Forensic eye opener

An update from PwC's Forensic Services team

Fall 2012

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.

Peter Vakof is a Partner with the Forensic Services practice in Toronto. He is the National Forensic Technology Services Leader and specializes in electronic discovery, computer forensics and data analytics.

Kas Rehman is a Partner with the Forensic Services practice in Ottawa. He is the National Public Sector Forensic Services Leader.

In this issue we include articles which cover:

Corruption of foreign public officials: A Canadian perspective

As anti-bribery and corruption enforcement intensifies in Canada and worldwide, the onus of self-regulation and self-monitoring has been placed firmly on management, Boards of Directors and Audit Committees. The financial and non-financial implications of CFPOA violations are significant and may be expected to increase over the next few years.

Photo cheque cashing

Through photo cheque cashing, cheques can be deposited without ever having to wait in line at the teller or make a trip to the ATM. While the only equipment required is a smartphone or a computer with a basic scanner, this technology advancement can also be accompanied by risk.

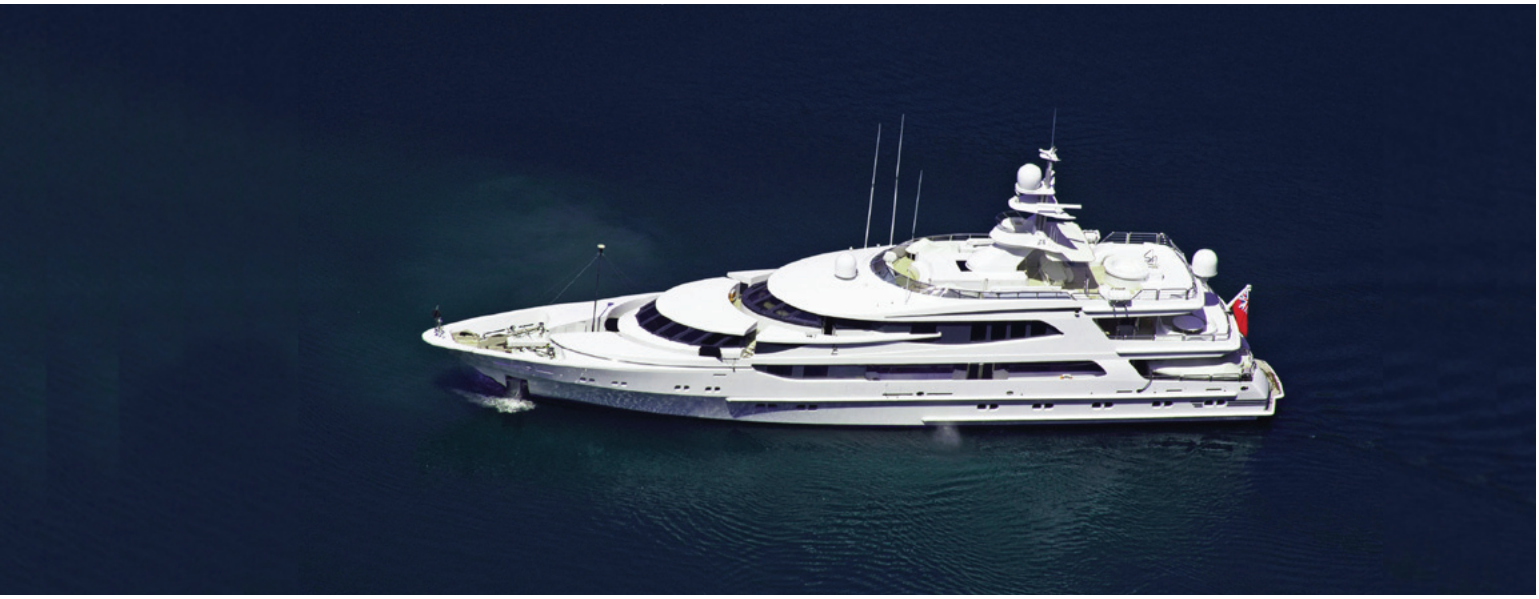
Software licensing: Why non-compliance is not an option

As business leaders worldwide are faced with increasing pressure to rein in costs and stabilize revenue, establishing transparency in managing IP technologies can still prove to be win-win for both software vendors and licensees, and will help nurture innovation that is the cornerstone for building a knowledge-based economy.

Anti-money laundering

Over the past decade, governments around the world have continuously strengthened anti-money laundering legislation and increased the obligations for businesses to know and document the identities and intentions of their customers. At the same time, monitoring and reporting obligations have also increased.

Corruption of foreign public officials: A Canadian perspective



The Corruption of Foreign Public Officials Act (CFPOA) was enacted in 1998 and more recently has become a primary investigation initiative for the Government of Canada.

The Royal Canadian Mounted Police (RCMP) has teams in Calgary and Ottawa specifically dedicated to investigate allegations of violations of the CFPOA. The Niko Resources Ltd.'s criminal conviction was the first significant prosecution under the CFPOA and resulted in severe penalties.

There are also ongoing investigations into alleged bribery payments made to foreign public officials by companies such as SNC-Lavalin Group Inc., which may result in a myriad of criminal and other legal issues. The investigation focus and public reporting of CFPOA investigations reinforces the need for Canadian companies and multinationals with a Canadian presence to ensure they have adequate procedures in place to minimize their bribery and corruption risks.

The CFPOA makes it an offence for Canadian companies and multinationals with a Canadian presence to make payments or promises of payments to foreign public officials, or to any person for the benefit of a foreign public official, that could be considered bribes towards any advantage in obtaining or retaining business.

A violation under the CFPOA is an indictable offence which carries severe penalties including a criminal fine at the discretion of the courts (with no set maximum) for companies, and a criminal conviction with up to five years' imprisonment for individuals. In addition to potential legal and regulatory implications, there's also the risk of adverse publicity and reputational damage if your company faces an allegation of bribery and corruption.

With an increase in the number of Canadian companies with operations abroad and the growing number of RCMP investigations into alleged bribery and foreign corruption, establishing appropriate anti-bribery and corruption compliance policies and procedures has never been more important. In addition to law enforcement, regulatory oversight into operations in foreign jurisdictions has also increased. An Ontario Securities Commission report issued in March 2012 raised concerns with the level of involvement and knowledge of Boards of Directors and Audit Committees in Ontario with regards to issues in foreign jurisdiction operations.

As anti-bribery and corruption enforcement intensifies in Canada and worldwide, the onus of self-regulation and self-monitoring has been placed firmly on management, Boards of Directors and Audit Committees. The financial and non-financial implications of CFPOA violations are significant and may be expected to increase over the next few years.

Your company is subject to the requirements of CFPOA if it is incorporated in Canada or if part of its business is conducted in Canada and your company:

- uses intermediaries such as agents, distributors, consultants, facilitators, market researchers, lobbyists, lawyers, etc.
- conducts business, or invests in businesses, in high-risk countries or regions such as China, South East Asia, India, Russia, Africa, the Middle East, South and Central America, Central, Eastern and Southern Europe.
- conducts business with the government, including central, regional and local governments and state-owned or state-controlled companies and institutions.
- has other interactions with the government for activities such as importing/exporting, obtaining licences, building or operating facilities, obtaining visas, navigating regulations concerning business operations, legal disputes, tax affairs, political donations and lobbying.

It's difficult to contemplate conducting business in a foreign jurisdiction without having some contact with government officials. In fact most companies will find they have several points of contact with government officials on a daily basis. It's not sufficient to accept status quo on the way business has been conducted in the region so far, or to assume that what you don't know will absolve your company of legal and other responsibilities. Companies may find themselves being answerable for behaviours and transactions that predate the current CFPOA enforcement focus by several years.

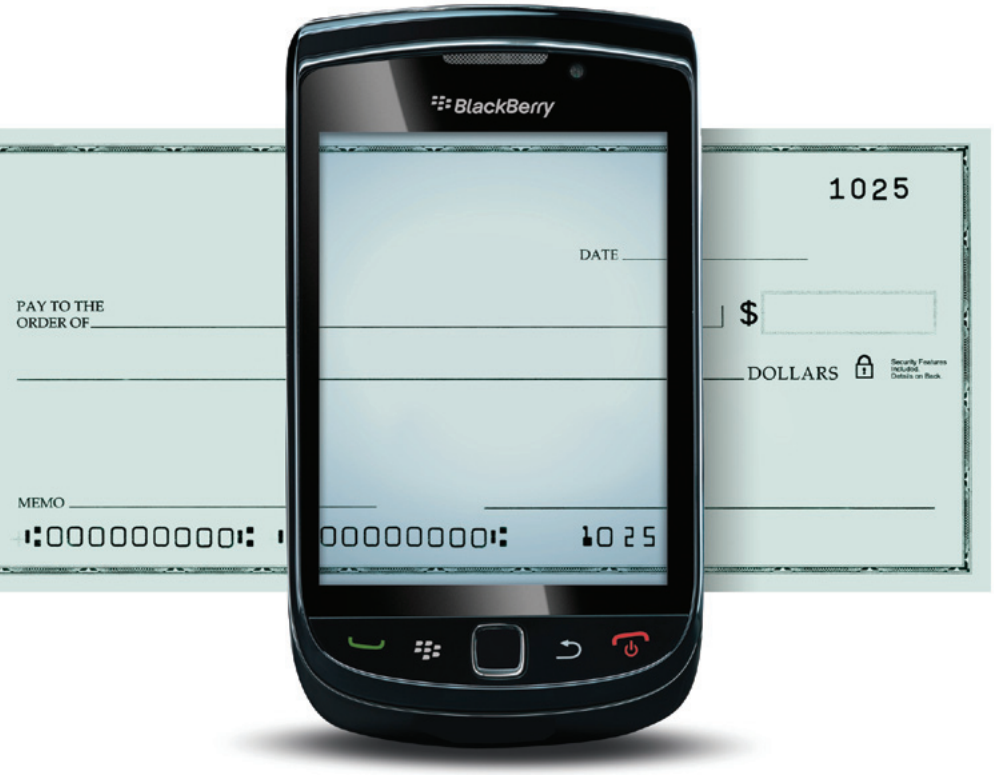
When a company is faced with allegations of bribery and corruption, an aspect that is scrutinized by law enforcement and regulators is the controls and safeguards the company has in place. Attention is paid to the company's level of tolerance towards acts of bribery and corruption, adequacy and regular testing of controls and the culture of compliance within the company.

To address these requirements, your company should begin by reviewing its framework for anti-bribery and corruption policies and procedures in the following areas:

- **Organizational responsibilities:** The Board of Directors is responsible for oversight and the CEO is responsible for implementation of the anti-bribery and corruption program.
- **Business relationships:** Apply your anti-bribery and corruption program to dealings with subsidiaries, joint venture partners, agents, contractors and other third parties who in any way represent your company.
- **Human resources:** Employees should be required to disclose relationships with government officials at the time of hiring and throughout their employment.
- **Training:** Employees, contractors and suppliers should receive training on the company's anti-bribery and corruption program.
- **Raising concerns and seeking guidance:** Employees should be encouraged and required to report concerns, and companies need to ensure that there are no adverse consequences for doing so.
- **Communication:** An effective incident hot line should assure confidentiality, independence and confidence that behaviours at all levels will be accepted and acted on.
- **Internal Controls:** Maintain accurate books and records supported by effective internal accounting controls.
- **Investigation and Remediation:** An investigation protocol should provide reports directly to appropriate resources and escalate serious matters to senior management or the Board.
- **Monitoring and Review:** Periodically assess the strength and adequacy of the anti-bribery and corruption programs and related controls.

An effective anti-bribery and corruption program will alert your company to areas of heightened risk and will reduce the risks associated with prosecution in the event an incident occurs. It also sends a clear message to employees and the business community that your organization is committed to ethical and compliant business practices.

Photo cheque cashing



Through photo cheque cashing, cheques can be deposited without ever having to wait in line at the teller or make a trip to the ATM. With over one billion cheques being issued each year in Canada[1], replacing the traditional in-person cheque deposit process with photo cheque cashing could save businesses an immense amount of time. The only equipment required is a smartphone or a computer with a basic scanner. But technology advancement can also be accompanied by risk.

Already widely used in the United States (US), during the past year and a half, customers of Chase Bank have cashed over US$3 billion cheques using this technology alone.[2] Now, photo cheque cashing is coming to Canada. Changes to industry rules in Canada, which are expected shortly, will enable Canadian banks to offer this capability as early as in 2012.

So, how does this technology work? In the US, banking customers download an application on their smartphones that guides them through the process of taking a picture of the front and back of the cheque. The application ensures the pictures are sufficiently bright and clear and then prompts the customer to destroy the hard copy cheque once the image is captured. With a few simple clicks of a button, individuals can have nearly instantaneous access to funds from anywhere in the world. While there are certainly benefits to both companies and individuals using this technology, these same benefits can lend themselves to abuse and manipulation. Fraudsters everywhere are taking note.

Cheque fraud is currently the fastest-growing financial crime. It is estimated that commercial fraud -- particularly cheque fraud -- costs North American businesses more than CA$20 billion a year.[3] This is consistent with PwC's 2011 Global Economic Crime Survey, which reflected asset misappropriation as the most common type of fraud experienced by respondents globally. The survey also ranked cybercrime as one of the top four economic crimes. Given the prevalence of cheque fraud and the increasing threat of cybercrime, the introduction of photo cheque cashing has widespread implications on both the manner in which the cheque fraud can be perpetrated and how it is investigated.

Impact on fraud

Photo cheque cashing may encourage would-be fraudsters to commit fraudulent cheque schemes. For example:

- Fraudsters can purchase new or used, inexpensive cell phones and prepaid SIM cards from anywhere in the world for use in their scheme. They would then have the tools necessary to make deposits of stolen cheques, transfers and electronic payments using the bank's application. These transactions are virtually untraceable due to the anonymity of the phones.
- Fraudsters can obtain bank account information from the black market, deposit cheques into unsuspecting individuals' bank accounts and then withdraw the funds through various methods. A fraudster could convert a fraudulent cheque and withdraw funds in less than 24 hours. The withdrawal of funds may include hard currency but could also take the form of email transfers to other accounts, payments to credit cards or purchases of prepaid cards. These types of withdrawals can be completed without fraudsters leaving their safe location while unsuspecting bank customers may be faced with substantial losses.

Impact on investigations

This technology also has an impact on the procedures and information used by forensic accountants, law enforcement and other types of investigators. For example:

- Investigators will often request the cancelled cheques to review for evidence of manipulation. Identifying anomalies with this new technology in place will become more difficult given the relative ease of computer imaging manipulation.
- ATM or bank security footage is often reviewed in an investigation to identify individuals who are committing various types of bank fraud. This technology allows individuals to commit cheque fraud with no risk of their personal image being caught on camera.
- Bank deposit information on cancelled cheques may be reviewed to identify anomalies or trends. Deposits at unusual times or locations can often assist investigators in identifying cheque fraud or even the individuals involved in the cheque fraud. Although cell phones and IP addresses can offer similar information, there are privacy implications in obtaining this information, making it more difficult for investigators to conduct this type of analysis.
- In criminal investigations, the lack of hard physical evidence which can be used to identify perpetrators or crime rings could pose a challenge. Law enforcement will no longer have the capability of reviewing the type of ink(s) or paper used to create the cheques. In addition, there will be no fingerprints to potentially capture from the cheques.

Despite some of the risks identified above, photo cheque cashing may offer investigators new data sources and types of analyses such as the use of IP addresses and digital comparisons of signatures.

In markets offering photo cheque cashing, the financial industry has not reported a considerable uptick in cheque fraud to date; however no detailed statistics are readily available. NCR Corporation, the creator of the technology, has stated that committing a crime using digital cheque cashing is no easier than with paper as it is fundamentally perpetrated in the same way.[4] However, many of the traditional methods of uncovering the fraud and identifying the perpetrators may be circumvented with this technology.

It appears that the adoption of the photo cheque cashing is simply a logical extension of Canada's current standards where cheques are cleared based on bank-captured images alone and often the physical cheques are not retained. Will the convenience of photo cheque cashing outweigh the risks? We'll soon find out.

1 Canadian Bankers Association. (December 21, 2011). *Protecting Yourself from Cheque Fraud*. Retrieved from http://www.cba.ca/en/consumer-information/42-safeguarding-your-money/599-protecting-yourself-from-cheque-fraud. Accessed August 2, 2012.

2 Robertson, G. (May 29, 2012). *Depositing Cheques? Soon your smartphone can help with that*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/globe-investor/personal-finance/financial-road-map/depositing-cheques-soon-your-smartphone-can-help-with-that/article2414716/. Accessed August 2, 2012.

3 Desjardins Financial Group. (n.d.). *Frequently asked questions about cheque fraud (FAQ) – Q. What is cheque fraud?* Retrieved from http://www.desjardins.com/en/a_propos/profil/securite_en_ligne/eviter_victime_fraude/fraude_cheque.jsp. Accessed August 2, 2012.

4 Robertson, G. (March 27, 2012). *Say Cheese! Photo chequing on its way to Canada*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/globe-investor/say-cheese-photo-chequing-on-its-way-to-canada/article2381965/. Accessed August 2, 2012.

Software licensing:

Why non-compliance is not an option

Since the financial meltdown of 2008, perhaps no word resonates as deeply with business executives as 'volatility'. Instability in financial markets, the credit crunch and the global economic slowdown have all led to a dramatic decrease in consumer confidence and have made business growth more challenging than ever before. Businesses are adjusting to operating in this new environment of demand volatility.

The resulting implication of this landscape is that business leaders worldwide are faced with increasing pressure to rein in costs and stabilize revenue. Information Technology (IT), which forms an integral part of business infrastructure today, is not immune to such priorities. Even though IT budgets are on the rebound, most organizations are still under pressure to keep the lid on IT operational costs. What does this all mean to software vendors? Significant challenges come to the forefront. For one thing, the rationalization of IT spend, a substantial proportion of which comprises software license fees, has direct consequence on the revenue streams of software publishers.

Software vendors are also observing a shift in their revenue distribution. As customers show more resistance towards paying upfront license fees and even renewal or upgrade fees, the revenues from maintenance and support are growing in comparison to license fees. Where IT is perceived as a cost-center as opposed to a business enabler, the software vendors have an even tougher challenge to overcome in promoting their products.

Another trend that has exacerbated the challenge is the advent of open source technologies. Software vendors are responding to this shift in demand in two ways. Firstly, they are taking an increasingly proactive approach to protecting their intellectual property (IP) rights in order to extract maximum value from their innovation. This strategic focus has translated into systematic enforcement programs to examine compliance with their licensees. Consequently, organizations have seen a dramatic increase in license compliance audits since 2009.[1] Gartner Inc., a leading IT research company, reported in its 2011 survey[2] that 61% of its respondents had been subjected to at least one audit in the past year. Secondly, software vendors are rethinking their pricing models and offering more flexible licensing to adapt to the changing needs of the customers. While compliance audits may appear to be an obvious attempt to make up for shortfalls in license revenue, it is a strategic move towards IP protection. The focus on pricing model, however, is a long-term strategy in direct response to changing customer needs. Nonetheless, the vendors are certainly likely to continue to exercise their audit rights clause of the license agreement in an attempt to address the widespread issue of under-reported deployment or usage.

From a licensee perspective, the rise in enforcement necessitates a rigorous, measurable and consistent process to manage software assets to avoid substantial non-compliance penalties. The penalties for non-compliance can be staggering, ranging from thousands to even millions of dollars. Because overuse of software licenses can be characterized as software piracy, the consequences can be severe for non-compliance.

Implementing a Software Asset Management (SAM) program is an effective way to manage software inventory—a first step in achieving compliance. The benefits of a SAM program do not stop at just avoiding penalties. Organizations that have successfully implemented SAM have a significant leg-up in contract negotiations with their software vendors over organizations that do not have a streamlined process to manage IT assets. Additionally, such organizations can continually monitor surpluses and harvest unused licenses, saving precious dollars in license fees.

In summary, there are clear compelling business justifications for both licensors and licensees alike to take steps to ensure license compliance. Establishing transparency in managing IP technologies can prove to be win-win for all organizations and will help nurture innovation that is the cornerstone for building a knowledge-based economy. Is your organization taking IP rights seriously?

1 Gartner Polls and Surveys Show an Increase in Software License Audits. 31 July 2009
2 Gartner, Survey Analysis: Survey Shows Another Increase in Software Vendor Audits? IT Asset Managers Should Prepare Now, 2 March 2011

Anti-money laundering

Knowing who you do business with is more important than ever before. In addition to the traditional concerns of a customer's ability to repay debts or a supplier's ability to meet deadlines, businesses have obligations to fully understand their customers.

Over the past decade, governments around the world have continuously strengthened anti-money laundering legislation and increased the obligations for businesses to know and document the identities and intentions of their customers. At the same time, monitoring and reporting obligations have also increased. The scope of these regulations now extends well beyond the traditional focus on the financial services industry.

The Royal Canadian Mounted Police (RCMP) estimates that CA$5 billion to CA$15 billion is laundered each year in Canada.[1] In an attempt to reduce instances of money laundering, businesses and individuals involved in a wide range of industries are obligated to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). They're also required to meet certain recordkeeping and transaction reporting requirements.

The industries covered by existing legislation include:

- Financial entities including banks, credit unions, caisses populaires (a cooperative, member-owned financial institution), trust and loan companies, life insurance companies and securities dealers
- Money services businesses including any business engaged in foreign exchange service, funds remittances and issuing or redeeming money orders, travellers cheques and similar instruments
- Professionals including accountants, notaries (in British Columbia), life insurance agents and realtors
- Dealers of precious metals and stones
- Casino operators

Knowing a customer's true identity -- whether they're acting on their own or with/on behalf of others, and the source of their funds or assets -- is fundamental to governments' efforts to combat money laundering. As a result, governments have implemented severe penalties for non-compliance. Maintaining an effective, well-documented anti-money laundering compliance program will help ensure regulatory compliance and avoid potential legal costs and penalties. It will also avoid public and media attention for unwittingly supporting money laundering.

FINTRAC, for example, requires the following five elements to be included in a compliance regime[2]:

1. Appointing a compliance officer.
2. Developing and applying written compliance policies and procedures.
3. Assessing and documenting risks related to money laundering and terrorist financing, and measures to mitigate against these high risk activities.
4. Implementing and documenting an ongoing compliance training program.
5. Documenting the effectiveness of policies and procedures, training programs and risk assessments.

The potential penalties for failing to comply with anti-money laundering and customer due diligence obligations can be severe. Administrative penalties of up to CA$500,000 for each violation can be administered by FINTRAC and criminal sanctions can be even more severe. The criminal penalty for failing to report a suspicious transaction is up to five years of imprisonment and/or a CA$2 million fine.

Failing to maintain adequate records can lead to five years of imprisonment and/or CA$500,000 fine. Since penalties can be applied for each breach of the law, the total penalties applied can greatly exceed these individual maximums.

Penalties are also severe internationally. Earlier this year in the United Kingdom, two men were sentenced to 6 and 11 years in prison for laundering £17 million of illegal drug proceeds.[3] Argentina has introduced regulations to combat money laundering in soccer with penalties of up to ten times the amount of the money involved.[4] Even closer to home, it was reported this summer that HSBC has been fined US$27.5 million in Mexico[5] and faces penalties in the United States of up to US$1 billion for failing to maintain adequate customer due diligence and anti-money laundering procedures, allowing customers to launder money easily.[6]

In Canada, the expectations for businesses to know their clients are increasing. Regulations proposed in November 2011 set out new requirements that obligate businesses to understand the nature of their business relationship with customers and apply risk-based principles when evaluating customers. It's becoming increasingly important for businesses to understand their evolving legal obligations and to implement well designed anti-money laundering policies and processes.

1 Royal Canadian Mounted Police. *Money Laundering*. Retrieved from http://www.rcmp-grc.gc.ca/qc/pub/blanch-launder/blanchiment-laundering-eng.pdf. Accessed July 17, 2012.
2 Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (May 2011). *Guideline 4: Implementation of a Compliance Regime*. Retrieved from http://www.fintrac.gc.ca/publications/guide/Guide4/4-eng.asp. Accessed July 14, 2012.
3 FINTRAC. *Money Laundering and Terrorist Activity Financing Watch: January – March 2012*. Retrieved from http://www.fintrac.gc.ca/publications/watch-regard/2012-07-eng.asp. Accessed July 14, 2012.
4 *Ibid*.
5 Buchanan, R and Nasiripour, S. (July 25, 2012). *Mexican regulator fines HSBC unit $27.5m*. FT.com.
6 Slater, J. (July 17, 2012). *HSBC failed to control drug-money laundering, Senate finds*. The Globe and Mail. Retrieved from http://www.theglobeandmail.com/report-on-business/international-business/us-business/hsbc-failed-to-control-drug-money-laundering-senate-finds/article4422546/. Accessed July 17, 2012.

Who to call
National Forensic Services Team

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

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

Kas Rehman
National Public Sector Forensic Services Leader
613 755 4328
514 205 5171
kas.rehman@ca.pwc.com

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

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

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

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

Marie-Chantal Dréau
Vice President, Forensic Services
514 205 5407
marie-chantal.dreau@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
GTA Forensic Services Leader
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

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