

**BRITISH COLUMBIA LOTTERY CORPORATION**

**BOARD MEETING JULY 23, 2010**

**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

Alison R. Manzer

**PERSONAL INFORMATION** h

[REDACTED]  
[REDACTED]

1. **What is money laundering and what is terrorist financing?**

2. **What does the law require:**

- Recording
- Reporting
- Identifying

And what is the law focussed on:

- Large cash transactions
- Suspicious transactions
- Dealing with the wrong people
- Identifying persons who are dealing for third parties

3. **Why casinos have been selected as a reporting entity**

**What is FINTRAC concerned about that is specific to casinos**

- The conversion of dollars into casino cheque
- The conversion of cash into casino issued goods
- The conversion of foreign dollars to Canadian dollars
- The conversion of cash to casino chips
- The conversion of cash to casino with the reconversion to cash

- 2 -

4. **What is unique about casinos - what are the inherent risks and needed controls:**

- The ability to deal with large volumes of cash on a basis that readily appears legitimate
- High drug related involvement
- Confirmed winnings as against stoppage of play to cash out
- Refining: small denomination currency converted to large denomination currency

5. **Board Responsibilities**

- Setting Policy
- Understanding Risks
- Determining and directing management strategies
- Receiving reporting
- Monitoring effectiveness
- Assuring appropriate independent oversight

6. **Current Hot Buttons at FINTRAC**

- Move to more risk based compliance programs
- Enhanced corporate governance and changing relationships to the CAMLO
- Enhanced responsibility and training requirements for CAMLOs
- Increased training and updating training for front line employees
- Auditor effectiveness testing
- Regular efficiency testing

7. **The Risks of Failure**

- Fines - administrative monetary fines can now be imposed and are increasingly being used by FINTRAC
- Deliberate failure to comply leads to criminal offences
- Reputational risk
- Regulator intervention

**PRIVILEGED**



- 3 -

**BRITISH COLUMBIA LOTTERY CORPORATION**

**BOARD MEETING JULY 23, 2010**

**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

**BACKGROUNDER – WHAT IS ANTI-MONEY  
LAUNDERING**

## 1. INTRODUCTION

### A. The Origins and Status of Canada's Anti-Money Laundering Efforts

Law enforcement agencies, around the world, have focussed in recent years on money laundering as a tool in crime prevention seeking greater sanctions and increased reporting by non-police entities in an attempt to discourage other criminal activity by depriving the perpetrators of the profits of the criminal activity.

The G-7 countries<sup>1</sup> established the Financial Action Task Force on Money Laundering (the "Task Force") in 1989 as a result of proposals put forward by the United States of America that were based on the idea that stopping the ability to benefit from the profit of crime would reduce criminal activity. The Task Force was an inter-governmental body consisting of 29 countries and two international organizations<sup>2</sup> whose purpose was to develop and promote policies to generate a global attack on money laundering. In 1990, the Task Force released a report with forty recommendations (the "Task Force Recommendations") which has formed the basis of anti-money laundering legislation in most countries which are members of the World Trade Organization.<sup>3</sup>

The Task Force Recommendations, among other things, recommended the adoption of local measures to enable law enforcement and other authorities to more readily confiscate laundered property by: (a) identifying, tracing and evaluating property which could be traced to criminal activity and therefore subject to confiscation; (b) carrying out provisional measures such

---

<sup>1</sup> The G-7 countries are: Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

<sup>2</sup> Financial Action Task Force, "*The Forty Recommendations*", released 1990, Task Force Recommendation, p. 1.

<sup>3</sup> *Ibid.*

- 2 -

as freezing and seizing property which is reasonably identified as relating to criminal activity to prevent any dealing, transfer or disposal of such property; and (c) taking investigative measures to improve the identification and reporting, of financial activity which utilizes proceeds of criminal activity.<sup>4</sup> Other of the Task Force Recommendations recommended passing legislation requiring financial institutions to: (a) take reasonable measures to obtain information about the true identity of the persons on whose behalf a banking or securities account is opened or financial transactions are conducted, and to determine whether the clients, or customers, are acting on their own behalf or for another;<sup>5</sup> (b) report financial transactions to competent authorities where there is suspicion that the funds may stem from a criminal activity;<sup>6</sup> and (c) develop programs to assist in countering money laundering, including (i) the development of internal policies, procedures and controls requiring the obtaining of customer information, identifying the source of funds and reporting suspicious transactions, (ii) the implementation of ongoing employee training programs to educate employees as to these requirements, and (iii) an audit process to test the effectiveness of the procedures developed.<sup>7</sup>

Canada was a signatory to the Task Force Recommendations and agreed to implement legislation effectively encompassing these recommendations. Canada first enacted legislation to respond to the Task Force money laundering recommendations on October 10, 1991, when *The Proceeds of Crime (Money Laundering) Act* (the “1991 Act”), was proclaimed in force. The 1991 Act operated together with the Canadian *Criminal Code*<sup>8</sup> provisions related to money

---

<sup>4</sup> *Ibid.*, p. 2.

<sup>5</sup> *Ibid.*, p. 3.

<sup>6</sup> *Ibid.*, p. 4.

<sup>7</sup> *Ibid.*, p. 5.

<sup>8</sup> R.S.C. 1985, c. C-46, Section 462.31 creates an offence to use, transfer, possess etc. any proceeds or property with intent to conceal or convert that property knowing or believing it is a result of enterprise crime or designated substance offence.

laundering, which made it a crime to further activity which was related to money laundering. Voluntary measures largely in keeping with the Task Force Recommendations were adopted by the Canadian chartered banks at that time. The 1991 Act and those additional measures remained in effect until June 19, 2000, when the 1991 Act was replaced by new legislation<sup>9</sup> having the same name but with significantly expanded scope (the “2000 Act”).

The 1991 Act was replaced by the 2000 Act for several reasons. The 1991 Act applied to only a limited number of the types of persons who it was perceived might be in a position to identify and report money laundering activity (for example, it applied to banks and securities dealers, but not accountants). It was believed that expansion of the types of persons required to report would enhance effectiveness. The lack of mandatory reporting requirements was also identified as a matter of concern. A further short coming was the lack of a central agency to collect information from reporting requirements and to coordinate anti-money laundering activities outside of law enforcement. Under the 2000 Act, Canada’s legislative requirements are now generally consistent with those in place in the rest of the G-7 countries, and particularly those in the United States, and includes measures to eliminate those perceived short comings of the 1991 Act.

The stated objects of the 2000 Act are to: (a) implement specific measures to detect and deter money laundering and to facilitate the investigation and prosecution of money laundering offences; (b) respond to the threat posed by organized crime by providing law enforcement officials with the information they need to deprive criminals of the proceeds of their criminal activities, while ensuring that appropriate safeguards are put in place to protect the privacy of

---

<sup>9</sup> *The Proceeds of Crime (Money Laundering) Act, S.C. 2000, c. 17.*

- 4 -

persons regarding personal information about themselves; and (c) assist in fulfilling Canada's international commitments to participate in the fight against trans-national crime, particularly money laundering. The objectives have been expanded by amendments enacted under the Anti-terrorism Act, in December, 2001, discussed later, which has added provisions intended to deter terrorist activity by cutting off the sources of funding to terrorist linked groups.

To supplement the legislative and regulatory requirements, FINTRAC issues guidelines as to expected standards for compliance. The guidelines do not have the force of law, and are not equivalent to regulations; they are designed to assist reporting entities to better understand and fulfill their obligations under the 2000 Act.

Bill C-7 of the Third Session, 37<sup>th</sup> Parliament, 52-53 Elizabeth II, 2004, *An Act to Amend Certain Acts of Canada and to Enact Measures for Implementing the Biological and Toxin Weapons Convention*, in order to enhance public safety, being originally Bill C-17 of the Second Session of the 37<sup>th</sup> Parliament, was adopted by the House of Commons at Third Reading on October 7, 2003, *The Public Safety Act*, 2002. At Part 19, Bill C-7, *The Public Safety Act*, 2002, amends the *Proceeds of Crime (Money Laundering) and Terrorism Financing Act* by extending the types of government databases from which the Financial Transactions and Report Analysis Centre of Canada may collect information which is considered relevant to money laundering or terrorist financing, this expansion allows FINTRAC access to national security databases. The amendments also authorized FINTRAC to exchange information related to compliance with Part I of the 2000 Act with regulators and supervisors of persons and entities that are subject to the 2000 Act. It is stated that this expansion of access to information, including the expanded requirement to provide information has been enacted in order to facilitate FINTRAC's



compliance responsibilities under the 2000 Act. The relevant sections of *The Public Safety Act* were proclaimed in force effective on June 1, 2004.

## B. What is Money Laundering?

The 2000 Act does not define “money laundering”, but rather defines “money laundering offences” by referencing definitions of offences under the *Criminal Code* and other statutes.<sup>10</sup> Money laundering includes offences under Section 462.31(1) of the *Criminal Code*, Section 9(2) of the *Controlled Drugs and Substances Act*,<sup>11</sup> Section 126.2(2) of the *Excise Act*,<sup>12</sup> Section 163.2(2) of the *Customs Act*<sup>13</sup> and Section 5(2) of the *Corruption of Public Officials Act*.<sup>14</sup> Money laundering is generally defined as “the process whereby ‘dirty money’, produced through criminal activity, is transformed into ‘clean money’ whose criminal origin is difficult to trace.”<sup>15</sup> Criminals do this by disguising sources, changing the form, or moving funds to a place or places where they are less likely to attract attention.

Section 7 of the 2000 Act requires reporting of any financial transaction which, in addition to appearing suspicious, is related to a money laundering offence. The definition of a money laundering offence is relatively narrow and includes only those offences which fall under the specific listing of criminal activities. If the suspected activity appears to be illegal but is not on the specific list of criminal activities it is not a money laundering offence.

---

<sup>10</sup> Section 2 of the 2000 Act. Section 462.31(1) of the *Criminal Code* says that: every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of: (a) the commission in Canada of an enterprise crime offence or a designated substance offence; or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted an enterprise crime offence or a designated substance offence.

<sup>11</sup> S.C. 1996, c. 19.

<sup>12</sup> R.S.C. 1985, c. E-14.

<sup>13</sup> R.S.C. 1985, c. 1 (2<sup>nd</sup> Supp.).

A money laundering offence specifically means any of the following offences:

- a) Section 462.31(1) of the *Criminal Code*. This is a section which provides that it is an offence for a person to deal with property with the intent to conceal or convert that property, knowing or believing that it was obtained or derived as a result of (i) an enterprise crime offence, which covers numerous listed offences associated with organized crime, or, (ii) a drug related offence.
- b) Section 9 of the *Controlled Drugs and Substances Act* which is similar to the *Criminal Code* provision noted, and which includes various activities relating to dealing in drugs, and includes being an accessory after the fact in counselling certain activities in relation to the offence.
- c) Section 126.2 of the *Excise Act*, which involves fraudulently marking tobacco or cigars to indicate that excise tax or customs duty have been paid, or selling unstamped manufactured tobacco products and cigars, effectively smuggling tobacco.
- d) Section 163.2 of the *Customs Act*, which relates to the evasion of customs duties on, or the smuggling of, spirits and tobacco products.
- e) Section 5 of the *Corruption of Foreign Public Officials Act*, which relates to the bribing of foreign public officials, other than payments to expedite acts of a routine nature.

---

<sup>14</sup> S.C. 1998, c. 34.

<sup>15</sup> See FINTRAC discussion at Guideline 1. [www.fintrac.gc.ca/en/static/faq.htm](http://www.fintrac.gc.ca/en/static/faq.htm)

Bill C-7 *The Public Safety Act*, 2002 has made amendments to the Criminal Code, at Section 183, expanding the definition of an "Offence", to include Section 462.31 Laundering Proceeds of Crime, and includes any other offence where there are reasonable grounds to believe there is a criminal organization offence or any other of "Terrorism Offence."

There are three stages which are generally involved in the money laundering process. First, there is placement, whereby the proceeds of crime are placed in the financial system. This might be done by breaking up large amounts of cash into less conspicuous sums that are then deposited in various bank accounts or other depositories. Alternatively, a series of monetary instruments such as cheques and money orders may be purchased and then deposited into accounts at other locations. The concept is that monetary instruments must be of a nature where the source and the holder of those instruments is not generally traceable. This requires that they be instruments of a money like quality, that is those which can be tendered and cash received or a monetary exchange completed by any person who tenders the instrument without identification and proof of entitlement. The monetary instrument must effectively be a direct substitute for the bills and coins which constitute cash.

Second, there is layering, whereby the proceeds of crime are converted into another form. This usually occurs through a series of complex layers of financial transactions that are created to disguise the source and ownership of funds and make it difficult to trace by any audit trail. For example, funds might be wired through a series of different accounts throughout the world. The use of a sequence of wire transfers of funds has been one of the most prevalent methods of carrying out money laundering. The ability to rapidly complete back-to-back transfers is perfect for the purpose of money laundering, which is to disguise the source, and ultimately the destination, of the funds which have been gained from criminal activity. Electronic transfers of

funds can result in cross-border transfers several times in a day, effectively, by the speed of transfer disguising the original source of the funds as it becomes increasingly difficult to trace the funds back to the origin.

Third, there is integration, which occurs when the laundered proceeds are placed back in the economy to create the perception of legitimacy. Typically, the funds are invested into real estate, luxury assets, or business ventures.<sup>16</sup> Initially, money laundering must involve investment into assets which can be rapidly reconverted to cash or will generate large cash returns. The essence of money laundering is the rapid turnover of the original cash, such that its source, arising from criminal activities, is disguised. Ultimately, when the source has been effectively blurred or disguised, the funds can be invested into assets which, generally, will be subsequently, resold. The essence of money laundering is not the use of the assets by the criminals benefiting, but the transfer of the assets in a manner which will hide them as having been proceeds of criminal activity and re-conversion to cash. The provisions of Section 462.31 of the Criminal Code, “Laundering Proceeds of Crime”, clearly establishes this by making the essence of the offence the intent to conceal or convert the proceeds or property arising from the named criminal acts.

Money launderers will use either a knowing participant (i.e. an active accomplice) or an unknowing participant to assist in furthering the money laundering scheme. Generally, the money launderer must make arrangements to convert cash which has been received from crime into an asset, generally a monetary instrument or a similar non-traceable asset or into an asset which will not attract attention as arising from proceeds of crime.

Money laundering requires that the end result of the series of activities is that the origin of the money, both as to the person and as to the activity, is effectively disguised. The money must appear, at the end of the money laundering chain, to be legitimate funds in the hands of the persons then using them for business or personal purposes. It is the rapid turnover, moving of the funds through a number of hands, which best disguises the original source of the monies as criminal. Those who have initiated the money laundering process did not wish to be associated with funds which in any manner can be traced back to the criminal activity. Although the funds may ultimately end up back in the hands of those involved in the criminal activity, at that point in time it is apparently legitimate funds which they are receiving.

### **C. Overview of the 2000 Act**

The 2000 Act is divided into five parts. Part 1 establishes mandatory reporting and record keeping measures to detect and deter money laundering, and to facilitate the investigation and prosecution of money laundering offences. Part 2 requires all persons or entities importing into or exporting from Canada currency and monetary instruments in excess of the prescribed amount to file a report with the “officers” in the named circumstances. “Officers” are customs officers and the Royal Canadian Mounted Police. Failure to report will result in seizure and forfeiture of the amount imported or exported, and various criminal sanctions. Part 3 establishes the new agency responsible to carry out the objects of Part 1 of the 2000 Act, the “Financial Transactions and Reports Analysis Centre of Canada” (“FINTRAC”). Part 4 authorizes the Governor in Council to make regulations for carrying out the purposes and provisions of the 2000 Act. Part 5 creates offences for failing to report suspicious financial transactions and for the inappropriate

---

<sup>16</sup> Financial Action Task Force, *Policy Brief* (July 1999), p. 2.

disclosure or use of information under the control of FINTRAC, and the sanctions for these offences.

The reporting and record keeping provisions of the 2000 Act apply to a wide variety of persons. They are listed in Section 5 of the 2000 Act, including domestic and foreign banks, co-operative credit societies, savings and credit unions, casinos, government departments and agencies, foreign exchange dealers, life insurance companies, life insurance brokers and agents and securities dealers. In addition, Section 5 provides that persons engaged in any “business, profession or activity” may be added to the list by designation by virtue of the power to make regulations under Section 73(1)(a) and (b) of the 2000 Act. The expansion of the list of reporting entities from financial institutions who traditionally deal in the transfer of funds, is designed to add persons who primarily, or as part of other services, engage in financial intermediation. This expanded list includes the life insurance industry, securities industry, accountants, and similar persons.

Only financial transactions are the subject matter of the recording and reporting requirements under the 2000 Act, however, “financial transaction” is not a defined term in the 2000 Act. It is expected that a financial transaction should be defined considering the basic scheme of the 2000 Act which deals with the receipt and transfer of cash and monetary instruments in specific circumstances. A financial transaction should in the ordinary sense involve the transfer of cash or monetary instruments. It is difficult to offer a precise definition of a concept which is not generally used in business or considered in law. No legal definition of “financial transaction” was found in the commonly used legal dictionaries, however, a “financial intermediary” was defined, generally as an entity that “advances the transfer of funds”. This arises both as a consequence of the context in which the expression is used, and as a consequence

- 11 -

of its use with the requirement that the financial transaction relate to a money laundering offence. The exchange of monies, or money equivalent, is necessarily required for an activity to amount to “money laundering”.

This definition is somewhat expanded by the *Anti-terrorism Act* amendments, which add to the offences which are subject to the 2000 Act transactions relating to the financing of terrorist activity. The *Anti-terrorism Act* amends the 2000 Act, renaming the 2000 Act to “The Proceeds of Crime (Money Laundering) and Terrorist Activity Financing Act” and including, along with money laundering offences, under effectively every section of the 2000 Act, a terrorist activity financing offence as if it was money laundering. A terrorist activity financing offence is an offence under Section 83.02 and 83.03 or 83.04 of the *Criminal Code*, or an offence under Section 83.12 of the *Criminal Code*, and includes threats to the security of Canada. The *Anti-terrorism Act* adds to all sections of the 2000 Act where reference is made to money laundering, by addition, the financing of terrorist activities.

“Terrorist activities financing offences” are defined in the new Section 83.01 of the *Criminal Code*, where it is given a fairly vague definition, and a significant number of offences are incorporated from other Canadian and international statutes. The general definition of terrorist activity is in section 83.01(b) which defines it as activity being undertaken for political, religious or ideological purposes with the purpose or intention of the activity to intimidate the public or a segment of the public. Comment has been made by several commentators that the definition of a “terrorist activity” is extremely vague and therefore the offence of “terrorist activity financing offence” is so broad as to be incapable of any reasonable definition.

There are provisions in criminal law under the Criminal Code, which create other compliance requirements for money laundering activity. The Criminal Code provides that a person cannot knowingly assist in the conduct of a criminal offence, including where related to money laundering activities.<sup>17</sup>

The destination of funds which are transferred or transformed in a financial transaction should also now be considered. The need to review the use and recipient of the funds relates to both money laundering and anti-terrorism reporting. If funds are designated to be transferred in bearer form or to be transferred to a third party where there is no apparent business relationship, then this may give rise to suspicion there is money laundering activity. If funds are coming from any source (even if openly disclosed and legitimate) and is directed to any one of a named list of terrorist linked organizations or countries, then anti-terrorism reporting requirements may be applicable.

Because the definitions of both “terrorist activity” and of “terrorist activity financing offences” are extremely vague, persons dealing with receipt and disbursement of funds will need to be aware of the prescribed list of suspected organizations. The only practical way of identifying terrorist financing activity, given the broad definition, is to use the list of suspected terrorist organizations which will be issued by authority of the Anti-terrorism Act. The organisations are updated periodically and are listed on the FINTRAC website, among other sites. Although reference to this list will not be definitive as to whether terrorist financing is involved, in general, a person receiving and disbursing funds will be in a poor position to determine whether they are being used for political, religious or ideologic activities, and will not

---

<sup>17</sup> Criminal Codes, Section 462.31 (as to dealing with proceeds of certain times), Section 21 (as to aiding and abetting).



be in a position to directly be aware of whether they are intended to be used for intimidation. It would appear that the only practical way of identifying terrorist activity financing is to use the list of suspected organizations.

The 2000 Act has been designed to rely extensively on regulation; the statute is very brief, broadly drafted and includes frequent reference to regulation. In addition, FINTRAC has issued guidelines which do not have the legal authority of statute or regulation but have been drafted to act as policy commentary to assist reporting entities in understanding the basics of the reporting requirements and of establishing and administering a compliance regime. FINTRAC has expressly stated that the guidelines are not intended to form law, however, as a practical matter, it will be necessary to ensure that there is compliance with the basic outline of the suggested compliance regime and reporting forms and to ensure there is recognition in any compliance program of the listed indicators set out in the guidelines as comprising elements of suspicious transactions.

The compliance recommendations of the guidelines are likely to constitute the base level of performance that will be expected under the 2000 Act. It would appear that the closest parallel to the nature and effect of the FINTRAC Guidelines would be the issuance of “Interpretation Bulletins” by the Canada Customs and Revenue Agency. Any court looking to determine whether someone has appropriately complied with the legislative requirements of the 2000 Act is likely to look to the guidelines, and would generally find that the guidelines represent not the entire scope of responsibility but at least the minimum scope of responsibility. In general, compliance will require at least the recognition of, and the education of employees as to, the contents of the guidelines. The guidelines will necessarily form a basic part of any compliance program, and recognition of the key indicators as to what constitutes a suspicious transaction and

terrorist financing activity, will need to be taken into account in any education and compliance program.

The money laundering legislation has a focus on individual responsibility for identification and reporting of money laundering. Effectively individuals, regardless of how they may be associated with the reporting entity, which have a connection with a reporting entity, are individually responsible for the recording and reporting as required under the legislation. Further, there is a very high level of responsibility placed upon persons who do not directly have the ability to control this recording and reporting, being senior officers and directors. Although due diligence is a defence, it will be necessary to meet very high standards as to education of employees, and as to the enunciation of corporate policy and the provision of effective means for recording. The difficulty of establishing personal responsibility for reporting, while maintaining obligation and liability at the employer level was addressed in the November 2003 amendments. However, Section 6, relating to employees or agents, was considerably expanded from the initial version and clarifies that it is the employer rather than the employee who is responsible for meeting requirements in the vast majority of cases.

#### **D. An Overview of the Regulations**

Three regulations, on a consolidated basis, have now been enacted pursuant to the 2000 Act. The most general is the “Regulation” which is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* - November 6, 2003, consolidated as SOR/2002-184, SOR/2002-413, SOR/2003-102 and SOR/2003-358, generally deals with large cash transactions, providing the necessary definitions and reporting requirements, and provides certain general provisions which supplement the terms of the 2000 Act. The regulation, the regulation provides

for some of the basic interpretative terms required to supplement the definitions and application of the 2000 Act. It also generally outlines the requirements for reporting of large cash transactions, including transfers made by electronic wire transfer. Amendments made subsequent to initial enactment of the regulation provides a useful illustration of the intentions of the regulation, specific issues which were identified subsequent to initial enactment.

The general provisions of the Regulation include basic provisions for currency conversion for the purposes of providing currency equivalents to Canadian funds, the definition of a “single transaction” for the purpose of providing for reporting of large cash transactions, a requirement that reporting be done in electronic format, and outlining the specific responsibilities of employees. The Regulation also enhances the requirements for delivery of information as to whether a transaction is being carried out for a third party.

The Regulation in general provides the detail of the reporting requirements for large cash transactions, including the electronic transfer of large amounts of cash. “Large amounts of cash” are defined as \$10,000, Canadian, in a “single transaction” (a single transaction is any transaction occurring over a twenty-four hour period). The contents and transactions triggering reporting requirements are specific by industry, with different types of reporting entities being required to report to different transactions and in somewhat different ways. Exceptions to reporting requirements are also included in the Regulation.

A number of the sections of the Regulation are provisions setting out when it is necessary to ascertain the identity of a person in relation to a financial transaction, again this is segregated and differentiated by industry type, and sets the basic standards and identification to be reviewed

in ascertaining identity. The Regulation also sets out the basic requirements for the retention of records.

The Regulation establishes the need to establish a compliance regime, which is discussed in considerably more detail elsewhere in these materials. The most significant portion of the Regulation is a specific outline of the required format of the reports to be provided relating to large cash transactions, including electronic transfers of funds. Schedules 1 to 6 of the Regulation provide for the specific contents of the reports required to be submitted.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulation* - November 6, 2003 consolidated SOR/2001-317, SOR/2002-185, SOR/2003-102 and SOR/2003-358, the “Suspicious Transaction Reporting Regulation”, establishes the requirements for suspicious transactions identification and reporting, which is outlined in significant detail elsewhere in these materials. The Suspicious Transaction Reporting Regulation outlines the activities which would give rise to the need to consider a transaction is suspicious and a report is required to be made. This regulation also establishes the basic nature of the reporting requirements for this type of transaction. The guidelines, as is discussed elsewhere, give more detail as to the expected details and contents of the required report and the judgements needed to be made in connection with suspicious transactions reporting.

The Suspicious Transaction Reporting Regulation provides the regulatory requirement as to how to send reports of suspicious transactions to FINTRAC, essentially by electronic reporting requirements. It also outlines the required information to be included in the reports. Schedule 1 to the Suspicious Transaction Reporting Regulation provides for the details of a suspicious transaction report and Schedule 2 the details of a terrorist group property report.

The *Cross Border Currency and Monetary Instruments Reporting Regulations* under the 2000 Act, November 6, 2003, consolidating SOR/2002-412 and SOR/2003-358, the “Cross Border Reporting Regulation”, provides the definitions clarifying the nature of monetary instruments that will require reporting on a cross border transfer. “Monetary instruments” for the purposes of this regulation mean instruments in bearer form or in such form as title to them passes on delivery, includes securities, including stocks, bonds, debentures and treasury bills, and negotiable instruments. The definition does not however apply to securities or negotiable instruments that bear restrictive endorsements, stamped for the purpose of clearing or made payable to a named person that have not been endorsed into bearer form. The definitions also include “conveyance”, “commercial passenger conveyance” and “non-commercial passenger conveyance” to identify the manner of transportation which may be subject to the Cross Border Reporting Regulation requirements.

The *Cross Border Currency and Monetary Instruments Reporting Regulations* establishes the basis for the reporting of importations and exportations of currency, at present involving transfers of \$10,000, Canadian, or more to and from Canada. Exceptions to the reporting requirements are then outlined, including specifically importation and exportation by the Bank of Canada, and if relating to shares excluding those with identifiable ownership. Retention of records requirements and penalties are also outlined. Schedules 1 to 3 of the *Cross Border Reporting Regulations* outlines the information required to be given by a person engaging in the import or export of currency from Canada.

- 2 -

**BRITISH COLUMBIA LOTTERY CORPORATION**

**BOARD MEETING JULY 23, 2010**

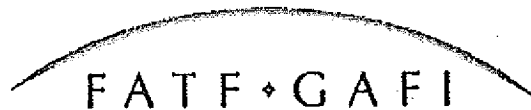
**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

**FAFT'S VIEW OF CASINOS AND AML/ATF**

**THE TACTICS THEY ARE SEEKING TO CONTROL**

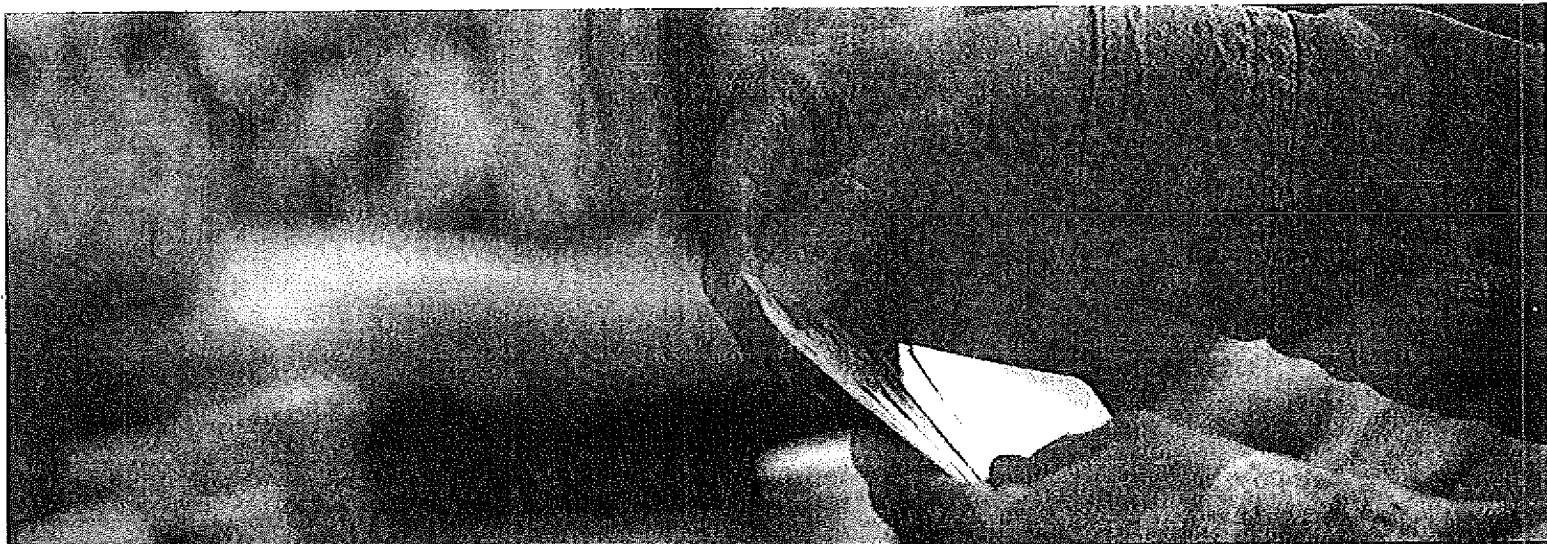


The Asia/Pacific Group on Money Laundering



Financial Action Task Force

Groupe d'action financière



*FATF Report*

# Vulnerabilities of Casinos and Gaming Sector

*March 2009*

## CHAPTER 2: MONEY LAUNDERING METHODOLOGIES AND INDICATORS

85. This chapter will identify and examine money laundering methods from known cases and draw out related indicators to support the detection of money laundering activity.

### Broad risks in casinos

86. Casinos are by definition non-financial institutions. As part of their operation casinos offer gambling for entertainment, but also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering. Most, if not all, casinos conduct financial activities akin to financial institutions including: accepting funds on account; conducting money exchange; conducting money transfers; foreign currency exchange; stored value services; debit card cashing facilities, cheque cashing; safety deposit boxes; etc. In many cases these financial services are available 24 hours a day.

87. It is the variety, frequency and volume of transactions that makes the casino sector particularly vulnerable to money laundering. Casinos are by nature a cash intensive business and the majority of transactions are cash based. During a single visit to a casino a customer may undertake one or many cash or electronic transactions, at either the 'buy in' stage, during play, or at the 'cash out' stage.<sup>13</sup> It is this routine exchange of cash for casino chips or plaques<sup>14</sup>, TITO tickets<sup>15</sup>, and certified cheques, as well as the provision of electronic transactions to and from casino deposit accounts, casinos in other jurisdictions and the movement of funds in and out of the financial sector, which makes casinos an attractive target for those attempting to launder money.

88. As this research is solely focused on casinos, the data collected is not wide enough to carry out statistical trend analysis. Chapter 3, however, does provide specific sector vulnerabilities and emerging issues as a start to this broader study. It is also recognised that methods and indicators are immediately useful to private sector organisations seeking to develop effective AML/CFT processes.

---

<sup>13</sup> The 'buy in' stage is when a customer enters a casino and purchases casino chips, tickets, or gaming machine credits in order to commence gambling. The 'cash out' stage is when a customer converts casino chips, tickets or gaming machine credits for cash, casino cheque, credits an account or transfers funds to another casino.

<sup>14</sup> The term 'casino chip' also refers to plaques and other wagering instruments provided by the casino.

<sup>15</sup> Ticket In/Ticket Out (TITO) is a gaming machine system that allows a gaming machine to accept either banknotes or tickets with a credit value printed on them (Ticket In) to commence play. TITO also prints tickets with a credit value when a player wishes to 'cash out' of the gaming machine (Ticket Out). The player can then redeem his/her ticket for cash at a cashier's desk, ticket redemption kiosk, or insert the ticket into another TITO machine and continue playing. A ticket redemption kiosk machine is a multifunctional device, connected to a gateway or kiosk server, that can perform a variety of financial transactions for customers, such as redeeming slot machine/video lottery tickets for currency, exchanging currency for currency (*i.e.*, breaking bills or paper money), redeeming player slot club points, purchasing slot machine vouchers (*i.e.*, tickets), and initiating electronic transfers of money to or from a wagering account including currency withdrawals from a casino ATM.



surveillance and security systems. This ensures public confidence in the gaming product, minimises opportunities for criminal activity and provides certainty of government revenue streams.

96. Criminal influence and exploitation of casinos appears to be both for possible money laundering, but also for recreation and in some cases enhancing their criminal endeavours outside the casino. Casinos have been noted as a place where criminals and organised crime figures like to socialise and particularly like to spend and launder their criminal proceeds.

97. Feedback from police also indicates that large casinos with sophisticated security and surveillance systems may be viewed by criminals as providing a safe haven to meet and associate in without fear for their personal safety.

98. Gaming venues attract ancillary criminal activities including loan sharking, vice and other crimes.

#### Box 4. Loan Sharking

Loan Sharking (also known as usury) is prevalent in casinos in a number of jurisdictions. Loan sharking is a crime that involves loaning money to individuals at an interest rate that is above a maximum legal rate, sometimes collected under blackmail or threats of violence. Loan sharks may be financed and supported by organised crime networks who are also involved in money laundering activities. A loan shark usually preys on individuals who are problem gamblers, struggling financially or, for some reason, are unwilling to seek credit from legal sources.

Persons in debt to loan sharks may be coerced into assisting with money laundering schemes in the casino.

#### Box 5. Credit card scam using the casino

A jurisdiction reported a credit card point scam where casino chips are purchased using credit cards. The chips are then cashed out and instead of crediting the credit card, casinos usually issue cash or a casino cheque. The balance on the credit card is eligible for consumer points. The balance on the credit card is paid back using the cash or cheque received from the casino. This method enabled large amounts of credit card points to be accumulated in a short period of time and can be used for merchandise purchases.

### Money laundering methods and techniques in Casinos

99. The money laundering methods outlined in this chapter are:

- Use of Casino Value Instruments (cash / casino chips / TTTO / gaming machine credits / cashier's orders / casino cheques / gift certificates / chip purchase vouchers / casino reward cards).
- Structuring / Refining.
- Use of Casino Accounts (credit accounts, markers<sup>17</sup>, foreign holding accounts) / facilities.
- Intentional losses.
- Winnings / intentional losses.

<sup>17</sup> Casino markers act as a credit line through a personal checking account, no transaction occurs, but are issued once a patron submits their checking account number and a cheque to the casino. The casino has the right to deposit the marker at any time but usually waits a few months to allow for customers to pay back the credit if the losses are high. Money launderers will pay back the debt with the proceeds of crime.

- Currency Exchange.
- Employee Complicity.
- Credit Cards / Debit Cards.
- False Documents.

100. Each method is illustrated by representative cases<sup>18</sup> and followed up with related indicators that can be used to detect suspicious or unusual transactions by casino owners and operators. The methods, cases and indicators have been generated from the following research material:<sup>19</sup>

- Sanitised case material from regulatory, law enforcement and security organisations.
- International case study and typology reports including FATF, APG and the Egmont Group.
- Open source research.

#### Casino value instruments

*Cash / Casino Chips / TITO / Gaming Machine Credits / Cashier's Orders / Casino Cheques / Gift Certificates / Chip Purchase Vouchers / Casino Reward Cards*

101. Casinos utilise various value instruments to facilitate gambling by their customers. The type and use of the value instruments listed above differs between casinos and is influenced by local regulation and casino operating structures. Casino value instruments are most often used for money laundering by converting illicit funds from one form to another.

102. Casino chips are the most common casino value instruments. Casino chips are issued by casinos and used in lieu of cash in gaming transactions between the house and players. Chips are round and marked with the denomination and name of the casino and are negotiable within the casino, or, in some cases, within casinos in the same group. Casinos may issue 'credit chips' which are different in colour and only used by patrons playing on credit. Casinos may issue 'dead chips' which are only used by *junket* patrons (*see section below on junkets*).

103. *Buying chips for cash or on account, then redeeming value by way of a casino cheque, bank draft or money transfer.* Launderers typically buy chips with cash or through their casino account. Chips bought on account may use a Chip Purchase Voucher (CPV) or similar value instrument. Repayment is then requested by a cheque, draft or transfer drawn on the casino's account. This method can be made more opaque by using a chain of casinos where the chips that were purchased with illicit cash are converted to credit, and transferred to another jurisdiction in which the casino chain has an establishment; the credit is then converted into in the form of a casino cheque at the second casino.

---

<sup>18</sup> The cases outlined are provided from jurisdictions contributing to the project research, and while some countries may appear to be over/under-represented in the cases, this is not an indicator of high or low levels of money laundering within that country, but merely a reflection of that government's willingness to share money laundering information to support global AML awareness.

<sup>19</sup> It is important to note that this chapter does not provide a description of all methods used to facilitate money laundering. It is limited to those methods that have been reported to FATF or APG and from cases that have been approved for use in the public forum.

104. Money launderers may hold the chips for a period of time, either using the chips to gamble in hopes of generating certifiable winnings or later redeeming the chips for cash/ cheque / transfer.

105. *Purchase of chips from 'clean' players at a higher price* – Money launderers may purchase chips from other money launderers or un-associated casino patrons with 'clean' backgrounds. This is done at a price greater than the chips' face value. This is referred to as *value tampering*.

106. *Casino cheques payable to cash* – in some jurisdictions, casinos allow winning cheques to be made payable to 'cash'. High-value casino cheques payable to cash have been observed in secondary circulation as bearer negotiable instruments and used as payment for goods or for reinvestment in criminal ventures, such as purchasing drugs. High-value casino cheques may originate from VIP rooms, which may provide alternative remittance services between player's home jurisdictions and the casino VIP room.

107. *Combining winnings and cash into casino cheques* – although few jurisdictions allow this, money launderers seek to add cash to casino winnings and then exchange the combined cash and winnings for a single cheque.

108. *Use of chips as currency in illegal transactions* – money launderers may retain casino chips to be used as currency to purchase drugs or other illegal goods. Carrying chips from a drug transaction may also contribute to an alibi for the predicate offence. The recipient of the chips will later cash them at the casino.

109. Casino chips to be used as currency may be taken across borders and exchanged for payment of an illegal enterprise then returned by the third parties and cashed at the issuing or honouring casino in amounts below a reporting threshold. Most jurisdictions do not list casino chips as money value instruments and therefore do not require Customs declaration.

110. In some jurisdictions, casino chips from one casino can be utilised in another associated casino. Cases showed that the money launderers will take advantage of this arrangement to avoid attracting attention to their activities at the one casino. This may take in another jurisdiction. To prevent this some jurisdictions require casinos to have casino-specific chips and do not allow inter-casino chip cashing.

111. *Purchase of large numbers of 'casino gift certificates'* – Cases have been detected of money launderers purchasing high value or numerous low value casino gift certificates which can be redeemed by 3<sup>rd</sup> parties. The certificates are then sold or given to other persons distancing the money launderer from the illicit funds.

112. *Purchase of casino reward cards* – Money launderers use illicit funds to purchase casino reward cards from legitimate customers paying them a premium above the value of the reward.

**Case 1: Casino used as preferred method to launder millions**

Offence:	Money Laundering
Jurisdiction:	Australia
Technique:	Chip purchase and cash out, claiming credits as jackpot wins, playing games with low return and high win.
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Information identified alleged money launderers using the casino as a preferred method of laundering millions of dollars accumulated from criminal activities. The methods used to launder the money included purchasing and cashing out chips without playing, putting funds through slot machines and claiming credits as a jackpot win and playing games with low returns but higher chances of winning. The same group were also utilising bank

**Case 6. Casino reward cards traded for gold coins**

Offence: Money Laundering  
Jurisdiction: United States  
Technique: Purchase casino reward cards from legitimate customers  
Mechanism: Casino  
Instrument: Casino reward cards, gold coins

A suspect purchased casino reward cards from legitimate customers at a US casino. The cards increase in value with each casino visit and with each gambling session. The cards were purchased with illicit funds and were then traded for gold coins at the casino's store. An employee at the store was an accomplice in the laundering scheme.

**Case 7. Embezzled money laundered through casino**

Offence: Money Laundering  
Jurisdiction: United States  
Technique: Purchase and cash out with little or no gaming activity  
Mechanism: Casino  
Instrument: Casino chips

A lawyer was sentenced in New Jersey for embezzling more than USD 500 000 and laundering USD 250 000 of it through an Atlantic City casino. The defendant wire transferred USD 250 000 to the casino and arrived at the casino later the same day to launder the funds. He purchased casino chips and gambled for an hour on a roulette table losing USD 10 000. He then cashed out the remaining USD 240 000 into currency and left the casino.

**Case 8. Embezzled money laundered through casino**

Offence: Money Laundering  
Jurisdiction: Spain  
Technique: Purchase and cash out with little or no gaming activity, casino cheques in the name of 3rd parties  
Mechanism: Casino  
Instrument: Casino chips

Different people entered separately in a casino and bought chips. After playing minor amounts of chips they tried to change chips and requested a cheque paid to the name of a third person. They tried to do the same operation with different people and lower amounts one day later, which raised suspicion of casino operators.

**Indicators of ML using casino value instruments**

- Inserting funds into gaming machines and immediately claiming those funds as credits.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.
- Noticeable spending/betting pattern changes.
- Customers frequently inserting substantial amounts of banknotes in gaming machines that have high payout percentages and do not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
- Frequent even-money wagering when conducted by a pair of betters covering both sides of an even bet (e.g., in roulette, baccarat/mini-baccarat, or craps).
- Customer's intention to win is absent or secondary.

- Two or more customers frequently wagering against one another on even-money games.
- Customer in possession of large amounts of coinage or bills.
- Customer befriending/attempting to befriend casino employees.
- Purchasing and cashing out casino chips with little or no gaming activity.
- Customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single cheque.
- Multiple cheques being requested or drawn on account.
- High volume of transactions within a short period.
- Multiple chip cash outs on the same day.
- Structuring of chip/cheque transactions.
- Chip cash out is same/similar to chip purchase.
- Requests for credit transfers to other casinos.
- Use of multiple names to conduct similar activity.
- Use of third parties to purchase casino chips.
- Use of credit cards to purchase casino chips.
- Use of personal cheques, bank cheques and traveller's cheques to purchase casino chips.
- Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade.
- Customer purchases chips and leaves casino shortly after.
- CPV, TITO, ticket or voucher dated prior to date of redemption.
- Large chip purchases.
- Frequent purchase of casino gift certificates.
- Unexplained income inconsistent with financial situation/customer profile.
- Supposed winnings do not correspond with recorded winnings.
- Dramatic or rapid increase in size and frequency of transactions for regular account holder.
- Detection of chips brought into the casino.

## Structuring

113. Structuring or ‘smurfing’ involves the distribution of a large amount of cash into a number of smaller transactions in order to minimise suspicion and evade threshold reporting requirements. Common methods of structuring include:

- Regularly depositing or transacting similar amounts of cash, which are below a country’s reporting disclosure limit.
- The use of third parties to undertake transactions using single or multiple accounts.
- Using cheques from multiple financial institutions or branches of a financial institution to ‘buy in’ while the amount of each cheque is below the reporting threshold.
- Utilising shift changes to systematically ‘cash in’ chips or other value instruments to avoid threshold reporting.
- Regularly switching gaming tables, gaming rooms, junkets or casinos within a chain when the wagering amounts are approaching the reporting threshold.
- Requesting the division of winnings or prize money, which exceeds the reporting threshold, to be broken down into cash and chips below the reporting threshold in order to exchange it at the cashier’s desk.

114. While money launderers will often structure their transactions to avoid financial institutions filing reports to authorities, it has been found that some money launderers using casinos have the opposite strategy and seek to trigger a cash transaction report to further authenticate a transaction.

### Case 9. Using reporting thresholds to legitimise suspicious transactions

Offence:	Money laundering
Jurisdiction:	United States
Technique:	Use of third parties, triggering transaction reports to legitimise suspicious transactions
Mechanism:	Casino
Instrument:	Casino chips, casino cheque

A number of persons purchased chips with illicit cash in amounts below the CTR threshold, but then passed the chips to one individual who cashed out, receiving a casino cheque and triggering the filing of a CTRC that gave the appearance of further authenticating the transaction. Over a twelve-month period, one individual was named in casino CTRCs reporting USD\$1.1million paid out, but was not named in a single CTRC for cash taken in.

## Refining

### *Exchanging low denomination for high denomination currency*

115. Individual launderers or organised groups use casino services to refine large amounts of low denomination bank notes into more manageable high denomination notes. Some countries note this as being associated with drug dealers who accumulate large amounts of small denomination bills from drug sales. In cases of groups, they may seek to refine money by dividing it amongst the group before entering the casino. The group enter the casino, individually refine their portion of the money and meet again outside the casino to assemble the total amount. The refining techniques most commonly identified are listed below:

116. **Refining using the cashier's desk** – money launderers exchange coins or small denomination bills for larger denomination bills at the cashier's desk.

117. **Refining using 'note acceptors' or gaming machines that accept cash** – Most casinos with gaming machines have 'note acceptors'. Money launderers will feed currency notes into the machine to accumulate credit with little or no play before redeeming the credits. As the amount can be quite large, it requires a 'ticket' or similar document provided by the slot attendant as proof to enable the exchange for cash or cheque at the casino cashier's desk. Gaming machines, Video Lottery Terminals (VLTs) and Ticket In/ Ticket Out (TITO) machines are used to refine currency. Gaming machines, TITO machines and VLTs are fed large sums of low denomination cash. Launderers redeem credits with minimal play. The ticket is then cashed at the cashier's desk, ticket redemption kiosk, for high denomination bills.

118. **Use of casino account for refining** – launderers pay low denomination cash into their casino accounts and withdrawn funds with cash of higher denominations.

**Case 10. Refining low denomination notes**

Jurisdiction:	Spain
Technique:	Refining, Use of third parties
Mechanism:	Casino
Instrument:	Cash, casino chips, remittance arrangement

A group of three foreign people entered separately in a casino and bought chips, paying with low denomination notes. They didn't play any game, and after they changed the chips that they had bought trying to obtain high denomination notes.

**Case 11. Drug proceeds converted into casino chips by third parties**

Offence:	Drug Importation
Jurisdiction:	Australia, Vietnam
Technique:	Use of third parties
Mechanism:	Casino, remittance agent
Instrument:	Casino chips, remittance arrangement

A person was involved in the importation and distribution of heroin into Australia from Vietnam. The person gambled a large proportion of the proceeds at casinos and used third parties to purchase gaming chips on his behalf. Reports from the casino noted multiple chip cash outs on the same day, with some of these transactions being structured to avoid the AUD 10 000 reporting threshold.

Further investigations noted that he would send large cash payments to various entities in Vietnam through a remittance dealer. The remittance dealer was a trusted associate of the person and had been non-compliant with his reporting obligations.

**Indicators of ML using structuring/refining methods**

- Activity was inconsistent with the customer's profile.
- Associations with multiple accounts under multiple names.
- Use of multiple names to conduct similar activity.
- Depositing multiple amounts of cash and receiving multiple cheques drawn on that account.
- Multiple individuals sending funds to the one beneficiary.
- Cheque issued to a family member of the person.

- Third party presents for all transactions but does not participate in the actual transaction.
- Transferring funds into third party accounts.
- Transactions on casino accounts conducted by persons other than the account holder.
- Use of third parties to undertake structuring of deposits and wire transfers.
- Use of a remittance dealer / junket operators to deposit or withdraw cash.
- Use of third parties to purchase gaming chips.
- Use of third party to conduct wagering.
- Cash handed to third party after cash out.
- High volume of transactions within a short period.
- Purchasing and cashing out casino chips with no gaming activity.
- Exchanging large quantities of quarters from non-gaming proceeds for paper currency.
- Frequent betting transactions just under thresholds.
- Frequent 'buy in' and 'cash out' transactions just under thresholds.
- Cash deposits / withdrawals just under thresholds.
- Wire transfers / currency exchanges just under thresholds.
- Requests for winnings in separate cash or chip amounts under reporting threshold.
- Cashing in winnings in a multiple combination of chips, cheque and cash.
- Customer conducts several transactions under reporting thresholds over several shift changes.
- Customer moving from table to table or room to room before the wagering amounts reach the reporting threshold.
- Opening a casino account or purchasing casino chips with small denominations bills.
- Customer gambling with large amounts of small denomination bills.
- Currency exchange from small denomination bills to larger denomination bills.
- Frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.
- Dramatic or rapid increase in frequency of currency transactions for regular account holders.
- Noticeable spending/betting pattern changes.



- Insert banknotes in electronic gaming devices with no gaming activity, press the “cash out” button which generates a TITO ticket, and redeem ticket at cashier’s desk or ticket redemption kiosk machine.

## Casino accounts & facilities

### *Credit accounts / Markers / Foreign holding accounts / safe deposit boxes*

119. Casino accounts provide criminals further opportunities to attempt to laundering crime proceeds. Many casinos offer deposit accounts and lines of credit with less scrutiny and CDD requirements than financial institutions. The frequent movement of funds between financial institutions and casinos, or between casino accounts held in different casinos may be vulnerable for money laundering. Many casinos offer private safe deposit boxes, particularly to VIP/’high roller’ customers.

120. *Cashing cheques into casino accounts* – Some casinos allow customers to cash various types of cheques and use the proceeds for gambling. Cheques could be signed over to the bearer by the cheque recipient. In the cases studied, proceeds from illegal activity were initially used to draw these cheques with the aim of avoiding the casino’s suspicion.

121. *Deposits into casino accounts by wire transfers or bank cashier’s cheque* – funds are deposited by wire transfer of bank cheque, then cashed out or moved to other accounts with minimal or no gambling activity.

122. Cashed out funds are stored in casino safety deposit boxes or held in the form of safekeeping markers and then cashed out.

123. *Foreign Holding Accounts (FHAs)* – Accounts that are held in one jurisdiction by the casino, but the funds can be used to gamble in another jurisdiction under the same casino group. For example, funds held in a FHA account in Macao, China can be used to gamble at a casino in Las Vegas. The money held in the account does not physically leave the country and is not subject to cash declarations. Large casinos may operate marketing offices in jurisdictions other than where the casino is located. Patrons are able to pay in funds to their casino account to be played when they travel to the casino without sending a cross-border wire transfer. *See the Junkets section for further details.*

124. *Wire transfers from Casas de Cambio to casino accounts* – Casas de Cambio in another jurisdiction may wire transfer funds to casinos. As an example, in the United States Casas de Cambio businesses are concentrated along the southwest border, with over 1 000 located along the border from California to Texas. These businesses are generally unregistered and do not comply with AML reporting requirements, and are suspected of being a significant money laundering risk. These *Casas de Cambio* have corresponding bank accounts which allow them wire transfer of large amounts of cash to casinos and other institutions throughout the world.

125. *Safety deposit boxes* – A number of casinos offer safety deposit boxes to patrons, in particular to ‘high roller’ patrons in VIP rooms. These present a risk due to the lack of transparency with the use of such boxes and the possibility for 3<sup>rd</sup> parties to be given access to safety deposit boxes via a password or key, to facilitate financial transactions. Very few jurisdictions regulate the safety deposit boxes in casinos.

**Vulnerabilities of Casinos and Gaming Sector – March 2009**

defendant. Buyer 2 sent another USD 100 000 certified cheque.

- Buyer 3 deposited USD 600 000 cheque into an account against which a cheque in the amount of USD 180 000 was made payable to the same casino. Accomplice then tried to withdraw all of the money, but the casino refused and permitted only a USD 50 000 withdraw. Accomplice then gambled with some funds and won USD 15 000. Casino then permitted withdrawal of funds and allowed accomplice to cash out.

**Case 15. Loan-sharking profits laundered at casino**

Offence:	Money laundering
Jurisdiction:	Japan, United States
Technique:	Purchase and cash out with little or no gaming activity
Mechanism:	Casino
Instrument:	Cash, casino chips, casino credit

A boss of a loan-shark business ordered his associates to convert the profits from Yen into US currency using false names. These funds were then distributed to numerous bank accounts around the world. Some of the money was also invested with a foreign agent of a Las Vegas casino, who kept the money in a safety deposit box in the head office of a major Tokyo bank. Against the security of this money, the boss played frequently at Las Vegas casinos as a VIP player. Although he gambled in the VIP room, he would never place big bets and, after minimal play, would frequently cash in his chips for US currency. His associated were also circulated through a number of Las Vegas casinos cashing in chips worth USD 2 000 or less.

**Indicators of ML using casino accounts:**

- Frequent deposits of cash, cheques, bank cheques, wire transfers into casino account.
- Funds withdrawn from account shortly after being deposited.
- Significant account activity within a short period of time.
- Account activity with little or no gambling activity.
- Casino account transactions conducted by persons other than the account holder.
- Funds credited into account from country of concern.
- Large amounts of cash deposited from unexplained sources.
- Associations with multiple accounts under multiple names.
- Transfer of funds from/to a foreign casino/bank account.
- Transfer of funds into third party accounts.
- Funds transferred from casino account to a charity fund.
- Multiple individuals transferring funds to a single beneficiary.
- Structuring of deposits / withdrawals or wire transfers.
- Using third parties to undertake wire transfers and structuring of deposits.
- Use of an intermediary to make large cash deposits.

- Use of gatekeepers, e.g. accountants and lawyers to undertake transactions.
- Use of multiple names to conduct similar activity.
- Use of casino account as a savings account.
- Activity is inconsistent with the customer's profile.
- Unexplained income inconsistent with financial situation.
- Transfers with no apparent business or lawful purpose.
- Transfer of company accounts to casino accounts.
- Use of false and stolen identities to open and operate casino accounts.
- Customer name and name of account do not match.
- U-turn transactions occurring with funds being transferred out of country and then portions of those funds being returned.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.
- Requests for casino accounts from Politically Exposed Persons (PEPs).

### Winnings

126. *Use of illicit funds to gamble* – this is the simplest method of gambling illicit funds in the home hopes of generating certifiable winnings. One way to do this is to play gaming machines or other games with low payout higher win/loss ratios. The money launderer will then receive a casino cheque for the total amount of credits remaining on the machine plus the jackpot.

127. Some jurisdictions require casinos to endorse the casino cheques from jackpots as 'winnings' in order to differentiate it from a cheque generated as a result of cashing out large amounts of machine credits.

128. *Buying winnings from legitimate customers* - is another method used across the gaming sector. Money launderers will approach customers and offer them cash at a premium above their winnings. This was evident with customers who had won gaming machine jackpots, or accumulated a large amount in casino chips from winnings on table games, or customers that had won in other forms of betting offered by some casinos, such as electronic lotteries, horse racing and sports betting.

129. *Parallel Even money betting* – In cases where gambling is undertaken to launder funds, it is usually on low odds, low risk games such as the even money options on roulette. This would involve two or more persons placing opposite equivalent bets on even money wagers in the same game. As an example Person A places USD 1 400 on red, while Person B places USD 1 400 on black in a game of roulette. The bet is 'double or nothing'. In this case the winning party would win just under USD 3 000 which could be paid out with a 'winnings' cheque and the size of the win would not trigger CDD requirements at the roulette table.

130. **Betting against associates / intentional losses** – This is also the case in games where which provide money launderers the option to bet against an associate so that in most cases one party will win. These ‘intentional losses’ where money launderers are intentionally losing to one of the party, who is able to receive a casino issued cheque or wire transfer of ‘legitimate’ winnings.

**Case 16. Overseas nationals purchase winning jackpots with illegal proceeds**

Offence:	Drug trafficking & money laundering
Jurisdiction:	Spain
Technique:	Buying winning lottery tickets
Mechanism:	Lotteries
Instrument:	Winning jackpots, cash

Investigations in Spain related, mainly with drug trafficking, corruption and tax fraud identified the use of gaming to launder funds. The technique consisted of buying winning lottery tickets from legitimate gamblers.

**Case 17. Overseas nationals purchase winning jackpots with illegal proceeds**

Offence:	Money Laundering
Jurisdiction:	Australia
Technique:	Buying winning jackpots
Mechanism:	Gambling clubs
Instrument:	Winning jackpots, casino cheques

A group of overseas nationals were identified buying winning jackpots from other persons at various clubs in Sydney, Australia. The suspects deposited approximately AUD 1.7 million in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of the funds used to buy winning jackpots was suspected to be from illegal means.

**Indicators of ML using winnings:**

- Frequent claims for winning jackpots.
- Frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash.
- Customers watching/hanging around jackpots sites but not participating in gambling.
- Multiple chip cash outs on the same day.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.
- Purchasing and cashing out casino chips with no gaming activity.
- Requests for winnings in separate cash or chip amounts under reporting threshold.
- Frequent ‘cash out’ transactions without corresponding ‘buy in’ transactions.
- Cashing in winnings in a multiple combination of chips, cheque and cash.

## Currency exchange

131. Given the popularity of casino-based tourism and the willingness of customers to travel to legal casino sectors, most casinos offer currency exchange services.

132. *Conversion of large sums of foreign currency* – launderers may use large, one-off, or frequent foreign currency exchanges or deposits of a foreign currency. This may not appear suspicious in jurisdictions with high numbers of foreign players.

133. Reported cases indicate that criminals involved in the distribution and supply illegal drugs are using casino currency exchange services to convert their criminal proceeds from one currency to another, in order to alter its original form.

134. Individuals and groups will also employ structuring methods to undertake currency exchanges without triggering threshold reports. They will use multiple casino locations and once the currencies are exchanged, will meet again to assemble the total amount.

135. *Casino play is undertaken in foreign currency* – in some poorly regulated jurisdiction, customers are able to purchase chips directly in a foreign currency (for example in Nepal with USD and Indian Rupees).

### Case 18. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Money Laundering
Jurisdiction:	Spain
Technique:	Currency conversion
Mechanism:	Casino
Instrument:	Cash – various currencies

A group of foreign people entered separately in a casino to buy casino chips using Swiss Francs (CHF). The purpose of the syndicate was not to play in the casino, but to redeem the chips in Euros. The casino detected the operations, stopped the transactions and filed an STR.

### Indicators of ML using currency exchange:

- Bank drafts/cheques cashed in for foreign currency, e.g. Euros, USD.
- Multiple currency exchanges.
- Dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders.
- Currency exchange for no reasonable purpose.
- Currency exchanges with low denomination bills for high denomination bills.
- Currency exchanges carried out by third parties.
- Large, one-off, or frequent currency exchanges for customers not known to the casino.
- Requests for casino cheques from foreign currency.
- Currency exchanges with little or no gambling activity.

- Structured currency exchanges.

### Employee complicity

136. Employee complicity is another method in which third parties are used to facilitate money laundering. Individual employees or organised groups comprising of staff from different departments conspire with customers to enable money laundering transactions to go undetected. Methods include:

- Failing to file suspicious transaction reports or threshold transaction reports.
- Destroying documents/transactions reports related to due diligence or reporting processes.
- Falsifying player ratings and other gambling records to justify the accumulation of casino chips/gaming machine credits.

137. Some jurisdictions have raised vulnerabilities from providers of gaming equipment and machines as well as contractors that supply goods with a potential to impact on the integrity of the operation. Major contracts can be an avenue for criminal exploitation of the operation (e.g. through corrupt purchasing and under supply of contract goods). Criminals will try to exploit gaming equipment and associated computer systems to achieve theft and money laundering in the casino.

#### Case 19. Suspected falsified player ratings

Offence:	Money laundering
Jurisdiction:	Australia
Technique:	Falsifying player ratings to legitimise criminal proceeds
Mechanism:	Casino
Instrument:	Cash

An ex-employee of one casino was investigated by Australian authorities after he was able to purchase a house for cash. The family of this person is alleged to be involved in illegal drug activity and it was suspected that the funds used to purchase the house were provided by his family. The person, however, was able to show 'player ratings' from a second casino to show how he had turned NZD 20 000 into over NZD 400 000 in two weeks. It is suspected that an accomplice at the second casino falsified these 'player ratings', but this was not able to be proven.

#### Case 20. Back door corruption

Offence:	Money laundering
Jurisdiction:	United States (Indian casino)
Technique:	Casino staff bribed to facilitate money laundering
Mechanism:	Casino
Instrument:	Cash, jackpots

In Florida drug proceeds were laundered through gaming machines. Some gaming machines are controlled by software that have certain override features, or 'back doors' that give key casino staff the ability to force jackpot payouts. In Florida drug dealers bribed casino staff who accessed the override features and rigged a number of machines for the drug dealers to play and win jackpots from their drug proceeds.

### Indicators of employee complicity:

- Contact between patrons and casino staff outside of the casino.
- Supposed winnings do not correspond with recorded winnings.

- Dramatic or rapid increases in size and frequency of currency transactions for regular account holders.
- Large sums of cash from unexplained sources.
- Large sums credited into accounts from other jurisdictions or countries of concern.<sup>20</sup>
- Associations with multiple accounts under multiple names.
- Transactions on casino accounts conducted by persons other than the account holder.
- Deposits into casino account using multiple methods.
- Cheques issued to a family member of the person.
- Multiple individuals sending funds to a single beneficiary.
- Third party presents for all transactions but does not participate in the actual transaction.
- Transferring funds into third party accounts.
- Use of third parties to undertake wire transfers.
- Use of an intermediary to make large cash deposits.
- Use of gatekeepers, e.g. accountants and lawyers to undertake transactions
- U-turn transactions occurring with funds being transferred out of a country and then portions of those funds being returned.
- Use of remittance agents to move funds across borders.
- Use of third parties to purchase gaming chips.
- Use of third party to conduct wagering.
- Wire transfers from third parties in tax haven countries.
- Junket tours where funds can be concealed amongst the pool for the group.
- Cash handed to third party after cash out.

#### Credit cards / debit cards

138. *Laundering proceeds from stolen credit cards* – Casinos in some jurisdictions allow customers to purchase casino chips using credit cards. In cases where the cards are not stolen or fraudulently obtained, the outstanding credit card balances are paid by the card holder at the bank using the illicit funds.

---

20. TBD.

139. **Credit cards** – criminals use of credit cards provides an opportunity for authorities to follow the money trail more readily.

**Case 21: Debit card scheme**

Offence:	Fraud, money laundering
Jurisdiction:	Belgium
Technique:	Use of credit cards to conduct money laundering transactions
Mechanism:	Casino
Instrument:	Credit cards, casino chips.

A person residing in Belgium, originally from Eastern Europe, visited a casino on the Belgian coast on two occasions and bought gaming chips for a total value of EUR 400 000 paid for in cash and with credit cards. The casino reported these transactions to the FIU.

Based on the history of gambler's purchases using credit cards it was determined that his account had been extremely active; it had been inundated with various transfers from companies and, in particular, with many cash deposits. The spouse of the party concerned ran a business in Belgium and maintained underworld links with organised crime from Central and Eastern Europe. The party concerned received citizens from those countries at his personal address and that financial transactions were carried out in cash. The gambler was in frequent contact with a person who was being investigated for the laundering of money deriving from organised crime.

140. **Debit cards** – are another value instrument used to conduct fraud and money laundering crimes. In the case below, criminals would join a casino and use their debit card to draw up to the casino's maximum standard daily limit and purchase casino chips. The subjects either do not put any funds at risk or there would be minimal play. The subjects would then typically cash out. In similar cases, plaques would be passed to an associate for play. Sometimes all the funds would be put at risk. The major operators quickly identified this trend and put risk control mechanisms in place to limit the initial debit card transaction to a much lower limit for first time transactions in high risk situations.

**Case 22: Debit card scheme**

Offence:	Fraud, money laundering
Jurisdiction:	United Kingdom
Technique:	Use of debit cards to conduct money laundering transactions
Mechanism:	Casino
Instrument:	Casino plaques

An existing member of a casino introduced a number of people over a period of time. Suspicious was raised as the new members were completing debit card transactions to the maximum limit and receiving gaming plaques in exchange, which in turn were passed to the existing member. Most of the new members never returned to the casino after the initial visit. The nationalities of the new members varied widely, but all are believed to have recently arrived from foreign jurisdictions. The transactions varied from GBP 1 000 to 7 000. Some money was put at risk and lost by the existing main member.

**Indicators of ML using credit/debit cards:**

- Purchasing casino chips using credit card.
- Purchasing casino chips using debit card.
- Purchasing and cashing out casino chips/plaques with no gaming activity.
- Customer purchases chips and leaves casino shortly after.
- Use of stolen or fraudulently obtained credit card.



- Use of multiple credit/debit cards to purchase casino chips.
- Use of third parties to purchase chips using credit/debit card.
- Structuring of credit card transactions.
- Conducting debit card transactions up to the maximum limit.
- Chip cash out is same/similar to chip purchase.
- Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade.

#### False documents

141. As with financial institutions, money launderers use false documentation to disguise the origin of criminal proceeds and to protect the identity of those laundering the proceeds.

142. *False identification documents* – often used to conduct financial transactions at the casino, open casino accounts, undertake gambling transactions and redeem winnings.


#### Case 23. Money launderer uses third parties and false identities to launder drug proceeds

Offence:	Money laundering, identity fraud
Jurisdiction:	United States
Technique:	Use of 3rd parties and false identities to structure gambling transactions
Mechanism:	Casino
Instrument:	Cash, casino chips

A Person of Interest (POI) of a drug trafficking organisation, utilising both the money he was paid for his services and the large sums of money put into his possession to be laundered, elevated his previously modest gambling practices to that of a high-roller. The person would recruit third parties at the casino to purchase, or cash in, chips for him, paying them a nominal fee to do so. After gambling, he would cash some of these third-party purchased chips back out again, claiming they were his gambling winnings. According to the CTRs a USD 313 000 discrepancy was found to exist between chip purchases and cash out. Twenty-four of the CTRCs recording his activities revealed the use of aliases and multiple social security numbers. On numerous other CTRCs he had refused to provide a social security number.

#### Indicators of ML using false documents and counterfeit currency:

- Associations with multiple accounts under multiple names.
- Purchasing chips or undertaking cash transaction and immediately leaves casino.
- Transferring funds into third party accounts.
- Use of multiple names to conduct similar activity.
- Use of altered/fraudulent or stolen identification to conceal identity.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.

 Vulnerabilities of Casinos and Gaming Sector – March 2009

---

- Inconsistent identity information presented.
- Refusal to provide identification / false identification or Social Security numbers.
- Using false or multiple Social Security numbers.
- Refusing to provide required identification.

## Terrorist Financing

191. Throughout this report, the term money laundering has also referred to terrorist financing. It should be pointed out that the research undertaken failed to find any reported cases of terrorist financing in the casino sector. This may be due to the characteristics of terrorist financing that make it difficult to detect, characteristics such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

192. It would be a mistake, however, to assume that terrorist financing has not and could not occur in the casino sector. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing and includes the methods and indicators described in Chapter 2, though these indicators would only support suspicious activity, and may not be identified as or connected to terrorist financing once further investigation is undertaken.

193. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which may not be the type of transactions that are reflected in the indicators for money laundering. Where funds are from legal sources, it is even more difficult to determine if they could be used for terrorist purposes. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimate sources, transactions related to terrorist financing may not exhibit the same traits as conventional money laundering.

194. The ability of casinos to detect and identify potential terrorist financing transactions without guidance on terrorist financing typologies or unless acting on specific intelligence provided by the authorities is significantly more challenging than is the case for potential money laundering and other suspicious activity.

195. Detection efforts, absent specific national guidance and typologies, are likely to be based on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering). Particular individuals, organisations or countries may be the subject of terrorist financing sanctions, in a particular country. In such cases a listing of individuals, organisations or countries to which sanctions apply and the obligations on casinos to comply with those sanctions are decided by individual countries.

**BRITISH COLUMBIA LOTTERY CORPORATION**

**BOARD MEETING JULY 23, 2010**

**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

**FINTRAC'S VIEW OF CASINOS AND AML/ATF**

This is no game

# The game has changed 2007

Law before June 23	Law starting June 23
Report suspicious transactions when the transactions are completed	Report suspicious transactions when the transactions are completed or attempted
Retain a foreign currency exchange transaction ticket for sums of \$3,000 or more	Retain a foreign currency transaction ticket for any foreign currency exchange transaction of any amount
Date of birth of individual clients: not required	Date of birth of individual clients: required
	<b>Changes to the compliance regime</b> <ul style="list-style-type: none"><li>• Develop and keep up to date written compliance policies and procedure</li><li>• Document risk related to money laundering and terrorist activity financing</li><li>• Develop an ongoing compliance training program</li><li>• Complete anti-money laundering/anti-terrorist funding (AML/ATF) policy and procedures compliance review every two years by either an internal or external auditor</li></ul>

These are only the highlights. There is much more.

This is no game

# The mandate

The legislation requires that every anti-money laundering (AML) compliance program include a money laundering and terrorist financing risk assessment. You are also required to identify high-risk areas and monitor them on an ongoing basis. These can be complex and resource draining activities.

## Where do you stand?

- Do you know what risk factors should be included in your risk assessment program?
- How are you conducting on-going monitoring of transactions that pose high risk?
- Have you defined attempted suspicious transactions and trained employees on detecting these transactions?
- Have you built in continuous improvement programs to reflect changing legislation?

- Can you stress-test your capabilities to detect risk?
- Have you completed an anti-money laundering/anti-terrorist funding (AML/ATF) policy and a procedure compliance review?
- Do you have policies, procedures and controls to monitor and report suspicious transactions attempted and completed?
- Do you know how combining data and manual techniques can expose potential money laundering, fraud, and suspicious or unusual transactions?

## What's your next move?

There are significant changes that you will have to comply with right now. **And there may be additional legislative changes on the way.** To play by the new rules, you need the right information. Consider getting help from people who've been there before.

In 2007, Canada's Financial Transactions and Reports Analysis Centre (FINTRAC) investigated 193 cases involving close to \$10 billion in financial transactions.

The Globe and Mail, April 17, 2008

This is no game

# What cards are you holding?

- Have you developed a comprehensive program to combat money laundering and terrorist financing?
- Are you paying enough attention to customer identification including non face-to-face relationships and transactions?
- Are you equipped to detect and report unusual or suspicious transactions?
- Have you completed a money laundering and terrorist financing risk assessment appropriate to each of your business relationships, products, delivery channels and geographic areas of operation?
- What independent party will you use to perform an AM/ATF policy and procedures compliance review? Do they have sufficient expertise?
- Have you maintained continuity of data systems and records? Can you retrieve and use data as old as the oldest transaction when requested by your regulator?

If you don't like what you see, you need a plan.

When a series of money laundering schemes appear to be constructed in a similar fashion or using the same methods, the similar schemes are generally classified as a *typology*. A *method* refers to the particular procedure or series of actions used to carry out money laundering activity and normally involves a number of different techniques. A *technique* is the particular action or way that the money laundering activity is carried out.<sup>7</sup>

The following table identifies the most common money laundering methods observed in case disclosures involving transactions at Canadian casinos.<sup>8</sup> Many, if not all, of the methods described are well known to casino operators and regulators, and have been employed by money launderers for some time. However, these methods continue to be employed in Canadian casinos, as demonstrated by FINTRAC's case review. Brief descriptions of the money laundering methods follow, in order of the frequency in which they were observed. Techniques observed in FINTRAC's 2008-2009 case disclosures, suspected of being related to the money laundering method, are also described.

Money Laundering Method	% of Cases in Which Method Used
Use of Casino Value Instrument	68%
Refining	20%
Currency Exchange	19%
Structuring	14%
Front Money Account	13%
Use of Credit Cards	5%

### Use of casino value instrument

Casinos use a variety of value instruments to facilitate gaming on the part of their customers. The most common casino value instruments are casino chips, issued in various denominations and used, in lieu of cash, for gaming transactions.<sup>9</sup>

Casino value instruments are used in the placement and layering phases of money laundering activity. Typically, illicit funds are placed when they are used to purchase casino chips, and then layered when after minimal play, the casino chips are redeemed for a casino cheque. This results in providing an air of legitimacy as to the source of the funds, especially if casino operators do not confirm that the casino cheque represents gaming winnings.

### ML techniques observed

The following highlights the techniques observed by FINTRAC in 2008-2009, which suggest the use of casino value instruments for money laundering activity<sup>10</sup>:

- Customers made casino chip purchases, using illicit cash<sup>11</sup> (in some instances small denomination bank notes) or a bank draft, purchased with illicit funds and made payable to the casino-the customers engaged in minimal or no game play and then redeemed the chips for a casino cheque;
- The amount and/or frequency of casino chip purchases made by a customer did not correspond with the stated income/occupation of the customer (or the income/occupation details provided by the customer were vague and/or insufficient)-for example, a customer claimed full time employment, but was observed attending the casino on a daily basis, during working hours;
- Customers made casino chip purchases, engaged in minimal or no gaming, and left the casino in possession of chips-casino chips may be used as an alternate currency in illegal transactions such as drug sales.<sup>12</sup>

### Refining

Refining refers to the conversion of small denomination bank notes to large denomination bank notes. The method is commonly associated with drug trafficking, as drug dealers accumulate a large amount of smaller denomination bank notes through the course of their activities. Large quantities of cash, especially in smaller denomination bank notes, can be difficult to transport. In addition, large amounts of small



denomination bank notes may raise greater suspicion as criminals attempt to place these funds into the financial system. Money launderers will therefore seek to convert, or "refine", small denomination bank notes, such as \$5, \$10, \$20 and even \$50 dollar bank notes, into \$100 dollar bank notes.

### **ML techniques observed**

The following highlights the techniques observed by FINTRAC in 2008-2009 which suggest the use refining as part of money laundering activity:

- A customer attended a cashier window to exchange small denomination bills for larger denomination bills. In some instances, the bills exchanged had a strange odour;
- A third party attended a cashier window to exchange small denomination bills for larger denomination bills on behalf of another casino customer;
- A customer exchanged a large amount of small denomination bills for TITO<sup>13</sup> tickets, and later exchanged the TITO tickets at the cashier window for large denomination bills.

At least one provincial gaming authority in Canada has prohibited the direct exchange of small denomination bills to large denomination bills through its cashier windows. Refining through the use of TITO tickets is, however, less obvious. The use of TITO tickets in money laundering activity is addressed in the fourth section of the report, which discusses the risks associated with this casino service.

### **Currency exchange**

Casinos in Canada play host to thousands of foreign tourists every year, and as such, most casinos offer currency exchange services. Such services are attractive to criminals, who may seek to convert currency obtained, for example, in cross-border drug transactions, in an effort to make the funds available for further use or to disguise their true source.

### **ML techniques observed**

The following highlights the techniques observed by FINTRAC in 2008-2009 which suggest the use currency exchange(s) as part of money laundering activity:

- A customer frequently (over time) and/or repeatedly (over the course of one casino visit) attended a cashier window and exchanged a large amount of foreign currency (most often USD) for Canadian currency, with minimal or no gaming activity observed;<sup>14</sup>
- A customer attended a cashier window and exchanged a large amount of foreign currency, which had a strange odour, for Canadian currency.

Refining activity occurring in conjunction with currency exchanges has also been observed by FINTRAC:

- A customer attended a cashier window and exchanged a large amount of low denomination foreign currency bank notes for high denomination Canadian currency bank notes.

Automated currency exchange machines are available in certain casinos in Canada, and allow customers to exchange currency up to \$3,000, which is the client identification threshold. It is therefore possible for a money launderer, or a group of money launderers, to refine and/or exchange currencies without interacting with casino staff. The automated currency exchange machine itself has no mechanism to identify, monitor and/or control this type of money laundering activity, and casinos must therefore rely on alternate surveillance and security measures to identify this technique.

### **Structuring**

"Structuring" is a money laundering method that involves the division of cash or casino value instrument (s) to conduct a series of smaller value transactions in order to minimise suspicion and, in the case of cash, avoid threshold reporting requirements.<sup>15</sup> Structuring can also be combined with refining (structured refining) and currency exchanges (structured currency exchanges). When undertaken by a group of

individuals, the method is also known as "smurfing."

### **ML techniques observed**

The following highlights the techniques observed by FINTRAC in 2008-2009 which suggest the use of structuring and/or smurfing as part of money laundering activity:

- Customers who appeared to be associated made cash purchases of casino chips in amounts below the reporting threshold;
- Customers who appeared to be associated exchanged small denomination bills for large denomination bills, again in amounts below the reporting threshold;
- A customer used multiple cashiers to cash out casino chips in amounts below the reporting threshold;
- A customer passed cash, chips or other casino value instrument to another customer, or multiple customers:
  - Prior to entering the casino;
  - On the casino floor;
  - At the gaming table; or
  - Prior to cashing out.<sup>16</sup>

### **Front money accounts**

Some of the larger commercial casinos in Canada allow customers to establish accounts with them. There are generally two types of accounts that are offered: credit accounts and front money accounts.

A credit account allows the customer to borrow funds from the casino, which are to be repaid within an agreed upon period of time. Very few casinos in Canada offer this service, and only a small fraction of their customers have active credit accounts. Accounts are only made available to customers following a successful background check.<sup>17</sup> The possibility exists, however, for a customer to launder funds by establishing a credit account with a casino, and later repay the credit with the proceeds of crime. Credit accounts can also be used in conjunction with front money accounts to launder criminal proceeds.

Front money accounts are more widely available in Canadian casinos, and allow a customer to deposit money with the casino, which they can draw upon for gaming purposes. This service not only provides a measure of convenience for the customer, but provides increased security, as customers do not have to arrive at or depart the casino carrying large amounts of cash with them.

Despite the relative novelty of front money accounts, and the fact that the service is not available in all casinos across Canada, the use of front money accounts featured significantly in FINTRAC cases disclosed in 2008-2009. Their use in suspected money laundering activity in Canadian casinos was almost on par with the use of structuring.

One reason for the importance of front money accounts in FINTRAC case disclosures is that they offer similar services to those offered by more traditional financial institutions, at least with regard to the storage of funds. Money launderers and other criminals may believe that, despite these similarities, front money accounts are subject to less scrutiny than accounts at financial institutions used for the same purposes. Front money accounts can also be used in conjunction with many of the money laundering methods previously described.

### **ML techniques observed**

As previously mentioned, front money accounts were featured in a number of FINTRAC cases disclosed in 2008-2009. The following highlights the techniques observed by FINTRAC in these cases which suggest the use of front money accounts as part of money laundering activity:

- A customer deposited cash, a cheque or bank draft (made payable to the casino or to the customer) to a front money account and shortly after, purchased casino chips-the customer later redeemed the chips for a casino cheque, with minimal or no gaming observed.

- A customer deposited cash, a cheque or bank draft (made payable to the casino or to the customer) to a front money account, and later withdrew all or part of the funds, with minimal or no gaming observed.
- A customer requested casino credit, which was deposited to a front money account-the funds were later withdrawn and redeemed for a casino cheque (in some instances, the funds withdrawn were combined with casino chips, and the total was redeemed for a casino cheque).
- A customer deposited small denomination bills to a front money account, and later withdrew the funds in higher denomination bills;
- A third party made cash deposits to a customer's front money account-in some instances, the cash deposits were frequent and below the reporting threshold.

## Credit cards

Most, if not all, casinos in Canada allow credit card purchases of casino value instruments, such as casino chips. The increase in identity theft and the rise of fraudulent and stolen credit cards makes casinos, like many other Canadian businesses, susceptible to fraudulent credit card transactions. In instances where the credit card has been stolen or fraudulently obtained, the customer may attempt to redeem the casino chips for cash, avoiding other types of payment to conceal the audit trail.

In cases where the credit card has not been stolen or fraudulently obtained, a money launderer may seek to purchase casino value instruments using a credit card, obtain a casino cheque for the majority of the value of the chips purchased, and use illicit funds to pay down the credit card balance.

## ML techniques observed

The following highlights the techniques observed by FINTRAC in 2008-2009 which suggest the use of credit cards as part of money laundering activity:

- A customer made cash deposits of illicit cash to a business or personal bank account which were followed by transfers to a personal credit card account, then by credit card purchases of casino chips.
- A customer made credit card purchases of casino chips which were followed by minimal or no gaming and then by cash out in the form of a casino cheque-the cheque was deposited to the customer's bank account, while illicit cash was used to pay the credit card balance.

The description of the use of credit cards in casinos as part of money laundering activity highlights another feature common to many FINTRAC case disclosures involving Canadian casinos. Often, the overall money laundering process includes transactions in more than one financial sector, and transactions at casinos represent only a part of the overall laundering scheme. Although casinos may not be privy to the transactions occurring through other sectors, knowledge of how certain casino transactions may be part of a money laundering scheme, or how certain casino transactions may be indicative of money laundering activity, will help casino staff identify suspicious transactions that should be reported to FINTRAC.

## Sanitized Cases

In an effort to provide additional insight, the following are actual cases that were disclosed to law enforcement in 2008-2009. The cases have been sanitized; all identifying information has been removed, and they were chosen for inclusion as they involved transactions incorporating many of the money laundering methods previously described. The "red flags" associated with each case assisted FINTRAC in reaching the threshold for reasonable grounds to suspect that the information would be relevant to a money laundering investigation, and thus disclose the case.

### Sanitized Case 1 - Money laundering related to drug trafficking

The following chart illustrates the suspected money laundering scheme:



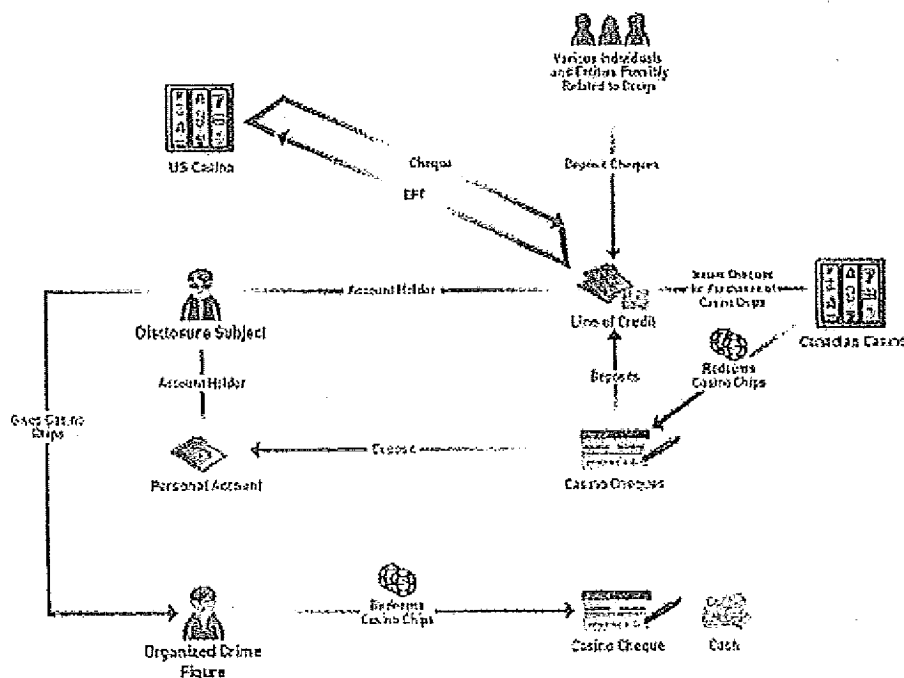
### Red flags associated with this case:

- Multiple reporting from financial institutions and casinos, as well as provincial records, indicated that the individual had provided different information regarding his/her employment. It varied from being unemployed, being an employee of a beauty salon, a homemaker or the owner of a restaurant. Casino staff also reported that the amount of casino chip purchases, which totalled over \$1.1 million, was not in line with the individual's reported employment.
- Financial institutions reported that the individual's account activity was unusual, and did not reflect payroll deposits, purchases or bill payments. Rather, large cash deposits were often followed by large cash withdrawals at casinos. Financial Institutions also indicated that the individual conducted credit card cash advances at casinos, and later made cash deposits to the credit card account.
- Financial institutions also reported the deposit of cheques from casinos. FINTRAC determined that the value of the casino cheques were within 10% of the value of the casino chip purchases made a few days prior.

This case highlights the use of *casino value instruments* and *credit cards* as methods of money laundering in casinos. Illicit funds were *placed* in the financial system, having been deposited to the individual's bank account and used to pay the individual's credit card account balance. The individual also *layered* transactions by obtaining funds from the bank account or credit card to purchase casino chips, and later converting the chips to a casino cheque which was deposited in the individual's bank account.

### Sanitized Case 2 - Money laundering related to organized crime

The following chart illustrates the suspected money laundering scheme:



[View a larger version of this image](#)

This case was generated following the receipt of a suspicious transaction report from a financial institution. According to the reporting entity, the individual in question was an associate of a high level organized crime figure involved in drug trafficking and illegal gaming. Analysis of reports submitted by financial institutions and casinos led FINTRAC to suspect that the financial activity of the individual was related to money laundering associated to organized crime activity.

Various individuals and entities deposited cheques in the individual's line of credit account. FINTRAC suspected that these individuals and entities were related to organized crime and/or drug trafficking

activity. The main individual issued cheques from the line of credit account to the benefit of casinos, which were negotiated for the purchase of casino chips.

It appears that a portion of the chips were redeemed for casino cheques, which were mostly deposited to the line of credit account. Some of them were deposited to a personal account held by the individual. No other activity was observed in this account except for the deposit of casino cheques, and FINTRAC suspects that these cheques were payments to the individual for money laundering services.

During at least one casino visit, the individual was observed passing chips to the organized crime figure on a number of occasions throughout the same visit, for a total of approximately \$100,000. The organized crime figure subsequently passed chips to a third party, who engaged in gaming activity. Winnings and unused chips were later passed back to the organized crime figure, who redeemed the chips for a casino cheque, or cash. Given that the total value of casino chip purchases appeared to be higher than the redemptions, it is suspected that a portion of the chips might have left the casino with the individual. These chips may have been provided to the organized crime figure, who attended the casino in possession of the chips, and in the company of the individual.

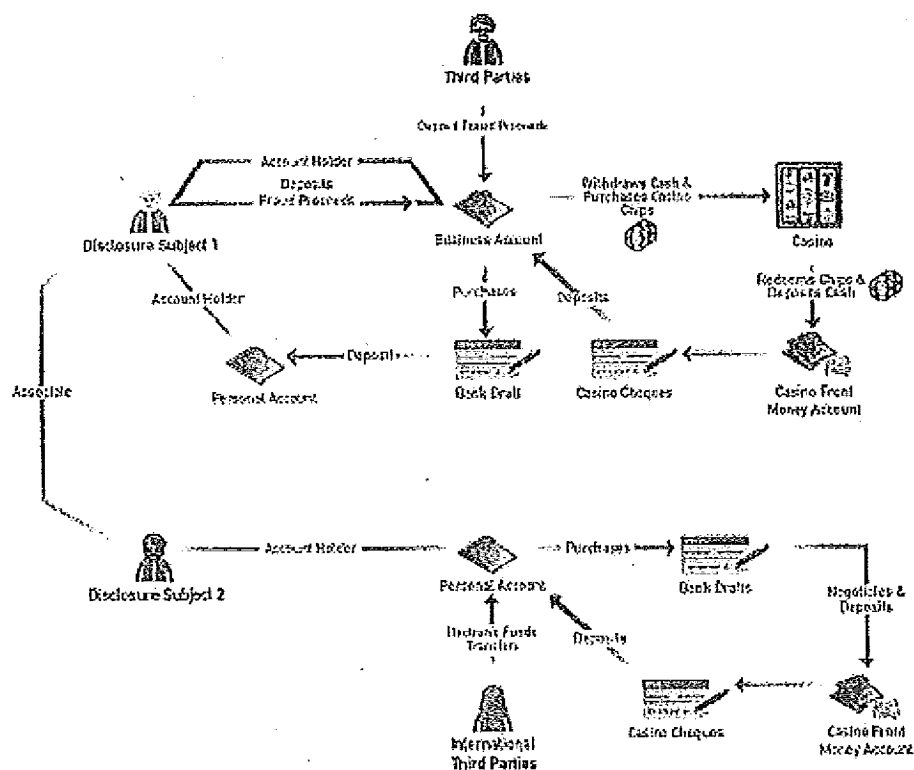
#### **Red flags associated with this case:**

- Casinos reported cash transactions on the part of the subject totalling approximately \$1.5 million over the course of a few years.
- A casino reported that the individual attended the casino accompanied by the aforementioned organized crime figure. The casino reported that the organized crime figure arrived at the casino in possession of over \$130,000 in casino chips. The casino indicated that the source of the chips was unknown, since casino records show no activity on the part of the organized crime figure for several months.
- The individual ordered an electronic funds transfer (EFT) to the benefit of a casino in the United States. A few days following this EFT, the subject deposited a cheque drawn on the account of the U.S. casino, in the same amount as the outgoing EFT.

This case also highlights the use of *casino value instruments* as a method of money laundering, although in this example, different techniques are used. Illicit funds are *placed* in the individual's line of credit account through the deposit of cheques. The individual *layered* transactions by purchasing casino chips, and redeeming the chips for casino cheques, which are deposited to the individual's line of credit account and a personal account. The individual also possibly engaged in layering activity by leaving the casino with chips, and passing the chips to an organized crime figure, who continued the layering process by redeeming the chips for a casino cheque.

#### **Sanitized Case 3 - Money laundering related to fraud, using front money account**

The following chart illustrates the suspected money laundering scheme:



[View a larger version of this image](#)

This case was generated following the receipt of a suspicious transaction report from a casino. The individual mentioned in the report was the subject of a previous FINTRAC case disclosure to law enforcement. The subject was allegedly involved in advance fee and telemarketing scams, and had defrauded victims by advising them that they had won millions of dollars, but had to pay "taxes" before the winnings could be collected.

The principal subject made cash deposits to a business bank account, which was also credited with cash deposits made by third parties. FINTRAC suspected that these deposits were related to fraud schemes. The funds were withdrawn and used to purchase casino chips. The subject engaged in minimal gaming, and redeemed the chips in cash, depositing the payout to the front money account. Once the front money account had accumulated sufficient funds, the subject made a withdrawal by requesting a casino cheque. The casino cheque was negotiated at a financial institution, and the funds were used to purchase a bank draft payable to the subject. FINTRAC suspected that the bank draft was deposited to an account held by the subject at another financial institution.

An associate of the subject engaged in similar activity. An account held by this individual at a financial institution was credited primarily with electronic fund transfers ordered by various individuals. FINTRAC suspected that the credits were related to fraudulent activity with an international dimension, a feature of many advance fee fraud schemes. These funds were used to purchase bank drafts payable to a casino, which were deposited to the individual's front money account. The individual engaged in minimal gaming activity. FINTRAC suspected that this individual also withdrew the funds held in the front money account once sufficient funds had accumulated, requesting cash or a casino cheque as desired.

**Red flags associated with this case:**

- Financial institutions reported that financial transactions related to the subject's business accounts were not consistent with the reported business activity. The transactions included a number of large cash deposits, which were followed by large cash withdrawals.
- One of the subject's business accounts received third party cash deposits, purportedly from employees depositing funds into their employer's business account. However, a number of these deposits took place after the company had been dissolved.
- Casinos reported that the subject had conducted a number of large cash purchases of casino chips. One casino reported that the subject made a large cash deposit to a front money account, using

\$20 bills. On two other occasions, the subject reportedly used the casino to exchange over \$20,000 in American currency to Canadian currency.

- A financial institution reported that the subject deposited a cheque drawn on the account of a casino. The proceeds from this deposit were used to purchase a bank draft made payable to the subject. The amount of the casino cheque was within 10% of the casino chip purchases the subject had made in the previous 10 months.

This case highlights the use of a *casino value instrument*, *front money account* and *currency exchange* as methods of money laundering. Illicit funds were placed into the financial system by way of cash deposits, in some cases by third parties, and electronic funds transfers to the business and personal accounts of the individuals. Both individuals undertook a series of *layered* transactions using a combination of money laundering methods and techniques, including cash withdrawals, bank draft purchases, casino chip purchases, casino chip redemptions, cash deposits to a *front money account*, cheque deposits to a front money account, and the withdrawal of front money account funds in the form of a casino cheque.

## Money Laundering Risk Associated with Ticket In Ticket Out Service

The compliance regimes of the casino sector are required to assess and document money laundering and terrorist financing risks associated with their business, as well as introduce measures to mitigate the risks identified. The following section identifies the money laundering risk associated with the Ticket In Ticket Out (TITO) service.<sup>18</sup>

As briefly mentioned in the section discussing the refining method, TITO is a relatively new system for slot machines and Video Lottery Terminals (VLTs) that is designed to replace coins or tokens. Traditionally, slot machine jackpots were paid by coins or tokens falling into the slot tray, which the customer would then collect in buckets. TITO replaces the coins with a slip of paper, or "ticket," that contains a unique bar code. The ticket can be fed into other slot machines to continue play, scanned at cashier stations for a cheque or cash, or redeemed at an automated redemption machine.

There are two factors related to the risk presented by the TITO service. The first factor is related to the difficulty of monitoring the behaviour of customers using the TITO service. The second factor relates to the inability of casino operators to identify customers using the service in combination with an automated redemption machine.

### Monitoring customer behaviour

TITO tickets may be used as currency in illegal transactions, offering the same advantages as casino chips, or may be used to directly launder the proceeds of crime. In both schemes, an individual inserts hundreds of dollars into a slot machine, engages in minimal play (or no play at all), and cashes out, receiving a TITO ticket. The ticket, which is usually valid for 30 days, can be used in illegal transactions, for example, the purchase of drugs. In this case, the drug dealer will redeem the ticket, or a number of tickets collected, for a casino cheque. The ticket can also be redeemed directly for a casino cheque.<sup>19</sup>

In some Canadian casinos, the ticket dispensed by the TITO machines indicates whether the ticket was issued as the result of a jackpot, or whether it was issued as a result of the customer cashing out. Casino staff benefit from TITO machines which include this feature, as it provides an additional indicator as to whether the customer's activity is suspect and should be reported to FINTRAC. However, the majority of TITO machines in Canada do not include this feature, and in these cases, casino staff must rely on other security and surveillance mechanisms in place to identify this type of activity.

All of the transactions observed in FINTRAC's 2008-2009 case disclosures that involved the suspected use of casino value instruments for money laundering, related to casino chips. Prior to May 2008, FINTRAC received a limited number of suspicious transaction reports (STRs) specifically referencing the redemption of TITO tickets. Since media reporting in May 2008, FINTRAC has received a number of STRs specifically referencing the redemption of TITO tickets, indicating a greater awareness amongst casino staff of the need to provide more details in STRs submitted to FINTRAC. In addition, the introduction of Casino Disbursement Reports in September 2009, which requires the automatic reporting of casino disbursements over \$10,000, will provide another mechanism for FINTRAC and Canadian casinos to



monitor possible money laundering activity through the use of TITO-enabled slot machines.

TITO machines may also be used to refine currency. As previously mentioned, refining refers to the conversion of small denomination bills to large denomination bills. An individual may insert a large number of small denomination bills into a TITO-enabled slot machine, cash out following minimal or no gaming, and receive a TITO ticket. The individual may attend a cashier window to redeem the ticket for cash, requesting large denomination bills. As previously mentioned, FINTRAC has observed increasing specificity in STRs from the casino sector related to TITO activity, suggesting increased awareness amongst casino staff of the use of TITO machines in this refining technique.

## Identifying customers

In most casinos, the TITO system has been supplemented with automated redemption machines, through which casino customers can cash out their TITO tickets automatically, without the need to visit a cashier. Although the majority of these machines include a limit in the amount of funds that will be dispensed, they often dispense \$100 bank notes. It is possible for a single money launderer, or a group of launderers, to feed small denomination bills into TITO-enabled slot machines and cash out when reaching or approaching the automated redemption machine's limit. The resulting ticket may be exchanged for large denomination bank notes at an automated redemption machine without ever interacting with casino staff. The prevalence of TITO systems and automated redemption machines in Canadian casinos may lead to an increase in the use of TITO for refining. The automated redemption machine itself is unable to identify, monitor and/or control customers engaging in this type of activity, and casinos must rely on alternate surveillance and security measures to identify this technique.

## Conclusion

Many of the money laundering methods and techniques described in this report are known to casino regulators and operators. Criminals will continue to employ these methods and techniques as long as they are successful.

Although this report has focused on money laundering activity in Canadian casinos, often the overall money laundering process includes transactions in more than one sector. Casinos may not be privy to these transactions, and so this report has described how certain casino transactions may be part of larger money laundering schemes, in an effort to help casino staff identify suspicious transactions that should be reported to FINTRAC.

The Centre continues to value the work and efforts of the Canadian casino sector and other reporting entities in the fight against money laundering and terrorist financing, and looks forward to continued collaboration with the casino sector in order to detect and deter money laundering and terrorist financing activities.

---

<sup>1</sup> Annual case reviews provide a complete picture of the trends and activities related to ML/TF within that year. Every case review better positions FINTRAC to be able to identify Canadian trends in ML/TF and ultimately share this information with reporting entities. [Back](#)

<sup>2</sup> For FINTRAC's purposes, a "predicate offence" is an offence under the *Criminal Code* or any other law under Parliament's jurisdiction from which proceeds of crime may be derived (with the exception of offences under certain acts, including the *Income Tax Act* and the *Excise Tax Act*.) that have been prescribed by regulation. [Back](#)

<sup>3</sup> The lower volume of reports provided by these sectors or about these services may have contributed to the lower number of ML cases involving their use. Consequently, these statistics are not necessarily an indication that they are less vulnerable to money laundering than financial institutions. [Back](#)

<sup>4</sup> Internet payments systems (IPS) include various payment services offered online which include: 1) payment processing providers allowing merchants to authorize, settle and manage transactions from websites; 2) debit-account providers allowing users to accept electronic payments and make person-to-person funds transfers; as well as 3) digital precious metals operators offer a debit-account type IPS issuing digital currencies that are backed by precious metals. [Back](#)

- 5 -

**BRITISH COLUMBIA LOTTERY CORPORATION**  
**BOARD MEETING JULY 23, 2010**  
**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

**DIRECTOR RESPONSIBILITIES – FOR A FINTRAC  
REPORTING ENTITY**



[FINTRAC Home](#) > [Publications](#) > [Guidelines](#) > [Guideline 4](#)

# Guideline 4: Implementation of a Compliance Regime

## December 2008

This replaces the previous version of *Guideline 4: Implementation of a Compliance Regime* Issued in February 2008. The changes made are indicated by a side bar to the right of the modified text in the PDF version.

### Table of Contents

- 1. **General**
- 2. **Who Has to Implement a Compliance Regime?**
  - 2.1 Financial Entities
  - 2.2 Life Insurance Companies, Brokers and Independent Agents
  - 2.3 Securities Dealers
  - 2.4 Casinos
  - 2.5 Real Estate Brokers or Sales Representatives
  - 2.6 Agents of the Crown that Sell or Redeem Money Orders
  - 2.7 Money Services Businesses
  - 2.8 Accountants and Accounting Firms
  - 2.9 Dealers in Precious Metals and Stones
  - 2.10 British Columbia Notaries
- 3. **What is a Compliance Regime?**
- 4. **Appointment of a Compliance Officer**
- 5. **Compliance Policies and Procedures**
- 6. **Risk-Based Approach**
  - 6.1 Risk assessment
  - 6.2 Risk mitigation
  - 6.3 Keeping client identification and beneficial ownership information up to date
  - 6.4 Ongoing monitoring
  - 6.5 High risk situations for certain sectors
- 7. **Ongoing Compliance Training**
- 8. **Review Every Two Years**
- 9. **FINTRAC's Approach to Compliance Monitoring**
- 10. **Penalties for Non-Compliance**
- 11. **Comments?**
- 12. **How to Contact FINTRAC**

- Appendix 1 :** Products, Services, Delivery Channels and Geographic Locations
- Appendix 2 :** Client and Business Relationships
- Appendix 3 :** Risk Level Assessment Matrix

- [Back to the guidelines menu](#)

Note: Content in this section may require additional software to view. Consult our [Help page](#).

[Guideline 4: Implementation of a Compliance Regime \(PDF version, 108 kb\)](#)

### 1. General

## FINTRAC - Guideline 4: Implementation of a Compliance Regime - FINANCIAL TRANSACTIONS AND REPORTING ACT

appoint another individual to help you implement a compliance regime.

In the case of a large business, the compliance officer should be from a senior level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed compliance officer in a large business should not be directly involved in the receipt, transfer or payment of funds.

For consistency and ongoing attention to the compliance regime, your appointed compliance officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the compliance officer retains responsibility for the implementation of the compliance regime.

### **5. Compliance Policies and Procedures**

An effective compliance regime includes policies and procedures and shows your commitment to prevent, detect and address non-compliance. Effective June 23, 2008, your compliance program has to include written policies and procedures to assess the risks related to money laundering and terrorist financing in the course of your activities.

The level of detail of these policies and procedures depends on your needs and the complexity of your business. It will also depend on your risk of exposure to money laundering or terrorist financing. See section 6 for more information on risk-based approach.

For example, the compliance policies and procedures of a small business may be less detailed and simpler than those of a large bank. However, effective June 23, 2008, your policies and procedures have to be in writing and be kept up to date, whether you are a small business, an individual or an entity. Several factors could trigger the need to update, as often as necessary, your policies and procedures, such as changes in legislation, non-compliance issues, or new services or products.

In addition, if you are an entity, your policies and procedures also have to be approved by a senior officer. A senior officer of an entity includes its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any person who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

It is important that your compliance policies and procedures are communicated, understood and adhered to by all within your business who deal with clients or any property owned or controlled on behalf of clients. This includes those who work in the areas relating to client identification, record keeping, and any of the types of transactions that have to be reported to FINTRAC. They need enough information to process and complete a transaction properly as well to identify clients and keep records as required.

They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering or anti-terrorist financing regimes consistent with international standards. See additional information about this in subsection 6.1.2 and Appendix 1.

Your compliance policies and procedures should incorporate, at a minimum, the reporting, record keeping, client identification, risk assessment and risk-mitigation requirements applicable to you. For example, in the case of your reporting obligations relating to terrorist property or suspicions of terrorist financing, your policies and procedures should include the verification of related lists published in Canada. These are available on the Office of the Superintendent of Financial Institutions' Web site at <http://www.osfi-bsif.gc.ca>, by referring to the "Terrorism Financing" link.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

### **6. Risk-Based Approach**

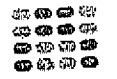
<http://www.fintrac.gc.ca/publications/guide/Guide4/4-eng.asp>

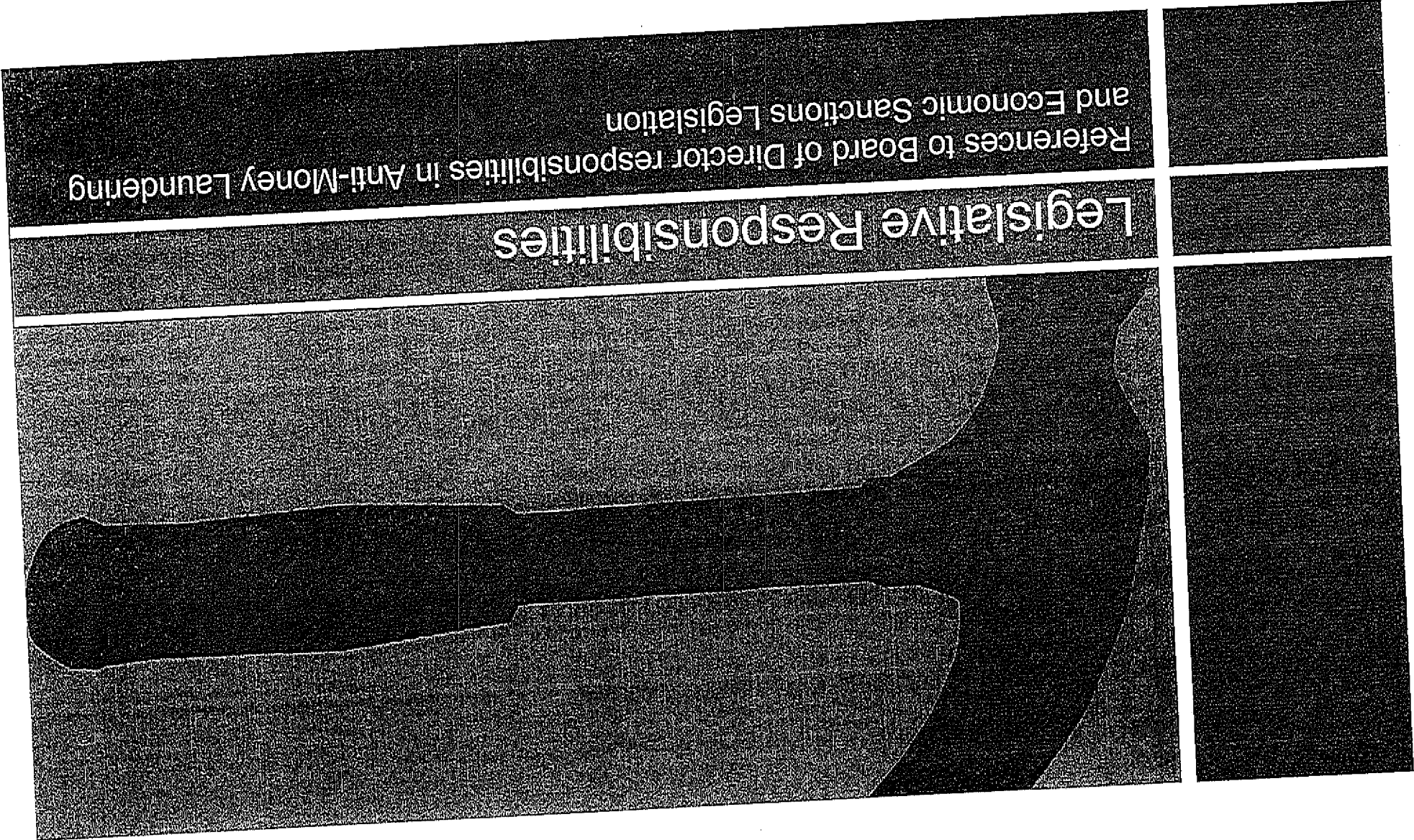
7/20/2010

BCLC0015239.060

# Governance and Compliance

Position	General Responsibilities	Compliance Responsibilities
Shareholders	Elect Directors and their Representatives Vote on significant structural issues of the corporation	•Elect Directors
Directors	Facilitate the achievement of corporate objectives and manage corporate risks through policy setting and management oversight	<ul style="list-style-type: none"> <li>•Set corporate policies</li> <li>•Understand risks and related measurement and management strategies</li> <li>•Receive timely and accurate reporting</li> <li>•Support independent oversight</li> </ul>
Senior Management	Executing the directives of the Board towards the achievement of objectives and management of risk	<ul style="list-style-type: none"> <li>•Advise the board on corporate policy</li> <li>•Create and implement risk measurement and management strategies</li> <li>•Receive timely and accurate reporting</li> <li>•Implement and support independent oversight</li> </ul>





## PCMLTFA & PCMLTFR

*78. If a person or an entity commits an offence under this Act, any officer, director or agent of the person or entity who directed, authorized, assented to, acquiesced in or participated in its commission is a party to and guilty of the offence and liable on conviction to the punishment provided for the offence, whether or not the person or entity has been prosecuted or*

## United Nations Act

*9. No officer, director, agent or other representative of a corporation shall knowingly do anything that causes, assists or promotes, or is intended to cause, assist or promote, the omission of any act or thing required to be done under sections 7 and 8.*



## Criminal Code of Canada

*“senior officer” means a representative who plays an important role in the establishment of an organization’s policies or is responsible for managing an important aspect of the organization’s activities and, in the case of a body corporate, includes a director, its chief executive officer and its chief financial officer*

# Criminal Code of Canada

*22.1 In respect of an offence that requires the prosecution to prove negligence, an organization is a party to the offence if*

*(a) acting within the scope of their authority*

*(i) one of its representatives is a party to the offence, or*

*(ii) two or more of its representatives engage in conduct, whether by act or omission, such that, if it had been the conduct of only one representative, that representative would have been a party to the offence; and*

*(b) the senior officer who is responsible for the aspect of the organization's activities that is relevant to the offence departs — or the senior officers, collectively, depart — markedly from the standard of care that, in the circumstances, could reasonably be expected to prevent a representative of the organization from being a party to the offence.*

# Criminal Code of Canada

**22.2** *In respect of an offence that requires the prosecution to prove fault — other than negligence — an organization is a party to the offence if, with the intent at least in part to benefit the organization, one of its senior officers*

- (a) acting within the scope of their authority, is a party to the offence;*
- (b) having the mental state required to be a party to the offence and acting within the scope of their authority, directs the work of other representatives of the organization so that they do the act or make the omission specified in the offence; or*
- (c) knowing that a representative of the organization is or is about to be a party to the offence, does not take all reasonable measures to stop them*

# FINTRAC Guidance

---

- FINTRAC's interpretation of PCMLTFA & PCMLTFR
- Guideline 4
  - Implementation of a compliance regime
    - Compliance Officer, Policies & Procedures, RBA, Training, Review



# OSFI Guidance

---

- Guideline B-8 (revised)
  - Builds on FINTRAC guidance
    - CAMLO (specific requirement beyond a compliance officer)
    - Oversight and accountability
- Corporate Governance Guideline



# Key Considerations for AML/ES Compliance

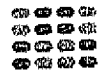
---

- ❑ Board of Director Responsibilities
- ❑ Significant Organizational Risks Related to AML/ES
- ❑ Frequency and Nature of Involvement
- ❑ Lines of Reporting and Responsibility
- ❑ Reporting Content and Frequency
- ❑ Red Flags the Board Should Look Out For



# Board and Senior Management Oversight

	<b>Board</b>	<b>Senior Management</b>
Documented Accountability	Approving policies and procedures and monitoring the effectiveness of the AML/ATF program on a regular basis	Managing the AML/ATF program to ensure that it is adequate to mitigate ML/TF risk, complies with PCMLTFA, implemented effectively in business areas
Reporting	From Senior Management to Board Using Information Obtained from CAMLO/Auditor: Sufficient pertinent information to ensure the adequacy and effectiveness of AML/ATF program <ul style="list-style-type: none"><li>- Enterprise wide assessment of inherent risks (patterns and trends in ML/TF)</li><li>- Self-assessment controls and material changes</li><li>- Remedial action plans</li></ul>	



## The Role of the Board in Risk Management

- ❑ General understanding of risks and techniques used to measure and manage those risks
- ❑ Review and approve the overall risk philosophy and risk tolerance of the institution
- ❑ Review and approve significant policies or changes in policies for accepting, monitoring, managing and reporting on the significant risks to which the institution is exposed.
- ❑ Require of management timely and accurate reporting on risks faced by the institution, the procedures and controls in place to manage these risks, and the overall effectiveness of risk management processes.
- ❑ Support of independent oversight functions (review mandates, be involved in selection, require independence in fact and appearance, unrestricted access, remuneration and budget adequate, discuss key findings of reports).





# Board Obligations – Policies

---

- Is there an enterprise wide AML/CTF policy?
- Did the board have a role in reviewing and approving this policy?
- Is there a process in place for the board to review and approve updates to

# OSFI Guideline B-8

## □ Section 4 - Board and Senior Management Oversight

### □ *Role of the Board*

- *FRFIs should ensure that the Board has oversight accountability for approving policies and procedures and monitoring the effectiveness of the AML/ATF program on a regular basis. The Board's oversight practices in respect of the AML/ATF program should align with OSFI's Corporate Governance Guideline, in particular the section "The Role of the Board in Risk Management."*



# OSFI Guideline B-8

---

## □ Section 12 – Training

- *Training programs for the Board and Senior Management should provide sufficient briefing with respect to inherent risks and controls to enable them to assess information reported by the CAMLO and Auditor, and exercise effective oversight over the AML/ATF program.*
- *An effective way of providing training for new members of the Board is to include an AML/ATF program overview information session in new director orientation.*



# Published AMPS

No.	Date Penalty Issued	Sector	Name	Penalty Amount	Registration	Designated CAMLO	Policies & Procedures	Risk Based Approach	Training	Ascertaining Identity	Reporting & Record Keeping	Request for Information
10	Mar-10-2010	Money Services Business	Fort Duty Free	\$ 6,000			*	*	*			
9	Mar-10-2010	Money Services Business	Galaxy International Canada Limited	17,380	*		*	*	*	*	*	
8	Jan-10-2010	Real Estate	Homelife Effect Realty Incorporated	27,000		*	*	*	*			*
7	Nov-23-2009	Money Services Business	Bharat Money Exchange Limited	36,100	*		*	*	*	*	*	*
6	Nov-23-2009	Money Services Business	SSCG International Trading Incorporated	12,750	*	*	*	*	*	*	*	
5	Nov-23-2009	Money Services Business	Ghanaco Financial Services	4,320	*							
4	Nov-10-2009	Money Services Business	Gigant Express	3,000	*							
3	Nov-10-2009	Real Estate	Weagle Realty Limited	6,750			*	*	*			
2	Jun-29-2009	Money Services Business	AM Exchange/AM Currency Exchange	3,940	*							
1	Jun-29-2009	Money Services Business	Envimaya	3,560	*							
			<b>Total</b>	<b>\$ 120,800</b>	<b>7</b>	<b>2</b>	<b>6</b>	<b>5</b>	<b>6</b>	<b>3</b>	<b>3</b>	<b>1</b>



# Board Obligations - Timing

---

- Training:
  - Periodically, generally interpreted as annually
- Signing off on Policies:
  - As necessary for major changes and at the time of review (bi-annually)



# Board Obligations - Timing

---

- Receiving CAMLO reporting
  - As events occur (within 30 days of the relevant event) or at least annually (where there are no events).
- Receiving effectiveness review or audit findings:
  - Within 30 days of the report
  - Effectiveness reviews occur at least bi-annually



# Board Obligations – Testing and Monitoring

---

- Is there regular testing and monitoring in place?
- Are the results reported to the board?
- What about action plans to correct any gaps?



# Board Obligations – Review and Audit

---

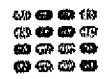
- Are there regular audits and reviews?
  - Are the results reported to the board?
  - What about action plans to correct any gaps?
  - Can you tell the difference between the CAMLO's report and the auditor's?





# Sample AML Program/Risk Red Flags

<b>CAMLO Role</b>	No training beyond front-line staff training Little direct knowledge of reporting and screening activities CAMLO has significant operational duties
<b>Budget</b>	CAMLO does not certify the sufficiency of the budget allocation annually Rule of 7
<b>CAMLO Reporting</b>	Does not contain sufficient detail (specifically with regards reporting)
<b>Regulator Involvement</b>	More than 2 years since last regulator involvement (correspondence etc.) Regulator deficiency letters conflict with self-assessment and external evaluation results
<b>Risk Assessment &amp; Mitigation</b>	No risk assessment/mitigation document has been produced for approval by the board No mention of the risk of known agreements with third party providers/new products
<b>Policies and Procedures</b>	Policies revisions have not been approved by the Board in the past two years. Policies do not reference money laundering risk
<b>Reporting</b>	No (or few) suspicious transaction reports filed in the past year Significant variations in large cash transaction or electronic funds transfers
<b>Evaluations</b>	More than 1 year has passed since a self-evaluation or external evaluation



- 4 -

**BRITISH COLUMBIA LOTTERY CORPORATION**

**BOARD MEETING JULY 23, 2010**

**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

**BACKGROUND – WHAT IS NEEDED FOR  
COMPLIANCE**

## **2. AN EFFECTIVE COMPLIANCE REGIME**

The requirement to establish a compliance regime under the 2000 Act is set out at Section 71 of the Regulation, which provides that, for the purpose of paragraph 3(a) of the 2000 Act, and to assist FINTRAC in carrying out its mandate under paragraph 40(e) of the 2000 Act, every person or entity to which any of paragraphs 5(a) to (l) of the 2000 Act applies shall implement a regime for complying with the 2000 Act and any regulations made under the 2000 Act. The Regulation goes on to provide that the compliance regime shall include, as far as practicable, the appointment of a person who is to be responsible for implementation of the regime, the development and application of compliance policies and procedures, a periodic review of the policies and procedures and an ongoing compliance training program. These requirements have been enhanced by the requirements of FINTRAC Guideline 4, which provides guidance as to FINTRAC's expectation as to what will be included in an effective compliance regime.

A compliance program would appear to require the following:

1. The reporting entity must ensure that they can properly file the electronic filing which is required by the 2000 Act and regulations. This will require review of the systems and software available to the reporting entity, and a review of the security requirements, including specifically the browser requirements necessary for reporting. These can be reviewed by way of reviewing the reporting requirements as outlined on the FINTRAC website. If electronic reporting is not possible as a consequence of the inability of the computer system and software of the entity to communicate with FINTRAC, paper reporting is permitted. If paper reporting must be used, then the appropriate forms for reporting must be prepared based

- 2 -

upon the reporting requirements. These are set out at the schedules to the regulations and clarified in the Guidelines.

2. Information appropriate to the needs of the reporting entity outlining the requirements of the 2000 Act and the regulations must be prepared, and circulated, to all employees. This should include circulation to all officers, directors, management, supervisory personnel and to all persons who would have a client interface in a manner which would put them in a position to see, and potentially identify, a suspicious or large cash transaction. It is suggested that this information and notification of the requirements to report must be in writing, and must have been adequately circulated so as to bring the requirements for reporting to the attention of all employees who would be in a position to identify a transaction which is required to be reported.
  
3. The reporting entity must prepare, they can use the guidelines as a basic outline, an outline of the applicable reporting requirements including the information which must be gathered and retained as to the customer and as to the transaction. It is suggested that all client contact forms must include the information required for a report as to the customer, any third parties they may be acting for, and the basis of the transaction. Employees should not be permitted to initiate a transaction unless they have obtained the compulsory information regarding the client and any third party involved and can record the details of the transaction. Electronic or paper based forms must be prepared and circulated, such that individuals have an appropriate format in which to record and forward the information. Restrictions on the commencement of a new client relationship, or a

specific transaction relationship, unless the information is obtained should be imposed.

4. Persons dealing with customers need to be provided with a specific, as clear as possible, handbook on the identification of a transaction which must be reported. This must include the general criteria for a suspicious, large cash or cross border transaction reporting requirement. The outline should specifically and clearly state the nature of the transactions which are required to be reported, and for suspicious transactions the criteria for those transactions which should be considered a suspicious transaction.
5. Employees should be provided with a brief training manual which indicates the basis for identification of a reportable transaction, the general criteria or indicators which should give rise to a concern that a financial transaction may be a suspicious transaction, and listing the industry specific indicators for the reporting entity.
6. A compliance officer needs to be appointed and the specific instructions as to how the transaction is to be reported, preferably through a central office or individual, must be established. Employees must know to whom, how, and when they make the report. The employees must have an appropriate form to complete with the information required for the report.
7. The reporting system must provide a means for the reporting information to be provided to the individual responsible for reporting within the time frames for

- 4 -

reporting, and that individual must have the means of providing the report to FINTRAC.

FINTRAC Guideline 4, in Part II, initially outlines who has to implement a compliance regime. This is done on the basis of outlining types of reporting entities, and listing the basic requirements for compliance. The entities which are listed are financial entities, life insurance companies, brokers and independent agents, securities dealers, portfolio managers and investment counsellors, casinos, real estate brokers or sales representatives, agents of the Crown that sell or redeem money orders, foreign exchange dealers, money services businesses and accountants and accounting firms. Each of these outlines indicate the activities in relation to which the compliance regime needs to be established, and the respective roles for employees and employers. The discussion of what is a compliance regime, notes that the compliance regime needs to be tailored to fit the individual needs of the reporting entity. The compliance regime needs to specifically reflect the nature, size and complexity of the operations.

The basics of a compliance regime, outlined at Part IV, start with the requirement for the appointment of a compliance officer. Specific note is made that the compliance officer must have the authority and the resources necessary to discharge responsibilities effectively. The compliance officer, on a regular basis, needs to report to a senior level such as the board of directors, senior management or the owner or chief operator. An appropriate compliance regime must include policies and procedures, and clearly state the commitment to prevent, detect and address non-compliance. Again note is made that the degree of detail, specificity and formality will vary according to the issues and transactions involved.

An essential part of an effective compliance policy is communication, and assurance that the policies are understood by and will be adhered to on the part of anyone who will deal with clients and property owned or controlled by clients. A compliance regime now must also include education and the requirement to be alert to transactions which might involve countries or territories who are the list of non-cooperative countries, or persons identified by regulation as being identified for terrorist financing purposes. At the very least, reporting obligations relating to terrorist property or suspicions of terrorist financing policies and procedures must reflect the need to check a new customer against the suspected terrorist organization lists published in Canada.

Periodic reviews of the policies and compliance program will need to be undertaken, and specific review can be triggered by factors such as changes in legislation, identification of a non-compliance issue or the introduction of new services or products. Review of the compliance regime must be conducted on an audit basis, and should include interviews with those employees actually handling transactions on an interface with the public.

The standards for the frequency and method of compliance training needs to be regularly reviewed. New employees must be trained before they begin to deal with customers and all employees should be periodically informed of changes. Employee training must include sensitization to the requirements for reporting and identification, and the policies and procedures required to be followed for obtaining customer information, reporting and recording of reportable transactions.

- 6 -

FINTRAC has a specific responsibility to monitor and ensure compliance with the legislative requirements under the 2000 Act. FINTRAC at any time can examine compliance regime and records, and can provide feedback about the adequacy of the program.

The appendices to Guideline 4 include reporting, record keeping, client identification, third party determination requirements by the reporting person or reporting entity sector. The appendices present summaries of these requirements which can be used to assist in formulating the compliance regime.



#### 4. REPORTING AND RECORD KEEPING REQUIREMENTS

The reporting requirements imposed on the reporting entities are the central provisions of the 2000 Act. It is important for reporting entities to familiarize themselves with these requirements because they may significantly affect the way they obtain and record information in their business. There are three different types of transactions that must be reported to FINTRAC: (a) suspicious transactions (Section 7 of the 2000 Act); (b) prescribed transactions (currently large cash and electronic funds transfers transactions of \$10,000 or more, Section 9 of the 2000 Act, as a prescribed transaction in the regulations); and (c) cross-border movements of currency and monetary instruments in excess of a prescribed amount (Section 12 of the 2000 Act).<sup>1</sup>

##### A. Suspicious Transactions

Reporting entities are required to inform FINTRAC whenever they encounter, in the course of their business activities, a transaction that they suspect may be related to money laundering or the financing of terrorist activity. Section 7 of the 2000 Act requires a report if there are reasonable grounds to suspect that the financial transaction is related to the commission of a money laundering offence.

There is no threshold, as to dollar amount, with regard to the requirement to report a suspicious transaction. There is often confusion between the large cash transactions reporting and the suspicious transactions reporting. Large cash transactions reporting requires reporting of the movement of cash where the amount is, under current regulation, \$10,000 or more. It is

---

<sup>1</sup> Section 1(1) of the Regulations defines “monetary instruments” as (a) securities, including stocks, bonds, debentures and treasury bills, in bearer form or in such other form as title to them passes upon delivery; and (b) negotiable instruments in bearer form, including bankers drafts, cheques, travellers cheques and money orders, other than (i) warehouse receipts or bills of lading, and (ii) negotiable instruments that bear restrictive endorsements or a stamp for the purposes of clearing or are made payable to a named person and have not been endorsed.

necessary to report a financial transaction as suspicious where there are reasonable grounds to suspect the transaction is related to money laundering regardless of the dollar amount of the transaction.

The 2000 Act and the regulations, particularly the Suspicious Transaction Reporting Regulation places significant emphasis on identifying whether the transaction is being undertaken for or on behalf of a third party. The requirement to identify transactions undertaken on behalf of a third party, and the details of third party information required to be gathered are extensively set out. The concept of reasonable measures to determine whether the account or transaction is being undertaken for a third party have been maintained, but a more extensive regime for requesting or requiring information, and the gathering and maintaining of information regarding third parties has been included.

Suspicious transactions must be looked at as to the transaction and the persons involved as a whole. Note is made at Section 3.1 of Guideline 2 that a suspicious transaction may involve several factors that seem individually insignificant but together may raise suspicion that the transaction is related to the commission of a money laundering offence. The most significant factor is to consider the context in which the transaction occurs. The reporting entity will need to be able to identify that the transaction is outside of the ordinary course of business, such that it does not appear to be in keeping with normal industry practices. Assessment of the suspicion should be based on a reasonable evaluation of relevant factors. Knowledge of the customer, the customer's business and financial circumstances will also be relevant.

A suspicious transaction is, by the definition in Section 7 of the 2000 Act, a financial transaction that the reporting entity has reasonable grounds to suspect is related to the

commission of a money laundering offence. Initially, the transaction must be a financial transaction, that is it must involve the transfer of money, or the exchange of money for an asset. Other transactions which are not financial in nature do not fall under the requirements. This is not necessarily the case with the transactions required to be reported under the amendments made by the *Anti-terrorism Act. The Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations*, consolidated November 6, 2003, provide the details as to the persons, activities and basic nature of reporting of suspicious transactions. As is the case throughout the 2000 Act and the regulations, the reporting requirements extend to and include suspicion that there is financing of terrorist activity.

Reporting under Section 7 of the 2000 Act is only required for “financial transactions”. The 2000 Act, the regulation and the guidelines do not define a “financial transaction”. The statute and the regulations were drafted to be as broad and vague as possible to capture a concept and not a narrow list of transactions. It would however seem that a financial transaction necessarily involves the transfer of money, otherwise the concepts necessary for the transaction to be related to money laundering don't exist. If the transaction trades money for an asset, that probably is a financial transaction. If you are trading two assets, but it is clear that these assets are of a monetary nature, for example bearer bonds, that is likely a financial transaction because the 2000 Act includes monetary instruments as an equivalent to cash for many purposes. The regulation defines monetary instruments as those that are effectively used in the same manner as, or are equivalent to, cash. If the transaction is a trade of assets that are not equivalent to money, it is probably not a financial transaction. It is necessary initially to determine if the transaction is a financial transaction because only financial transactions are included in the 2000 Act for reporting of suspicious transactions.

- 4 -

The Suspicious Transaction Reporting Regulation establishes the required report form and contents, but the requirement to report is under Section 7 of the 2000 Act. There is a series of considerations and judgements that must be made to determine if a report is required. The first consideration is the application of the provision to determine if there is reasonable grounds to "suspect". The overall starting point to considering if there is "suspicion" for the purpose of the 2000 Act should be suspicion as to the source of the funds, because reporting relates only to financial transactions relating to money laundering offences which requires the funds to have arisen from a specific list of criminal activities. The anti-terrorism amendments add the responsibility of considering the identity of the recipient of the funds. The *Anti-terrorism Act* adds as the activities which require reporting, the activity of financing of terrorist activities to that of money laundering.

Where there are any grounds to have concern about the source of the funds, the purpose of the movement of funds through a sequence of entities should be reviewed. Money laundering schemes will involve the movement of funds through a number of entities, ultimately intended to disguise the original source of the funds. If there is an appropriate explanation, and particularly where the transfer of funds is through a closed loop of identified related entities, it is unlikely that this should give rise to "suspicion". The typical tax structured arrangement moves monies through different types of entities, but all of which have a common ownership or control or identified business relationships. Money laundering efforts would need to move monies through unrelated or disguised entities to effectively disguise the source of the funds. The entire concept behind money laundering is that the original source, arising from criminal activity, is disguised. If the monies are moved in a manner which permits the clear identification of the source of those monies then the purpose of money laundering is not achieved.

- 5 -

The next concept in the definition is that the transaction is one that occurs “in the course of their activities”. There is some lack of clarity to that portion of the section, and it is difficult to determine whether in the course of their activities means the usual and ordinary course of business, so if you have a highly unusual request before you that that is not included. It would seem it is more likely that this phrase means anything that you might be doing that relates to the financial transaction or that relates to doing business in general that is in the course of business or employment duties. This is another example of the vague drafting of this statute. It is clear that the financial transaction must occur in the course of the general undertaking of the business of the reporting entity, but what it is intended to exclude is far from clear.

If a transaction request is made that you chose not to do the request does not give rise to a reporting requirement. Reporting is only required where the transaction is completed; if a transaction is not completed you do not need to report it.<sup>2</sup> Therefore in the course of their activities probably means that anything that generally has a business guise, and that is part of the business of the reporting entity is likely in the course of your activities. Inclusion of a concept limiting requirements to report to activities in the course of their activities is unusual and there is no directly applicable legislation to give guidance as to its meaning. It should be anticipated however that it will require that the necessity of recording and reporting extend to any activities actually done in the course of employment or business and not be limited to those in the usual course of employment or business.

The wording of Section 7 of the 2000 Act next requires that the reporting entity have “reasonable grounds” for suspicion, before the obligation to report arises. What does reasonable

grounds mean? Reasonable grounds is a difficult concept to deal with in law. Attempts to define the reasonable man, reasonable judgment, reasonable anything have been going on for hundreds of years, the best the courts have developed is the concept that a reasonable man is someone who is reasonable.<sup>3</sup> The answer in law is that there is no clear objective meaning to the word “reasonable”. The expression “grounds” has the legal meaning “reasons”, while “reasonable grounds” has been defined as “probable cause” which means “a reasonable ground to suspect” that person has committed a crime. This is generally more than bare suspicion but less than evidence that would justify a conviction (this is the general standard for issuing a search warrant).<sup>4</sup>

The issue is that an entity is only required to report a transaction if there are reasonable grounds, but the law does not clearly define what reasonable grounds are. Does reasonable mean that something is apparent beyond a reasonable doubt, or is something reasonable when there is only a vague concern. The legal definition as to what are reasonable grounds will evolve as the courts decide when a report should or shouldn't have been made. The exercise of judgment which will need to be made in the meantime are whether the indicators are sufficient that you reasonably should have identified the relation to money laundering. This is a statutory drafting attempt to avoid wilful blindness; to ensure that there is something less than an absolute certainty that a transaction is a suspicious transaction before reporting is required.

When asked the question of what are reasonable grounds FINTRAC representatives, in public speaking forums, have stated “when in doubt report”. That does not properly address the

---

<sup>2</sup> See section 2.4 of Guideline 2.

<sup>3</sup> A reasonable person is one who acts sensibly, does things without serious delay and takes proper but not excessive precautions.

<sup>4</sup> Black's Law Dictionary, Seventh Edition, these definitions are United States derived.

requirements of reporting entities who are balancing the rights of their clients to confidentiality and the need to report. The statute is stated to be for the purpose of assisting in law enforcement but is not a part of the Criminal Code,<sup>5</sup> therefore one must assume that the accusation inherent in a report does not require the criminal test of beyond a reasonable doubt, which assumption is supported by the more common definition of “reasonable grounds” as having “probable cause”. Therefore, a best guess as to reasonable grounds is that there are enough surrounding indications that something is outside of the ordinary course in the transaction, that doesn't amount to an absolute certainty but is more than a vague inkling. Not a great legal definition, but that is the one that we have to cope with for the present.

Reference must be made to the Suspicious Transactions Reporting Regulation to determine the extent and nature of the reporting requirements pursuant to the 2000 Act. A suggestion is made that while the 2000 Act and regulations do not require an automated system for detecting suspicious transactions, such a system may be beneficial to the business. The reason for the “beneficial” nature of an automated system, arises most specifically from the concept that the indicators may not be seen all at the same instance, for example at the presentation of an instrument at a counter or desk. An automated system would permit individual indicators to be easily aggregated with regard to a specific client. An automated system would record, and would highlight to a compliance officer, repeated, smaller transactions which would indicate an unusual pattern of commercial activity.

---

<sup>5</sup> See objects of the 2000 Act at Section 3.

## **B. Suspicious Transaction Reporting**

Effective November 8, 2001 all persons required to report under the 2000 Act were required to have implemented suspicious transactions reporting as required under the Suspicious Transactions Reporting Regulation, now consolidated as of November 6, 2003, as consolidation of SOR/2001-317, SOR/2002-185, SOR/2003-102 and SOR/2003-358.

The Suspicious Transactions Reporting Regulation imposes both individual and institutional responsibility. The regulation specifically states that an individual undertaking activities in the course of their employment will be deemed to be acting on behalf of their employer, except in very limited circumstances, which imposes responsibility on the entity for the activities of the employee. The legislation imposes responsibility on individuals, while requiring an institutional compliance regime, with responsibility laying with the reporting entity under the supervision of its directors and officers, to implement the compliance regime. This has been the pattern for compliance orientated legislation, such as the oversight of conflict of interest and investment policy for federal financial regulations, for some time. In this case, the legislation applies to each individual involved with a reporting entity, such that each individual who may encounter a transaction which is prescribed under the legislation to require reporting, including large cash transactions and suspicious transactions, is personally responsible for the recording and reporting, and personally liable for the sanctions under the 2000 Act. Employees can effectively discharge their duties and responsibilities by internal reporting to a superior within the organization. Persons who are not employees cannot comply, as to legal responsibility, using internal reporting.



A number of new reporting entities have been included under the 2000 Act as being required to record and report, although in some instances only for specified activities, under the concept that it is only financial transactions which are the subject matter of the requirement to report under the 2000 Act. As a consequence, reporting entities who would deal with other types of transactions on a routine basis have generally been required to undertake reporting only in relation to that part of their activities which would constitute financial intermediation, and in relation to financial transactions. In each instance, the listing of activities which has been included are those where the entity was considered by the legislative draftsman to be engaged in financial intermediation. Each of the reporting entities is required to ensure there is compliance as to reporting under Part I of the 2000 Act only as to that portion of their business which is directly described as being a listed activity for that reporting entity in the regulation.

The reporting of suspicions of terrorist financing, as well as any holding or control of terrorist property, forms part of the reporting regulations. The time period for reporting is included in at sections 9 and 10, and the form and manner at sections 9, 10 and 12. In addition to the other reporting requirements under the Suspicious Transaction Reporting Regulation, reports must be submitted to FINTRAC thirty (30) days after the entity first detects reasonable grounds to suspect that the transaction is related to terrorist financing. There has been no change as to the identity of reporting entities, as a consequence of the Anti-Terrorism Act amendments, and the related amended regulations.

The *United Nations Act*, R.S. 1985, c. U-2, gives the Governor in Council the power to enact regulations to give effect to measures passed by the Security Council of the United Nations. The United Nations Suppression of Terrorism Regulations, SOR/2001-260 was passed by the authority of that Act to create a list of persons where there is a reasonable ground to

- 10 -

believe that the person is engaged in a number of activities relating to terrorist activity. The Suspicious Transaction Reporting Regulation at Section 3 prohibits a person in Canada or a Canadian outside of Canada from knowingly providing or collecting by any means funds with the intention that the funds will be used, or having the knowledge that the funds will be used, by a listed person. In addition no person in Canada and no Canadian outside of Canada is permitted to deal directly or indirectly with any property of a listed person.

There is a requirement under Section 7 of the Suspicious Transactions Reporting Regulation for a Canadian financial institution within the meaning of Section 2 of the *Bank Act* to determine whether it is possession or control of property owned or controlled by or on behalf of a listed person. Under Section 8 every person in Canada and every Canadian outside of Canada is required to disclose to the Royal Canadian Mounted Police and to the Canadian Security Intelligence Service the existence of any property which is owned or controlled by or on behalf of a listed person. These provisions supplement the requirement to report under the 2000 Act, and related regulations, any dealing in funds which are reasonably believe to relate to a terrorist financing activity offense. The listing of persons, for the purposes of the regulations, are posted on the web site maintained by the Department of Foreign Affairs and International Trade, and those of FINTRAC and OSFI.

Section 9 of the Suspicious Transactions Reporting Regulation requires that where there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence that a report must be made which will contain the information set out in the schedules to that regulation. The reporting information required to be included is divided into two sections, that marked with an asterisk and that which is not. That which is not marked with an asterisk must be obtained and reported. That which is marked with an asterisk requires that

the person or entity only take reasonable measures to obtain the information under Section 51 of the regulation.<sup>6</sup> It should be noted that the asterisk code was reversed between the initial draft and the issued regulation.

All sections of the 2000 Act which involve a “money laundering offence”, now also include the “financing of terrorist activities” as an offence. As an example, the requirement under section 7 to report where there are reasonable grounds to suspect a transaction relating to a money laundering offence now includes reporting of the activity of a “terrorist activity financing offence”. Similar changes are made to effectively every section of the 2000 Act which involves a money laundering offence. Therefore, in considering whether there has been a transaction which gives rise to the need to make a report under section 7 of the 2000 Act, in addition to considering funds which appear to be related to a money laundering offence, it is also necessary to consider whether, on reasonable grounds, the transaction may involve the financing of terrorist activity, which falls under the definition of a terrorist activity financing offence.

Under Section 10 of the Suspicious Transactions Reporting Regulation suspicious transactions reports must be sent to FINTRAC within thirty days (30) after the person first detects a fact respecting the transaction that constitutes reasonable grounds to suspect the transaction is related to the commission of the money laundering offence.

FINTRAC has set up an electronic reporting system, and other than if the person or entity does not have the technical capability to send the report electronically, it must send reports to FINTRAC electronically. If the person or entity does not have the technical capability, then they

---

<sup>6</sup> The form appended to the Suspicious Transactions Reporting Regulations is mandatory, and reporting will only satisfy the regulatory requirements if filed in that form and fully completed.

may use a paper reporting format. The technical capability for reporting requires only that computer hardware and software meet the minimum standard which will support the privacy protocols which have been established by FINTRAC. If this type of hardware and software support is available, then the entity must use electronic reporting. The legislation does not however require that entities that do not have computer hardware and software which is capable of communicating with the FINTRAC computer, and of maintaining the confidentiality protocols, be required to obtain the hardware or software, rather they will be able to use paper reporting. The standards and levels of computer hardware and software support are relatively common, and it is anticipated that most reporting entities will have the appropriate support for electronic reporting. The FINTRAC website has made available programs necessary to ensure that confidentiality of the reports is maintained, and these can be downloaded from the FINTRAC website as required.

Prescribed information must be included in providing a report of a suspicious transaction. This requires two sets of information, one describing the client or any third party that the client is acting for in the transaction, and the other describing the financial transaction. Section 12 of the Suspicious Transactions Reporting Regulation sets out the information to be recorded and the schedule to the regulation, at Section 9, sets out the details of the form of report that must be used. The asterisk items must be included in the report while the non-asterisk items merely require reasonable due diligence be exercised to obtain and include that information.

The Suspicious Transaction Reporting Regulation and FINTRAC Guideline 2 outline of the standards to be followed with regard to obtaining the identification information which must be provided with the filing of a report. The standards which have been enunciated only give guidance as to the nature of the identification which must be reviewed. The difficulty for the

majority of reporting entities will be determining the level and extent of inquiry which they must make behind apparently official identification. The majority of employees of a reporting entity will have no experience in identifying falsified identification. It would seem that a visual examination of the identification provided should suffice. This is, however, not clear and the standard of inquiry has not been clearly enunciated. The reasonable expectation will be that an obvious alteration to the identification should not be accepted as required official identification. Short of an obvious alteration it would appear that the reporting entity can accept a presented, apparently valid, identification documentation. Care must however be taken to ensure that the required identification has been reviewed; the regulations and guidelines together provide an outline of the acceptable identification, which differs as to individuals and different types of legal entities.

Simply using the guideline indicators to identify suspicious transactions will not provide assurance of compliance to financial intermediaries with regard to the obligations to report and record suspicious transactions. If the financial intermediary determines to record and report only those transactions which appear to include the listed indicators under the guidelines, they could still be found to be in breach of the statute by failing to identify other, different, financial transactions that should have been noted as suspicious. It will be interesting to see whether, when funds are traced through financial intermediaries, and are found in the end result to arise from money laundering activities, there will be a *prima facie* assumption that suspicion requiring a report should have arisen.

There are no explicit statutory provisions providing objective requirements to report, which would give rise to the ability of financial intermediaries to point to those statutory requirements and indicate a compulsion to report. There will be a significant exercise of

judgment in determining whether to report a suspicious transaction. The regulations are not prescribing specific requirements, and the guidelines are purely that, guidelines. It would appear fairly clear that if a report is made based upon indicators set out in the guidelines, that should give rise to the argument that reasonable judgment has been exercised. This however is not stated and there will not be statutory protection such as would arise from objective standards as to compulsory reporting.

Although the money laundering legislation provides protection from legal claims arising as a result of a report, the question which will be raised by plaintiffs will be whether the report was required to be made in the first place. Because a judgment call has to be made as to (a) whether there are reasonable grounds to suspect, (b) whether the transaction is a financial transaction, (c) whether it is related to a money laundering offence or financing terrorist activities and (d) whether it is suspicious, a plaintiff would appear to have the right to claim that there was no mandatory requirements for making a report, and accordingly the report was inappropriately made. If inappropriately made then the protections of the statute may not be available despite the clear wording of the statute. The 2000 Act requires only that a report be made in "good faith" standard for protection from liability for making a report, but there are significant legal and constitutional questions as to the effectiveness of that provision.

FINTRAC has issued Guideline 2, to assist reporting entities with identifying situations when a suspicious transaction should be reported.<sup>7</sup> Guideline 2 lists a number of general indicators of suspicious transactions and a listing which are grouped according to reporting

---

<sup>7</sup> FINTRAC, *Guideline 2: Suspicious Transaction Reporting* (February 17, 2001); as posted on [www.fintrac.gc.ca/en/static/guidelines.htm](http://www.fintrac.gc.ca/en/static/guidelines.htm).

entity.<sup>8</sup> The guidelines presuppose industry knowledge of usual commercial practice, and indicate that transactions undertaken outside of usual commercial practice generally indicate that the funds being utilized may have originated from a criminal source, or are being channelled to terrorist activity, which gives rise to the requirement to report. Unfortunately, the guidelines cannot be taken as a complete and exclusive listing of transaction characteristics which must lead to suspicion of the transaction.

The listing of general indicators includes matters such as (a) the client admitting or making statements about the involvement in criminal activities, (b) the desire of the client not have correspondence sent to a home address, (c) the client has vague knowledge or presents confusing details about the transaction, (d) the client is secretive and reluctant to meet in person, among others. These generally indicate a client who appears to have a cavalier attitude as to the transaction or the funds or is nervous or suspicious of normal transaction enquiries or procedures. Section 4.2 indicators include an uncommon knowledge of money laundering reporting requirements. At Section 4.3 of the guideline there is a list of indicators which generally relate to the client not promptly, and effectively, providing identification. The obtaining of personal identification with regard to the client is a necessary component to money laundering recording and reporting. Other general indicators are listed in Section 4.4 which indicates an unusual pattern of cash transactions and 4.5 which provides a series of indicators generally related to there being no sound or usual economic purpose to the transaction. Section 4.6 and 4.7 provide more general indicators, the first relating to unusual account opening and use

---

<sup>8</sup> *Ibid.*, p. 14. Section 5.4 of Proposed Guideline 2 specifically lists indicators that life insurance companies and life insurance brokers and agents should consider as indicating a suspicious transaction. These include indicators such as a client who requests an insurance product that has no discernible purpose, a client who cancels an investment soon after purchase, and a client whose first or single premium is paid for from a bank account outside the country. Section 5.4 of Proposed Guideline 2 is at Schedule "A" attached hereto.

activity and the latter being the use of international transfer of funds, where it does not appear to be required in commercial transactions. Finally, Section 4.8 alerts the reporting entity to the suspicious nature of certain offshore business activity, such as frequent transfer of funds to offshore accounts or persons, where that does not appear to be a necessary part of the client's business.

Guideline No. 2 sets out for industry specific indicators that are intended to provide a basic means of identifying suspicious transactions which are most likely to occur in transactions of a reporting entity. It is suggested that if the compliance regime, and employee training, includes this listing of indicators from the guidelines, and if identification of transactions follows the recommendation of this list of indicators, that it is likely the reporting entity will be considered to have acted reasonably, and with an acceptable level of due diligence.

The 2000 Act states that the reasonable grounds must be to suspect. Again it is a poorly defined concept as to what is suspicion or "to suspect". To suspect is likely less than "I'm absolutely sure this is the case" but is somewhat more than "this doesn't feel right but there is nothing out of the ordinary". Suspicion is a very low standard for reporting, but it does have to be read in conjunction with the need for reasonable grounds. Next, the suspicion must be that the transaction is involved with money laundering, reporting is only required if the transaction is related to "the commission of a money laundering offence" or is related to a "terrorist activity financing offence". The definition of a money laundering offence does seem to be fairly clear, and it is in defined the statute. A money laundering offence, does not say includes, is part of, or any other expanding concept, it says "means", and then lists specific criminal offences which are



included.<sup>9</sup> Therefore, if the offence is not listed it is not a money laundering offence, and you don't have to report.

The listed offences, under the *Controlled Drug and Substances Act*, *Excise Act*, *Customs Act* and *Corruption of Foreign Public Officials Act*, effectively the smuggling of liquor, tobacco and or dealing in drugs should be fairly easy to define, if not to recognize. What is much more difficult is becoming familiar with the listing of offences under Section 462.31 of the *Criminal Code*. Section 462.31 specifically lists the criminal offences that constitute the money laundering offences.<sup>10</sup> It is a specific list, but the list is extensive, and it will be necessary to have some understanding of the criteria of these offences to know if the indicators involve an offence listed in that section of the *Criminal Code*. A course of action is only a money laundering offence if it falls under the specific list of criminal activity. Also the offences under statutes other than the *Criminal Code* are included and must be understood.

The *Anti-terrorism Act* provides that reporting under Section 7 must also be made where the transaction is related to the commission of a terrorist activity financing offence.<sup>11</sup> A terrorist activity financing offence means an offence under Section 83.02, 83.03 or 83.04 of the *Criminal Code* or an offence under Section 83.12 of the *Criminal Code* arising out of a contravention of Section 83.08 of that Act. The *Anti-terrorism Act* adds sections to the *Criminal Code*, as Section 83.01 and following. Those sections define “terrorist activity” and create offences, particularly at Sections 83.01 to 83.05. As an example, Section 83.02 provides that everyone who directly or indirectly provides or collects property intending that it be used or knowing that it will be used in

---

<sup>9</sup> These criminal offences are primarily the “enterprise crime” and “designated substance” offences, defined at *Criminal Code* Section 462.3.

<sup>10</sup> See also the definitions at Section 462.3 *Criminal Code*.

<sup>11</sup> See also the provisions regarding threats to the security of Canada.

whole or in part to carry out a terrorist activity, or any other act or omission intended to cause death or serious bodily harm if the purpose is to intimidate the public or to compel government or international organizations to do or refrain from doing any act is guilty of an indictable offence. Terrorism offences under the *Criminal Code* relate to the obtaining of money or property and providing it for an activity which will meet the definition of “terrorist activity”.

A “terrorist activity” is a violent act for the purpose of intimidation of the public or a government or international agency. The definition in the *Anti-terrorism Act* defines a terrorist activity as having the same meaning as in subsection 83.01(1) of the *Criminal Code*. A “terrorist activity financing offence”, which is the direct equivalent to a money laundering offence for the purpose of the 2000 Act, means an offence under Section 83.02, 83.03 and 83.04 of the *Criminal Code* or an offence under Section 83.12 of the *Criminal Code*. A terrorist activity also includes, in the sections amending the 2000 Act, threats to the security of Canada, which is given the same meaning as in Section 2 of the *Canadian Security Intelligence Service Act*. The *Anti-terrorism Act* amends the *Criminal Code* by adding after Section 83, Part 12.1 entitled “Part 11.1 Terrorism” and under Section 83.01 defines the various activities which are deemed to be “terrorist activity”. This provides for an extensive list of activities that will constitute terrorist activity.

The provisions of Section 83 of the *Criminal Code* define the offences by description of the sanctioned activity and grant powers and sanctions under the *Criminal Code* in relation to the investigation and suppression of these activities. Terrorist activity is defined as an act or omission committed inside or outside Canada, under a specified list of statutes, including matters such as aircraft hijacking, crimes against internationally protected persons, the taking of hostages and similar. The definition also includes an act or omission inside or outside of Canada in whole

or in part for political, religious or ideological purpose, objective or cause with the intention of intimidating the public, or a segment of the public with regard to its security, including economic security, or compelling a person to do or refrain from doing an act and that intentionally causes death or serious bodily harm, or creates dangers that cause serious risk to health to health or safety, causes substantial damage or causes serious interference with or disruption of an essential service facility or system. Conspiracy, attempt or threats to commit any such acts are also included.

Once a reporting entity files a suspicious transaction report with FINTRAC, the reporting entity is expressly prohibited from disclosing that it has made such a report. Section 8 of the 2000 Act states that “no person or entity shall disclose that they have made a report under Section 7 of the 2000 Act, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.” This provision prohibits reporting entities from telling their clients that they have “snitched” on them. As will be seen below, a violation of Section 8 of the 2000 Act is an offence that can lead to up to two years of imprisonment.

It is impossible to predict the standards that the courts will set in dealing with the violation of Section 8. The *Criminal Code* provides that a person cannot, at risk of criminal sanction, further criminal activity. The criminal activities which are contemplated by the relevant section of the *Criminal Code* includes money laundering. Accordingly, if a person suspects that there is a money laundering connection to a transaction, and reports it as a suspicious transaction, they have a simultaneous obligation under the *Criminal Code* not to further that suspected

criminal activity.<sup>12</sup> In such an event, it would appear that the reporting entity should withdraw from any transaction involving that person, or those activities, to avoid *Criminal Code* sanctions. If the transaction is not completed with the involvement of the reporting entity, then the reporting entity does not need to file the suspicious transaction report, based on the comments in Guideline 2. Guideline 2 issued by FINTRAC, in Section 2.4 states that the requirement to report a suspicious transaction applies only when the transaction has been completed, if the reporting entity, or the client, decides not to complete transaction there is no obligation to report.

### C. Prescribed Transactions – Large Cash Transactions

Section 9(1) of the 2000 Act states that every reporting entity shall report to FINTRAC every prescribed financial transaction that occurs in the course of their activities, subject to certain exceptions described in the regulations.<sup>13</sup> “Prescribed” means that a regulation has listed the transaction as a type of transaction to be reported. If a transaction is “prescribed” as requiring reporting it must be reported unless the transaction falls under an exception, in which case the reporting entities must keep a list of clients in respect of whom a report would have been required under Section 9(1) of the 2000 Act were it not for the exception.<sup>14</sup> The exceptions that are included are reasonably limited, and include clients such as a retail client who would normally be receiving large volumes of cash in the ordinary course of their business. The prescribed transactions can and do vary by type of reporting entity.

Changes were made to the initial draft Large Cash Transaction Regulation to better reflect the nature of the business undertaken by reporting entities. Examples of this are the

---

<sup>12</sup> See footnote 27

<sup>13</sup> Section 9(2) of the 2000 Act.

exclusion of charity casinos from the definition of "casino", and the inclusion of financial entities when they carry out various services for a person other than an account holder that would otherwise fall under the definition of another reporting entity such as a money services business. Clarification has also been included for accountants, resulting in reporting requirements being placed at the firm level, rather than the individual member of the firm. The purpose of the changes made in November of 2003 were to specifically deal with industry specific matters of application which were identified in consultation with reporting entities. They were to clarify the application of specific regulatory requirements to industries, and in many instances to add exceptions and make compliance functional for certain of the industry sectors for reporting entities.

Also included in the regulations are provisions requiring the reporting of electronic funds transfers, focusing initially on SWIFT, the Society for World Wide Inter Bank Financial Telecommunication, transfer systems, and thereafter other electronic transmission methods. Generally similar concepts to those which were included in the Regulation for the reporting of large cash transactions have been extended to electronic funds transfers, and the similar amount of \$10,000 or more has been included for the threshold for reporting of electronic funds transfers. The reporting of electronic funds transfers does include a more rapid reporting requirement, with electronic funds transfers being required to be reported in five working days, whereas a large cash transaction record is required to be sent within thirty days after any transaction occurring within twelve months after the regulation comes into force and fifteen days after the transaction occurs once the one year period expires.

---

<sup>14</sup> Section 9(3) of the 2000 Act.

The Large Cash Transaction Regulation establishes a series of exceptions to the reporting requirements. These exceptions are generally specific to the reporting entity and to specific financial transactions. The most significant exception is the exception to reporting of transactions in circumstances where the funds otherwise required to be reported have been received from another reporting entity with the responsibility to report.

Section 12 of the Large Cash Transaction Regulation establishes the reporting requirements for financial entities, and the sections following thereafter clarify these requirements and add those for other reporting entities. For a financial entity the requirement is to report receipt from a client of an amount in cash of \$10,000 or more, the sending out of Canada at the request of a client of an electronic funds transfer of \$10,000 or more and the receipt from outside of Canada of an electronic funds transfer sent at the request of a client at \$10,000 or more. The reporting requirement does not apply to a financial entity sending an electronic funds transfer to a person or entity in Canada, even if the final recipient is outside of Canada. There is a specific exemption where cash is received from another financial entity or public body. The details have been included as to the records which are required to be kept. Similar requirements have been included for other reporting entities, but in several instances deleting the requirement to report electronic funds transfers.

Reporting entities have been segregated by type of entity, and specific requirements have been included based upon the types of transaction and the nature of the customer that those reporting entities would be dealing with. Each reporting entity is specifically dealt with with an outline of the transactions to which reporting requirements apply, the contents of the reports required, and the exceptions which are available for that reporting entity. Amendments were made in 2003 to the regulation to tailor the reporting requirements to the nature of the financial

transactions that would be undertaken by each reporting entity. As an example, only financial entities which directly initiate or receive an electronic transfer of funds need report these transactions and only casinos have the need for specifically tailored requirements relating to the sale of chips or the use of casino cheques. Expanded provisions have been included relating to a department or agency of the federal or provincial government where they accept deposit liabilities in the course of providing financial services to the public.

Section 50 of the Large Cash Transaction Regulation includes a number of exceptions from reporting, primarily relating to retail businesses. These permit reporting entities to identify significant retailers, that they have dealt with for some time, where there is a routine deposit of cash in the course of business and except those deposits from large cash transaction reporting. These exemptions do not include businesses particularly prone to money laundering such as pawn brokering, or those engaged in retailing of luxury assets which have been identified as being frequent acquisitions using laundered funds.

The requirements for the ascertaining of identity of clients, commencing at section 53 of this regulation have been expanded from the initial draft, to clarify the nature of the required proof of identity, and to deal with matters such as minors and the settlers of an inter vivos trust, among others. Industry specific requirements have been included for the ascertaining of identity, and these specifically relate to the nature and type of business being undertaken, and client dealing with that particular reporting entity. Exceptions to ascertaining identity are included at section 63, and generally relate to insurance industry product purchases, or to persons who are readily identifiable from other sources or from dealings with other reporting entities.

The measures for ascertaining identity at section 64 of the Large Cash Transaction Regulation permit reliance on listed forms of identification, or the use of a cleared cheque by a reporting financial entity, confirming the focus of the regulations which permits reliance on identification, records or deposits by another reporting entity. The time for undertaking identification has also been specifically included at section 63 and the record keeping requirements arising from the review of identification at section 67.

The general requirements as to the nature of the reporting, such as requiring electronic filing, under Section 4, the time limits for reporting set out at Section 5, the requirement to determine whether a third party is involved in the transaction at Section 7, and similar are applicable to all reporting entities. The specific reports for financial transactions and record keeping is under the sections relating to specified reporting entities; for example, at Section 12 financial entities are required to report any receipt from a client of an amount in cash of \$10,000 or more, the sending of an electronic funds transfer of \$10,000 or more, the receipt of an electronic funds transfer of \$10,000 or more. The records to be kept by financial entities are specified under Section 14 and include the requirement to maintain records regarding cleared cheques. Other reporting entities require the reporting of only some specific transactions, as illustrated by the requirements for life insurance and securities dealers described later. For some reporting entities, the nature of the activities which imposes the requirement to report under the 2000 Act is limited, as it is with accountants, to financial intermediation. The intention is that the list of reporting requirements is intended to focus on the financial intermediation activities of the reporting entity.

The Large Cash Transaction Regulation also has separate, again separated by reporting entities, requirements as to the ascertaining of the identity of clients. These are again intended to



provide for identification requirements which are specifically oriented to the relationship which would be usual between the reporting entity and the customer.

Section 1, “Interpretation” of the Large Cash Transaction Regulation defines cash as notes or bills used as currency and coins. Monetary instruments are defined in the regulation. Funds is defined to include negotiable instruments such as securities, travellers cheques, blank endorsed certified cheques, and similar. These are effectively cash or an equivalent to cash, being able to be used as currency by any person because it is not in registered form, it is freely negotiable and tenderable as a close equivalent to cash. These instruments are of such nature that the person presenting the instrument can, without proving ownership, or identification, other than that which may be required under the provisions of the 2000 Act, receive replacement proceeds consisting of cash or another monetary instrument, or use the instrument for the purchase of other assets.

To deal with the compliance burden, it was decided that most reporting entities have to report cash transactions only, thereby eliminating monetary instruments and electronic funds transfers which would be the more common way of dealing with larger value transfers. The use of cash only reporting places the majority of the burden on monitoring anything other than the proverbial “suitcase of cash” on the banking institutions, who more routinely deal with monetary instruments. Reporting requirements are generally limited to financial activities.

Some reporting entities are required only to report cash and others both cash and electronic funds transfers or foreign currency exchanges. In general, financial institutions will be required to report both cash and electronic funds transfers, and reporting entities which have limited

financial intermediation such as real estate agents and accountants will be required to report cash receipts only.

The Large Cash Transaction Regulation also prescribes the large cash transaction record keeping requirements. Section 1(2) of the Regulations defines a large cash transaction record as a record that indicates the receipt of \$10,000 or more in cash in the course of a single transaction<sup>15</sup> and that contains the following information: (a) the name of each person or entity for whom the amount is deposited, or the name, address and principal business or occupation of the individual who gives the amount; (b) the nature of the transaction; (c) the time of the deposit, if it is made during business hours, or, if the deposit is made outside business hours, an indication that it was a night deposit; (d) the number and type of any account affected by the transaction, and the name of the person or entity who holds such account; (e) the purpose and details of the transaction; (f) whether the cash is received by armoured car, in person, by mail or in any other way; and (g) the amount and currency of the cash received. The requirements for the large cash transaction report must be read together with the industry specific requirements of the regulation as to transactions that are to be reported, and the nature of the records which must also be made and kept by that reporting entity with regard to the customer and the transaction.

Compliance requirements with regard to electronic funds transfer are included under the Large Cash Transaction Regulation. An electronic funds transfer means the transmission, through any electronic, magnetic or optical device, telephone instrument or computer of

---

<sup>15</sup> Section 3 of the Regulations states that two or more cash transactions or electronic funds transfers of less than \$10,000 each that are done within 24 consecutive hours and that total of \$10,000 or more are deemed to be a single transaction of \$10,000 or more if: (a) where the person who is required to keep a large cash transaction record or to report an electronic funds transfer in accordance with these Regulations is an individual, the person knows that the transactions or transfers are conducted by, or on behalf of, the same person or entity; (b) where the person or entity that is required to keep a large transaction record or to report an electronic funds transfer in accordance with these

instructions for the transfer of funds, other than a transfer of funds within Canada. In the basic reporting requirements, set out on a reporting entity by reporting entity basis, some reporting entities are required to report cash only, while others are also required to report the sending of electronic funds transfers. Essentially those required to report and record electronic funds transfers are those which would actively engage in the electronic transaction.

Most reporting entities will be entitled to rely on the financial institutions that are the generators and recipients of monetary instruments or electronic transfer of funds to report. This is the concept behind requiring most reporting entities to report based upon cash receipts only. Section 51(2) of the Large Cash Transaction Regulation states that a reporting entity does not have to keep or retain a separate Large Cash Transaction Record if the information that must be reported to FINTRAC is readily obtainable from other records that the Reporting Entity must keep or retain under the regulation.

Exceptions as to the reporting of a transaction are set out at Section 50 of the Large Cash Transaction Regulation. These provisions state that a reporting entity is not required to report transactions in the respect of a business of a client where specifically listed conditions are met. These exceptions generally relate to consistency with usual practice for the customer in the movement of funds and requires the maintenance of a list and periodic reporting of changes in practice. Exceptions are also set out in the regulation as to the need to ascertain identity of a customer, at Section 62. These generally relate to the acquisition of life insurance and pension products.

---

Regulations is not an individual, an employee or a senior officer of the person or entity knows that the transactions or transfers are conducted by, or on behalf of, the same person or entity.

Reporting entities who receive from a client, an amount in cash of \$10,000 or more in the course of a “Single Transaction”, a defined term under the regulation at Section 3, must report it to FINTRAC according to the form set out in Schedule 2 of the Regulations.<sup>16</sup> A “Single Transaction” is defined in Section 3 of the regulation which requires reporting entities to recognize and aggregate cash transaction made by a client in a 24 hour period. The standard for recognizing that more than one transaction has occurred to aggregate \$10,000 or more, is the knowledge of an employee or senior officer that is relevant. The guidelines do not give clear indication as to the level of diligence which will be required. Obviously, with extensive multi-branch financial institutions, it can be difficult to determine that this has occurred, even with prompt recording and reporting. It would seem that FINTRAC should only expect detection if it would be detected in the normal course of the undertaking of business. Any other standard of expectation would result in a requirement to engage in investigation and inquiry beyond that which appears to be contemplated by the legislation.

#### **D. Cross-Border Movements of Currency and Monetary Instruments**

Money laundering and terrorist activity is global in scope and much of the success of these activities depends on moving funds in and out of different countries. Therefore, Section 12(1) of the 2000 Act mandates that persons and entities must report to a customs officer (not to FINTRAC) the importation or exportation of any currency or monetary instruments of a value greater than the prescribed amount.<sup>17</sup> The specific wording of Section 12.1 is that the report must be made to an “officer”, and Section 12(3) specifically lists the persons who must report the

---

<sup>16</sup> Section 17 of the Regulations.

import or export of currency or monetary instruments. Note should be made that Section 12 includes more than the reporting of cash, and specifically includes the import and export of monetary instruments. An officer is defined as having the same meaning as in subsection 2(1) of the *Customs Act*, which means a person employed in the administration and enforcement of the *Customs Act* and includes any member of the Royal Canadian Mounted Police.

The dollar amount prescribed of cross border movement of funds is currently \$10,000.

Section 12 of the 2000 Act was amended by the Anti-Terrorism Act, by providing a concept that reporting is required where currency or monetary instruments are imported or exported having a value equal to or greater than the stated amount, whereas previously the reference was only to greater than. The purpose of this, is somewhat unclear. It merely moves by naming a dollar amount, the dollar amount as to the requirement down by a dollar, or so, but may be intended to add certainty as to the cut off point.

An amendment was made at Section 12(3)(a), requiring currency or monetary instruments that are in the possession of a person arriving or departing, or which forms part of their baggage, must be reported as import or export and made by that person or in prescribed circumstances by the person in charge of the conveyance. The addition is the extension of responsibility to persons in charge of a conveyance to make a report for a passenger. It is difficult to determine what would be a suitable level or nature of declaration which should be obtained from passengers by the operators of buses, ships, railway or aircraft. It is not practical to require persons operating export or transportation systems to undertake more than a

---

<sup>17</sup> Section 2 of the Regulations states that the term "officer" is used in the Regulations as such term is defined in Section 2(1) of the *Customs Act*, which reads as follows: "'officer" means a person employed in the administration or enforcement of this Act, the *Customs Tariff* or the

reasonable inquiry of their passengers, and it is downloading an unreasonable level of police type investigative powers if enquiry extends beyond that of a simple written declaration form. This is, however, an important change expanding the duties and responsibilities being placed on others to effectively do the job of identifying and reporting money laundering and terrorist activity.

An interesting amendment under the Anti-Terrorism Act is at Section 22(1). Section 22(1) under the 2000 Act required that an officer who retained money or monetary instruments forfeited under the 2000 Act should without delay send them to the Minister of Public Works and Government Services. The expression “without delay” has now been deleted by the amendments under the *Anti-terrorism Act*. One amendment which has been included, likely to some practicable purpose, is the amendment to Section 25, which extends the appeal period for a person whose currency or monetary instruments are seized from thirty days, under the 2000 Act, to ninety days after the date of seizure. A similar extension of the appeal period was made at Section 32(1), extending the sixty day appeal period by third parties entitled to claim seized funds to ninety days after the seizure.

The 2000 Act requires that any currency or monetary instruments in the actual possession of a person coming to or leaving Canada, that is imported or exported by courier or mail, or that is on board a conveyance arriving or leaving Canada must be reported to an officer.<sup>18</sup> The person reporting must truthfully answer any questions the officer poses with respect to the information contained in the report and must, on request of the officer, present the currency or monetary

---

*Special Import Measures Act* and includes any member of the Royal Canadian Mounted Police;”

<sup>18</sup> Section 12(3) of the 2000 Act.

instruments in question.<sup>19</sup> It is important to note that the requirement to report currency or monetary instruments applies to all importing or exporting persons and not just reporting entities.

**E. Anti-terrorism Act and Bill C-7 *The Public Safety Act*, 2002**

The 2000 Act was amended by an “Act to amend the *Criminal Code*, the *Official Secrets Act*, the *Canada Evidence Act*, the *Proceeds of Crime (Money Laundering) Act* and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism”, pursuant to Bill C-36 which was assented to on December 18, 2001. Under Part IV of that legislation, entitled “*Proceeds of Crime (Money Laundering) Act*”, various provisions were enacted to amend the *Proceeds of Crime (Money Laundering) Act*. Both the long and short title of the 2000 Act were amended, with the short title of the 2000 Act being amended to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Various changes were made to the money laundering legislation, most to include wherever the concept of a money laundering offence had been referenced in the 2000 Act, the additional reference of the offence of terrorist activity financing. In addition, there were a number of technical amendments made to several of the technical terms of the 2000 Act. These were not made to import the anti-terrorism provisions, but to deal with minor technical matters that had been identified in the review of the 2000 Act. As an example, the definition of “client” was amended in the latter part to delete the portion reading “and includes a person or an entity on whose behalf the person who engages in the transaction or activity is acting” with the phrase “and includes a person or an entity on whose behalf the person or the entity that engages in the

---

<sup>19</sup> Section 12(4) of the 2000 Act.

transaction or activity is acting”. Effectively the reference to “or entity” had been excluded from the prior drafting. Similarly, “courier” was defined in the 2000 Act as having the same meaning as subsection 2(1) of the *Customs Act*, whereas under the amendments, “courier” is defined to mean a courier as defined by regulation under this legislation.

The primary purpose of the changes arising from the amendments under the anti-terrorism legislation was to add the concept that the financing of terrorist activities is an offence to be dealt with in similar manner to money laundering offences, for the purposes of the money laundering legislation. Terrorist activity financing offences are defined in the amendments, and specifically means an offence under Section 83.02, 83.03 or 83.04 of the *Criminal Code*, or an offence under Section 83.12 of the *Criminal Code* arising out of a contravention of Section 83.08 of that Act. The offences referenced under the *Criminal Code* are amendments to the *Criminal Code* which were included in the *Anti-Terrorist Act*. The Criminal Code now, at Section 83.02, provides that it is an offence for anyone to directly or indirectly, wilfully and without lawful justification or excuse, provide or collect property intending that it be used, or knowing that it will be used, in whole or in part, in order to carry out an act or omission that constitutes an offence referred to in the definition of “terrorist activity”, or any act or omission intended to cause death or serious bodily harm to a civilian or any other person not taking an active part in the hostilities in a situation of armed conflict if the purpose is to intimidate the public or to compel a government or an international organization to do or refrain from doing any act. This is an indictable offence and is liable to prison for a term of not more than ten years.

“Terrorist activity” has an extensive definition under Section 83.01, but basically includes acts or omissions committed inside or outside of Canada involving (a) the seizure or the affecting of the safety of aircraft, (b) crimes against protected persons, (c) the taking of hostages,



(d) matters relating to nuclear material, (e) violence relating to aircraft or maritime navigation (piracy), (f) oil rigs, and (g) matters relating to issues such as terrorist bombing and the international conventions on the financing of terrorism. Section 83.01 goes on to include at Section (b) an act or omission in or outside of Canada that in whole or in part, for a political, religious or ideological purpose, objective or cause, is undertaken for the intention, in whole or in part, of intimidating the public, with regard to its security, including economic security, or compelling a person, government or organization to do or refrain from doing any act, and that intentionally causes death or serious bodily harm, or endangers or causes serious risk. Conspiracy, attempts or threats are also included under the offence.

Section 83.03 makes it an offence to directly or indirectly collect property, provide or invite a person to provide or make available financial or other related services, intending that they be used or knowing that they will be used for the purpose of facilitating or carrying out a terrorist activity, or knowing that they will be used by or will benefit a terrorist group. "Terrorist group" is defined as an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity or is a listed entity. Organizations periodically identified as being suspected of carrying out political, religious or ideological terrorist activity. The list created under this section is the list referred to in the discussion of compliance requirements as being the list which must be periodically reviewed and updated. This also is an indictable offence, with the offender being liable to imprisonment. Section 83.04 makes it an offence for anyone to use property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity or being in possession of property intending that it be used or knowing it will be used for such purpose. This is again an indictable offence.

At Section 83.05, the Governor-in-Council is given the power to establish a list on which it will place the entities which will then be constituted as listed entities known as terrorist groups. If the Governor-in-Council is satisfied there are reasonable grounds to believe that the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity, or the entity is knowingly acting on behalf of and at the direction of or in association with such an entity it may be added to the list and will then be considered a “terrorist group”. This list will provide guidance as to when a transaction will need to be reported; under these anti-terrorism amendments the sending of any money, or receipt of money, with or in association with one of the listed entities would require reporting. The definition of “terrorist” group is however broader than just a list of names and will require that some attention be made to the nature of entities other than those specifically listed. Simply relying upon the list published in the regulations as to what is a “terrorist group” will not be sufficient. The definition of terrorist group is not limited to the “list” but also includes an entity that has as one of its purposes or activities facilitating or carrying out terrorist activity and includes association with such groups. The requirement to determine if funding is being sent to such a group is very unclear at present.

The general basis for identifying that a transaction may relate to a terrorist activity financing offence will require being familiar with the list of named terrorist organization (under section 83.05 of the Criminal Code) or countries known for the harbouring of terrorists and terrorist activity. Preparation of the list of named terrorist organizations which will fall under the definition of terrorist group will be under Section 83.05 of the *Criminal Code*. The list is published in several government sources of information, readily available to the public, including the FINTRAC website. Reporting entities will need to become familiar with, and check periodic changes to, the list of terrorist groups for the purpose of complying with the anti-terrorism

portions of the 2000 Act. There are fairly extensive provisions now included in the amendments to the *Criminal Code*, underlying the basis for the preparation of the list of terrorist groups. If the monies are destined for one of the listed terrorist organizations, or for a country which is listed as being a haven for terrorist activity on the FINTRAC site, then it is likely that a report will be needed because of the broad definitions in the *Criminal Code*.

The *Suspicious Transaction Reporting Regulation* provides for the requirement to report a terrorist activity financing offence at Section 9.

There are significant amendments in the section of the *Anti-terrorism Act* dealing with the money laundering amendments. Section 7, the suspicious transactions reporting requirement has been amended by adding to it the requirement to report every financial transaction that occurs in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to a terrorist activity financing offence. In addition, Section 7.1 has been added, which adds the additional requirement stating that any person or entity that is required to make a disclosure under the new section 83.1 of the *Criminal Code* shall also make a report on it to FINTRAC in the prescribed form and manner. Section 83.1 of the *Criminal Code* provides that every person in Canada and every Canadian outside of Canada shall disclose to the Commissioner of the Royal Canadian Mounted Police and to the Director of the Canadian Security Intelligence Service the existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group, and information about a transaction or proposed transaction in respect of that property.

Section 9 of the *Money Laundering Act*, the general reporting section which requires every person or entity to report to the Centre in the prescribed form and manner every financial

transaction that occurs in the course of their activities, was amended by adding Section 9.1. Section 9.1 requires that every person or entity that is required to make a report to FINTRAC under any Act of parliament or any regulations shall make it in the form and manner prescribed under the 2000 Act for the report under that other act of parliament. Note should be made that reporting forms are largely dictated by FINTRAC electronic report requirements. These have been most recently changed on March 29, 2004.

The immunity section of the 2000 Act, Section 10, which provides that no criminal or civil proceedings lie against a person or entity who makes a report under Section 7 or 9 in good faith regarding their suspicions about money laundering or the financing of terrorist activities, has been amended, to add Section 7.1. Interestingly, the amendment has not added Section 9.1 to the list of protected reports and therefore the extent and scope of the civil and criminal immunity, difficult to determine at the best of times, because of the lack of constitutional authority and the uncertainty of the requirement for good faith, specifically will not extend to the reports which are required to be filed under Acts of parliament other than the 2000 Act. The purpose of this omission is unclear. [Check to ensure correct]

#### **F. Reporting Procedures**

The regulations and guidelines contain the technical provisions regarding the form of reports required to be filed. At present nine guidelines have been issued by FINTRAC, supplementing the requirements of the 2000 Act and the regulations under that Act. Guideline 1 is a backgrounder, which explains money laundering and terrorist financing, including alerting the reader to the international nature of the concern. This guideline provides an outline of legislative requirements, and an overview of FINTRAC's mandate and responsibilities, with a

view to providing a simple, plain language, guide to the view of FINTRAC as to the extent and nature of the statutory provisions. Guideline 4 outlines the basic requirements for the implementation of an acceptable compliance regime.

Guideline 2, Suspicious Transactions, includes the detailed guidance as to how to identify a suspicious transaction. It includes general and industry specific indicators. These can be used to help identify, conduct, and evaluate transactions which may involve a necessity for a suspicious transaction report.

The remaining guidelines all outline the requirements for the submission of reports, and provide the details as to the method of transmission and the contents of those reports. This includes Guideline 3, “Submitting Suspicious Transaction Reports to FINTRAC”, Guideline 5, “Submitting Terrorist Property Reports to FINTRAC”, Guideline 6, “Record Keeping and Client Identification”, Guideline 7, “Submitting Large Cash Transaction Reports to FINTRAC”, Guideline 8, “Submitting Electronic Funds Transfer Reports to FINTRAC” and Guideline 9, “Alternative to Large Cash Transaction Reports to FINTRAC”.

FINTRAC has stated it will assist reporting entities in organizing their responsibilities to complete electronic filing. The process of filing, the electronic requirements, and the confidentiality and security requirements of the browsers, are fully explained in the FINTRAC website materials. FINTRAC assists by providing downloadable browsers which will provide the appropriate level of security for the reporting process.

The electronic filing requirements are dictated initially by the nature of the reports. The report contents will dictate what must be provided, and the format for the provision of that information. The format for reports is included in the regulations and guideline information

assists in completion. The detailed contents of the reports are included in the regulations by including the report form, and this is supplemented by the guideline information. A number of the fields in the reports require mandatory completion. Failure to fully complete the report can constitute an offence because it will not constitute an appropriate filing of the report. FINTRAC has indicated in publicly issued statements that they will, at first, assist reporting entities in ensuring the reports are fully and properly completed. It should, however, be anticipated that the requirements will necessitate that the records of the reporting entity include the information necessary to complete the reports, and that the assistance will relate only to the appropriate format, and technological requirements, for a completion of the filing. The filing requirements have been amended as of March 29, 2004 and reference should be had to the FINTRAC web site for a review of technical filing requirements.

## 5. ASCERTAINING IDENTITY

### A. When One Must Ascertain Identity

An important aspect in the fight against money laundering is ensuring financial intermediaries are aware of who is conducting financial transactions and who is behind those persons. To that end, the Regulation, entitled “Proceeds of Crime (Money Laundering) and the Terrorist Financing Regulations”, sets out a number of “know your client” rules that require reporting entities to ascertain and verify the identity of their clients. The specific requirements differ somewhat by type of reporting entity.<sup>1</sup> However, generally, a reporting entity must ascertain the identity of any individual who conducts a transaction, on his or her own behalf or on behalf of a third party, for which a “client information record”<sup>2</sup> must be retained under Section 19 of the Regulation. The same requirement is made in respect of clients that are corporations, or that are neither individuals nor corporations (i.e. trusts or partnerships).<sup>3</sup> This requirement is waived if the person’s identity was already ascertained by another reporting entity in respect of the same transaction or series of transactions, or if any of the record exceptions apply.<sup>4</sup>

The tone of the Regulation is such that it appears that the reporting entity can rely on information provided by the customer, without need to officially or extensively verify, but

---

<sup>1</sup> See the “know your client” rules for financial entities and casinos at Sections 53 and 54 of the Regulation; persons engaged in foreign exchange dealing at Section 57 of the Regulation, money services businesses at Section 58 of the Regulation, casinos at Section 59 of the Regulation and government departments and agencies at Section 60 of the Regulation.

<sup>2</sup> Section 1(2) of the Regulation defines “client information record” as a record that sets out the client’s name, address and nature of the client’s business or occupation.

<sup>3</sup> Sections 55(3) and 55(4) of the Regulation.

<sup>4</sup> Sections 55(1) and 55(2) of the Regulation, provided by way of example only for the life insurance industry, the exceptions which are included in the proposed regulations generally will exclude from the need to record and report information regarding client, or transaction, where that information would be readily available in other records of the reporting entity, or would be available in the records of another reporting entity involved with that client and transaction.

reporting entities will need to ensure that they are making appropriate enquiries. It is suggested that the paperwork initiating any transaction include specific inquiries of the customer as to their identity, which must be verified by a review of publicly issued identification document, and to determine whether the transaction is being conducted on behalf of a third party. It does appear that the due diligence defences under the 2000 Act will protect the reporting entity which makes these inquiries, in written form, in the client application initiating the transaction. This list of required information can be taken from the compulsory elements of the required form of report. The compulsory information is clearly noted in the reporting forms included in the regulations. The information obtained for record purposes must include the compulsory reporting information for all transactions to be reported.

The Regulation specifies the detail of the reporting requirements, including the nature and form of report, and the contents of the report, appending the report forms as schedules. The Regulation sets out certain limited exceptions from recording and reporting which would otherwise be required, generally relating to information which would be included in the records and reports of another reporting entity. The reporting entity must confirm the identity of every individual who is authorized to give instructions in respect of an account for which a record must be kept under Section 23(1)<sup>5</sup> of the Regulation. The same requirement is made of clients that are

---

<sup>5</sup> As an example, Section 23(1) of the Regulation requires every securities dealer to keep the following records: (a) in respect of every account that the securities dealer opens, the account operating agreement or account application, which bears the signature of the applicant who is authorized to give instructions with respect to the account and which sets out the number of a bank, trust company, credit union or Caisse Populaire account in the name of that individual or in respect of which that individual is authorized to give instructions; (b) where the securities dealer opens an account in respect of a corporation, a copy of the part of official corporate records that contain any provision relating to the power to bind the corporation in respect of that account; (c) where the securities dealer opens an account in the name of the person that is not a corporation, the person's name, address and the nature of the principal business or occupation of the person; (d) every new account application, confirmation or purchase or sale, guarantee, trade authorization, power of attorney and a joint account agreement, and all correspondence that pertains to the operation of accounts that the securities dealer creates in the normal course of business; and (e) a copy of every statement that the securities dealer sends to a client. However, such reporting requirements with respect to paragraph (a) above do not apply in respect of an account in the name of, or in respect of which instructions are authorized to be given by, a financial entity or securities dealer.



corporations, or that are neither individuals nor corporations (i.e. trusts or partnerships).<sup>6</sup> The requirement does not apply to: (a) corporate accounts where the securities dealer has already identified at least three individuals authorized to give instructions; (b) accounts opened for the deposit and sale of shares from a corporate demutualization, an employee stock purchase plan or the privatization of a Crown corporation; (c) registered plan accounts; and (d) accounts in the names of foreign affiliates of a financial entity.<sup>7</sup>

There are also client identification requirements under the Suspicious Transaction Report Regulation. The reporting entity will need to obtain the customer identification necessary to complete these reports, if and when required to be filed. Those reporting forms for suspicious transactions are appended as schedules to the Suspicious Transactions Reporting Regulation.

To assure full compliance, the client records of a reporting entity should include all of the information required to be included in a report under each of the regulations. A specific question inquiring as to whether transactions have been, or will be, undertaken on behalf of third parties must be included. It does seem that written inquiry including all of the required information with a written and signed response by the customer, and a review of publicly issued identification, will suffice for satisfying the regulation's "know-your-client" rules and to have the necessary information to file the suspicious transaction or large cash transaction reports.

Note should be made that there are differences in the specifics for compliance dependent upon the industry sector, which is differentiated by the type of reporting entity.

---

<sup>6</sup> Sections 56(3) and 56(4) of the Regulation.

<sup>7</sup> Section 56(2) of the Regulation.

There are exceptions to the requirement to obtain and maintain full client information for each transaction. The exceptions are identified on a reporting entity basis, such that specific reporting entities are excluded from the requirement to provide certain of the specified information. In addition there are general exceptions included in the Regulation at Section 50, as to the nature of the transaction and Section 62 as to ascertaining identity of customers. They generally relate to transactions where the information would already be held, or where it would have been obtained and maintained, by another reporting entity. As an example, a securities dealer does not have to ascertain the identity of an individual who is authorized to give instructions in respect of an account that is opened for the sale of mutual funds where there are reasonable grounds to believe that that individual's identity has already been ascertained by another securities dealer in respect of the same transaction.<sup>8</sup> The same is true with respect to any individual who already has an account with the securities dealer or if there are reasonable grounds to believe that the account holder is a public body or a corporation with minimum net assets of \$75,000,000 and whose shares are traded on a Canadian Stock Exchange, the New York Stock Exchange, the NASDAQ Market or the American Stock Exchange.<sup>9</sup>

An effective compliance regime will require that every employee who initiates a client relationship, or an individual transaction relationship, is aware of the requirement to obtain the necessary information for obtaining of information, maintenance of records and the filing of the reports under the 2000 Act. This will include the information required in the suspicious transaction reports, as well as those required for the large cash transaction reporting requirements. The required client and transaction information is clearly outlined in the schedules

---

<sup>8</sup> Section 56(5) of the Regulation.

to the Regulation and the Suspicious Transactions Reporting Regulation. The most effective compliance regime will require that a transaction cannot be initiated unless the information has been obtained, recorded, and the back up verifications obtained. Instructions should specifically be given, together with an electronic or paper based information questionnaire, that the information must be obtained prior to undertaking a transaction which could give rise to a need to report a suspicious transaction or a large cash transaction. The list of required information can be readily prepared from the information required to be obtained and reported in the regulations, which outlines both the required client information, third party information, and transaction information.

Requirements to ascertain identity of customers are included at Section 53, to the exceptions at Section 62 of the Regulation. Section 53 of the Regulation specifically provides that every person or entity that is required to keep and retain a large cash transaction record must ascertain the identity of the individual with whom they conduct a transaction. This supplements the requirements at Section 8 of the Regulation which requires that those persons take reasonable measures to determine whether the individual is acting on behalf of a third party. Specific requirements are then included on a reporting entity basis, setting out the specifics applicable to each of the types of reporting entities. The Suspicious Transactions Reporting Regulation at Section 12 lists the prescribed information as to the client, importer, exporter, and as to the financial transaction. 12(a)(iv) requires that the prescribed information include the name and address of any person or entity on whose behalf the financial transaction, importation or exportation is conducted. Part F of the required suspicious transactions reporting form includes

---

<sup>9</sup> Section 61(2) of the Regulation.

the information relating to a person on whose behalf a transaction is conducted, although Part F is not an asterisked portion of the report, that is it is not a mandatory field to be completed, it will require the reasonable diligence be undertaken to obtain the necessary information. As a consequence, it is likely that a written inquiry, and response, as to whether the transaction is being undertaken on behalf of a third party will be needed to evidence the reasonable effort to obtain the information.

The Regulation also requires reporting entities to receive reliable evidence indicating whether or not an individual is acting on behalf of a third party. If the person is determined to be acting on behalf of a third party, the reporting entity must obtain and retain a statement, signed by the individual conducting the transaction, that sets out the third party's name, address and the nature of his, her or its principal business or occupation, and the nature of the relationship between the third party and the individual who signs the statement.<sup>10</sup> Where the reporting entity is advised that the individual is not acting on behalf of a third party, it should obtain a written statement from the individual stating that the individual is not acting on behalf of a third party.<sup>11</sup>

The identification of third parties is specifically required when a reporting entity is required to keep a signature card or an account operating agreement in respect of an account or a client information record.<sup>12</sup> It appears that, throughout the requirements for identification of third party participation, a direct question in writing to the person dealing with the reporting entity, and a written response by that person, will suffice for inquiry. Further investigation does not

---

<sup>10</sup> Section 7(2) of the Regulation.

<sup>11</sup> Section 7(3) of the Regulation.

<sup>12</sup> Sections 8 and 9 of the Regulation, respectively.

appear to be merited or required if the question is openly stated in the appropriate account opening or similar form and signed by the customer.

## **B. How One Must Ascertain Identity**

The Regulation prescribes not only when but also how a client's identity must be ascertained. This is initially to be done by referring to an individual's birth certificate, driver's licence, provincial health insurance card, passport or any similar record, other than the individual's social insurance card.<sup>13</sup> Where the individual is not physically present when the client information record is created, that person's identity may be ascertained by confirming that a cheque drawn by the individual on an account at a financial entity has been cleared or that the individual holds an account in the individual's name with a financial entity.<sup>14</sup> The Regulation also prescribes the information about an individual the must be recorded (i.e. date of birth or account number of financial entity on which cheque was drawn).<sup>15</sup>

Specific information is required to be verified with regard to corporations and partnerships, this is outlined in detail in the Regulation. These generally require review of the publicly issued or registered information included in the appropriate public record in the jurisdiction of incorporation or formation. This information will vary dependant upon the jurisdiction, but will generally require the filing maintained in the public recording office for the recording of business names, partnerships, limited partnerships or corporations.

---

<sup>13</sup> Sections 63(1)(b) and 63(1)(c) of the Regulation.

<sup>14</sup> *Ibid.*

<sup>15</sup> Section 66 of the Regulation.

- 8 -

For corporations the information can be verified from a public record which will permit confirmation of the incorporation, including the ability to obtain a copy of the incorporation documents, and the information filed with regard to the directors and officers.

Other entities may be registered under their systems, or in some instances can be formed without registration. Where an entity is formed without registration, such as a general partnership which does not require registration for the entity to be created, then the individual information as to each of the participants would appear to be required.

The legislation, even when read in the context of the Regulation and FINTRAC guidelines, does not provide an objective, statutorily dictated, level of diligence with regard to the review of presented identification and information. It would, however, appear that the standards to be followed by reporting entities must be considered in the context of the legislative intent, and the specific statements made that this is not intended to be criminal legislation. It has not been the stated intent of the legislation, or of FINTRAC in overseeing compliance with the legislation, that reporting entities are to become the equivalent to highly trained police investigators. The intention should be that reporting entities will have trained their employees, and have established their compliance systems, so as to be able to detect that a financial transaction is outside of the commercial norm, and that there is apparent reason for suspicion. This does not require that investigations be taken outside of the specific inquiries required to obtain the necessary filing information and the application of industry knowledge to identify that the transaction does not appear usual or normal.

The existence, name and address of a corporation and the name of its directors must be ascertained by referring to its certificate of corporate status and other required corporate public

findings.<sup>16</sup> Similarly, the existence of a person that is neither an individual nor a corporation would be ascertained by referring to the partnership agreement, articles of association or other similar record that proves its existence.<sup>17</sup> In both cases, the records may be in paper or electronic form provided that they are obtained from a source that is accessible to the public. This will require that a record, electronic or paper, be made of the inquiry, and that inquiry be made, beyond the information provided by the customer, of the public records. It would appear that it is not advisable to simply accept a photocopy of a partnership agreement or articles of incorporation, unless they are received from a reliable source, such as legal counsel. It would appear that access to the public records should be made and a copy of the public recording obtained and compared to that provided.

The sources for client information that are considered to be accessible to the public are those where either personal attendance, written inquiry or computer access would provide information with regard to that entity from public official maintained records. These would include the corporate profile reports for Canadian corporations now available online for both federal and provincial corporations. Similar inquiries would be available for partnerships, limited liability partnerships and limited partnerships, although the information included in the public record is more limited. For entities where only a partial public recording is available, such as registration under the *Business Names Act* or *Partnerships Act*, further inquiries should be made in many instances beyond that of the public record. For example, in the case of partnerships, this would include a written statement as to the legal relationship and the full listing of the participants in the legal relationship.

---

<sup>16</sup> Section 64(1) of the Regulation.

**BRITISH COLUMBIA LOTTERY CORPORATION**

**BOARD MEETING JULY 23, 2010**

**PRESENTATION REGARDING ANTI-MONEY LAUNDERING AND FINTRAC**

Alison R. Manzer

**PERSONAL INFORMATION**

[REDACTED]

1. **What is money laundering and what is terrorist financing?**

2. **What does the law require:**

- Recording
- Reporting
- Identifying

And what is the law focussed on:

- Large cash transactions
- Suspicious transactions
- Dealing with the wrong people
- Identifying persons who are dealing for third parties

3. **Why casinos have been selected as a reporting entity**

**What is FINTRAC concerned about that is specific to casinos**

- The conversion of dollars into casino cheque
- The conversion of cash into casino issued goods
- The conversion of foreign dollars to Canadian dollars
- The conversion of cash to casino chips
- The conversion of cash to casino with the reconversion to cash



**4. What is unique about casinos - what are the inherent risks and needed controls:**

- The ability to deal with large volumes of cash on a basis that readily appears legitimate
- High drug related involvement
- Confirmed winnings as against stoppage of play to cash out
- Refining: small denomination currency converted to large denomination currency

**5. Board Responsibilities**

- Setting Policy
- Understanding Risks
- Determining and directing management strategies
- Receiving reporting
- Monitoring effectiveness
- Assuring appropriate independent oversight

**6. Current Hot Buttons at FINTRAC**

- Move to more risk based compliance programs
- Enhanced corporate governance and changing relationships to the CAMLO
- Enhanced responsibility and training requirements for CAMLOs
- Increased training and updating training for front line employees
- Auditor effectiveness testing
- Regular efficiency testing

**7. The Risks of Failure**

- Fines - administrative monetary fines can now be imposed and are increasingly being used by FINTRAC
- Deliberate failure to comply leads to criminal offences
- Reputational risk
- Regulator intervention

**PRIVILEGED**

