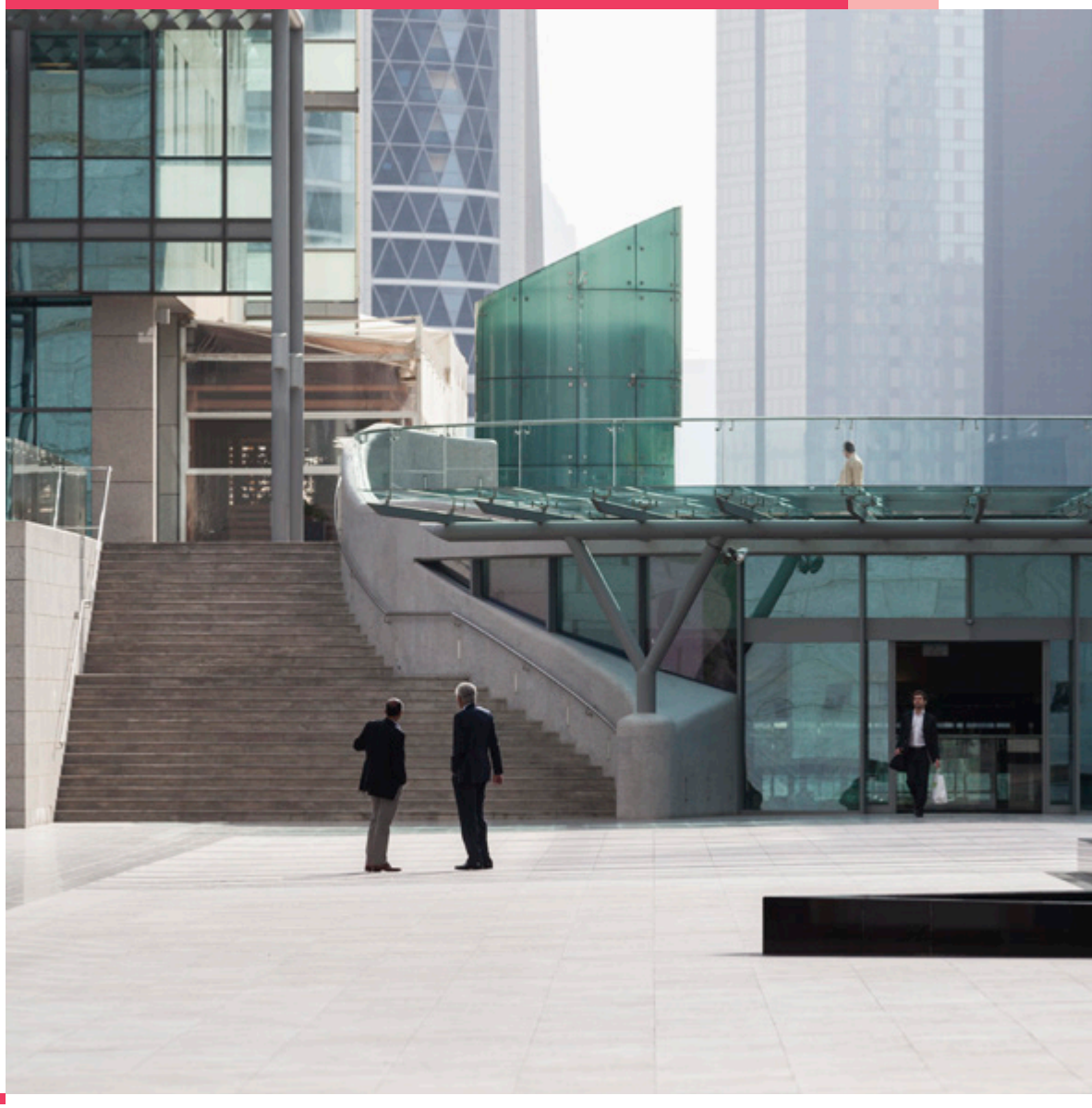
www.pwc.com/ca/forensics

Forensic eye opener

Exploring today's hottest issues in economic crime

An update from PwC's Forensic Services team

Summer 2013



pwc

Welcome to the *Forensic eye opener*. This newsletter is designed to introduce our Forensic Services leadership team and provide insight into current issues in the marketplace that are important to you.

Our Forensic Services leadership team is comprised of the following individuals:

Steven Henderson is a Partner with the Forensic Services practice in Toronto. He is the National Forensic Services Leader and serves as the Canadian firm's Global Forensic Services representative.

Lori-Ann Beausoleil is a Partner with the Forensic Services practice in Toronto. She is the National Forensic Consulting Leader and serves as National Leader for the Canadian Real Estate practice.

In this issue we include articles which cover:

What recent changes to Canada's anti-bribery and corruption legislation could mean to you

On June 19, 2013, Bill S-14 *Fighting Foreign Corruption Act* was given Royal Assent, amending the existing *Corruption of Foreign Public Officials Act* (CFPOA).

Anti-fraud regime: Prevention is better than reaction

Given recent headlines involving Canadian corporations dealing with allegations of fraud, you may find yourself considering what you would do in a similar situation that may threaten the existence of your organization.

Social media fraud

The ease of access and wide range of potential targets has triggered increasing concern for potential criminal activity within the various networks and platforms.

Ponzi schemes: a classic scam

Most people have heard of a Ponzi scheme, but what exactly does it consist of and how do you differentiate a potential Ponzi scheme from an attractive legitimate investment opportunity?

Canary in a coal mine?

After a forensic investigation winds down and the proposed recommendations have been implemented, organizations often realize that, with the benefit of hindsight, the overall costs would have been reduced had a more proactive approach been adopted by the organization prior to the incident.

What recent changes to Canada's anti-bribery and corruption legislation could mean to you

On June 19, 2013, Bill S-14 *Fighting Foreign Corruption Act*[1] was given Royal Assent, amending the existing *Corruption of Foreign Public Officials Act* (CFPOA), which has been in effect since 1999.

The CFPOA is Canada's anti-bribery and corruption legislation and the bill's amendments represent the Canadian government's latest efforts to strengthen anti-bribery and corruption enforcement in Canada. It will have substantial implications for Canadian organizations and individuals that conduct business abroad. Activities which were previously acceptable may now be considered criminal and potentially result in fines and imprisonment. Enforcement by the Royal Canadian Mounted Police (RCMP) and other regulatory agencies such as the Ontario Securities Commission continues to intensify, with three organizations convicted to date under the CFPOA resulting in fines totaling over $20 million.[2] In light of these changes, your organization should carefully review its activity overseas, including any interactions with foreign government officials, and assess the adequacy of its control framework for anti-bribery and corruption policies and procedures.

There are approximately 35 RCMP investigations[3] of potential foreign corruption in progress and anti-bribery and corruption enforcement continues to escalate. Your organization should determine its risk of CFPOA non-compliance and assess the adequacy of its controls and safeguards in place against bribery and corruption. An effective anti-bribery and corruption program will alert you to heightened risks associated with your organization and its activities and will assist in mitigating those risks. In the event an incident does occur, an effective program may also reduce the amount of penalties and fines you might face. Stay tuned for further updates on the impacts of the amended CFPOA.

1 Parliament of Canada. (June 19, 2013). *S-14 – An Act to amend the Corruption of Foreign Public Officials Act.* Retrieved from http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6246177&File=4

2 Foreign Affairs and International Trade Canada. (February 5, 2013). *Strengthening Canada's Fight Against Foreign Bribery.* Retrieved from http://www.international.gc.ca/media/aff/news-communiques/2013/02/05b.aspx?lang=eng

3 Foreign Affairs and International Trade Canada. (February 5, 2013). *Strengthening Canada's Fight Against Foreign Bribery.* Retrieved from http://www.international.gc.ca/media/aff/news-communiques/2013/02/05b.aspx?lang=eng

The changes brought into force with Bill S-14 are discussed in further detail below.

CFPOA before amendments	*Bill S-14 amendments*
Facilitation payments	
Facilitation payments are relatively small amounts paid to secure or obtain foreign public services, including mail delivery, processing of official documents, and customs clearances. They are often a routine part of obtaining public services abroad, are a specific exception under the current CFPOA, and generally not considered to be bribes.	The amendments eliminate the facilitation payments exception, however small they may be, and deem them to be bribes of foreign officials. This is similar to existing anti-corruption laws in the United Kingdom. However, there continues to be an exception for facilitation payments in the United States under its *Foreign Corrupt Practices Act*. Unlike other provisions of the legislation, this change comes into force at a later date.
Inadequate accounting books and records	
Although falsification of accounting records was already illegal under current Canadian laws, the concealment of illicit payments as well as their inadequate reflection in accounting records is not a separate, specific criminal offence.	The amendments create a new criminal offence which addresses the concealment of bribery in the books and records of Canadian organizations. These offences include activities such as establishing or maintaining off-book accounts for the purpose of disguising bribery, inadequately identifying illicit transactions, recording non-existent expenditures, knowingly using false documents, and intentionally destroying records earlier than permitted by law.
Expansion of jurisdiction based on nationality	
The application of the CFPOA has so far been limited to situations where the activity has a "real and substantial connection to Canada," and offences prosecuted under Canadian jurisdiction have been those where a significant portion of the activities that form the offence took place in Canada.	CFPOA jurisdiction is expanding to allow for the prosecution of Canadian companies, citizens, permanent residents, and entities formed under the law of Canada regardless of where the corruption was committed or planned. This will reduce jurisdictional challenges faced in prosecuting offenders and will also deter the use of foreign subsidiaries by Canadian organizations for bribery and other corrupt acts.
Definition of "business"	
The CFPOA previously only applied to corrupt acts committed in "the course of business," which has generally been interpreted to apply to entities which operate "for profit."	The amendments remove the requirement that a business be carried out for profit and expands the applicability of the Act to apply to non-profit entities as well. This will require a number of non-profit entities to implement a control framework specifically focused on anti-bribery and corruption policies and procedures to mitigate their risk of non-compliance with the CFPOA.
Increase of the maximum penalty	
Before having been amended, the CFPOA limited the punishment of a foreign corrupt act to a maximum of five years imprisonment.	The amendments include an increase of the maximum punishable imprisonment term to 14 years along with unlimited fines. This brings the foreign corruption legislation in line with the maximum punishable term for corruption and bribery under the Criminal Code of Canada. It also indicates the Canadian government's increased focus on prosecuting individuals.
Authority to lay charges	
The authority to lay charges previously rested with the RCMP as well as municipal and provincial police.	The RCMP will now have exclusive authority to lay charges with respect to CFPOA offenses in all stages of the act. This will result in a clear mandate of the RCMP to prosecute all CFPOA offenders and eliminate jurisdictional considerations between Canadian law enforcement agencies.

Anti-fraud regime: Prevention is better than reaction

Given recent headlines involving Canadian corporations dealing with allegations of fraud, you may find yourself considering what you would do in a similar situation that may threaten the existence of your organization. How would you pick up the pieces? Or better yet, how do you avoid it from happening in the first place?

Unfortunately, you don't have to work for one of the largest organizations in Canada to suspect or encounter fraud at some point in your career. Fraud investigations can be difficult, time consuming and draining on already limited resources.

Implementing an anti-fraud regime for your organization is an effective way to reduce your organization's exposure to fraud-related risks. A robust anti-fraud regime will also help you control and mitigate the effects of fraud or a suspected fraud. An effective anti-fraud regime has eight key components:

1. Governance – Oversight by the Audit Committee and the Board of Directors

An organization's Board of Directors and Audit Committee significantly influence the control environment and "tone at the top". The Audit Committee and Board of Directors' oversight should, at a minimum, include review of: management's anti-fraud programs and controls, the organization's fraud risk assessment, internal audit's testing and assessment of the anti-fraud regime, and involvement of other experts—legal, accounting and other professional advisers—as needed to investigate any alleged or suspected wrongdoing brought to their attention. More importantly, the tone from the top perceived by all employees is integral. By implementing and communicating policies and procedures that show a strong commitment to act not only in accordance with laws and regulations but ethically as well, employees have clear incentive to follow suit.

2. Fraud risk assessment

Management should evaluate the organizations exposure to fraud risks at various levels by considering different fraud schemes and scenarios and determining the likelihood and significance of the risks to the organization. For example, do we do business overseas? How common is corruption and bribery in those countries? Is there a risk of questionable practices in order to move certain projects forward in these countries? Will this new product line expose us to different risks? How does the new expense reimbursement program and policy impact the organization? This evaluation should be comprehensive and periodically reviewed, particularly if there's a change in the business or its operations. The business environment is also continually changing and the organization should assess external factors as well. It's encouraging to note that 39% of the respondents in PwC's recent *Global Economic Crime Survey*[1] who had performed a fraud risk assessment once or more often in the last 12 months, identified fraud. In comparison, only 28% who had not performed a fraud risk assessment in the last 12 months identified fraud. These figures confirm the dictum of 'seek and you shall find'.

3. Code of Business Conduct and Ethics

A Code of Conduct should be designed to deter wrongdoing and promote honest and ethical behaviour. Key areas to be addressed in the Code of Conduct include: conflict of interest; protection and proper use of the organization's assets and opportunities; confidentiality; compliance with laws, rules and regulations; and reporting of any illegal or unethical behaviour. Given the growing popularity of social media, it's recommended that organizations include a policy on employees' use of social media to reduce possible exposure to the organization. In addition, the Code of Conduct should explain what constitutes fraudulent behaviour, how accountability for the code is established and the sanctions imposed for noncompliance. By enforcing the Code of Conduct and properly documenting any violations, an organization will be able to reduce some legal and reputational exposure caused by employee misconduct.

4. Incident reporting mechanism

In 2011, 23% of global organizations that were victims of economic crime over the past 12 months detected the fraud by a whistle-blowing system/internal or external tip-off according to PwC's recent *Global Economic Crime Survey*. Examples of incident reporting mechanisms include: use of websites/emails, P.O. Box, 1-800 ethics/whistleblower hotlines, and direct reporting to the Audit Committee, management or Compliance Officer/Committee. Organizations should establish a process to receive, vet, investigate, report, remediate and maintain records for all related incidents reported. Best practices include the Audit Committee directly overseeing the incident reporting process. Normally a Compliance Officer/Committee is established to receive, log and vet reported incidents; confirm they have been appropriately investigated and remediated; and to communicate the results directly to the Audit Committee. The Compliance Officer/Committee should be comprised of individuals who are independent of the financial reporting process and least likely to be subject to a fraud allegation or oversee those persons subject to a fraud allegation, such as legal counsel, internal audit, and human resources.

5. Investigative protocol (including suspicious transaction reporting)

An investigative protocol is a written plan and process for tracking, investigating and responding to allegations of misconduct or fraud. Where appropriate, the investigative protocol should allow for an investigation independent of management. Target response time, key positions, legal liability, and requirement for external expertise are examples of key issues to consider when setting up the protocol. Documenting the organization's approach to an investigation in advance will allow for a more expedited response when a fraud situation arises.

6. Remediation protocol

A remediation protocol, to address issues noted during the organization's investigation of fraud, should address key areas such as: disciplinary action, restitution, enhanced controls and communication. An anti-fraud regime is greatly enhanced when investigation and resolution of misconducts are appropriately communicated to all employees. The reason for this is two-fold: 1) it provides a greater disincentive to those individuals thinking of violating the organization's policies or procedures; and, 2) it demonstrates to those individuals who are considering whether or not to report concerns that their concerns will be heard, investigated and remediated, as appropriate. These communications can demonstrate the organization's tone at the top as well as its priority to behave ethically.

7. Hiring and promotion policies and procedures

Hiring and promotion policies should include background checking procedures at various points of an employee's employment (for example prior to hiring, promotion, or significant change in job functions). Background checking should cover the following areas: criminal record checks, civil checks, media/reference searches, personal/education/professional background, and credit checks as appropriate given the level of the employee in the organization and their proximity to the financial reporting function.

8. Management evaluation and testing

Once the anti-fraud regime is in place, regular monitoring and evaluation is important. For instance, if there are no calls received on the whistleblower hotline, it does not necessarily mean there is no fraud. It may indicate that very few people know about the hotline or people are afraid to use it. The frequency of separate evaluations/audits required to provide management reasonable assurance about the effectiveness of its anti-fraud regime is a matter of management's judgment. To help determine the frequency and areas of focus, consideration should be given to the nature and degree of changes occurring in the organization and their associated risks, the competence and experience of the individuals implementing the controls, and the results of ongoing monitoring. Ongoing monitoring is most effective when built into the normal, recurring operating activities of an organization. It's essential that the organization's plan, approach and scope of monitoring activities be documented and reviewed from time to time.

Small to medium-sized organizations should consider how each of the eight components of the anti-fraud regime can be incorporated into their business environment most efficiently given existing policies and protocols. The key to a robust anti-fraud regime is that it's uniquely tailored to the organization, its operations and ultimately, their risks. A "one-size fits most" approach will not provide a sufficiently tailored program. In fact, all organizations, regardless of size, should develop an anti-fraud regime tailored to their needs. This should include an evaluation of the program in the context of the expectations of stakeholders, including regulators and law enforcement, and a comparison to organizations of same or similar composition.

No one wants fraud to occur within their organization—the key is to arm yourself and your organization with the right tools, including an effective anti-fraud regime, to assist in the prevention, detection and mitigation of fraud.

1 PwC. (November 2011). *Cybercrime: protecting against the growing threat, Global Economic Crime Survey.* Retrieved from http://www.pwc.com/crimesurvey

Social media fraud

With Facebook reaching over 1 billion users in 2013,[1] LinkedIn crossing the 200 million registered user mark in January, 2013[2] and over 140 million Twitter users as of early 2012,[3] online hackers and criminals are focusing their attention to prey on a wider base of individuals: social media users. The ease of access and wide range of potential targets has triggered increasing concern for potential criminal activity within the various networks and platforms.

Social media behaviours

There are several behaviours and characteristics that attract these scammers to social media networks: social proofing, sharing[4] and public availability of information:

- Social proofing, or informational social influence, is a psychological mindset where individuals adopt the actions or characteristics of others in a given situation.[5] For example, if a friend recommends a link or article, you are much more inclined to click on it. According to a 2012 Norton Cybercrime Report,[6] one in five people do not check the integrity of links from friends or other individuals before clicking on them. As a result, fake links and posts are easy methods for scammers to use. They rely on the trust that individuals put in their social network connections and friendships as a way to get people to click on links.

- Sharing is what social media is all about. From sharing the birth of a new child, to reminiscing about your old high school or celebrating an important birthday, sharing important personal information gives scammers and online criminals the ability to use these pieces of information for their benefit. The information is used to answer security questions, set up false identities and even to gain access to your personal bank accounts. This is of particular concern, as 36% of social media users report having accepted "friend requests" from individuals they don't know. [7]

- The very nature of social media networks allows your information to be public, which only increases the risk of being a target of social media fraud or scams. Only half of social media users report using privacy settings to control what information they share and who is allowed to see it.[8] In fact, most social media networks set the default privacy settings to "public" when you initially sign up for an account. As a result, many individuals have their information readily searchable, available and easily laid out for potential scammers to take advantage of.

Social media scams

The characteristics and design of social media has allowed online criminals to develop several types of scams and fraud schemes. For example:

- **Investing Online:** A recent U.S Security Exchange Commission Investor Alert[9] has outlined that the increasing use of social media such as Facebook, Twitter and YouTube to make financial investment decisions has increased the number of attempts to spread false information. Offers to invest in "100% risk free investments" will prey on individuals and can easily result in financial losses for the victim. The ease of creating an account allows criminals to send unsolicited messages, newsletters or "investment tips" in a cheap and relatively untraceable manner.

- **Fake Offering:** This scam involves asking the user to sign-up for an event or group in exchange for a free gift such as a coffee gift card or coupon, which the user never receives.[10] An individual may be asked to send a text message to a phone number to "sign-up" for the offer, resulting in a substantial fee charged to their phone bill without their knowledge. Fake offerings may also be perpetrated online by requesting an individual to "sign-up" using their personal information, which may result in identity theft. There's also the possibility of viruses such as malware or spyware being installed once the user registers for the offering. These viruses may corrupt or damage files on your computer rendering it useless or even worse, there's no damage to the computer but your personal information is being accessed or tracked using the spyware.

- **Likejacking:** By offering a funny video or eye-catching photo, the criminals encourage the user to "Like" the video or photo.[11] Once the user has clicked the "Like" button, malware may be installed automatically onto their computer. This creates the possibility for the malware to share the photo or video with the connections of the user and also track the personal information of the user's account, similar to a fake offering.

- **"Please send money" scam:** This scam involves an account being used to solicit requests for charitable donations or requests for money from friends in trouble. The scam is usually carried out when an account is seized and the requests for money are sent to the user's friends and connections from their online address book. Since the message is coming from a known friend or relative, the users are led to believe it's coming from a trusted source. As a result of this trust, money is then transferred over to an account that's controlled by the perpetrator.

Ways to avoid scams and fraud attempts

There are several ways to block or avoid scams and fraudulent attempts without hindering your social media experience. For example:

- **Friend Requests/Clicking Links:** Ensure that you do not accept "friend requests" or click on links from people you don't know. The age old adage "don't talk to strangers" is applicable in these situations as you don't know their intentions or even their true identity. It's also important to consider the integrity of links that you click. If it's a link to a site that you don't recognize it may be best to avoid clicking it or ask a friend if they've heard of the website before.

- **Privacy Settings:** Ensure that you have reviewed your privacy settings and that they meet your tolerable level of privacy. It's worth noting that the higher you set your privacy settings, the harder it can be for online criminals to access your information.
- **Passwords:** Create passwords that are complex, use a mix of upper and lowercase letters, and contain several characters and numbers. Don't include any variant of personal information that's publicly available through your social media account in your password. For example, if you tweeted that your daughter's middle name is Apple and her birthday is March 3, you shouldn't include this information as part of your password.
- **Log out:** Always ensure that you log out of your social media accounts when you're finished, especially on a public computer. Leaving your accounts open, on any computer, could lead to your account being hacked or hi-jacked by criminals.
- **Your Posts:** Be cognizant of the fact that your social media posts will remain on the Internet for a long time, if not forever. Individuals can download your information and use it in various ways even if you have deleted your profile or the specific post. Several sites also store cached files or archives of websites and Internet pages that can be retrieved at a later date.
- **Installing Applications or Add-Ons:** Ensure that any applications or add-ons that you install through your social media accounts are from reputable sources. Many apps are created to act as malware and could be harmful to your computer and the integrity of your personal information.
- **Public Wi-Fi:** Be weary of the information you transfer or upload to your social media accounts when using a public Wi-Fi or hotspot. Several individuals have access to this Internet connection and sophisticated criminals may be able to access your information.

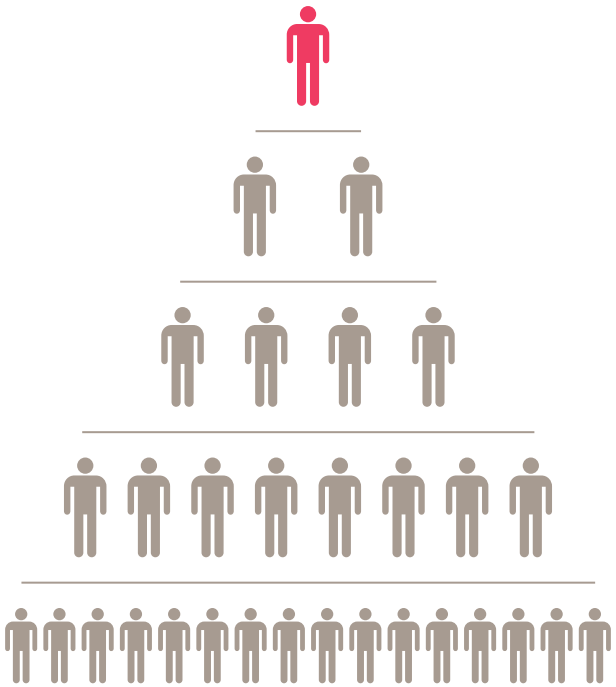
Conclusion

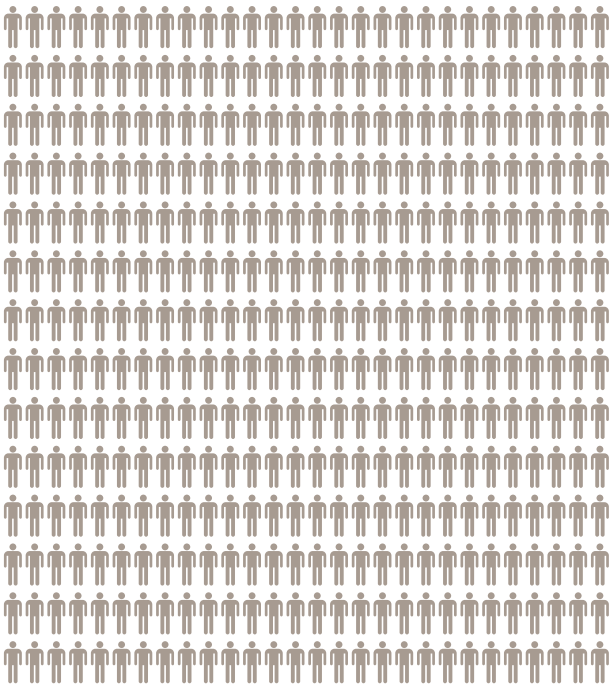
While the world of social media is becoming increasingly filled with tales of caution and warning of online criminals and scammers, simple measures can be taken to ensure that you can look at a family member's birthday photos or watch a video online without the fear that your account will be easily compromised.

1 Facebook. (December 2012). *Key Facts*. Retrieved from http://newsroom.fb.com/Key-Facts
2 LinkedIn. (January 2013). *200 Million Members!* Retrieved from http://blog.linkedin.com/2013/01/09/linkedin-200-million/
3 Twitter. (March 2012). *Twitter turns six*. Retrieved from http://blog.twitter.com/2012/03/twitter-turns-six.html
4 Symantec. (April 2013). *Internet Security Threat Report 2013: Volume 18*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
5 Symantec. (April 2013). *Internet Security Threat Report 2013: Volume 18*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
6 Norton by Symantec. (September 2012). *2012 Norton Cybercrime Report*. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
7 Norton by Symantec. (September 2012). *2012 Norton Cybercrime Report*. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
8 Norton by Symantec. (September 2012). *2012 Norton Cybercrime Report*. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
9 Security Exchange Commission: Office of Investor Education and Advocacy. (January 2012). *Social Media and Investing – Avoiding Fraud*. Retrieved from http://www.sec.gov/investor/alerts/socialmediaandfraud.pdf
10 Symantec. (April 2013). *Internet Security Threat Report 2013: Volume 18*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
11 Symantec. (April 2013). *Internet Security Threat Report 2013: Volume 18*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

Ponzi schemes: a classic scam

Ponzi schemes are one of the oldest frauds in the book. They are named after Charles Ponzi, who infamously perpetrated this investment scheme in the early 1900s. Most people have heard of a Ponzi scheme, but what exactly does it consist of and how do you differentiate a potential Ponzi scheme from an attractive legitimate investment opportunity?





What is a Ponzi scheme?

A Ponzi scheme is an investment ploy where the perpetrator convinces victims to give money for a non-existent investment that offers unusually high or consistent returns. It's important to remember that both individuals and organizations can be the target of a Ponzi scheme. The fraudster may ask for a small amount of money initially from the victim to build trust and subsequently request a much larger amount after the initial investment "pays off". The fraudster continually recruits new investors and uses the new investor money to pay the original investors their return. The cycle continues to repeat itself. The scheme can last for many years as long as enough new money is being raised to cover outflows including payments of principal, income or the perpetrator's expenses.

A Ponzi scheme can spread easily through word of mouth as early investors share news of their great investment returns with friends or family, inadvertently helping trick not-for-profit organizations, the elderly or even sophisticated investors into falling for the Ponzi scheme.

Ponzi schemes usually end in one of two ways: the culprit takes the remaining funds and abandons the investors abruptly, or the scheme collapses under the pressure of constantly having to find new funds to pay investors or for the perpetrator's lifestyle. Unfortunately for many Ponzi scheme victims, even if the culprit is caught, there is often little to no money left to distribute amongst the investors.

Using a simple example, Mr. Johnson (a persuasive fraudster) initially obtains $100,000 each from four different investors. Mr. Johnson guarantees they will receive a 20% return each year. Later in the year, Mr. Johnson persuades another four investors to invest $100,000 each in his "guaranteed" investment. Mr. Johnson then uses the investment proceeds to pay the first four investors their guaranteed 20% return (or $20,000 each for a total of $80,000). Mr. Johnson's ability to make payment on his "guaranteed" investment provides him the good reputation to continue with his scheme. At the end of the first year, Mr. Johnson will have cash in hand of $720,000 ($800,000 less $80,000). At this point, he can continue with the scheme or take the funds accumulated to date and exit the scheme.

Eventually, either subsequent proceeds from new investors will diminish and the 20% returns will not be met or investors decide to cash out and there's not enough cash remaining. This leads us to the inevitable question... how does one identify a scheme?

How to identify a potential Ponzi scheme

Below is a list of red flags that are indicative of a potential Ponzi scheme. Note that additional diligence should be completed if any of the red flags exist, to determine the legitimacy of the investment vehicle, and the presence or absence of any red flag in isolation should not be the basis for an investment decision.

Red Flag: Guaranteed high investment returns and little to no risk

This promise is music to an investor's ears, but there's no such thing as a no-risk investment with high returns. Similarly, constant rates of return year after year regardless of market performance may also be an indication of a scheme.

Recommendation: If the investment sounds too good to be true, it probably is. As investment scams get more media coverage and investors become more aware of common red flags, some fraudsters are substituting the promise of abnormally high returns with the offer of abnormally consistent performance.

Red Flag: Credibility

The investment and/or perpetrator does not have relevant and recognized industry credentials, does not work for a licensed firm, and/or is not selling a registered investment.

Recommendation: In addition to analyzing the investment itself by evaluating financial information verified by experienced professionals, conduct appropriate diligence on the individual presenting the investment opportunity. There are certificates of accreditation and professional designations in Canada that allow an individual to sell securities and offer investment advice.[1,2] An investment of time to understand the opportunity and key individuals can be a sound decision to protect your overall investment. Depending on the magnitude of the potential investment, it may be worthwhile to involve outside assistance in evaluating the qualifications of the individual, conducting searches of media, court and other databases to search for items of concern.

Red Flag: Supporting documentation

The investment organizer provides minimal or no paper work to support the investment or the account history. Proof of ownership and other supporting documentation of the investment may arrive unusually late or not be issued to investors at all. If it is issued, it might be inaccurate, incomplete or lacking pertinent information such as account number or transaction details.

Recommendation: Ensure you receive supporting documentation for your investments in a timely manner. You can also attempt to verify the information on the certificates or monthly statements with a third party on a sample basis. Depending on the magnitude of the investment, it may make sense to seek outside legal or other professional advice to perform due diligence to ensure you understand those you are doing business with as well as the underlying investments.

Red Flag: Investment strategy or structure

The investment is based on a very complex strategy. If the seller says "it's hard to explain what the business does or how it makes money..." in their sales pitch, it should be considered a red flag. The same is true of investments with payments flowing through tax havens or other offshore jurisdictions where there is no clear business purpose.

Recommendation: If the organizer cannot explain the investment structure, how it generates income or pays its returns, it is better to look for an investment that you can understand.

Red Flag: Communication

The organizer is difficult to get in touch with and communication is based on his/her schedule.

Recommendation: Though this is not true in all cases, if it's hard to reach your contact, it may be a sign that the organizer is facing a need for cash and is trying to avoid investor calls in hopes that they can delay withdrawals or difficult questions. Ensure that you monitor the responsiveness of the organizer and be cautious if replies are not received in a timely manner.

Why are Ponzi schemes still successful?

The Ponzi schemer is usually a very persuasive individual. Many people will invest because they're promised an attractive risk-reward proposition. Often, investors will earn high returns in the beginning and they'll invest even more money in this scheme. Individuals are busy and may not be able to find the time to conduct the proper investment research. Sometimes, the culprit will take advantage of their own close friends, relatives, social acquaintances, busy professionals, pensioners, not-for-profit or members of their own cultural community for money.

There are also instances where individuals create a legitimate investment fund with the best intentions but, at some point, suffer losses from which they cannot recover. In an attempt to prevent investors from losing faith and withdrawing funds, the well-intended fund manager will begin to cover up the losses and can end up in a full-blown Ponzi scheme.

It is important that you never invest money in an opportunity on the basis of a recommendation or first meeting alone. Every investor should be prudent in evaluating the appropriateness and risk of an investment opportunity along with the offering individual or company.

Punishment for Ponzi scheme fraudsters

Victims might be lucky enough to get some of their money back through litigation if there are any assets of the perpetrator remaining. The perpetrator may also face jail time, which can vary in duration case by case. Bernard Madoff, perhaps our generation's "Charles Ponzi," received a lengthy 150 year prison sentence for his multi-billion US dollar fraud[3] whereas Canadian Ponzi schemer Earl Jones was sentenced to 11 years in prison for his decades-long CA$50 million Ponzi scheme.[4]

What is the financial impact of Ponzi schemes?

In the largest Ponzi scheme uncovered to date, Bernard Madoff provided investors with investment statements reflecting a combined US$64.8 billion of assets with his firm.[5] The total loss for investors from this elaborate scheme was estimated to be US$50 billion[6] including up to US$837 million in the first 6 months of 2011 alone.[7] Victims included individual investors and sophisticated institutions alike.

While the total losses for Ponzi schemes can be staggering, arming investors with the right tools and education to appropriately understand and evaluate investment opportunities will greatly reduce the impact of these schemes.

1 This website, maintained by the Canadian Securities Institute, provides a free service to verify designations and certificates in Canada.
The Canadian Securities Institute offers a number of certificates and designations, which can be found here: https://www.csi.ca/student/en_ca/designations/index.xhtml

2 This website allows you to check if the individual and/or firm is registered with the OSC. The OSC is the governing body in Ontario that administers and enforces all securities law in the province. Check with your provincial regulator for a similar service. http://www.osc.gov.on.ca/en/Investors_check-registration_index.htm.
In Canada, the Investment Industry Regulatory Organization of Canada (IIROC) regulates and oversees all investment dealers and activity in Canada. A list of regulated investment dealer firms can be found: http://www.iiroc.ca/industry/Pages/Dealers-We-Regulate.aspx

3 Smith, A. (June 30, 2009). *Madoff sentenced to 150 years.* CNN Money. Retrieved from http://money.cnn.com/2009/06/29/news/economy/madoff_prison_sentence/index.htm. Accessed January 14, 2013

4 Banerjee, S. (February 16, 2010). *Jones gets 11 years for $50-M fraud.* Winnipeg Free Press. Retrieved from http://www.winnipegfreepress.com/canada/jones-gets-11-years-for-50-m-fraud-84437757.html. Accessed January 9, 2013.

5 Lauricella T., Lucchetti A. (March 10, 2009). *Were Told They Had a Total of $64.8 Billion.* The Wall Street Journal. Retrieved from http://online.wsj.com/article/SB123673521911590783.html . Accessed December 12, 2012.

6 Lezner, R. (December 12, 2008). *Bernie Madoff's $50 Billion Ponzi Scheme.* Forbes. Retrieved from http://www.forbes.com/2008/12/12/madoff-ponzi-hedge-pf-ii-in_rl_1212croesus_inl.html. Accessed January 9, 2013.

7 Willingham B. (July 5, 2011). *2011 Ponzi Schemes By the Numbers.* Diligentia Group. Retrieved from http://www.diligentiagroup.com/due-diligence/2011-ponzi-schemes-by-the-numbers/. Accessed December 12, 2012.

Canary in a coal mine?

After a forensic investigation winds down and the proposed recommendations have been implemented, organizations often realize that, with the benefit of hindsight, the overall costs would have been reduced had a more proactive approach been adopted by the organization prior to the incident.

This is an important point to remember when your organization is faced with an issue and the following question is raised: "Why would our organization pay forensic specialists to investigate, for example, a whistleblower complaint alleging misappropriation of less than $200 or failure to follow internal procurement procedures?"

In an ever more cost conscious environment, the business case to investigate allegations concerning such a small monetary amount may seem less than compelling. In addition to the cost of the service provider, there are the internal resources that are involved in the investigation and the disruptions to employees' daily schedules in order to review information and participate in interviews. Why should an organization dedicate their scarce resources and undergo a potentially stressful process for minor allegations with little to no immediate apparent benefit?

The answer is surprisingly simple: the costs of not investigating these allegations or conducting an inadequate investigation can be much more costly than thoroughly investigating and resolving the allegations. The fines and penalties from several recent cases are staggering.

- In June 2012, Barclays Bank was fined US$455 million to settle charges of rigging the LIBOR benchmark interest rate.[1] In December, 2012, UBS announced it would pay fines of US$1.5 billion.[2] Other banks are expected to be investigated in the LIBOR scandal and could also be fined.

- In October 2012, Pfizer agreed to pay US$60 million to settle Foreign Corrupt Practices Act ("FCPA") charges related to its emerging markets sales. The settlement covered allegations related to kickbacks and bribes in various countries including Russia, China and Italy. [3]

- The Ontario Securities Commission has advised that they may pursue monetary penalties up to CA$84 million[4] against the former officers and directors of Sino-Forest Corporation and has alleged that the former Chief Financial Officer "did not comply with Ontario securities law and acted contrary to the public interest."[5] Moreover, the executives and directors of Sino-Forest Corp. are facing a CA$9.2 billion[6] potential class-action suit filed by investors as a result of allegations of fraud.

- In December 2012, global bank Standard Chartered agreed to pay US$327 million in penalties for allegedly violating U.S. sanctions against Iran, Sudan, Libya and other nations.[7] In September 2012, the bank paid an additional US$340 million to settle allegations that the bank had disguised over 60,000 transactions totaling US$250 billion from Iranian clients.[8]

- In December 2012, HSBC agreed to pay a US$1.9 billion settlement after an investigation determined the bank violated federal laws against anti-money laundering. As part of their deferred prosecution agreement, the bank will need to appoint an independent monitor in addition to the costs of improving their money-laundering prevention programs and Know-Your-Customer efforts. To date, HSBC has spent more than US$290 million to improve its money-laundering prevention policies.[9]

Allegations of wrongdoing or financial irregularities must be treated appropriately as even small or minor issues can have serious consequences. Engage your legal counsel and reach out to your auditor and other service providers in order to determine the best course of action. Taking a more prudent approach to seemingly trivial anomalies may have avoided the magnitude of the penalties faced by the above-noted companies and their directors. It's difficult to determine without a comprehensive investigation by qualified independent investigators whether an issue is a one-off or whether it is a serious matter in consideration of all regulatory and legal implications. As such, it can be difficult to discharge your fiduciary duties without having an approved process.

1 Slater, S. and M. Scuffham (July 27, 2012). *Barclays Dragged into New Probe After LIBOR Blow.* Reuters. Retrieved from http://www.reuters.com/article/2012/07/27/us-barclays-earnings-idUSBRE86Q06Q20120727. Accessed December 10, 2012.
2 Bart, K. and T. Miles (December 19, 2012). *UBS Admits Fraud, to Pay Whopping Fine in LIBOR Rigging Settlement.* The Globe and Mail. Retrieved from http://www.theglobeandmail.com/report-on-business/international-business/ubs-admits-fraud-to-pay-whopping-fine-in-libor-rigging-settlement/article6552496/ Accessed December 19, 2012.
3 Berkrot, B. (October 29, 2012). *Analysis: U.S. Foreign Bribery Penalties for Drugmakers May Lack Bite.* Reuters. Retrieved from http://www.reuters.com/article/2012/10/29/us-drugmakers-fcpa-idUSBRE89S0IQ20121029 Accessed December 11, 2012.
4 Gray, J. (December 12, 2012). *Former Sino-Forest Brass may Face $84-million in Penalties, OSC says*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/globe-investor/former-sino-forest-brass-may-face-84-million-in-penalties-osc-says/article6273364/ Accessed December 14, 2012.
5 Gray, J. (December 12, 2012). *Former Sino-Forest Brass may Face $84-million in Penalties, OSC says*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/globe-investor/former-sino-forest-brass-may-face-84-million-in-penalties-osc-says/article6273364/ Accessed December 14, 2012.
6 Gray, J. (December 12, 2012). *Former Sino-Forest Brass may Face $84-million in Penalties, OSC says*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/globe-investor/former-sino-forest-brass-may-face-84-million-in-penalties-osc-says/article6273364/ Accessed December 14, 2012.
7 Sparshott, J. (December 10, 2012). *Standard Chartered Settles U.S. Sanctions Allegations*. The Wall Street Journal. Retrieved from http://online.wsj.com/article/SB10001424127887324478304578171150886564188.html Accessed December 13, 2012.
8 Sparshott, J. (December 10, 2012). *Standard Chartered Settles U.S. Sanctions Allegations*. The Wall Street Journal. Retrieved from http://online.wsj.com/article/SB10001424127887324478304578171150886564188.html Accessed December 13, 2012.
9 McCoy, K. (December 11, 2012). *HSBC Will Pay $1.9 Billion for Money Laundering*. USA Today. Retrieved from http://www.usatoday.com/story/money/business/2012/12/11/hsbc-laundering-probe/1760351/ Accessed December 13, 2012.

Who to call
National Forensic Services Team

Steven Henderson
National Forensic Services Leader
416 941 8328
steven.p.henderson@ca.pwc.com

Lori-Ann Beausoleil
National Forensic Consulting Leader
416 687 8617
lori-ann.beausoleil@ca.pwc.com

Peter Vakof
National Forensic Technology Services Leader
416 814 5841
peter.vakof@ca.pwc.com

Paul Bradley
Associate Partner, Forensic Services
902 491 7436
paul.f.bradley@ca.pwc.com

Marie-Chantal Dréau
Partner, Forensic Services
514 205 5407
marie-chantal.dreau@ca.pwc.com

Sarah MacGregor
Partner, Forensic Services
416 814 5763
sarah.e.macgregor@ca.pwc.com

Kas Rehman
Partner, Forensic Services
613 755 4328
514 205 5171
kas.rehman@ca.pwc.com

Harm Atwal
Director, Forensic Technology Services
416 869 2330
harm.k.atwal@ca.pwc.com

Jason Armstrong
Director, Forensic Services
613 755 8743
jason.r.armstrong@ca.pwc.com

Chris Gray
Vice President, Forensic Services
519 640 8011
chris.gray@ca.pwc.com

René Hamel
Director, Forensic Technology Services
416 687 8488
rene.j.hamel@ca.pwc.com

Ray Haywood
Director, Forensic Services
416 814 5801
h.ray.haywood@ca.pwc.com

Dave Johnson
Vice President, Forensic Services
204 926 2423
dave.a.johnson@ca.pwc.com

Kyla Kramps
Vice President, Forensic Services
204 926 2434
kyla.kramps@ca.pwc.com

Benoit Legault
Director, Forensic Services
902 491 7453
benoit.legault@ca.pwc.com

Steven Malette
Vice President, Forensic Services
613 755 5979
steven.m.malette@ca.pwc.com

Krista Mooney
Director, Forensic Services
416 941 8290
krista.a.mooney@ca.pwc.com

Kelly Ohayon
Director, Forensic Consulting
514 205 5146
kelly.ohayon@ca.pwc.com

James Pomeroy
Vice President, Forensic Services
902 491 7416
james.a.pomeroy@ca.pwc.com

Nikki Robar
Vice President, Forensic Services
902 491 7453
nikki.l.robar@ca.pwc.com

Lloyd Wilks
Director, Forensic Technology Services
416 687 8115
lloyd.wilks@ca.pwc.com