report with the intention of prejudicing a criminal inquiry.

• Failure to report a suspicious transaction carries penalties that include up to 5 years’ imprisonment, a fine of C$2 million, or both.

• No criminal or civil proceedings may be brought against an entity or person who makes a report in good faith.

*Recognizing Reasonable Grounds for Suspicion*

• Reasonable grounds are largely determined by normal business practices in the business in which the transaction occurs.

• Suspicious may centre on corporate activity or personal activity. A hierarchy of suspicious behaviours can be determined; activities that are particularly suspicious are those in which there is a pattern of multiple transactions or people involved.
Across the Financial Industry

- These general indicators of questionable transactions appear on FINTRAC’s website, (Guideline 2: 7.1); it is suggested the reader review the entire list on www.fintrac.gc.ca (see also Chapter 14: Money Laundering Red Flags):
  - Client admits or makes statements about involvement in criminal activities.
  - Client does not want correspondence sent to home address.
  - Client appears to have accounts with several financial institutions in one area for no apparent reason.
  - Client conducts transactions at different physical locations.
  - Client is accompanied and watched.
  - Client shows uncommon curiosity about internal systems, controls and policies.
  - Client overjustifies or overexplains the transaction.
  - Client is secretive and reluctant to meet in person.
  - Client’s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact the client shortly after the account is opened.
  - Normal attempts to verify the background of a new or prospective client are difficult.
  - Client appears to be acting on behalf of a third party, but does not tell you.
  - Client is involved in activity out of keeping for that individual or business.
  - Client attempts to develop close rapport with staff.
  - Client uses a post-office box or General Delivery address, or other type of mail-drop address, instead of a street address when this is not the norm for that area.
  - Client offers you money, gratuities, or unusual favours for the provision of services that may appear unusual or suspicious.
  - Client pays for services or products using financial instruments, such as money orders or traveller’s cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps, or notes.
  - Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations, or other reason to exist).

Financial Entities

- Some indicators of reasonable grounds to suspect money laundering that apply specifically to financial entities include the following (more indicators can be read on FINTRAC’s website, Guideline 2).
  - An unemployed client has too much money in account.
  - Client has numerous accounts, and deposits enough cash into each that, collectively, they contain a large sum.
  - A third party or parties is involved with the account, either through a large cheque endorsed by a third party, or through deposits made by third parties to the account or credit card of the account holder.
  - Numerous small deposits are made by third parties.
  - Frequent currency exchange occurs.
  - There is frequent use of safety-deposit boxes and visit to the safety-deposit box immediately preceding deposits to the account.
  - There are unexplained transactions between personal and business accounts.
Insurers

- Some indicators of reasonable grounds to suspect money laundering that apply specifically to insurers include the following (more indicators can be read on FINTRAC’s website, Guideline 2):
  - a premium payment is received from a third-party account;
  - a policy is cancelled within the rescission period;
  - the duration of the contract is less than three years;
  - the client is more interested in the cancellation/surrender of the policy than its performance.

Securities Firms

- Some indicators of reasonable grounds to suspect money laundering that apply specifically to securities firms include the following (more indicators can be read on FINTRAC’s website, Guideline 2):
  - the client makes settlements with cash;
  - a third party or parties is involved (either as providing payment, nominee accounts, as undisclosed beneficiary, etc.);
  - the client is uninterested in usual performance indicators;
  - the client uses traveller’s cheques, cashier’s cheques, money orders, or bank drafts in amounts just under C$10,000;
  - funds are held in account at the broker without being traded when this is not usual for the client.

Terrorist Property Reports

- A person or entity must submit a Terrorist Property report to FINTRAC if the person or entity possesses or controls property on behalf of a terrorist or terrorist group.
- A person or entity that suspects that he or she or the entity possesses or controls property on behalf of a terrorist or terrorist group must also submit a Suspicious Transaction report to FINTRAC.
- Property includes any deed or instrument giving title or right to:
  - property, including cash, insurance policies, securities, or real estate;
  - money;
  - goods.
- A terrorist or terrorist group is defined as anyone who plans, facilitates, or carries out terrorist activity.
- Even if you are not required to report by the Act, the Criminal Code requires you to report to the RCMP or CSIS if you have property, or information about property, that is within your possession or control that is owned by or controlled by or on behalf of a terrorist or terrorist group.
- Fax numbers to which a report can be sent are:
Anti-Money Laundering in the Financial Services Industry

- RCMP: 613-993-9474
- CSIS: 613-231-0266.

- FINTRAC can accept a Terrorist Property report only via hard copy (on paper).
- The form can be obtained from: <www.fintrac.gc.ca/publications/TPR-2008-eng.pdf>
  or by calling 1-800-346-8722.
- The form may be submitted by fax to 1-866-226-2346 or to:
  FINTRAC Section A
  234 Laurier Ave. W., 24th Floor
  Ottawa, ON
  K1P 1H7

- There will be no acknowledgement of a report submitted.
- Detailed information will be required in a report, including but not limited to:
  - the reason for filing the report, including how the reporter came to know that the property is terrorist property;
  - information about the property, including its value and a description;
  - account information if an account is involved;
  - information about any transaction or proposed transaction;
  - information about how the transaction was completed or proposed to be completed;
  - information about the individual who conducted the transaction or who proposed to conduct the transaction;
  - information on any third party involved or proposed for involvement in the transaction.

**Electronic Fund Transfer Reports (EFTs)**

- The EFT report is required of financial entities, not insurers nor securities dealers.
- An EFT is the transmission of instructions for a transfer of funds through any electronic, magnetic or optical device, telephone instrument, or computer.
- If an EFT is initiated in cash in an amount of C$10,000 or more, a Large Cash Transaction report is required, in addition to the EFT report.
- If an EFT gives cause for suspicion, a Suspicious Transaction report is required, in addition to the EFT report, and – if applicable – the Large Cash Transaction report.
- There are different types of EFT reports, depending on the nature of the transaction:

**Outgoing EFTs**

- When a client within Canada requests a single transfer of $10,000 or more outside Canada or two or more transfers that total $10,000 or more within 24 consecutive hours by, or on behalf of, the same individual or entity, then an Outgoing International non-SWIFT EFT report (EFTO) must be sent to FINTRAC. (For an explanation of SWIFT, see below.)
• If another financial entity, money-services business or a foreign-exchange dealer in Canada transfers the funds, after you have given them your client’s name and address, you do not have to report the EFT.

Incoming EFTs

• When a client within Canada requests a single transfer of $10,000 or more outside Canada or two or more transfers that total $10,000 or more within 24 consecutive hours by, or on behalf of, the same individual or entity, then an Incoming International non-SWIFT EFT report (EFTI) must be made to FINTRAC.

• All financial entities must make the related EFT report (EFTI) to FINTRAC when instructions have been received for a transfer of funds from an individual or entity outside Canada. If instructions come from within Canada, an EFT report is not required.

• The EFT reporting limit is C$10,000, or, if foreign currency is being transferred, it must be an equivalent amount. The actual exchange rate used to process the transaction is not used, but instead the last noon rate from the Bank of Canada.

• All EFT reports must be submitted electronically if the technical capability exists to do so; computer requirements are the same as for Large Cash Transaction reports.

• Paper EFT reports may be submitted, except for SWIFT transfers. A form can be accessed at www.fintrac.gc.ca/publications/TPR-2008-eng.pdf; address information is the same as previously provided for Large Cash Transaction reports.

• Electronic EFT reports will be acknowledged by FINTRAC; paper reports will not.

• Anyone who fails to report an EFT transaction is punishable by a fine of up to $500,000 for a first offence and $1 million for each subsequent offence.

• It is an offence to “tip off” clients.

SWIFT EFTs

• SWIFT messages are sent by SWIFT members through the SWIFT network. SWIFT is the Society for Worldwide Interbank Financial Telecommunication, a cooperative owned by the international banking community for the transmission of financial messages.

• SWIFT 103 messages require a SWIFT EFT report for the same type of transactions as non-SWIFT transfers.

• SWIFT EFT reports can only be submitted electronically.

• An EFT report must be sent within five business days after the date of the transfer.

Cross-Border Currency Reporting

• There is no limit to the amount of money that can be brought into Canada or taken out of the country.
• However, persons and entities have to report all imports and exports of currency and monetary instruments equal to or greater than C$10,000, or equivalent. These reports must be made in writing, signed, and given to a Canadian Border Services Agency officer.

• Failure to report currency and monetary instruments may result in search, seizure, and a subsequent penalty, ranging from $250 to $5,000.

• All completed reports are sent to FINTRAC for assessment and analysis.

**Ascertain Identity**

• The identity of the initiator of financial transactions relevant to FINTRAC reporting requirements must be confirmed for any transaction other than the initial deposit.

**Individual Physically Present**

• ID is acceptable when it meets the following four conditions:
  
  o It is original. When the original document cannot be viewed by you, an agent or mandatory can be used to verify the original document on your behalf. Responsibility for the originality of the document that is used to prove identity rests with you.

  o It has a unique identifier number; thus a birth certificate is acceptable but a baptismal certificate is not.

  o It was issued by a provincial, territorial or federal government.

  o It is valid and not past its expiration date.

**Individual Not Physically Present**

• When the individual is not physically present, a third party must be called upon. There are numerous restrictions on who that party can be.

• Affiliate:
  
  o An affiliated entity can be used to prove identity when the following conditions are met. An entity is considered affiliated if your firm owns it or it owns your firm or both your firm and the entity are fully owned by a same, other, entity.

  o Your firm must first acquire the individual’s name, address, and date of birth.

  o This information must then be confirmed by the records of one of the following:

    • a financial entity, life insurer, or securities dealer affiliated with you;

    • an entity affiliated with you whose activities outside Canada are similar to a financial entity, life insurer, or securities dealer;

    • a member of a central cooperative credit society to which you also belong.

• Non-Affiliate:
  
  o Two of the following methods (1a or 1b, plus 2 or 3; or 2 plus 3) must be combined if ID is being sought through a non-affiliate.

  o All information across all sources must be consistent.
1. ID product or credit file method:
   (a) Refer to a reliable, independent product based on personal information and 
       Canadian credit history of the individual of at least six months’ duration.
   (b) Refer to the individual’s credit file after obtaining his or her permission to do so. 
       The file must have been in existence for at least six months.
2. Attestation:
   (a) Obtain an attestation by a commissioner of oaths or a guarantor that he or she 
       has seen an original identification document for the individual. The attestation 
       will include the commissioner or guarantor’s name, profession, address, and 
       signature on a legible photocopy of the ID, plus the type and number of the 
       original ID.
   (b) Canadian guarantors include dentists, doctors, chiropractors, judges, magistrates, 
       lawyers, notaries (in Quebec) or a notary public, optometrists, pharmacists, all 
       accredited accountants (CA, CGA, CMA, PA, RPA), professional engineers, 
       engineers (in Quebec), and veterinarians.
   • Additional methods of identification are available for those opening a credit card account. 
     Please refer to FINTRAC Guideline 6G: 4.12
3. Cleared cheque or deposit account:
   (a) confirm that a cheque on a deposit account in the name of the individual has cleared;
   (b) confirm that the individual has a deposit account with a financial entity.

Proof of Corporate Identity
• The existence of the corporation must be proved in addition to its name, address, and the 
  names of its directors.
• The following documents can be used for these purposes:
  o the corporation’s certificate of corporate status;
  o the record that is filed annually under provincial securities legislation;
  o any other record that confirms existence such as the company’s annual report signed by 
    independent auditors, or a letter to the corporation from any government;
  o the application for incorporation (to verify directors);
• The beneficial owner of the corporation (one who enjoys the benefits of ownership of an 
  asset, regardless of whose name it is in) must also be confirmed.

Politically Exposed Foreign Person (PEFP)
• It is necessary to identify whether a politically exposed foreign person conducts financial 
  transactions with you or your employer for new or existing accounts or certain electronic 
  funds transfers.
• There is a 14-day time frame in which the identity of the account-holder must be proved after 
  the account is opened.
• A politically exposed foreign person is one who holds, or has held, one of the following positions in or on behalf of a foreign country:
  o head of state or government;
  o member of the executive council of government;
  o member of a legislature;
  o deputy minister or equivalent;
  o ambassador, attaché, or counsellor;
  o general or higher rank in the military;
  o president of a state-owned company or bank;
  o head of a government agency;
  o judge;
  o leader or president of a political party in a legislature.
• The PEFP designation also includes the individual’s:
  o mother or father;
  o child;
  o spouse or common-law partner;
  o parents of the spouse or common-law partner;
  o siblings or half-siblings.
• If a PEFP opens a new account or has an existing account, it is also necessary for senior management to approve the account within 14 days after it has been opened or determined as belonging to a PEFP; to establish the source of funds that will be deposited to the account; to monitor the account on an ongoing basis to be aware of suspicious transactions.
• When an individual initiates or is the beneficiary of an electronic funds transfer of $100,000 or more, it is necessary to determine if he or she is a PEFP. Senior management approval of the transaction within 14 days is required as is a determination of the source of the funds.

Transactions Requiring Identification

Financial Entities
• Individuals and entities must be identified when the following transactions take place:
  o a signature card is signed;
  o a large cash transaction is made;
  o an account is opened for a corporation or other entity;
a settler or co-trustee of a trust wishes to make a transaction;
traveller’s cheques, money orders, or other negotiable instruments worth $3,000 or more are purchased or redeemed when a signature card does not exist;
a fund transfer of $1,000 or more is requested when a signature card does not exist;
a credit-card account is opened;
group plan account contributions are not made by payroll deduction or the plan sponsor.

Securities
- Individuals and entities must be identified when the following transactions take place:
  - a signature card is signed
  - a Large Cash Transaction is made
  - instructions are given for an account
  - an account is opened for a corporation or other entity
  - a Suspicious Transaction report is sent
  - group plan account contributions are not made by payroll deduction or the plan sponsor.

Insurers
- Individuals and entities must be identified when the following transactions take place:
  - a large cash transaction is made;
  - an annuity or life policy worth $10,000 or more is purchased;
  - a Suspicious Transaction report is sent;
  - group plan account contributions are not made by payroll deduction or the plan sponsor.

Record-Keeping Requirements
- Financial entities, insurers, and securities dealers must keep the following records:
  - records of large cash transactions;
  - copies of official corporate records;
  - copies of Suspicious Transaction reports;
  - beneficial ownership records.
- Financial entities and securities dealers must also keep the following records:
  - signature cards;
  - account-holder information (securities dealers must also keep account operating agreements or account applications);
  - stated intended use of an account.
Anti-Money Laundering in the Financial Services Industry

- Financial entities alone must also keep:
  - account operating agreements;
  - deposit slips;
  - debit and credit memos;
  - account statements;
  - cleared cheques;
  - credit files;
  - foreign-currency-exchange transaction tickets;
  - a copy of the trust deed and settler’s identification (for trust companies);
  - credit-card account records;
  - records for the sale of traveller’s cheques, money orders, or similar negotiable instruments of $3,000 or more;
  - records for money orders redeemed for $3,000 or more;
  - records of specified funds transfers;
  - correspondent banking relationship records.

- Securities dealers must also keep:
  - new account applications;
  - confirmation of sale or purchase;
  - guarantees;
  - trade authorizations;
  - powers of attorney;
  - joint account agreements;
  - correspondence pertaining to accounts;
  - account statements.

- Only insurers must also keep:
  - client information records.

- Any large cash transaction must be recorded; requirements for what must be in each record are the same for all entities:
  - the amount and currency of cash received;
  - the date and nature of the transaction;
  - the purpose of the transaction, and relevant details;
  - the involvement of any third parties in the transaction;
  - how the cash was received;
the account affected by the transaction;

- the name of the client with the account. Also, all entities share similar obligations in terms of third-party involvement in a transaction; these requirements are waived on the part of a financial entity when an account is opened by a legal counsel, an accountant, a real estate broker, or a sales representative, and the account is to be used by their clients.

- Failure to retain records carries a possible fine of up to $500,000 and up to five years’ imprisonment.

- Records have to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them.

- They must be retained for a period of five years.

**The Compliance Regime**

- Proper compliance is mandated by FINTRAC, however, compliance should be a matter of personal will and corporate ethics.

- Compliance with the Act and its regulations can illustrate a serious desire to deter money laundering within the organization rather than the attitude that it has been forced on the individual or entity.

- A compliance regime must be in place for financial entities, securities dealers, and insurers.

- They share the need to:
  - appoint a compliance officer;
  - develop and apply written compliance policies and procedures;
  - assess and document the risks of money laundering and terrorist financing specific to the business and what measures are taken to mitigate those risks;
  - implement and document an ongoing training program;
  - review and document the effectiveness of policies, procedures, training, and risk assessment.

- Failure to implement any of these elements could lead to an administrative monetary penalty of up to $100,000 for each one.

**The Compliance Officer**

- The person appointed as compliance officer must have the authority to check on individuals and procedures throughout the organization. For this reason, he or she should be a senior employee who can access management at all levels and report to the board of directors. The officer should not be directly involved with the receipt, transfer, or payment of funds.

- In a small company, the compliance officer could be the owner or operator of the business.

- Employee knowledge must be tested to provide assurance that regulations are being followed.

- Such tests are often referred to as “audits,” and they can be practical or theoretical in nature.
Development of Compliance Policies and Procedures

- Policies and procedures must be communicated, understood, and followed by everyone within the organization who has reporting requirements.
- These individuals must be particularly cautious in dealing with foreign entities that have not established anti-money-laundering regimes consistent with international standards and in avoiding those organizations within Canada that have been identified as supporting terrorist financing. A list of these organizations is available at [http://www.osfi-bsif.gc.ca/eng/docs/entstld.xls](http://www.osfi-bsif.gc.ca/eng/docs/entstld.xls). The list was developed by the Department of Foreign Affairs and International Trade and modified by the addition of names provided by the Department of Public Safety and Emergency Preparedness. As of June 2008, over 700 organizations appeared on this list.

Risk Assessment

- A risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which your business is exposed. The complexity of the assessment depends on the size and risk factors of your business.
- You have to document and consider the following factors in your assessment:
  - your products and services and the delivery channels through which you offer them;
  - the geographic locations where you conduct your activities and the geographic locations of your clients;
  - other relevant factors unique to your business; and
  - your clients and the business relationships you have with them.
- Completing a client risk assessment should be appropriate where there is an ongoing relationship. An ongoing relationship is one in which a client opens an account or undertakes multiple transactions over a time period, regardless of whether the transactions are related to each other. When dealings with a client are limited to a single transaction, this is not considered to be an ongoing relationship.
- Risk assessment will lead to conclusions about how risk can be mitigated; these strategies must be incorporated into written policies and procedures.

Review of Compliance Policies and Procedures

- A review must be done every two years. It has to cover policies and procedures, assessment of risks related to money laundering and terrorist financing, and the training program to test their effectiveness.
- An internal or external auditor can be used to:
  - interview those who handle transactions, and their superiors;
  - review the process for suspicious transactions;
  - sample large cash transactions and their reports;
  - sample electronic funds transfers and their reports
test whether exceptions to Large Cash Transaction reports are valid and reasonable;

test the record-keeping system;

test client identification procedures.

A practical audit may see an individual engaged who tries to “break the rules.” He or she may have inadequate identification or display other warning signs. It will be clearly evident whether employees follow procedures or not.

A theoretical audit may be a training session, or self-study of procedures.

Training

- The formality of training will depend largely on the size of the entity implementing a training program. Small companies and individuals need only be concerned with keeping a small number of people knowledgeable and current. In large companies, the number of people needing training can be a significant proportion of the whole.

- Training is mandatory for:
  - senior management;
  - those who have contact with customers;
  - those who handle money;
  - new employees;
  - those who change jobs to a position in which anti-money-laundering regulations are in effect;
  - information-technology employees;
  - those in charge of internal controls;
  - the compliance officer;
  - internal auditors;

- In addition, changes to legislation should be communicated throughout the organization.

Penalties for Non-Compliance

- Non-compliance with Part 1 of the PCMLTFA may result in criminal or administrative penalties. FINTRAC has legislative authority to issue an administrative monetary penalty (AMP) to reporting entities that are in non-compliance with PCMLTFA, effective December 30, 2008.
Administrative Monetary Penalties

- Under FINTRAC administrative monetary penalties (AMPs) represent an additional tool to current criminal sanctions to help enforce compliance on behalf of reporting entities. AMPs have been designed to provide a measured and proportionate response to instances of non-compliance.

Violations

- There are three types of violations under PCMLTF Regulations: Minor, Serious, and Very Serious and carry a maximum penalty of $1,000, $100,000 and $500,000 respectively.
- The AMPs program has maximum penalties for individuals and entities (e.g. corporations) according to the following list:
  - Minor (individual / entity): $1 to $1,000
  - Serious (individual / entity): $1 to $100,000
  - Very Serious (individual): $1 to $100,000
  - Very serious (entity): $1 to $500,000
- While the above limits apply to each violation, multiple violations can apply and the total penalty amounts can exceed these limits.

Penalty Determination

- FINTRAC determines penalties according to the following three criteria: the harm caused by the violations(s); the compliance history of the reporting entity; the non-punitive nature of an administrative penalty.
- The first criterion is based on the degree to which the violation obstructs Canada’s ability to detect and deter money laundering and terrorist financing (e.g. minor, serious, etc.).
- The second criterion provides FINTRAC with the means to adjust the base penalty upwards or downwards in conjunction with the individual’s or entity’s previous five-year history.
- The third criterion and the goal of the AMPs program is to encourage compliance with the PCMLTFA, rather than to punish non-compliance. FINTRAC is provided with additional means to determine penalties that may apply under a non-punitive criterion and its application to the reporting entity in question.

Additional Facts

- Where violations have been settled, payments are made directly to FINTRAC, care of the Receiver General of Canada.
All violators may request a review of an administrative monetary penalty by making representation to the Director of FINTRAC within 30 days of receiving a notice of violation.

FINTRAC will make public on its web site a list of the AMP(s) and include the nature of the violation, penalty, name of the person or entity that committed the violation, and city where the business is located. This list is found through the Public Notice link on the FINTRAC web site.

Criminal Penalties

FINTRAC can disclose cases of non-compliance under PCMLTFA to law enforcement when there is evidence of extensive non-compliance or no expectation of future compliance. Criminal penalties can include any of the following violations.

Violations

- Failure to report suspicious transactions: up to $2 million and / or 5 years imprisonment.
- Failure to report a large cash transaction (LCTR) or an electronic fund transfer (EFT): up to $500,000 for the first offence, $1 million for each subsequent offence.
- Failure to meet record keeping requirements: up to $500,000 and / or 5 years imprisonment.
- Failure to provide assistance or provide information during compliance examination: up to $500,000 and / or 5 years imprisonment.
- Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.
Chapter 11
Reporting Requirements and PIPEDA

- Many of the reports required for submission to FINTRAC appear to be contrary to the intent of Canada’s privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA).
- However, the PCMLTFA makes reporting of suspicious transactions mandatory for many of those within the financial services industry.
- PIPEDA recognizes the need of law-enforcement agencies to collect personal information without the consent of the individual and exempts the collection of information that assists in legal investigations.
- Therefore, FINTRAC reporting takes priority over PIPEDA requirements.
Chapter 12
Catching the Crooks:
The Micro Approach
(Taking Personal Responsibility)

In addition to the legal responsibility of an individual in the workplace to prepare transaction reports, there are five ways the effectiveness of anti-money laundering efforts can be enhanced through personal actions. These are:

- providing education to employees and coworkers;
- volunteering information;
- compliance;
- “Know” directives;
- whistleblowing.

**Education**

- Large firms will have anti-money laundering and terrorist financing initiatives in place to make all employees aware of the problem and their responsibilities.

- However, many small businesses will not have the luxury of appointing anti-money-laundering or terrorist-financing specialists within their firm, and yet small firms are easily targeted by money launderers for the very reason that they are less likely to have rigid controls in place.

- FINTRAC’s guidelines should be available to all employees of all firms in which there is a reporting requirement. They are available in PDF format from [www.fintrac.gc.ca](http://www.fintrac.gc.ca). There is no cost to download these files. The guidelines should be checked annually at a minimum for updates and changes to regulations.

- Make the list of Money Laundering Red Flags in Chapter 14 available to all employees and co-workers; make sure new, or part-time employees know the signs, in addition to full-time staff.

- Frequent reminders of indicators of money laundering will be more effective than infrequent education sessions.
Volunteering Information

- FINTRAC accepts voluntary information from the public about suspicions of money laundering and terrorist financing.
- As much information as possible needs to be provided, including the identities of person(s) or organization(s) that are involved.
- FINTRAC will attempt to maintain the privacy of the person providing the information.

“Know” Directives

- Know Your Client has been a long-standing directive in the financial services industry. However, with anti-money-laundering and terrorist-financing requirements, it is necessary to:
  - know your client;
  - know your employee;
  - know your agent.
- Know Your Client requires ID to be provided, even if the customer has a long-standing relationship with the institution.
- Know Your Client has different meanings, based on whether the client is retail or institutional.
- Know Your Employee may require reference checks and ongoing monitoring of employee behaviour.
- Know Your Agent is a directive towards those who are providing legitimate funds to an institution to ensure the funds are not illegally manipulated to hide the audit trail.
- Knowing your client is not limited to identification or record-keeping requirements. It is about understanding your clients, including their activities, transaction patterns, and how they operate.

Whistleblowing

- Whistleblowing might be more aptly named as Know Your Employer; it is the act of the employee reporting wrongdoing by the corporation or business without suffering retaliation by being fired by the corporation or business.
- Wrongdoing is an act that:
  - violates a law or regulation;
  - is a misuse of funds or assets;
  - is evidence of gross mismanagement;
  - represents a substantial and specific danger to the life, health, and safety of Canadians or the environment.
- It applies to disclosure of all unacceptable conduct of the organization, and it is clearly relevant to money laundering and terrorist financing, which are violations of a law.
- The activity of whistleblowing was addressed by the 40 Recommendations of the FATF.
The United Kingdom has taken an aggressive position on whistleblowing in the Public Interest Disclosure Act (PIDA), enshrining the right of a worker to make disclosures that are in the public interest, and giving protection from victimization by the employer. Canada does not have equivalent legislation.

However, the Competition Act in Canada enables employees to make complaints without disclosing their identities and general statutory and common-law provisions protect employees from being fired without just cause.

Most whistleblowing legislation is directed at protecting the employee from reprisals if he or she does “blow the whistle” on the employer.

Whistleblowing is a pejorative term (e.g. snitch, traitor); this perception must be overcome, because whistleblowers take a high degree of personal interest in the integrity of their employer and the enforcement of laws.

**Whistleblowing and the Employee**

- Whistleblowing can occur by the employee disclosing wrongdoings to:
  - superiors within the organization;
  - the police or a regulatory body;
  - the media.

- The employee may blow the whistle on:
  - superiors within the organization;
  - co-employees;
  - the organization itself;
  - individuals or entities with which the employer has a close business relationship.

- An employee who considers whistleblowing must think about the risks and outcomes before acting.

- The employee must not attempt to become a private detective, but only use the facts in his or her possession to support the case.

- Whistleblowing is typically not appreciated; the employee must not expect appreciation or thanks.

- The employee who chooses to blow the whistle must follow internal processes within the organization to show evidence of wrongdoing and respect individual rights by not making accusations that are trivial or vexatious.

**Whistleblowing and the Employer**

- If accusations have been made internally, it will be in the employer’s best interest to address them before the whistleblower becomes frustrated and goes public with complaints.

- Whistleblowing is a positive action and is evidence of a “culture of communication.” It should be encouraged, and employees should be educated about their whistleblowing responsibilities.
Anti-Money Laundering in the Financial Services Industry

- Managers and executives should be trained about how to deal with whistleblowers to ensure people come forward with information. They must make their employees aware of the internal mechanisms that exist for the whistleblower to use.
- Internal mechanisms should exist to allow employees to disclose wrongdoings, to ensure the disclosures are addressed in an appropriate and timely fashion, and to ensure employees who blow the whistle are protected from reprisal and are treated fairly.
- Privacy issues are particularly thorny; the privacy of those accused must be respected while investigations are made.

**When to Blow the Whistle**
- Public whistleblowing should occur only after normal channels for information-sharing and dispute resolution have been exhausted and no progress has been seen on the issue by relevant officers within the company or organization within a reasonable period of time.

**Whistleblowing and Money Laundering**
- Whistleblowing may be an appropriate remedy for an employee in the financial services industry, or any activity identified as prone to the injection of laundered money, who:
  - sees another employee enjoying a lifestyle obviously beyond his or her means;
  - is aware of client or corporate practices contrary to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.
Chapter 13
Keeping Paranoia in Check

- It is easy to become paranoid and begin to suspect that all large cash transactions are evidence of money laundering, or that members of certain ethnic groups are engaged in money laundering.

- As FINTRAC points out in its Guidelines, there are many factors that lead to suspicions, not just one. Therefore, for instance, because a person has an offshore bank account is not reason enough to suspect money laundering. However, if that person makes a number of cash deposits just under $10,000 to an account in Canada, deposits are made to the account by a number of third parties, and the offshore account is located in a country known to facilitate money laundering, then it is fair to have suspicions.

- Good judgement by front-line employees in the financial services industry can go a long way towards supporting suspicions that are well-grounded.

Common Sense Steps to Deter Money Laundering

- Know the client.
- Question the reason why a large amount of cash is used in a situation when it might be expected that other forms of payment are more appropriate.
- Follow the procedures of your organization in regards to money laundering and terrorist financing.
- File transaction reports and Terrorist Property reports when required and Suspicious Transaction reports when appropriate.
- Take note when you become aware of a series of “flagged” financial transactions.
- Exercise caution in any dealings (e.g., credit cards, cheques, loans) with financial entities in those countries identified by the FATF as non-cooperative.

Suspicious Behaviours

- Client Behaviour:
  - a client is nervous;
  - a client has accounts with several financial institutions for no apparent reason;
  - a client insists a transaction be done quickly;
  - a client attempts to explain or provide too much information about a transaction;
Anti-Money Laundering in the Financial Services Industry

- a client makes a single unusual transaction amount;
- you are aware the client is the subject of a money-laundering investigation;
- a client either admits involvement in criminal activities or seems overly knowledgeable about criminal activities;
- a client attempts bribery of financial services personnel;
- a client states that funds are “clean” or “not laundered”;
- client ID seems counterfeit or inaccurate;
- a client makes cash transactions in rounded-off amounts just under the reporting levels (e.g., $9,400, $8,900);
- there are frequent purchases of traveller’s cheques, foreign-currency drafts, or money orders with cash by a client who has no obvious requirement for these “near cash” instruments;
- an account has many small cash deposits and a few large cash withdrawals;
- funds are deposited into multiple accounts, consolidated, and transferred abroad;
- there are multiple deposits by multiple third parties.

**Corporate Behaviour:**

- you are aware that the company or officers or employees of the company are the subject of a money-laundering investigation;
- a company shows activity that is inconsistent for the type of business;
- a client presents bills for deposit in denominations that are unusual for their type of business (e.g., a video arcade presenting $100s; a jeweller presenting $5s and $10s);
- a client’s financial statements are very different from similar businesses;
- large balances, inconsistent with the type of business, accumulate and are subsequently transferred to a foreign account in a non-cooperative country;
- there are deposits of sequentially numbered monetary instruments;
- letters-of-credit are used to move money between countries when such trade is inconsistent with the business;
- transactions are made with offshore banks with names similar to legitimate institutions;
- representatives avoid meeting providers of financial services;
- a client delays presenting corporate documents;
- activity in the account exceeds projections at the time of opening.
Chapter 14
Money Laundering Red Flags

A client showing any of these behaviours may be laundering money. Know your client.

- Is the client reluctant to provide the usual information?
- Does the client avoid contact with the branch?
- Can the client prove his or her identity with photo ID? Have you looked at it carefully?
- Does the client have a reason to use this branch or office? (live or work nearby?)
- Did the client arrive via a cold call?
- Does the client use cash when other means of payment might be expected?
- Does the client show more interest in redemption features than investment performance?
- Is a third party involved?
- Does the client make a large number of transactions?
- Does the client buy and sell for no discernible reason?
- Does the client enjoy a lifestyle apparently beyond his or her means?
- Are outside jurisdictions involved?
- Is foreign currency being used to buy an investment in Canada?
Appendix A

References

*Report of the Auditor General of Canada to the House of Commons, April 2003*
*Joint Money Laundering Study Group Guidance Notes, BBA Enterprises Ltd.*
*Report from the U.S. Treasury Department*
*FINTRAC Guidelines, March 24, 2003 and June 23, 2008*
*FATF, June 2003 and June 2008*
*www.moneylaundering.com, June 2003-06*
*KPMG*
*Office of the Superintendent of Financial Institutions Canada, May 23, 2002*
*www.just1world.com*
*www.subcontinent.com*
*www.laundryman.u-net.com*
*www.iirusa.com*