The Business Crime Solution

Helping Build Practical Compliance Strategies

January 2017

Tax Evasion

Money Laundering Made Easy

This past month, articles in the press have been systematically peeling back the layers on the ease with which individuals and businesses hide their earnings from Revenue Canada using various legal vehicles available in tax haven countries. These same articles are pointing out that Canada is a major player in the 'tax haven' league through our various veiled legal practices that distance the money from who it actually belongs to --- a key piece of evidence in the tax evasion trail.

Advantages of a Tax Haven

As reported by the CBC, Barbados, a tax haven, is the number three destination for Canadian money going abroad. Corporations and wealthy Canadians have moved nearly $80 billion to the island nation, which is behind only the U.S. and U.K. as an investment destination. There is more Canadian money parked in Barbados than in France, Germany, Italy, Japan, and Russia combined.

According to the article, Barbados is where Canada first seriously waded into the waters of offshore, legal tax avoidance. Canadian companies such as Petro Canada, Loblaws and Eldorado Gold have had affiliates there for years, while Canadian banks have branches on many street

(Continued on page 4)

The Business Crime Solution

Publisher
About Business Crime Solutions, Inc.

Editorial Director
C. Jason Walker

Subscriber & Privacy Services
EDUCON Marketing & Research Systems

Contributing Experts
Christopher Walker, M.Criminology
EDUCON Marketing & Research Systems
Jennifer Wilson., BA, CAMLI-PA
Julian Arend, MA

Yearly electronic subscriptions (12 issues) to *The Business Crime Solution* are available at $250 + HST/GST where applicable (in Canadian funds).

www.moneylaundering.ca

About Business Crime Solutions, Inc.
PO Box 427
Merrickville, ON
K0G 1N0
Phone: **(613) 283-2862**
FAX: **(613) 283-7775**
E-mail: info@moneylaundering.ca

ISBN: **0-9689436-0-8**

A Word from the Editors

The spotlight has been placed on Canada this past month by several media outlets, but unfortunately not for a positive reason. Tax evasion and the ease with which it is facilitated for businesses in this country has been explored in depth on the websites of the CBC and other sources. We begin this month's issue by trying to make sense of it all.

In other news, we are pleased to announce that Money Laundering in Canada 2017 is scheduled for September 11-13, 2017 at the beautiful Hotel Grand Pacific in Victoria, British Columbia. There are a number of exciting changes planned for this year that will provide all delegates with a more in-depth and interactive experience. The preliminary list of workshops and plenary sessions is scheduled for release in early February. As space is limited in 2017, make sure to register early to secure your spot and take advantage of Early Bird pricing.

CAMLI Update: A CAMLI seminar has been confirmed to take place at the Hotel Grand Pacific in Victoria, BC immediately following Money Laundering in Canada 2017 on September 13, 2017. More details will be available soon. Join our mailing list or follow us on social media to receive the latest updates.

In This Issue:

Next Month:

- ⇨ Measuring Organized Crime in Canada
- ⇨ SIM Phone Information
- ⇨ Laundering through Trusts
- ⇨ Money Laundering in Bermuda

In the News

$425 Million Fine for Deutsche Bank

On January 30th, the New York State Department of Financial Services (DFS) announced that Deutsche Bank AG and its New York branch will pay a $425 million fine and hire an independent monitor as part of a consent order entered into with the for violations of New York anti-money laundering laws involving a "mirror trading" scheme among the bank's Moscow, London and New York offices that laundered $10 billion out of Russia.

> *Operating through the equities desk at Deutsche Bank's Moscow branch, certain companies that were clients of the Moscow equities desk issued orders to purchase Russian blue chip stocks, always paying in rubles. Shortly thereafter, sometimes on the same day, a related counterparty would sell the identical Russian blue chip stock in the same quantity and at the same price through Deutsche Bank's London branch. The counterparties involved were always closely related, often linked by common beneficial owners, management or agents. The trades were routinely cleared through the bank's Deutsche Bank Trust Company of the Americas (DBTCA) unit. The selling counterparty was typically registered in an offshore territory and would be paid for its shares in U.S. dollars. At least 12 entities were involved, and none of the trades demonstrated any legitimate economic rationale."*

The DFS statement identified a number of violations at Deutsche Bank, including:

- failing to maintain an effective AML compliance program;
- failure to keep accurate and complete records;
- inadequate risk assessments and no global standards for risk appetite;
- a weak Know Your Client program; and
- insufficient staffing in anti-financial crime, AML, and compliance units.

The DFS said Deutsche "missed numerous opportunities to detect, investigate and stop the scheme due to extensive compliance failures, allowing the scheme to continue for years."

Sources:
http://www.dfs.ny.gov/about/press/pr1701301.htm

http://www.cnbc.com/2017/01/30/deutsche-bank-to-pay-425-million-fine-over-russian-money-laundering.html

Responsible Art Market Initiative

In an attempt to curb illicit trafficking of fine art and antiques, a group of Geneva-based art professionals known as the Responsible Art Market Initiative (RAM) has published a set of guidelines designed to counter illicit activity, including ten principles for vetting buyers and sellers of art. These guidelines are intended to apply internationally.

RAM's mission is: "To raise awareness amongst Art Businesses of risks faced by the art industry and provide practical guidance on establishing and implementing responsible practices to address those risks."

Reported incidents at the Geneva art market include: the seizure of pillaged Syrian antiquities from the city's free port and the recovery of after an Amedeo Modigliani painting allegedly stolen by the Nazis

"The idea is to make sure people understand what the threat is, and it is a real threat facing the art market," said Mathilde Heaton, a former legal director at auction house Christie's who helped draft the new guidelines. "We want to play our role in also combating a much wider problem."

At a conference held in January, Riccardo Sansonetti, head of fi-

(Continued on page 7)

(Front Page - Continued from page 1)
corners. So, what is the advantage?

Alain Deneault, a Quebec sociologist and university lecturer who has written several books about tax havens, describes it this way:

You create a subsidiary in Barbados. You send to that subsidiary some assets and from there, you may transfer the assets once more to another tax haven, to another subsidiary where Canada has no link. With Barbados' very low corporate tax rate of between 1 and 2.5 percent; and a 1980 tax treaty between Canada and the Barbados, all leftover profits earned at a subsidiary based or linked to there can be brought back to Canada tax free. That 1980 treaty has enabled Canadian corporations registered in Barbados to earn income that is not being taxed at the Canadian corporate level, and subsequently Canada must replace that lost tax revenue through increasing the load of taxation on the average Canadian citizen.

A Case in Point

In the 1992 annual report of Canada's Auditor General, an entire section of the report described the "schemes" companies use to shrink their tax burden in this country. One company, which was not named, had shifted $318 million in investments to a subsidiary in Barbados. The investments earned $37 million over just six months, on which a sliver of income tax was paid to Barbados. The rest could be sent back to Canada tax free and then paid out as dividends to the company's shareholders — who themselves would enjoy generous dividend tax credits. Meanwhile, the parent company, having borrowed money to fund its subsidiary, deducted the interest it was paying as an expense and ended up with a loss on its books in Canada, paying no tax as a result.

Canada is being recognized for its tax haven activities

Canada's legal system is being used at will by corrupt politicians, drug traffickers, tax evaders, and anyone else wanting to launder the money from their criminal enterprises. Canada is one of easiest places in the world to set up an anonymous company --- a basic but effective shield to avoid inquiries from law enforcement or tax authorities. For example, a corrupt foreign politician can come to Canada and have a nominee set up a company or trust for their benefit, and make it nearly impossible for anyone to determine its true ownership.

A study of RCMP proceeds of crime cases found that nominees – individuals who front for anonymous owners – are used in more than 60 percent of cases where real estate is bought with criminal proceeds. Another review of RCMP statistics pointed out that corporate structures are used in more than 70 percent of money laundering cases in Canada. Similarly, the recent Charbonneau Commission into corruption in Quebec's public works sector identified multiple instances where anonymous companies were used to defraud the government.

Real Estate and Trusts are ways to hide dirty money sources

A Toronto Star investigation reported this month that the RCMP knows of multiple cases of Chinese government officials laundering the proceeds of corruption through Vancouver real estate. The Chinese government has also flagged Canada as a major destination for corrupt funds it plans to recover. Transparency International identified several cases that show how individuals who embezzled millions of dollars from banks and other businesses overseas have brought the money into Canada and invested it in real estate.

In the absence of beneficial ownership disclosure on property titles, Canada is seeing widespread use of nominees on titles in order to take advantage of principle residency tax exemptions and to avoid foreign ownership taxes. This problem could be addressed by requiring beneficial owners to be listed on title.

Trusts are also being widely used to avoid tax obligations. The Toronto Star investigation reported that there are around 210,000 trusts registered with the CRA, but the government estimates there to be millions of trusts with assets in the country. The exact number of trusts is unknown, as registration is not required by law and only carried through self-reporting for tax purposes. Potentially, millions of trusts could be used for tax evasion. The Canadian and provincial governments are losing millions in revenue due to these legal gaps.

One Possible Solution

A low-cost, high-impact solution to the anonymous ownership problem would be to introduce a public registry of companies, trusts, and their beneficial owners. It will cut down on red tape in police investigations, save the government money, reduce business risk, and make it more difficult for criminals to launder money and remain anonymous.

Case Study

The Use of Intermediaries, KYC Due Diligence & Beneficial Ownership

A syndicate involved in this case laundered millions of dollars using intermediaries and allowed the central criminal figure, 'Browen' of the drug supply ring, to maintain a front of being unemployed and the beneficiary of disability payments. The vast majority of transactions identified during the financial investigation involved intermediaries for Browen rather than Browen himself to deflect any possible scrutiny of his finances.

Does the profile match what you know about the customer/ business?

Even when excluding money laundering transactions, Browen's lifestyle would have appeared suspicious given his declared source of income as being a long-term benefit. While on the unemployment benefit, he owned several high value vehicles (cars, trucks, and boats), acquired a bar and later established a company with no identifiable business purpose. His business practices were also unusual, for example business expenses for the bar were paid in cash. He used intermediaries in interactions with the financial institutions and dealers which may have otherwise aroused suspicions about his unusual financial profile.

The intermediaries conducted transactions to place the cash proceeds of his drug supply so as to integrate the funds in the form of high value assets. Browen would give cash to one or more intermediaries who would purchase the vehicle from a car dealer either using Browen's cash or banking that cash and using a bank cheque. In some instances Browen's company was used as a front by the intermediary. When the vehicle was purchased, it was registered either in a Browen family member's name or in Brown's company's name.

Browen also used intermediaries to send proceeds of crime to multiple countries overseas. This was accomplished by intermediaries banking cash and wiring funds or by cash deposits to remitters. In one instance this involved the same individual remitting hundreds of thousands of dollars in multiple transactions over a few months with little explanation. Cash was also carried internationally by Lithuanian cash couriers using false passports.

Money laundering indicators:

- unexplained activity that does not fit the profile of the customer
- customers who do not know the origin of funds
- customers who do not know the receiver of funds (i.e. in cases where money is being remitted overseas)
- another individual accompanying the person making the transaction and instructing them
- purchases of valuable assets made in a third party's name
- large cash transactions to purchase assets (vehicles).

Typologies

- use of third party intermediaries
- use of front companies
- wire transfers
- cash couriers and cash deposits
- purchase of assets (vehicles)

Money Laundering Indicators in Human Trafficking

Indicators of money laundering in the context of human trafficking for sexual exploitation can be understood through three broad categories: the types of financial transactions associated with this illicit enterprise, the patterns of financial activity engaged in by those involved in human trafficking, and contextual factors. The key to appropriately identifying the significance of any of these indicators is to know your client. It is important to be able to ascertain whether financial activity is inconsistent with that expected based the client's financial status, stated occupation, type of account, or stated business activity, as well as to be aware of the number of users associated with a given account and whether any of these may be aliases. Any of the given indicators below should always be considered in conjunction with the facts of a financial transaction rather than taken in isolation: a single transaction taken in isolation may lead to a false assumption of normalcy; conversely, taking into account all indicators as well as the contexts of the customer's expected financial activity may reveal otherwise unknown links that, when looked at as a whole, might produce reasonable grounds to suspect that the transaction involves the proceeds from human trafficking.

Types of Financial Transactions

The types of transactions for which to be alert include those related to travel, accommodation, and retail purchasing that are inconsistent with the customer's expected behaviour. For example:

- multiple small payments to advertising and related promotional services over very short time periods;
- frequent purchases of both long distance and local transportation services for multiple individuals within a brief timeline;
- frequent bookings of accommodation (hotels, motels, etc.) for short stays and/or in multiple cities in rapid succession, or rent payments to multiple rental properties; and excessive low-value purchases of fast food in short timelines;
- frequent retail purchases related to the industry (make-up, lingerie, clothing, contraception) that are inconsistent with that client's expected behavior;
- credit card payments to businesses associated with the industry (strip clubs, massage parlours, modelling agencies), particularly those made after normal business hours; and
- frequent low-value purchases of bitcoin or other virtual currency, and multiple low-value electronic funds transfers (both incoming and outgoing) that appear inconsistent with normal financial activity.

Patterns of Financial Activity

Clients generally follow established patterns in their day-to-day financial activity. Abrupt changes in those patterns are a general indicator of money laundering; however, certain recurrent patterns are also indicators of money laundering related specifically to human trafficking. In particular, reporting entities should be on the look-out for recurrent transactions in unusual

(Beneficial Ownership - Continued from page 6)
locations or at unusual times, particularly those involving cash; patterns of account activity involving frequent third-party deposits; and activity that indicates a personal account may be used for business activity. Indicators to watch for include:

- Cash deposits/withdrawals between the hours of 10 p.m. and 6 a.m.; multiple cash deposits conducted at different bank branches/ATMs, possibly across different cities and provinces or an account funded primarily via third-party cash transactions.
- Frequent transactions conducted in different cities and provinces within short timelines, or an account in which deposits regularly occur in locations where the client does not reside or conduct business.
- Multiple deposits and/or incoming email money transfers or other forms of electronic transfers, possibly using a temporary address (e.g. hotel), from unrelated third parties with little or no explanation.
- A personal account that receives frequent deposits, but is typically kept depleted, showing no purchases or transactions that would indicate normal activity or an account, or an account where deposits are followed rapidly by cash withdrawals, and/or electronic transfers of equivalent amounts, particularly when those withdrawals are in a different city.
- Accounts that frequently receive email money transfers or other types of EFTs to the same beneficiary with no apparent relation to the recipient, or no stated purpose for the transfers.
- Email money transfers to third parties with alternate names (usually female) provided in brackets [e.g. betty@emailprovider.com (Bambi)].
- Large and frequent electronic transfers between senders and receivers with no apparent relationship.
- Common address provided by different people undertaking domestic/international funds transfers.
- Hotel transactions by the same individual for two separate rooms for the same dates, or hotel transactions followed by a refund for the same amount.
- Pre-authorized hotel by credit card, but accommodations are actually paid for using cash, often in rounded sums.

Contextual Indicators

There are numerous non-financial indicators that should be taken into account when considering whether a transaction may be linked to the proceeds of human trafficking. Most obviously, the presence of media reports or reports from other reliable sources suggesting that the client may be involved in criminal activity that could be the source of the funds used, particularly media reports linking the client to the sex trade. Other factors to consider include the address and phone number(s) provided by the client, particularly when these appear in media, law enforcement reports, or advertising as locations associated with prostitution. The use of third parties to execute transactions or the frequent presence of third parties watching or possessing and handing over to the client the client's own identification are also indicators of which to be aware.

By understanding these indicators and appropriately examining the contexts of the transaction reporting entities can be more certain of being able to appropriately determine which transactions should be reported to FINTRAC as suspicious transactions or suspicious attempted transactions, and to demonstrate reasonable grounds for suspicion in those reports.

(Headlines - Continued from page 3)
nancial crime at the Swiss State Secretariat for International Finance, said he welcomed the effort. "It shows the will of the private sector to set out good practice, indicated a certain maturity of the sector, and third it's very useful as a way of managing the risks," he said.

Sources:
https://www.bloomberg.com/news/articles/2017-01-25/geneva-art-world-pens-anti-money-laundering-guide-amid-scandals

http://artlawfoundation.com/fda-events/art-money-laundering-responsible-art-market-practice-guidelines/

Criminal Threat Environment & the Financial Planning Sector

Offences can occur at any stage of the money laundering cycle in which a customer engages a financial planner. The **AUSTRAC** report on the *Financial Planning Sector and Money Laundering and Terrorist Financing Risk Assessment (December 2016)* indicates that this sector is being exploited to launder money and conceal the proceeds of crime. This summary highlights some of the suspicious transactions involving this sector and includes those involving the customer, the financial planner as the conveyance, and cyber-related instances.

The customer was the suspicious party:

- A financial planner was approached by a prospective customer who had accumulated cash savings well in excess of their annual income from running their own business.
- A foreign national used a financial planner to invest a large sum of money; however, this was inconsistent with the customer's profile and the source of the funds was unclear.
- A financial planner received a phone inquiry from an individual who was seeking advice, and that individual was known to be the subject of a corruption investigation.

The financial planner as being involved in suspicious activity:

They involved structured cash deposits into financial planners' accounts.

- A bank observed that a financial planner received a number of cash deposits of less than $10,000 made by several different individuals at different bank branches, in an apparent attempt to avoid detection.
- A bank received a request by a financial planner to transfer very large sums of money between numerous bank accounts held by the planner's customer, in what the bank suspected was an attempt to obscure the source of the funds.

Cyber-enabled fraud:

The most frequently reported suspected crime type in the financial planning sector was cyber-enabled fraud. Although this threat has been apparent in this sector for several years, it has been growing in scale and sophistication. Financial planners are particularly vulnerable to cyber-enabled fraud attacks when acting as a gateway between customers and financial institutions or product issuers.

There were many reported cases in which a third party hacked a customer's email and used it to instruct the financial planner to make a withdrawal or transfer of funds, often into intermediary, or 'mule', bank accounts. There were also cases in which a financial planner's email was hacked and used to email the product issuer to request a funds transfer, supposedly at the request of the customer.

Cyber sophisticated incidents involving third parties:

- diverting a customer's phone number, in an attempt to circumvent callback controls;
- accessing a customer's email history (including attachments, drafts, and sent items) to more accurately impersonate the customer (for example, by referencing personal situations such as home renovations);
- using social media (either by hacking the account or relying on publicly available information) to gather information about the customer;
- creating a new email account using the customer's name in order to impersonate the customer;
- hacking an email account and then creating an automatic forwarding rule so that emails from the financial institution are deleted; and
- hacking a customer's computer to compromise online banking accounts.

Identifying potential cyber-enabled fraud attacks:

Many of the cyber-related suspicious transaction reported by banks referenced the constructive role that financial planners played in resolving cases, as financial planners were often well-positioned to recognize anomalous behaviour. Some reporting entities had policies to ensure that financial planners personally called customers to verify transaction requests received by email. This had proved to be a critical mitigation technique.

Financial planners described a number of indicators used to detect instances of cyber-enabled fraud, including:

- customer's email has different tone/language to customer's usual communications;
- customer's email has poor

(Continued on page 15)

Lawyers Attempting to Control AML Compliance across Society Members

A Law Society of B.C. disciplinary hearing has put under scrutiny the legal regulator's ability to police money-laundering, scams and illicit foreign investment involving lawyers.

The Case in Question

In the face of an overheated real estate market and public concerns about foreign capital last year, the society cited a West Vancouver lawyer for professional misconduct over his involvement in four questionable, three-year-old transactions. It alleged he ignored numerous badges of suspicion and misused his trust account by allowing $25,845,489.87 of offshore cash to float through it between May and November 2013. The dodgy money moves occurred under more than 20 "suspicious circumstances", according to the law society.

The Law Society's Assessment of the Case

With the veneer of legitimacy the lawyer provided, the cited money was beyond the usual purview of the authorities and could have been used in crime or even to finance terrorism. The Society lawyer said the accused lawyer "provided no substantial legal services and there was no need for him to be involved in the transactions that came to light during a [scheduled] society compliance audit" --- a professional oversight check the society makes on law firms roughly every six years.

The audit found that the first $5 million went in and out of the trust account before the lawyer in question even met the client. Specifically, there was no evidence that the accused lawyer had asked questions to determine where in fact the money was coming from.

The accused's representative argued that the whole situation was simply private parties involved in "unconventional" transactions, but that was their right and the accused decided not to interfere. The representative went on to argue that the Law Society's accusations were not clear, cogent, convincing evidence on which to tarnish his client's reputation. He went on to say that lawyers had no responsibility to investigate the source of funds beyond what their client told them.

These arguments are seen as a direct attack on the law society's stand that lawyers play a gatekeeping role recognized by the Supreme Court of Canada to ensure the integrity of trust-account transactions because money that goes in enters a "zone of secrecy" behind the shield of solicitor-client privilege.

The Law Society's Position

The law society put forth that the 'privileged communication' right serves as a curtain blocking the view of financial police and the RCMP, and as such it imposes a legal duty on lawyers to take reasonable steps before accepting any money to avoid becoming a tool or a dupe of money launderers, terrorists, or those involved in questionable real estate transactions, apparently a favourite of those engaged in hiding their dirty money.

The law society's representative argued that it is of fundamental importance that lawyers ensure their trust accounts and solicitor-client privilege are not misused. When practicing lawyers fail in that obligation, there must be robust professional discipline with a view to ensuring public confidence in the profession and its ability to regulate itself.

China Contributes Indirectly to the Control of Real Estate Prices

China has begun to dam the flood of money pouring out of its borders through new barriers to companies buying abroad and moving money out of the country. These controls extend to individuals who are putting their cash into overseas markets to buy homes and other investments.

People in China, who can normally only convert $50,000 (U.S.) a year in foreign currency, have long been technically barred from buying property overseas, but those rules have not been rigorously enforced. Now with the new year, China implemented a series of new documentation requirements on currency transactions and punishments for using money in ways the rules don't allow.

In the past, changing Chinese yuan into Canadian dollars could be done with the tap of a smartphone screen. Now, Chinese banks require paperwork that entails submitting for approval the reason a person wants to obtain foreign currency and when it will be used. A new rule then holds people liable for what they do with that money – and could bar them from exchanging money for up to three years if they are found to have used it improperly, such as for the purchase of a home.

Those in the know point out that wealthy Chinese, with corporate assets and access to sophisticated market tools for stealthily routing money around the world, are unlikely to feel much difference from the change. However, the middle class, which has become an important force in property markets in places such as Canada, the United States and Australia, will have greater difficulty to undertake such purchases.

Families that once bundled together converted currency to buy condominiums and modest houses abroad will face reviews of their currency conversions and new risks to falling afoul of the rules. The new rules include giving banks much more latitude to simply deny transactions.

The government determination to choke cash outflows appears to be serious, and could have implications that extend far beyond property and into other sectors whose payrolls and future plans are increasingly dependent on Chinese money, such as universities and tourism operators.

The goal with currency conversion restrictions is to deter the vast majority of people from converting sizable amounts of money through undertaking foreign spending practices. For example, every month, Chinese people spend between $15-billion and $20-billion abroad on services such as tourism and education. China's new money-flow requirements will restrict the number of people who can travel and study abroad. The same controls will inhibit the purchase of foreign real estate and consequently close the opportunities to launder illegal profits through such purchases. Only time and good statistics about the outcomes will confirm that these new rules are having an effect.

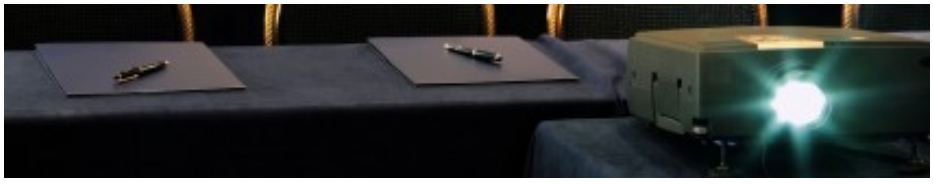
Upcoming Events:

September 11 - 13, 2017
Money Laundering in Canada 2017
Hotel Grand Pacific
Victoria, British Columbia

http://www.moneylaundering.ca/public/service/servicemlincanada.php

September 13, 2017
CAMLI Workshop
Hotel Grand Pacific
Victoria, British Columbia

More information coming soon



The DARK Side of Giving

Gift Card Fraud

Gift cards are an easy and convenient way to get a little something special for loved ones and **e-gift cards** are increasingly becoming a lucrative way to commit fraud and to launder money. A recent article reported that "Gift card fraud is rampant online, spiking between Black Friday and Christmas". One study looked at hundreds of millions of transactions from global retailers during the 2014 and 2015 holiday shopping season --- designated as a combination of the Black Friday sales period through the Christmas/New Year holiday season --- and electronic gift cards showed the highest fraud attempt rate; specifically in 2015, 9.5% of all online fraud attempts involved downloadable e-gift cards.

Online shopping has been the significant driving force behind this growth. In Canada alone, authorities estimate that organized crime are using the gift card loophole to launder money to the tune of somewhere between $5-billion and $55-billion a year.

Why this is an attractive way for money laundering is clear -- there's relative anonymity without the need for buyers to disclose their identity. This makes it easy to store money on a gift card without leaving a trace. Gift cards are not considered monetary instruments, therefore, there is no requirement for merchants or sellers of gift cards to track, record, or report suspicious transactions. As a result, someone can load a gift card with the intention of money laundering thousands of dollars, bring it across Canadian borders without declaration, and have no legal repercussions or have the gift card seized by authorities.

Can this be Controlled?

Some experts suggest that reforms and immediate action need to be taken to stem this flow of dirty money through the gift card sector. One step would be to expand the use of Regulatory Technologies (RegTech) solutions to the retail or ecommerce sector. RegTech such as *Identity Verification tools* help businesses instantly identify and verify customers electronically. Financial institutions use these tools to satisfy compliance obligations and to identify possible fraudsters before they can commit fraudulent transactions or financial crime activities, including money laundering and terrorism financing.

Those businesses that integrate electronic Identity Verification tools are able verify the identity of the cardholder and check it against fraud and AML watch lists upon online registration. For example, a retailer can verify the full name, address, and date of birth of the cardholder by checking the customer data against records from credit bureaus, government, utility files, telecommunications and other reliable data sources.

By checking against the records, a positive and seamless ID verification process can keep legitimate customers happy, while shutting out criminals. This also helps the merchant de-risk and cancel the order if they feel any transaction may be fraudulent. Other solutions will emerge over time, but until the current risks are managed, gift cards as a loophole for online fraud and money laundering will be a gift that keeps on giving for criminals.

Mortgage Fraud on the Rise

Equifax Canada recently reported that high-risk and suspected fraudulent mortgage activity is on the rise, citing a 52 percent increase in suspected fraudulent mortgage applications since 2013. This survey, involving a cross-Canada sample of 1,547 respondents, noted the following observations regarding mortgage applicant beliefs:

- 13% of Canadians indicated they felt it was okay to tell "a little white lie" when applying for a mortgage to get the house they want;
- 16% viewed mortgage fraud as a victimless crime; and
- 8% admitted to misrepresenting the facts on a credit or loan application.

More mortgage applications are being flagged as suspicious by reporting institutions according to an Equifax Canada official.

Equifax wants to remind people that there are serious consequences for making false or inaccurate claims on any loan or mortgage applications. Not only will it stretch the mortgage holder's finances, but it is also a breach of the mortgage holder's contractual obligations with the lender, and bottom line, it's against the law.

When the survey respondents were asked about who they trust in the home-buying experience, the responses showed the following:

- 44% of Canadians trust real estate agents the least during the home-buying experience;
- 27% distrust homeowners;
- 26% distrust home inspectors;
- 20% distrust mortgage brokers;
- 16% don't trust their bank or their insurance agent; and
- Only 9% said they trusted all professionals involved in the home-buying experience.

The increase is significant. The rationales for doing it are not surprising. Furthermore, the breadth of distrust says a lot about home purchasers' experiences with the whole process.

RCMP Identify a New Fraud Threat

The RCMP have issued a warning to retailers to check all point-of-sale card readers for a new security threat, a threat they have linked to organized crime: so-called "shimmers". These are an evolution of the well-known credit card skimmer, and they are the newest method fraudsters have developed to steal debit card and credit card information. Smaller and more powerful than their predecessors, shimmers are effective and very difficult to detect.

According to the RCMP, they have essentially made the old skimmers obsolete. Unlike the skimmers that have been in use so far, shimmers fit inside card readers and are designed to be installed quickly and without being detected. Criminals can slide the shimmer into the card reader while pretending to make a purchase or withdrawal from the machine. Once the shimmer has been installed, it records information from any cards inserted into the machine, including the user's PIN. The information can be retrieved by the criminals at a later date by inserting a specially designed card that downloads the data from the shimmer – again, under the guise of using the machine to make a purchase or withdrawal. Once extracted, the data can be used to make fake cards.

The RCMP is advising businesses to test all of their point-of-sale card readers – the telltale sign of a shimmer having been installed is the cards consistently sticking when one attempts to pull them out: beyond that there is little sign. In order to avoid the dangers of stolen data from shimmers, the RCMP suggests that consumers use the tap function, as little data is transferred in such instances and the data involved cannot be used to clone cards.

Money Laundering on a Large Scale Requires Insiders

Investigators across the globe report that a truly successful money laundering scheme requires help from the inside. In other words, banks caught up in helping bad guys launder their money must assist directly in that process. The massive fines levied by banking regulators over the last five or six years are clear evidence that this is the case. The latest fine of USD $235 million laid by New York's state bank regulator against the Italian bank *Intesa Sanpaolo* was in response to identified "sweeping violations" of anti-money laundering laws as well as deliberately concealing information from bank examiners.

Specifically, this large financial institution was shown to have failed to flag questionable transactions and deviated from policies designed to root out wrongdoing, which "seriously (compromised) the security of the international financial system".

The problems were first identified in and addressed in 2007. Since then, Intesa has failed to upgrade its practices for combating money laundering, as it promised in a 2007 agreement, and failed to maintain "true and accurate books" of transactions, as required under New York banking law.

Bank staff have missed thousands of alerts of suspicious transactions and wrongly classified a large percentage of alerts as "false positives", which meant they were dismissed when they should have been probed more fully. Bank officials used "opaque methods and practices" to conduct more than 2,700 US dollar clearing transactions between 2002 and 2006, amounting to more than $11 billion on behalf of Iranian entities, the agency said. This allowed Intesa to thwart supervision from regulators of transactions that may have violated US sanctions.

The agreement signed by the bank to pay the $235 million fine included an agreement to extend for up to two years an independent consultant to upgrade its anti-money laundering system.

Money laundering on a large scale requires insider cooperation and the activities of Intesa Sanpaolo demonstrate the degree of cooperation that can be involved. Compliance officers can be involved as well. Regular, scheduled assessments of the effectiveness of AML/CTF compliance controls is one method to determine if such internal complicity is at play in your organization.

...You Asked

By definition, my company operates as a payments processor. In other words, our customers contract with us to collect regular payments from their customers, such as monthly rent and mortgage payments; as well as make payroll payments to company employees. Am I required to put in place an AML/CTF compliance regime as a reporting entity under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*? --- *Payment Processor, Alberta*

FINTRAC has been very clear about businesses that operate as payment processors. Specifically, it takes the position that persons or entities engaged in the business of: utility bill payments, tuition fees payments, payroll and commission payments, and mortgage and rent payments, that involve the "remitting or transmitting of funds by any means or through any person, entity or electronic funds transfer network" are not considered to be MSBs because they are not engaged in the business of doing remittance or transfers of funds.

In the same way, if the only reason a person or entity sends funds in a foreign currency is to pay the client's bills that are in a different country, that tends to indicate the person or entity is in the payment processing business, as opposed to being engaged in the business of foreign exchange dealing.

In this case, the remittance or transferring of funds or the act of foreign exchange are reflective of the payment processing process and included in that activity. Therefore, you are not required to put in place an associated compliance regime.

Beyond Our Borders

Vietnam & Money Laundering

The Socialist Republic of Vietnam is located in Southeastern Asia, bordering the Gulf of Thailand, Gulf of Tonkin, and South China Sea, alongside China, Laos, and Cambodia. According to the U.S. State Department, ***International Narcotics Control Strategy Report*** **(INCSR - 2016)**, Vietnam is not an important regional financial centre, but it is the second fastest growing economy in Asia, and is a site of significant money laundering activities. Vietnam remains a largely cash-based economy and both U.S. dollars and gold are widely used as a store of value and means of exchange. However, aided by a stable Vietnamese dong and low inflation, the government is reducing the use of both gold and U.S. dollars, and continues to be successful in de-dollarizing the economy.

Remittances are a large source of foreign exchange, exceeding annual disbursements of development assistance and rivaling foreign direct investment in size. Remittances from the proceeds of narcotics in Canada and the United States are also a source of money laundering as are proceeds attributed to Vietnam's role as a transit country for narcotics. Other sources of illicit funds in Vietnam include public corruption, fraud, gambling, prostitution, counterfeiting of goods and trading in counterfeits, and human trafficking.

Money Laundering & Terrorist Financing

The Vietnamese banking sector is in a state of transition from a state-owned to a partially privatized industry. Currently, approximately 50 percent of the assets of the banking system are held by state-owned commercial banks, which allocate much of the available credit to state-owned enterprises. In 2015, the State Bank of Vietnam (SBV) took over three failing private commercial banks, effectively increasing the consolidation of the banking sector under state control. Almost all trade and investment receipts and expenditures are processed by the banking system, but neither trade nor investment transactions are monitored effectively. As a result, the banking system could be used for money laundering either through over or under-invoicing exports or imports or through phony investment transactions. The INCSR – 2016 lists Vietnam as a Country of Concern for money laundering.

After making high-level political commitments to address its strategic anti-money laundering/countering the financing of terrorism (AML/CFT) deficiencies, the government of Vietnam set out a revised action plan in 2011 to adequately criminalize money laundering and terrorist financing, establish adequate procedures to identify and freeze terrorist assets, improve the AML/CFT supervisory framework, enhance customer due diligence and reporting, and strengthen international cooperation. However, the INCSR – 2016 claims that Vietnam has not made adequate progress in bolstering its AML/CFT regime. Despite being somewhat compliant with international standards, Vietnam and its AML/CFT regime remain deficient in several sectors, including banking, law enforcement and the judiciary.

Vietnam takes an *all serious crimes* approach to predicate offences for money laundering, but under the Penal Code, all offences can be predicate offences. Furthermore, the Penal Code does not cover all of the FATF-designated categories of offences. Current provisions define money laundering as an independent criminal offence; however, they do not comply with international standards, as they require an inordinately high burden of proof to pursue money laundering allegations. Self-laundering is not an offence.

There is also a lack of regulations providing guidance on how to implement the legislation effectively. The Penal Code does not define “property” in line with international standards, which limits the offence for money

laundering. The legal profession is not subject to criminality under the legal code as it currently stands, and there is no provision for enhanced due diligence pertaining to domestic Politically Exposed Persons.

Credit institutions, money changers, remittance agents, insurance, securities dealers, casinos and games of chance are all subject to Suspicious Transaction Reporting (STR) obligations, but compliance is seen as low. While Vietnam has now instituted an electronic database for STRs and STR filings have subsequently increased, there is no mechanism to monitor compliance with STR reporting guidelines, and the SBV cannot share data with law enforcement electronically, which further limits its enforcement. Vietnam has a system in place for asset forfeiture, but it is not in line with international standards, particularly with respect to implementing UN resolutions and freezing terrorist assets in accordance with these resolutions.

Drug Flow / Transit

Vietnam remains an attractive illicit drug transshipment point for local and international criminal organizations, including West African drug syndicates. Vietnamese law enforcement have identified both Vietnamese and foreign nationals smuggling illicit narcotics from China, Laos, and Cambodia through Vietnam and onwards to Canada, Australia, and the United States. In addition to conventional land- and sea-based drug trafficking routes, there has also been an increasing use of commercial aviation routes.

In June 2012, Vietnam ratified the UN Convention against Transnational Organized Crime (UNCTOC).

Corruption

As a matter of government policy, Vietnam does not encourage or facilitate illicit production or distribution of narcotic or psychotropic drugs or other controlled substances, or the laundering of proceeds from illegal drug transactions. No information specifically links any senior government official with engaging in, encouraging, or facilitating the illicit production or distribution of drugs or substances, or the laundering of proceeds from illegal drug transactions. Nonetheless, Vietnam is ranked 112 on Transparency International's *Corruption Perceptions Index* for 2015, which ranked 168 countries world-wide, based on how corrupt their public sector is perceived to be. Vietnam ratified the UN Convention against Corruption in June 2009.

Next Steps

The INCSR – 2016 recommends that Vietnam take the following steps to begin to bring its AML/CFT regime into compliance with international standards:

- reform and clarify the Penal Code to strengthen and clarify its system for asset seizure;
- improve enforcement by mitigating corruption and developing the political will to investigate and prosecute money laundering offences;
- encourage the SBV to analyze the financial data generated by reporting and work with government officials to share this data with law enforcement.

(Continued from page 8)

grammar, spelling mistakes, or uncommon terminology;

- customer usually contacts the financial planner by telephone, then suddenly makes contact by email;
- customer changes bank details soon after changing other details such as contact address or phone number;
- customer emails express urgency – for example, claiming the customer is travelling overseas, attending a funeral, or purchasing a property;
- requests for the financial planner to complete application forms on the customer's behalf, then to send back to customer for signing; and
- email requests to send funds overseas.

Source:
http://www.austrac.gov.au/sites/default/files/financial-planning-sector-risk-assessment-WEB.pdf