Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

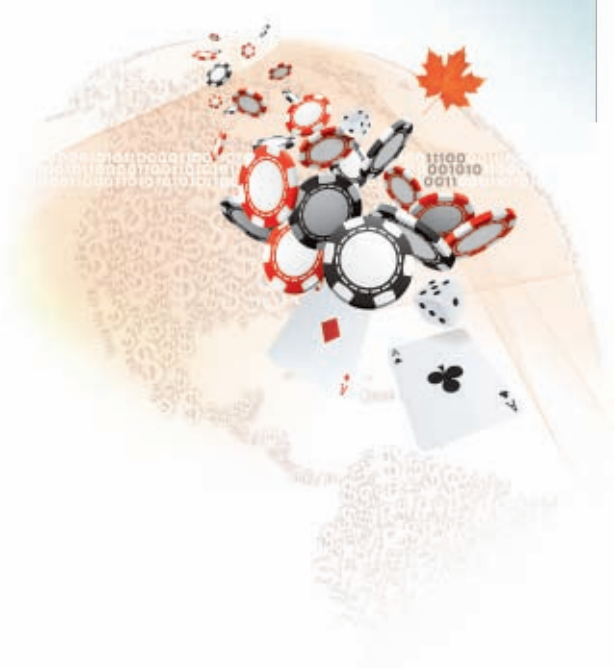
MONEY LAUNDERING TYPOLOGIES AND TRENDS IN CANADIAN CASINOS

NOVEMBER 2009

Canada

MONEY LAUNDERING TYPOLOGIES AND TRENDS IN CANADIAN CASINOS

NOVEMBER 2009



November 2009

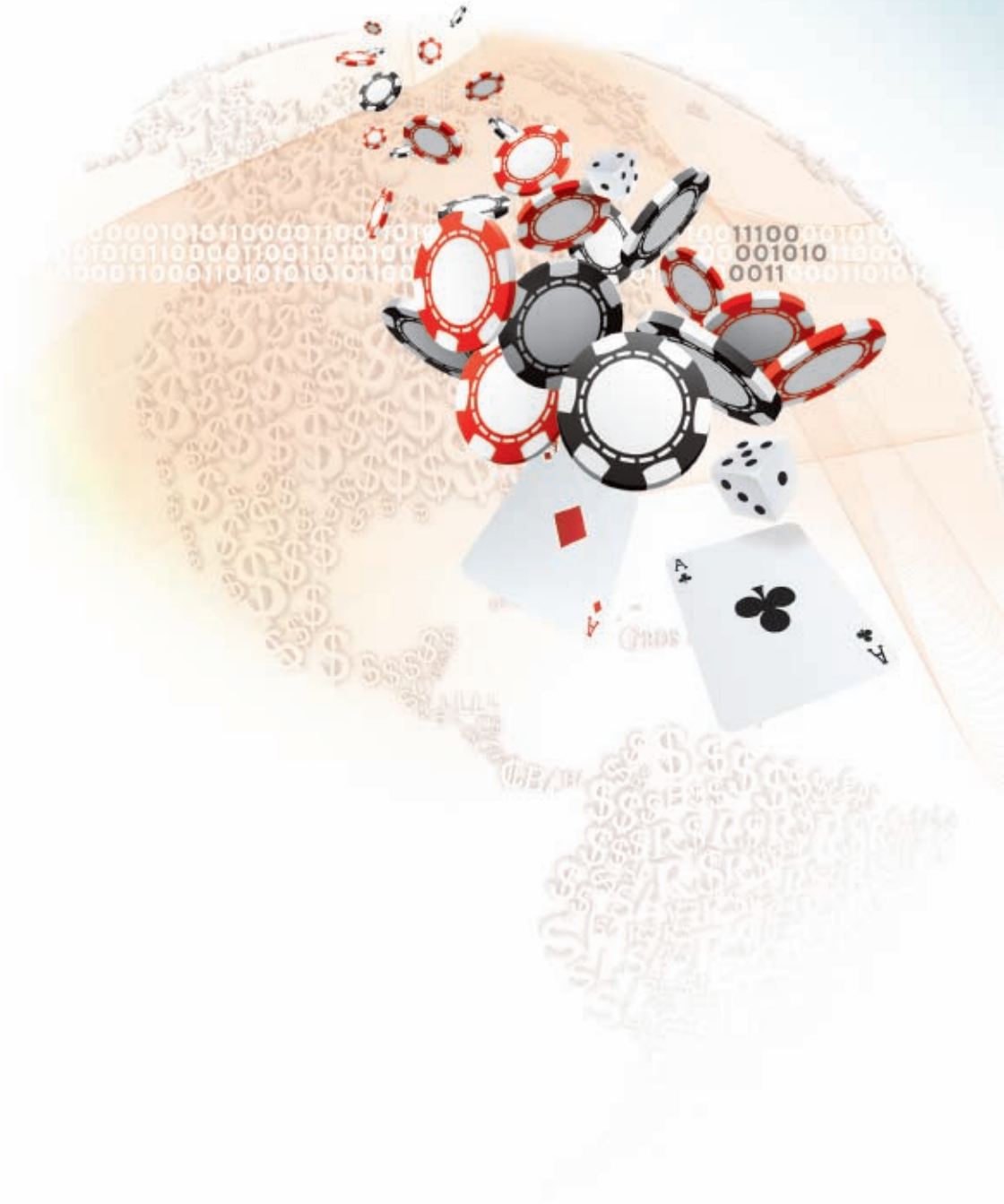
MESSAGE FROM THE DIRECTOR

I am pleased to present **Money Laundering Typologies and Trends in Canadian Casinos**. FINTRAC undertook this analysis in collaboration with the Canadian casino sector to assist it in strengthening its compliance regimes pursuant to obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. These obligations include record keeping, customer identification and reporting certain transactions to FINTRAC.

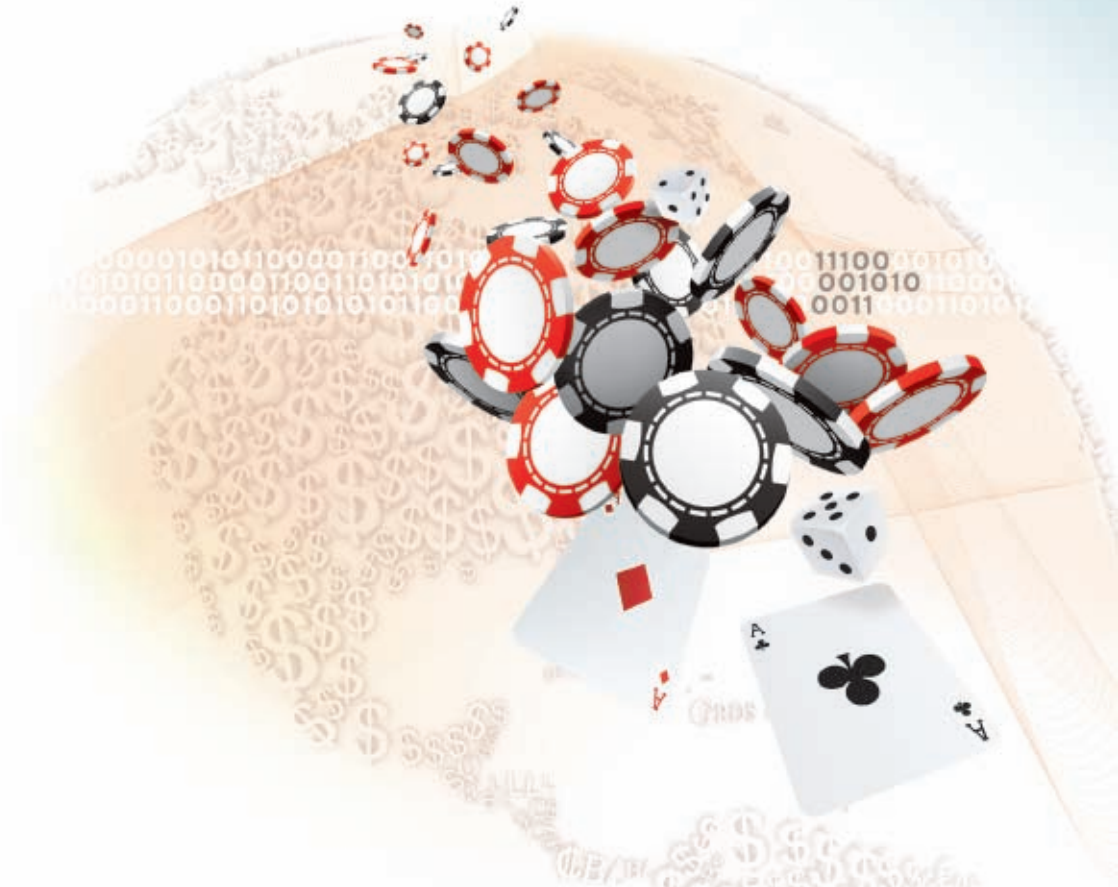
Given the nature of its business, the Casino sector is an important stakeholder in the national effort to deter, detect and prevent money laundering. As FINTRAC's Director, it is my hope that this special report will improve collaboration in support of better financial intelligence for our law enforcement and national security agencies. FINTRAC depends on receiving reports from many different sectors, such as casinos and banks, to produce this financial intelligence. The previous Typologies and Trends report produced for banks provided assistance to that sector, and I believe this special report will also go a long way in helping the casino sector with its compliance regimes.

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

Jeanne M. Flemming
Director


11100
001010
0011

CONTENTS



INTRODUCTION

This FINTRAC report is the first of its kind for the casino sector and was made possible through collaboration between FINTRAC and certain Canadian gaming operators, including Loto-Québec, the Ontario Lottery and Gaming Corporation and the British Columbia Lottery Corporation. The discussions between the casino sector and the Centre have guided the subjects that are examined in this report.

Through this paper FINTRAC seeks to address questions about money laundering (ML) that are unique to the Canadian casino sector and have been observed in our analysis of financial transactions in casinos.

There are four key sections to the report. The first section highlights the observations from a review of all of the cases FINTRAC disclosed to law enforcement and/or intelligence agencies in 2008-2009. The second section identifies typologies, methods and techniques of money laundering observed in FINTRAC case disclosures involving transactions in Canadian casinos. The third section presents actual FINTRAC cases, sanitized to ensure confidentiality, and the final section identifies money laundering risks associated with one casino service.

It is important to note that because FINTRAC is not an investigative agency, statistics related to the prosecution of, or asset forfeiture from, a money laundering or a terrorist financing case that may contain information that FINTRAC disclosed, is not included in the report. This report's focus is the intelligence that FINTRAC has been able to produce to assist investigations and the observed trends as they relate to Canadian casinos.

REVIEW OF CASES DISCLOSED BY FINTRAC IN 2008-2009

For this report, FINTRAC conducted an extensive review and analysis of all cases disclosed over the fiscal year 2008-2009 (April 2008 to March 2009).[1] The methodology for the case review involved a complete examination of all cases with a focus on some key characteristics within a FINTRAC case disclosure. For clarification, a FINTRAC case disclosure contains what is referred to as "designated information" that is prescribed by our enabling legislation. This designated information includes key identifying information from FINTRAC's analysis (e.g. name, address, bank account numbers, etc.). For the purposes of this document, the general observations presented place emphasis on the following characteristics:

- types of case/activities;
- most common predicate offences[2];
- sectors and services used for various activities associated to ML/TF;
- most common ML/TF stages and techniques used;
- most common types of businesses used in ML/TF schemes; and
- the involvement of organized crime in FINTRAC's cases.

General observations

TYPES OF SUSPECTED ACTIVITIES AND PREDICATE OFFENCES

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

- 474 cases associated with money laundering
- 30 cases associated with money laundering, terrorist financing and threats to national security
- 52 cases associated with terrorist financing and threats to national security

FINTRAC may be informed of the suspected predicate offence through information that is volunteered by law enforcement or that is included in a suspicious transaction report. In instances where FINTRAC was able to link suspected money laundering activity to a predicate criminal offence, fraud and drug-related activity were the most frequently observed suspected offences. As in previous years, for the cases where fraud was suspected, investment/securities and telemarketing fraud were the most observed. For cases where drug-related activity was suspected, the majority of cases involved the trafficking of cocaine and/or marijuana.

COMMON PHASES AND TECHNIQUES OF MONEY LAUNDERING

In reviewing the most common phases and techniques of money laundering appearing in FINTRAC case disclosures, the results are similar to previous years. The most often observed stages of money laundering were placement and layering and the most common techniques for money laundering were structuring and "smurfing." Structuring normally involves multiple cash deposits at amounts below the reporting threshold and "smurfing" is defined as multiple deposits of cash, and/or low-value monetary instruments, typically purchased from banks or money services businesses, by various individuals. Nominees (individuals and businesses) were also found to be involved in 15% of all cases disclosed in 2008-2009, a significant increase in comparison to approximately 4% of cases disclosed in 2007-2008.

[1] 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.

[2] 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.

MONEY LAUNDERING is the process whereby "dirty money"—produced through criminal activity—is transformed into "clean money," the criminal origin of which is difficult to trace.

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

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

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

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

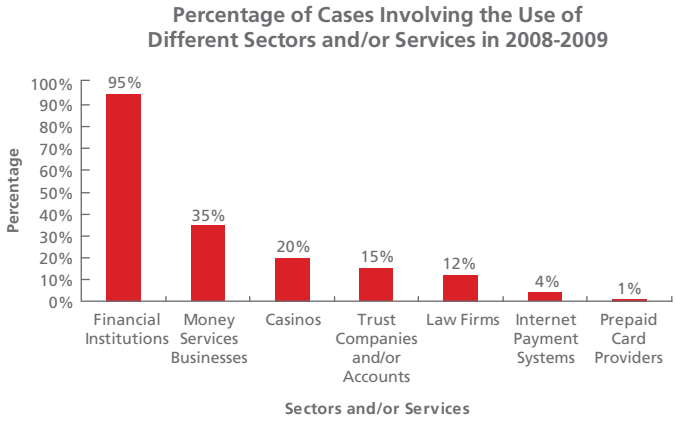
The money laundering process is continuous, with new dirty money constantly being introduced into the financial system.

SECTORS AND SERVICES USED

Reports submitted by various sectors to FINTRAC, which include suspicious transactions reports (STRs), large cash transaction reports (LCTRs) and electronic funds transfer reports (EFTRs) played a major role in assisting FINTRAC in identifying individuals and entities suspected of being involved in activities associated with money laundering and/or terrorist financing. Financial institutions were still the major contributor in terms of the number of reports received by FINTRAC. Consequently, as observed in previous years, the majority of financial transactions associated to cases disclosed to law enforcement and intelligence agencies in 2008-2009 were conducted through financial institutions.

Casinos, money services businesses (MSBs), and some trust companies or accounts—the latter service offered by trust companies or law firms—were also used to conduct financial transactions in cases disclosed by FINTRAC in 2008-2009, but to a lesser extent.[3] It was found that financial transactions were conducted at casinos in more than 100 disclosed cases. These transactions were mostly related to suspected drug offences and also to suspected fraud, organized crime activities and terrorist financing. Trust companies or accounts were involved in at least 80 cases that were suspected to be related to the same types of activities. The use of Internet payment systems[4] was observed in 20 cases, that is, 4% of all cases in comparison to 2% of all cases last year.

The following chart represents the use of various sectors and/or services for ML/TF purposes in 2008-2009.



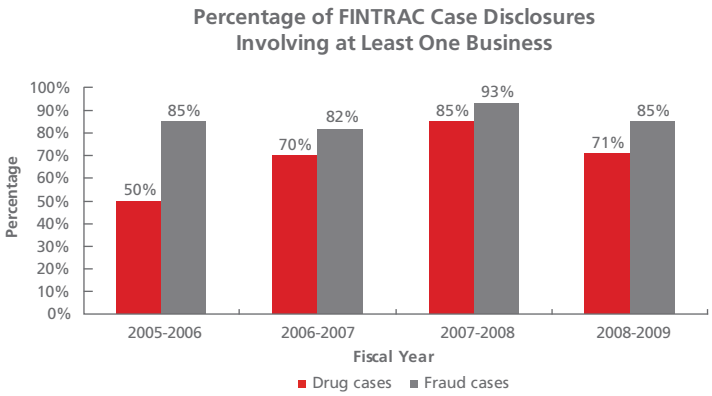
It should be noted that certain money laundering/terrorist activity financing schemes can involve the use of different sectors and/or services at the same time. For example, in 33% of all 2008-2009 cases, financial transactions were conducted through both financial institutions and MSBs. Similarly, 17% of 2008-2009 cases contained financial transactions conducted through both financial institutions and casinos. Finally, 6% of all cases involved suspicious financial transactions conducted through all three sectors (i.e. financial institutions, MSBs and casinos).

[3] 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.

[4] 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.

TYPES OF BUSINESSES INVOLVED

While in some instances, case disclosures only involved individuals, they often also involved businesses. In fact, over 70% of 2008-2009 cases suspected to be related to drugs or fraud involved individuals and at least one business and, in most instances, multiple businesses. The chart below provides an illustration of how the number of cases involving businesses has changed over the last few years.



Contrary to the noted increase from 2005-2006 to 2007-2008 of cases involving at least one business, a slight decrease was observed for both drug-related and fraud-related cases in 2008-2009, and is almost identical to the 2006-2007 percentages.

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

The following types of businesses were found to be associated to *all types of cases*, that is, they were suspected to be involved in laundering illicit proceeds or acting as vehicles for terrorist financing:

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

Additional businesses, listed here in no particular order, were found to be associated to both fraud and drug/organized crime cases[5] and included the following:

BUSINESSES ASSOCIATED TO DRUG CASES, ORGANIZED CRIME AND FRAUD CASES
Investment/securities
Food and entertainment
Business management & marketing
Construction/renovation/landscaping
Mining development or exploration
Beauty salons
Retail
Precious metals
Internet payment systems
Travel agencies

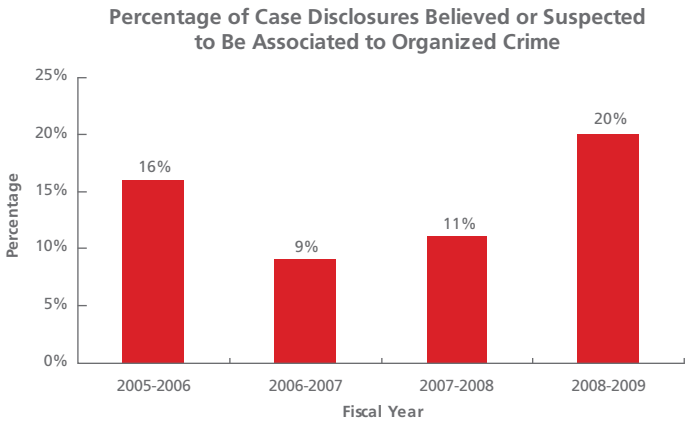
[5] Organized crime groups are often involved in various types of criminal activities which include drugs, fraud, prostitution, loan sharking, cigarette and tobacco contraband, and so on. However, because most of these cases involved drugs and similar types of businesses were used in each, organized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

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

DRUG CASES/ ORGANIZED CRIME	FRAUD	TERRORIST FINANCING
Farms/ hydroponics/ indoor gardening	Life insurance	Long distance prepaid phone cards
Real estate/land development	Technology (e.g. aviation)	
Jewellery	Medical supplies	
White-label ATMs		

ORGANIZED CRIME INVOLVEMENT IN FINTRAC CASES

The following chart shows that the percentage of cases involving individuals and/or businesses suspected to be associated to organized crime groups has almost doubled in 2008-2009 after having remained fairly stable in the previous two years: 11% in 2007-2008 and 9% in 2006-2007. It appears that FINTRAC cases have become increasingly associated with organized crime since 2005-2006, when the percentage of cases associated to organized crime was almost half that of the previous year. This increase might be due to a number of factors, including a possible increase in the number of law enforcement investigations involving organized crime.



Casino Sector

The number of cases disclosed by FINTRAC that include transactions at Canadian casinos increased significantly in 2008-2009, keeping pace with the overall increase in the number of cases disclosed. In 2008-2009, FINTRAC disclosed 112 cases which included transactions in the casino sector, compared with 43 cases disclosed in 2007-2008. This represents 20% of the total number of cases disclosed by FINTRAC, which is the same percentage as observed in 2007-2008.

TYPES OF SUSPECTED ACTIVITIES AND PREDICATE OFFENCES

All of the 112 cases involving the casino sector were associated to suspected money laundering activity. Five of these cases were also suspected to be related to terrorist activity financing and/or threats to the security of Canada.

The following table describes the most common predicate offences related to FINTRAC case disclosures involving the casino sector. Drug-related activity was most commonly observed, followed by various types of fraud.[6]

In addition, approximately 20% of the cases which included transactions in Canadian casinos involved organized crime, from street gangs, to outlaw motorcycle gangs, to traditional, transnational organized crime groups. While case disclosures involving organized crime groups related to a variety of predicate offences, the majority of case disclosures involving the presence of organized crime in Canadian casinos were associated with drug-related activity.

NUMBER OF CASE DISCLOSURES INVOLVING TRANSACTIONS AT CANADIAN CASINOS	PREDICATE OFFENCES	DETAILS
112	49% Drugs	39 % Distribution of various drugs including heroin, MDMA and methamphetamine
		23% Distribution of cocaine
		15% Production of various drugs including hashish and synthetic drugs
		12% Distribution of marijuana
	15% Fraud	40% Unknown fraud
		24% Investment/ securities fraud
		12% Credit/debit card fraud
		12% Telemarketing fraud
		12% Loan sharking
	47% Other offences, including theft, human trafficking, cigarette smuggling and corruption.	

[6] Figures included in the table do not total 100% given that some cases involve multiple predicate offences.

MONEY LAUNDERING TYPOLOGIES, METHODS AND TECHNIQUES OBSERVED IN FINTRAC CASES DISCLOSED IN 2008-2009

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.[7]

The following table identifies the most common money laundering methods observed in case disclosures involving transactions at Canadian casinos.[8] 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.[9]

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.

[7] "Vulnerabilities of Casinos and Gaming Sector." Financial Action Task Force & The Asia/Pacific Group on Money Laundering. March 2009. The terminology used by the Financial Action Task Force and the Asia/Pacific Group on Money Laundering has been adopted for this report.
[8] Figures included in the table do not total 100% given that some cases involve multiple money laundering methods.
[9] Ticket In Ticket Out (TITO) "tickets" are also an increasingly popular casino value instrument used in many Canadian casinos. Money laundering issues associated with TITO "tickets" are addressed in the fourth section of this report, which deals with vulnerabilities of specific casino services.

MONEY LAUNDERING 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[10]:

- Customers made casino chip purchases, using illicit cash[11] (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.[12]

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.

MONEY LAUNDERING 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[13] tickets, and later exchanged the TITO tickets at the cashier window for large denomination bills.

[10] Additional techniques not observed in cases disclosed by FINTRAC in 2008-2009, but which may have been observed in FINTRAC case disclosures in previous years, include:
- Using illicit funds to purchase casino chips from another casino customer, either another money launderer or an un-associated casino customer. The purchase may be made for a price higher than the face value of the casino chips which are later redeemed for a casino cheque;
- Combining casino chips with illicit funds, and redeeming both for a casino cheque.

[11] To simplify the text throughout the rest of the document, "illicit cash" or "illicit funds" is used when FINTRAC or reporting entities suspected that the origin of the funds were criminal in nature.

[12] The drug dealer receiving the casino chips may attend the same casino at a later date, and redeem the chips for cash or a casino cheque. Casino chips can also be moved across borders, to be used as currency in illegal transactions or for money laundering activity. A large dollar value can be contained within a small number of chips, which are less bulky than cash, and the chips can cross borders without declaration, since most jurisdictions do not consider them to be monetary value instruments.

[13] TITO refers to the Ticket In Ticket Out system adopted by most Canadian casinos. The system is designed to replace coins and tokens used in slot machines and video lottery terminals.

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.

MONEY LAUNDERING 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;[14]
- 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.[15] 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."

[14] The conversion of foreign currency at casinos may be related to the need to use Canadian currency in slot machines.
[15] "Vulnerabilities of Casinos and Gaming Sector." Financial Action Task Force & The Asia/Pacific Group on Money Laundering. March 2009.

ML TECHNIQUES OBSERVED

The following highlights the techniques observed by FINTRAC in 2008-2009 which suggest the use 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.[16]

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.[17] 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.

[16] In instances where this type of activity was observed, the amount of the cash or casino value instrument that was passed was not known. However, most casinos generally prohibit this type of activity, and consider it suspicious. Given that in many cases, the subjects involved in this type of activity were repeat offenders, it is inferred that this activity is undertaken to avoid casino reporting, which as of September 2009 is required for disbursements over $10,000.

[17] Priest, Lisa. "Casinos spend millions to make losers feel like winners." *Globe and Mail*. October 2, 2009.

- 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.

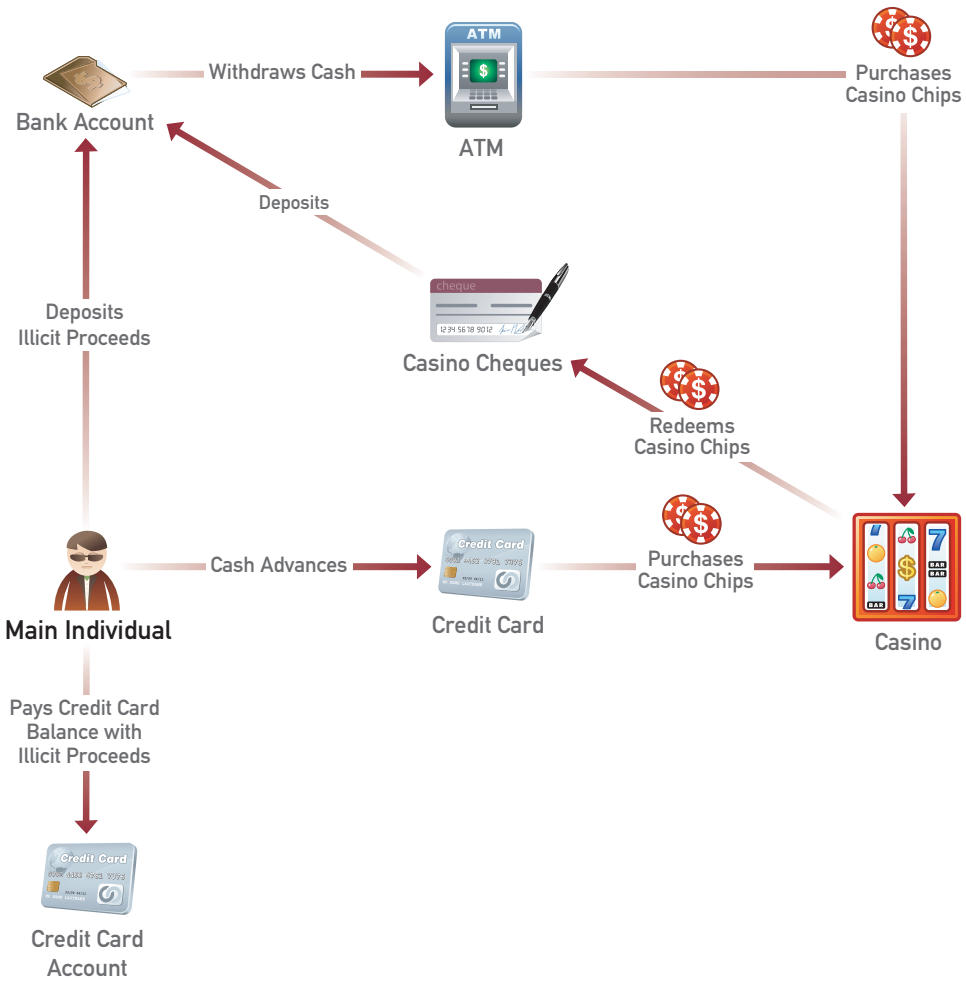
The description of the use of credit cards in casinos as part of money laundering activity highlights another feature common to many FINTRAC case disclosures involving Canadian casinos. Often, the overall money laundering process includes transactions in more than one financial sector, and transactions 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:



This case was instigated following the receipt of a suspicious transaction report from a financial institution identifying an individual that was the subject of a law enforcement investigation related to drug trafficking.

FINTRAC determined that this individual was linked to the subject of a previous case related to drug importation/exportation, residential marijuana grow operations, the exportation of stolen vehicles and fraud. Canadian law enforcement was working with a foreign partner on the international dimensions of this investigation.

Analysis of reports submitted to FINTRAC by financial institutions and casinos gave FINTRAC reasonable grounds to suspect that the individual was involved in money laundering activity using two methods.

First, it appeared that the individual deposited the proceeds of criminal activity to a bank account. The individual then layered the funds through casino transactions, making automated banking machine withdrawals at casinos and using the funds to purchase casino chips. Chips were later redeemed for casino cheques, which were deposited to the individual's bank account.

In addition, the individual obtained credit card cash advances at casinos and used the funds to purchase casino chips. The chips were later redeemed for casino cheques, which were deposited to the individual's bank account. Proceeds of criminal activity were used to pay the credit card account balance resulting from the cash advances.

Reporting from the casino sector also assisted FINTRAC in identifying two additional subjects, who were linked to the individual through financial transactions. One casino reported that a third party purchased casino chips on behalf of the main individual, and also reported that the main individual purchased casino chips for the benefit of another party. The relevant designated information related to these third parties, as well as the main individual, were disclosed to two different law enforcement agencies.

RED FLAGS associated with this case:

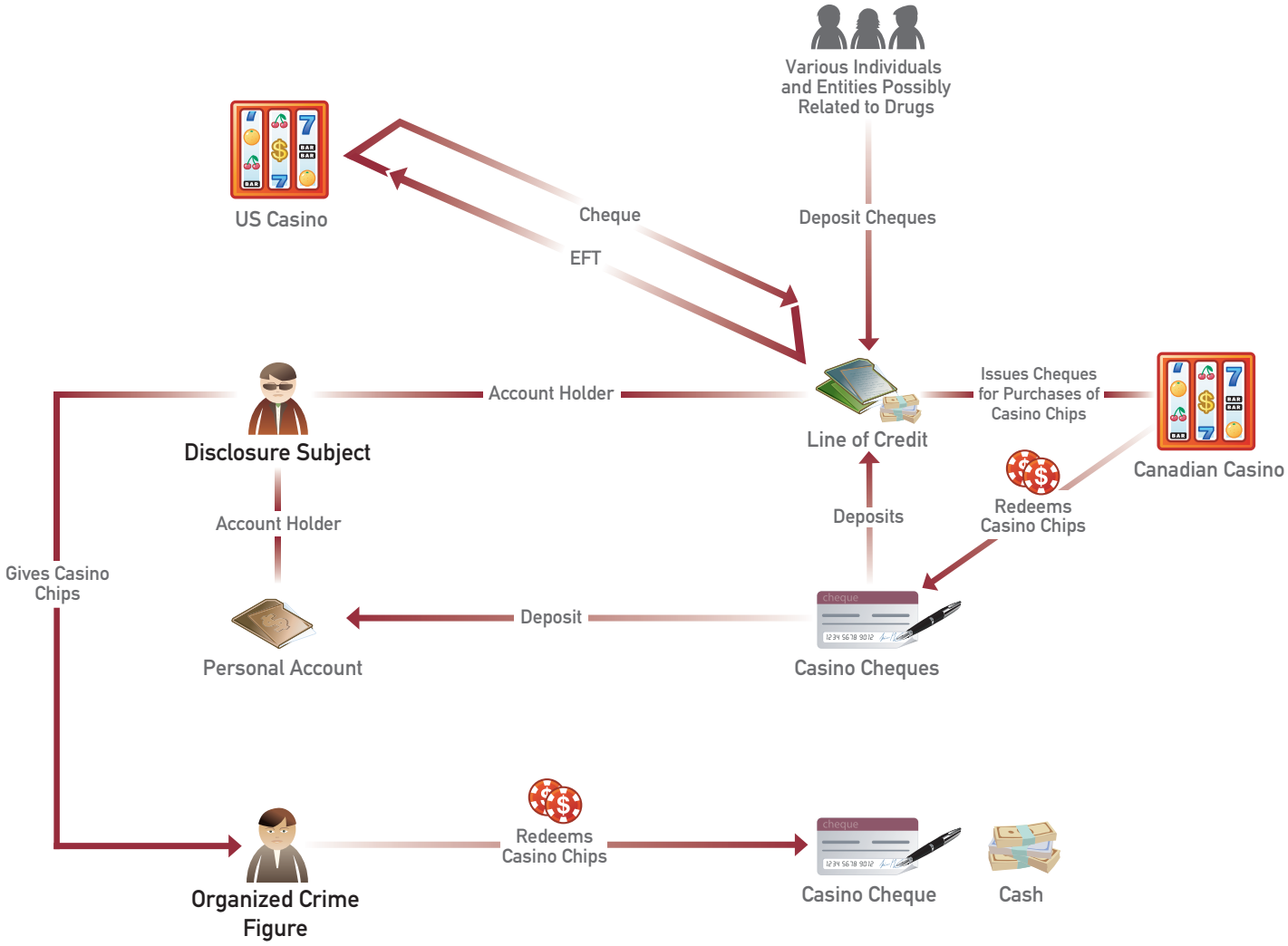
- Multiple reporting from financial institutions and casinos, as well as provincial records, indicated that the individual had provided different information regarding his/her employment. It varied from being unemployed, being an employee of a beauty salon, a homemaker or the owner of a restaurant. Casino 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:

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:

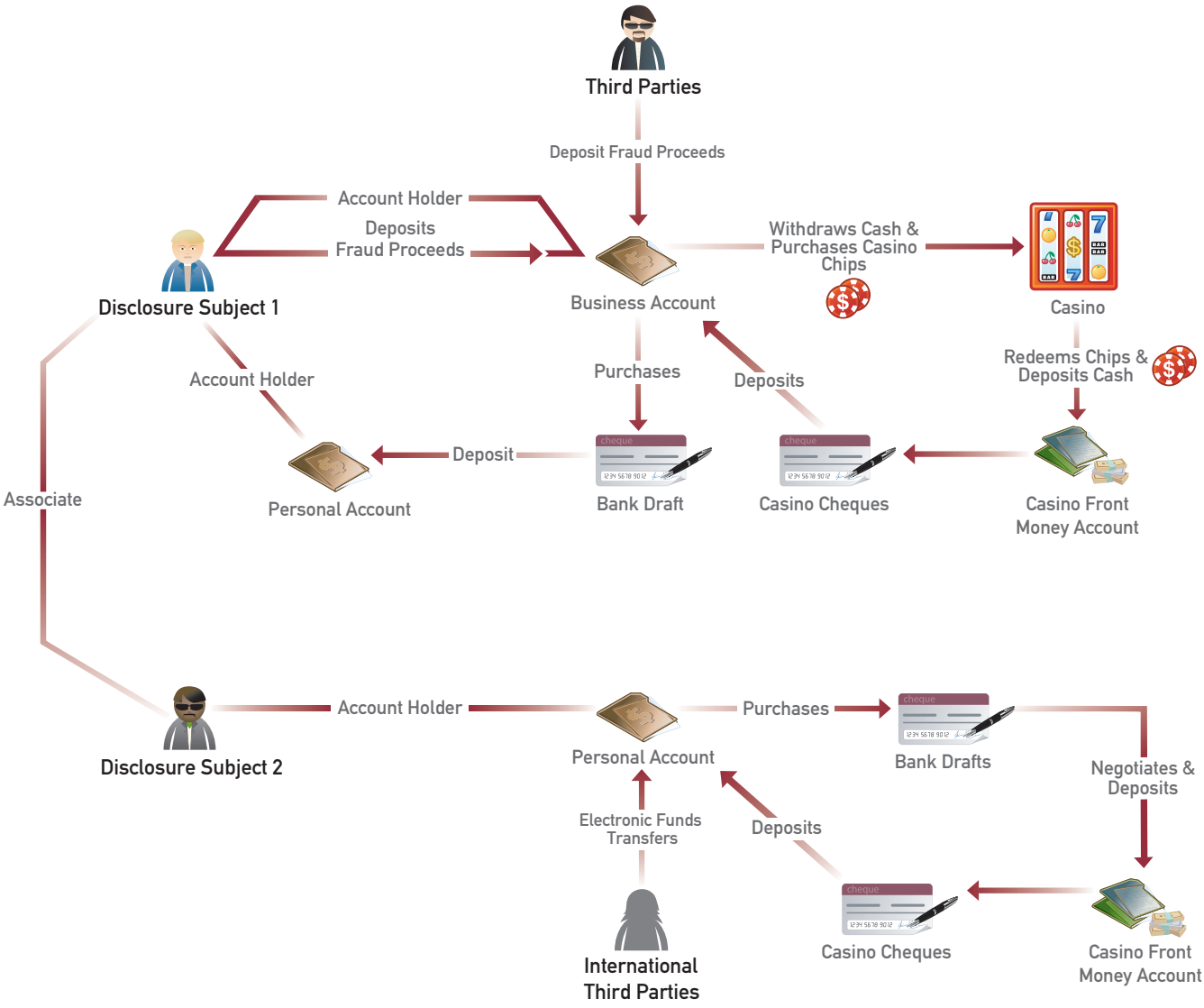
- Casinos reported cash transactions on the part of the subject totalling approximately $1.5 million over the course of a few years.
- A casino reported that the individual attended the casino accompanied by the aforementioned organized crime figure. The casino reported that the organized crime figure 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:

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.[18]

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.[19]

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

[18] The information provided is not exhaustive, and should not be construed as the risk assessment for the service. Rather, the information is meant to serve as a guide to casinos as they conduct their own risk-based assessment for the services which they provide.

[19] In May 2008, reports by the Canadian Broadcasting Corporation (CBC) into possible money laundering in Canadian casinos attracted a significant amount of media attention. These articles described how reporters were able to feed thousands of dollars into TITO-enabled slot machines, cash out without playing, and exchange a TITO ticket for a cheque issued by the casino. See "Casino loophole lets criminals launder cash, RCMP fear." *CBCNews*. May 20, 2008. See also "CBC tests system by visiting casinos, cashing out large amounts." *CBCNews*. May 20, 2008.

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

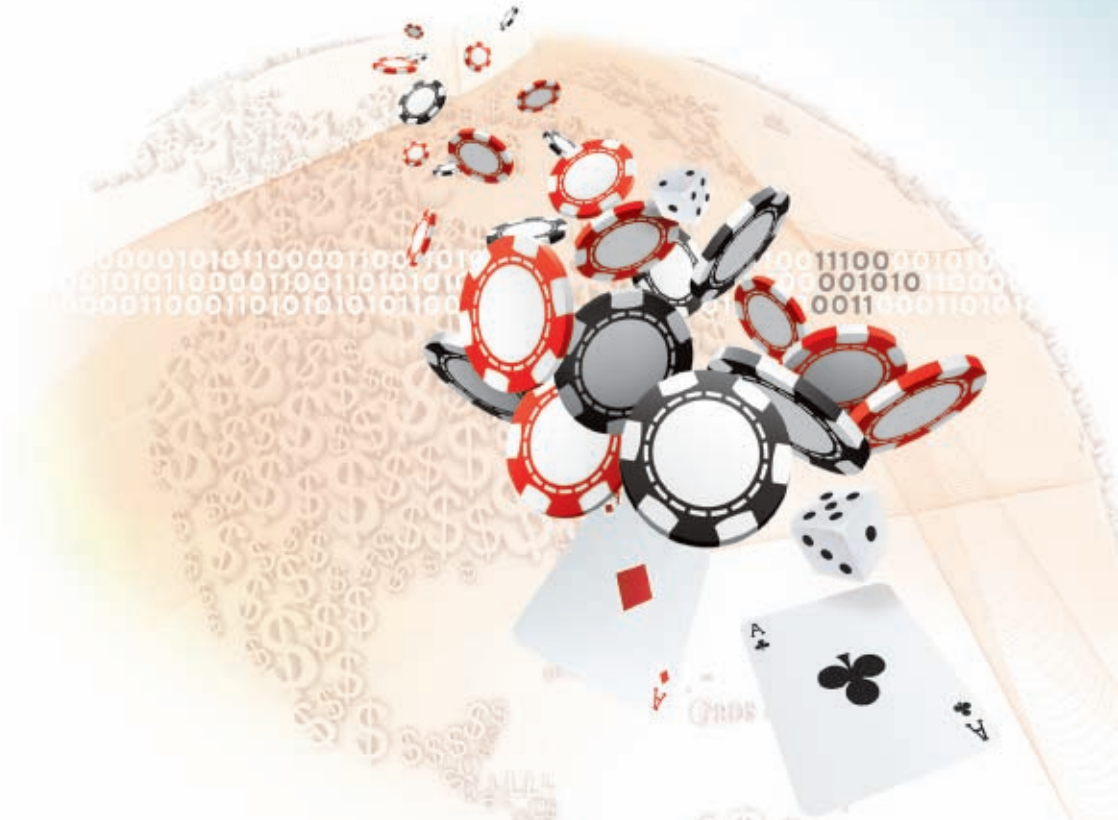
In most casinos, the TITO system has been supplemented with automated redemption machines, through which casino customers can cash out their TITO tickets automatically, without the need to visit a cashier. Although the majority of these machines include a limit in the amount of funds that will be dispensed, 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.


11100
001010
0011