Grant Thornton

An instinct for growth™

Fraud in the spotlight

A multi-region perspective on fraud

Contents

Foreword

Fraud is a major concern for organizations worldwide—and for good reason. This type of criminal activity has the potential to damage shareholder and consumer trust, erode brand value and result in serious financial and legal implications. And in today's highly-interconnected digital world, these negative impacts can be disseminated in seconds.

In light of this reality, it's clear that today's businesses can't afford to put fraud on the backburner. Organizations must invest appropriate efforts and resources in building a robust anti-fraud framework if they hope to detect and mitigate incidents in an effective manner. This report is designed to help Canadian companies in this endeavour.

Drawing on data from the Association of Certified Fraud Examiners (ACFE) *Report to the Nations–2018 Global Study on Occupational Fraud and Abuse*, the first section of our report offers an overview of pertinent fraud trends across the globe—focusing specifically on the fraud landscapes in Canada, the United States, the United Kingdom, India, Hong Kong and Shanghai. This data is then complemented by insights from our regional forensic practitioners—exploring how companies can effectively mitigate these fraud risks, heighten their preparedness, and adopt appropriate counter-measures.

We hope you find this report to be a useful tool as you move forward on your journey to protect yourself from fraud. And, as always, if you require support along the way, your Grant Thornton team is happy to help.

Sincerely,

Jennifer Fiddian-Green, CPA, CA/IFA, CAMS, CFF, CFE, CFI
National Advisory Partner
Grant Thornton Canada

Canada: A regional fraud perspective

As in every global region, fraud takes a variety of complex forms in Canada—ranging from sophisticated cyber breaches and holding corporate data for ransom, to spoofing executive email addresses to gain access to internal systems. While all these threats are real, businesses often overlook one of the largest risks to their companies: occupational fraud, which is fraud committed against an organization by its own people.

In the ACFE's *Report to the Nations–2018 Global Study on Occupational Fraud and Abuse*, the organization examined 2,690 real incidences of occupational fraud that occurred in 2017. The report revealed that private companies—which constitute the majority of Canada's economy—fell victim to fraud more often than their public counterparts. Similarly, small- to medium-sized businesses, on average, lost twice as much money to occupational fraud schemes than larger companies—a median loss of US$200,000 per scheme compared to US$104,000 for companies with over 100 people. With fewer resources to combat fraud, less robust anti-fraud controls and a tendency to implicitly trust their people, these companies are often hit the hardest.[1]

Current fraud trends

Despite stronger regulations to combat fraud in general, and the availability of increasingly sophisticated technology to fight it, occupational fraud continues apace. According to the ACFE, the three most common categories of occupational fraud in Canada are corruption schemes, billing fraud and non-cash fraud.

- Corruption schemes, which account for roughly 40% of Canada's occupational fraud, occur when employees or managers form personal alliances with external parties and put those relationships ahead of the best interests of the company. These schemes can include conflicts of interest (e.g., purchasing or sales schemes), illegal gratuities and bribery (e.g., vendor kickbacks or bid rigging).
- Billing fraud can include using corporate resources to make personal purchases or diverting funds to shell corporations. Roughly 20% of occupational fraud in Canada takes this form

- Non-cash fraud, or the misappropriation of assets, takes place when an individual fraudulently takes possession of materials or goods rather than cash or financial instruments. It accounts for 18% of Canada's occupational fraud cases.[2]

1 Association of Certified Fraud Examiners, 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse." Accessed at https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf on February 19, 2019.

2 Association of Certified Fraud Examiners, 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse." Accessed at https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf on February 19, 2019.

United States: A regional fraud perspective

As in other regions in the world, fraud in the United States remains pervasive and has the potential to take a significant financial and reputational toll on virtually every type of organization—large and small, public and private. It also manifests in myriad ways—from bribery and corruption to occupational fraud and money laundering. Yet, given the rapid pace of digitization in the country, cyber fraud is particularly prevalent.

US organizations are taking significant strides to tackle this risk. In addition to conducting enterprise-level fraud risk assessments, they are also developing data analytics tools to detect and prevent fraud by uncovering trends and patterns in large data sets.

Current fraud trends

Fraudulent activity extends to every sector of the US economy—including financial services (e.g., banks, insurance companies, securities firms), manufacturing, healthcare, government services and beyond. In the cybercrime space alone, fraudsters use tactics such as business email compromise to gain access to internal systems, ransomware attacks that hold proprietary corporate data for ransom, and credential stuffing—which involves the automated injection of breached username/password pairs into corporate networks to fraudulently gain access to user accounts.

Indeed, account takeover attacks stemming from breached information continue to pose a significant threat to a variety of industries. A recent study, commissioned by Bromium, found that the cybercrime economy has grown to $1.5 trillion annually in illicit profits being acquired, laundered and spent by cybercriminals.[3] This may partly explain why companies experience data breaches almost daily, as fraudsters attempt to gain control over proprietary information assets, intellectual property and personally identifiable information (PII). These PII breaches often contain critical data about a company's constituents, partners, customers and employees—including account credentials—and expose companies not only to the risk of financial loss, but to severe reputational damage and regulatory penalties as well.

Data breaches are notable for another reason: They also enable complex fraud schemes. Much of the stolen information obtained via data breaches ends up on underground digital marketplaces, which is underscored by the fact that there are hundreds of marketplaces on the dark web advertising billions of PII records for sale.

3 Bromium, April 20, 2018. "Hyper-connected web of profit emerges, as global cybercriminal revenues hit $1.5 trillion annually." https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/

United Kingdom: A regional fraud perspective

In an attempt to curb fraudulent activities, the United Kingdom has introduced more stringent regulations in recent years, and has begun to actively impose fines for breaches of the UK Bribery Act (UKBA). Although this seems to be reducing certain instances of fraud, cyberattacks remain alive and well. According to the World Economic Forum, cyberattacks are considered the risk of highest concern to business leaders in advanced economies.[4] The UK economy is no exception: in late 2017 and again in early 2018, two major banks in the country fell prey to cyberattacks.

Current fraud trends

Over the past few years, the level of fraud in the United Kingdom has mainly been influenced by two different trends: heightened regulatory enforcement and advancements in technology.

- **Regulatory enforcement.** As already noted, enforcement of the UKBA is picking up. In February 2018, Skansen Interior Limited (SIL) became the first corporate to be convicted by a jury at trial of the offence of failing to prevent bribery under Section 7 of the Act. This came in the wake of guilty plea lodged by Sweett Group. As table 1 shows, other companies are taking steps to settle potential action through Deferred Prosecution Agreements (DPAs)—demonstrating a newfound willingness by companies to engage with authorities. In January 2018, changes to the Criminal Finances Act also came into effect introducing the Unexplained Wealth Orders regime, which allows five enforcement authorities to require respondents to state the nature and extent of their interest in certain properties—a step intended to help recover the proceeds of crime.

Table 1: UK enforcement action

Date	Company	UK penalty (£ m)	Enforcement process
15 September	Brand-Rex	0.2	Civil settlement (Scotland)
15 November	ICBC Std Bank	32.5	DPA (SFO)
16 February	Sweett Group	2.3	Prosecution with guilty plea (SFO)
16 April	Braid Group	2.2	Civil settlement (Scotland)
16 July	XYZ	6.6	DPA (SFO)
17 January	Rolls-Royce	497.3	DPA (SFO)
17 April	Tesco Plc	129	DPA (SFO)

- **Use of technology in investigations**. In a bid to fight fraud at its source, the Serious Fraud Office (SFO) recently made the first use of artificial intelligence (AI) in a criminal case in the UK, to assist in the identification and removal of privileged documents—a decision that reduced document review times by 80%, from an estimated two years to a few months. Following a successful implementation in the Rolls-Royce case, the SFO announced that AI-powered Robo-Lawyers, capable of processing more than half a million documents a day, would be made available in April 2018. The robots are roughly 2,000 times faster than a human lawyer, enabling authorities to speed up investigation. .

4 World Economic Forum, January 17, 2018. "Cyber risk is a growing challenge. So how can we prepare?" by John Drzik. https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/

India: A regional fraud perspective

Despite India's impressive growth rates—estimated at 7.3% in fiscal 2018-2019 and 7.5% in fiscal 2019-2020[5]—and the sheer size and diversity of its market, the country is still struggling to manage risk. Fraud incidents have been on the rise, underscoring a gap in effective governance practices.

According to the ACFE's *2018 Report to the Nation*, of the 96 reported cases of occupational fraud in Southern Asia, 72 took place in India. The country has also been plagued with public sector corruption, complex bureaucracy and a lack of transparency—challenges it is now trying to address through the *Prevention of Corruption (Amendment) Act, 2018*.

Current fraud trends

The fraud environment in India is changing rapidly. While fraud schemes vary across industries (see table 2), traditional fraud schemes like accounting and procurement fraud, bribes and kickbacks, and siphoning of funds continue to dominate and proliferate. Endemic challenges also persist. For instance, when dealing with public officials, companies are often expected to remit improper payments to obtain government licenses, renew contracts or gain permits. Custom and forwarding agents frequently make similar demands. At the same time, cybercrime is on the rise, with mounting instances of identity theft, digital fraud and corporate espionage.

Table 2: Fraud schemes by industry

Sector	Fraud risks	Red flags
Manufacturing	Third-party fraud, substandard product, falsified invoices, theft of inventory/equipment, diversion of goods, intentional modification of a finished product, misuse of company assets, registration of factory lands in promoter's name, receipt fraud, shipment fraud, bid rigging	Favouritism or preferential terms to a particular vendor
Healthcare and pharmaceutical	Counterfeit drugs, price cartels, misappropriation of assets, bribery, collusion, adulteration of mix, selling samples at cost, phony drug trials for research grants/subsidies, manipulation of clinical trials through bribes, off-label marketing, pricing fraud	Kickbacks to vendors or their agents or inappropriate incentives to promote specific products
Real estate and construction	Collusion, bid rigging, diversion of funds, improper contract awards	Unusual bid patterns
Information technology	Data theft, IP infringement, financial misreporting, procurement fraud, payroll fraud, recruitment fraud, misappropriation of funds, service level agreement (SLA) violations, side agreements with vendors, corporate espionage, harvesting of codes	Non-compliance with license agreements
Financial and banking (including insurance)	Money laundering, employee fraud, improper financial disclosures, undisclosed related-party transactions, lending at preferred rates, insufficient due diligence before lending, violation of Know Your Customer (KYC) norms, forgery, online banking fraud, credit card scams, loan fraud, diversion of assets, faking vehicle accidents, home loan-related fraud	Fraudulent documentation, misrepresentation of financial information
Consumer and retail	Procurement and supply chain fraud, pilfering, adulteration, contamination, concealment, mis-labelling, dilution, ingredient substitution, fake goods, weight-related, counterfeiting, collusion, diversion of goods, misuse of advertising spends or discount coupons, theft of promotional items	Inventory shrinkage, fabricated sales documents, vendor favouritism

5 http://pubdocs.worldbank.org/en/533201526416533271/Global-Economic-Prospects-June-2018-Regional-Overview-SAR.pdf

Hong Kong: A regional fraud perspective

Hong Kong is one of the most prominent commercial and financial hubs in the world and, in turn, a natural target for fraudsters. Studies from the Federal Bureau of Investigation (FBI) reveal that China and Hong Kong are the primary destinations of fraudulent funds. According to the Hong Kong Anti-Deception Coordination Centre (ADCC), although the overall crime figure has decreased in recent years, the number of fraud cases has remained the same, with approximately 7,000 cases per year in 2016 and 2017, and a similar trend in 2018.

While measures have been taken to rectify this trend—including zero-tolerance policies implemented by police agencies, as well as higher levels of transparency on the part of companies—it's nevertheless still challenging to detect. This is largely due to the broad variety of frauds committed and the high volume of business transactions that occur in this international hub.

Current fraud trends

Fraud incidents in Hong Kong continue to be diverse, with cyber, telephone and investment fraud considered to be the most common.

Cyber fraud

Online business frauds top the charts in Hong Kong, accounting for **27%** of all cases.

This is followed by social media deception and unauthorized access to computers, which has seen the largest surge in cases recently. In 2016, financial losses arising from corporate-level email scams grew by 363% to HK$1.8 billion.

In addition, malware attacks are also growing in number, due largely to the limited availability of IT security experts in Hong Kong. According to the Legislative Council Research Office, there are only 769 IT security experts in Hong Kong, equalling just 0.9% of all the IT employees in the country.

Telephone and investment fraud

From 2008 to 2015 telephone deception cases increased by **77%** in Hong Kong

While the number of telephone frauds has since dropped, the total amount of loss from these cases is still valued at approximately HKD $220 million.

With this type of fraud, criminals commonly pose as government officials from the Hong Kong Inland Revenue Department (IRD)—or officers in banks and courier companies—and ask potential victims to make online transfer payments. Others imitate professional investment managers, tricking victims into opening accounts in fake investment companies and then making huge deposits into these accounts in lieu of a promised high rate of return.

Investment fraud

Of the 2,000-plus companies listed on the Hong Kong Stock Exchange, **40** are currently facing fraud allegations and are currently suspended from trading.

These companies are under investigation by the Securities and Futures Commission (SFC), and are either undergoing forensic investigation or required to demonstrate the integrity of the management. While the figure still remains low, it's important to note that the SFC launched more investigations in 2017 and 2018 than in prior years.

Shanghai: A regional fraud perspective

The Shanghai region continues to be a diverse and evolving fraud theatre, making it challenging for forensic professionals to stay ahead of the curve. According to the Association of Certified Fraud Examiners' (ACFE) *Report to the Nations*, China recorded the most cases of occupational fraud in the Asia-Pacific region in 2017.

Because of these changes, several multi-national corporations (MNCs) have had no choice but to become more integrated and sophisticated in their compliance efforts. These companies have taken great strides to strengthen their in-house capabilities for fraud prevention and detection—reducing their compliance budgets, and their reliance on external vendors, in the process. This has raised the bar for fraud protection in the region—and smaller companies are starting to follow suit, slowly but surely maturing their prevention and detection skills.

Current fraud trends

Even as the depth and complexity of schemes continues to evolve, occupational fraud remains the prime source of financial loss in the region.

Corruption and bribery make up **51%** of fraud cases, followed by fictitious expense reimbursements.

According to the ACFE *Report to the Nations*, Shanghai isn't an anomaly. Across the world, managers are the culprit in 41% of occupational fraud schemes—thanks largely to their access to upper-level security clearances—while employees and executives made up 30% and 26% of the cases respectively. Employee fraud cases typically have a median loss of $58,000, according to the report, while managers caused losses of $323,000 and owners/executives created losses of $1,000,000.

Taking action: How to win the fight against fraud

Become fraud-aware

The ACFE estimates that an average organization loses five percent of revenue annually to fraud. The extent of fraud an organization suffers depends largely on its business model and how seriously it manages fraud risk. The more "fraud-aware" an organization is, the less fraud it is likely to experience, as almost half of all frauds committed are due to weaknesses in internal controls (ACFE *Report to the Nations 2018*). Fraud-aware organizations are those that adopt strong anti-fraud controls and focus on proactive fraud detection.

In September 2016, the ACFE and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) jointly issued a framework for a proactive fraud risk management approach. The *Fraud Risk Management Guide* describes five phases of a leading fraud risk management program.

In the United States, the Government Accountability Office (GAO) issued the *Framework for Managing Fraud Risks in Federal Programs* in July 2015, which describes a similar anti-fraud approach for government agencies. These approaches focus on creating a culture conducive to anti-fraud efforts by identifying and combating fraud risks through enterprise-wide fraud risk assessments and implementing fraud-focused analytics.

Develop a fraud risk management program

An effective fraud risk management program starts by assessing all forms of organizational risk—both internal and external—and defining a company's risk appetite. Once these parameters are established, it becomes easier to devise effective prevention strategies, implement early detection controls, create avenues for internal reporting, mitigate third-party risk and establish clearly-defined anti-fraud policies.

01 A formal assessment of fraud risks

02 The development of mitigating control activities aimed at the highest risk areas

03 A fraud reporting process and an approach for investigating fraud

04 An oversight and monitoring function to ensure properly functioning controls and that new fraud schemes are considered

05 A governance structure with top level commitment to anti-fraud efforts

To better understand how such a program is constructed, and ultimately how a fraud-aware organization comes into being, let's examine each component in more detail.

01 Assess your fraud risks

Today's fraud-aware organizations are increasingly undertaking comprehensive, enterprise-level fraud risk assessments and charging senior executives with fraud risk management responsibilities. While a fraud risk assessment can take many forms, certain common elements can help drive success:

- To identify hidden fraud risks, develop fraud scenarios that apply directly to your organization and focus risk discussions on the processes most likely to be compromised by those scenarios.
- Bring key stakeholders together in facilitated fraud risk workshops to discuss specific risks and their related controls, and assess the organization's greatest fraud risk exposures.
- Cultivate a risk aware culture that encourages stakeholders both within and outside the organization to enforce ethical behaviour and alert executives to potential problems.
- Use the first fraud risk assessment as a baseline to build on lessons learned and improve over time.

By taking these steps, you can gain a better understanding of your fraud vulnerabilities and establish more effective prevention strategies, programs, processes, policies and controls. It can also help you identify behavioural red flags in existing officers and directors.

While a fraud risk assessment is integral at the beginning of any fraud risk management journey, it shouldn't be treated as a one-time event. Even after all employees have attended fraud training and fraud controls have been put into place, regular fraud risk assessments are a necessity. Fraud is constantly changing, and companies must change accordingly.

02 Create robust internal controls

Internal controls are the most effective way to prevent fraud, and one of the most basic safeguards that every company should have—and yet, according to the ACFE, "lack of internal controls" is the most common reason behind fraudulent activity. The organization says 30% of internal fraud cases are caused by not having a simple risk prevention strategy in place.

While most organizations tend to have basic controls in place—such as codes of conduct, external audit of financial statements, whistleblower hotlines, regular management reviews, internal audit departments and independent audit committees—many aren't being used appropriately. For instance, random internal audits are an effective way to detect fraud and are also a strong deterrent to potential fraudsters—but they should be a surprise, not conducted in a regular pattern. Similarly, many companies have whistleblower hotlines that are rarely, if ever, used.

There are also many controls companies can implement but simply aren't—like enforcing mandatory vacations, separation of duties and job rotations, which prevent employees from getting too comfortable in any specific role.

A clearly articulated anti-corruption policy is also a must-have. This policy should be integrated with your company's code of conduct and address compliance training programs, ongoing monitoring and audit testing, surprise site visits and internal reporting mechanisms. It should also address your organization's approach to document retention so, once a fraud is suspected, documents can be easily leveraged to investigate it.

03 Implement early detection controls

Thanks to advances in technology and cybersecurity practices, organizations no longer have to wait until a fraud is committed—and causing damage—to identify it. Rather, through advanced methods such as data analytics and cyber threat intelligence, it's now possible to actually predict when a fraud might take place. While implementing such measures is unquestionably a complex undertaking, it comes with a high return on investment.

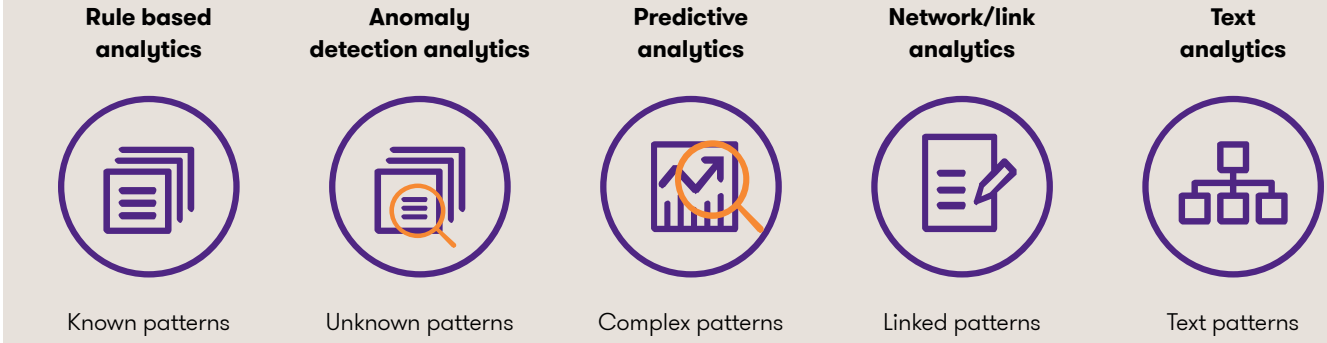
The power of analytics

According to the ACFE, organizations that employ analytics to combat fraud experience a 54% reduction in the total loss and duration of a fraud scheme. That's why a well-considered fraud analytics strategy can foster much quicker fraud detection and help organizations avoid the traditional "pay-and-chase" approach.

To reap the benefits of such a strategy, it's important to first uncover where your organization currently stands from an analytics perspective—and what steps need to be taken to employ predictive techniques.

In predictive analytics, future conditions are estimated based on historical data, as opposed to descriptive analysis. As shown in the Fraud risk assessment figure to the right, there are essentially five categories of fraud analytics techniques. The proper category to use depends on the nature of the problem and the maturity of an organization's analytics capability.

Fraud risk assessment



01 Rule-based analytics

A transaction-level technique used to prevent common fraud based on known patterns. Rule-based analytics focuses on transactions that do not adhere to organizationally-accepted rules, such as using a company purchase card to buy alcohol on a Saturday evening.

02 Anomaly detection analytics

Focused on investigating aggregate-level transactions, anomaly detection uses "unsupervised modelling" to identify outlier transactions within peer groups. This type of analytic technique allows organizations to understand outlier patterns across the data that may reveal fraud incidents and might warrant follow-up investigation.

03 Predictive analytics

As patterns become more complex, predictive analytics can identify unobserved attributes that lead to the identification of potential fraud, based on known cases of prior fraud. For example, an analytic model could be designed to automatically reject a payment when known fraudulent characteristics are present within a given transaction.

04 Network/link analytics

This technique can be useful for uncovering organized fraud and associations between fraudsters by using social network analytics. For example, an individual's activities may not be suspicious in isolation, but suspicions may arise when this individual's activities are connected to others exhibiting shared attributes, thus revealing schemes that may have otherwise gone undetected.

05 Text analytics

By scraping information from large data troves (e.g., IoT devices, call logs, email records, etc.), text analytics can break strings of text and scan for fraud indicators. Natural language processing tools can be employed to divide text into segments that are then analyzed for patterns, which in turn can be examined based on a contextual agenda deemed important by the organization (e.g., employee morale, common fraud indicators).

The use of data monitoring analysis is also swiftly working its way onto the fraud analytics scene—and has already dramatically

increased the speed of fraud detection by

58%

and reduced losses by

52%

This can be attributed to the rapid evolution of such technologies as Machine Learning and Artificial Intelligence, which are helping companies identify potential anomalies and detect fraudulent or suspicious behaviours better than ever before.

Leverage cyber threat intelligence

Cyber threat intelligence can also be an excellent tool in combatting today's fraudsters. Borrowing practices from government intelligence disciplines, such techniques leverage intelligence resources to guide the allocation of defensive and offensive anti-fraud resources.

When implemented correctly, intelligence feeds save time and conserve resources by instructing cyber defence systems to block traffic from "blacklisted" origins. Threat intelligence providers use software and human intelligence techniques to mine markets, conversations, forums and other sources looking for customer-specific data.

For example, if an insurance provider's call centre receives an inbound call about an account, but that accountholder's information is known to be compromised or for sale, the record can be flagged as "high risk." This enables further screening of the individual making the request. Additionally, measures can be applied on the front end of account provisions, where the threatened data can be used to determine if a new account request is linked to a known breach—providing an avenue for further scrutiny prior to granting access.

Establish an avenue for internal reporting

While data analytics and surveillance are effective tools in combatting external fraud, most occupational frauds actually come to light as a result of an insider tip. In fact, internal reporting—where employees uncover wrongdoing and reporting—can be more effective than internal audit and surveillance/monitoring combined.

Because of this, organizations hoping to combat fraud should look internally as well as externally—and consider implementing measures to encourage internal reporting. There are a number of ways to do this:

- **Set a strong tone at the top:** If a business owner or executive team believes that fraud is only something that happens to large corporations or thinks their employees are above reproach, it will be nearly impossible for the rest of the organization to take the necessary steps to move forward. As such, it is paramount that these individuals not only educate themselves on the current threats facing their organizations, but also communicate this information to their people as well. This type of top-down approach is the key to successfully implementing an effective fraud-prevention system.

Similarly, the board has an important role to play in creating a culture that's tough on fraud. Without an engaged board of directors that is willing to participate and ask the right questions, it becomes all too easy for management to set an improper tone—and either become an accomplice in fraud or create a culture that leads to unethical leadership practices.

- **Invest in education:** Senior executives must empower all departments, and not just IT, to devote the necessary financial and educational resources to combat fraud—and implement appropriate tools, training and safeguards to stress the importance of fraud prevention. This includes developing and enforcing an effective code of conduct, adopting an anti-fraud policy and conducting formal fraud-risk assessments.

  Additionally, to achieve a level of fraud awareness that spans the entire organization, fraud awareness training should be an ongoing activity, not a one-time event. It should be provided to both new employees during their onboarding process and existing employees and managers on a regular basis. To track and measure how your employees' level of fraud awareness is improving over time—and assess how well you are addressing the identified vulnerabilities—you may also want to conduct both planned and surprise audits, including external audits of your financial statements and internal controls, and internal audits of your staff's performance.

- **Implement an effective whistleblower hotline:** Whistleblower hotlines are one of the most cost-effective fraud-fighting measures—and they work. According to the ACFE's report, 46% of victim organizations with hotlines were notified of their fraud schemes via a tip, versus 30% of organizations without hotlines.

  However, to get the most out of your hotline—and ensure employees feel comfortable using it—it is essential to:
  - demonstrate commitment to the program through proper awareness, training and a strong tone at the top;
  - boost program transparency by providing regular, big-picture feedback (i.e., how many reports were received annually and organizational changes that came about because of such reports);
  - make the program available to all vulnerable touchpoints, including third-party agents, clients and employees;
  - implement measures to protect the whistleblower from retaliation; and
  - commit to continuous improvement and communicate improvements to your employees.

- **Mitigate third-party risks**: In today's business environment, when many companies rely on vast and complex supply chains, fraudulent third-party vendors can cause significant damage. For instance, if the agents of a multinational's Indian subsidiary offer bribes in exchange for permits to operate a factory, the entire organization can be found liable.

  As a result, when implementing anti-fraud measures throughout your organization, it's important to also include your supply chain—and take the necessary steps to ensure your third-party vendors are ethical and vigilant in their approach to fraud.

Know how to respond

Once fraud is identified, corporations must move quickly to carry out their fraud response plan. This plan should be clearly outlined in your anti-corruption policy, and explain the procedures required to gather and collate evidence.

Having a proper response plan in place allows leaders to act efficiently during an investigation and prevent more loss from occurring. After a fraudulent incident is detected, investigated and appropriate follow up and recovery actions are executed, time must be taken for reflection. There are lessons to be learned from each fraudulent incident. As such, leaders should examine the conditions that allowed the fraud to occur and strive to improve systems and procedures to prevent history from repeating itself.

Charting a path forward

There's no question that advances in society are creating new and exciting opportunities for businesses across the globe—but they're also introducing new fraud risks. To truly maximize the former while mitigating the latter, organizations must pay close attention to the evolving threat landscape—both in their local regions and beyond—and respond accordingly.

For many, this means conducting thorough fraud assessments, strengthening (and, in some cases, implementing) internal controls, establishing effective internal reporting mechanisms and having a fraud response plan in place. It will also require anti-fraud professionals to continually upgrade their knowledge of anti-fraud controls and skills to remain one step ahead of savvy criminals.

With these fundamentals in place, it will become easier for industry to work alongside governments and regulators—and offer valuable insight to create powerful fraud-related policies and regulations to effectively fight fraud across the world.

Contributors

Contact us to learn more about how Grant Thornton can help your organization take the necessary steps to protect itself from fraud.

If you would like to discuss anything further with our contributors, please get in touch with one of the contacts listed in the regions here or your local Grant Thornton advisor.

Canada

Jennifer Fiddian-Green
National Advisory Partner
E Jennifer.Fiddian-Green@ca.gt.com

United States

Johnny Lee
Principal, Forensic Technology Services
E J.lee@us.gt.com

Bryan Moser
Partner, Forensic Advisory Services
E Bryan.Moser@us.gt.com

Linda Miller
Director, Global Public Sector
E Linda.S.Miller@us.gt.com

United Kingdom

Kevin Shergold
Partner
E Kevin.W.Shergold@uk.gt.com

James Helme
Director
E James.Helme@uk.gt.com

James Mackey
Manager
E James.I.Mackey@uk.gt.com

India

Vidya Rajarao
Partner
E Vidya.Rajarao@in.gt.com

Samir Paranjpe
Partner
E Samir.Paranjpe@in.gt.com

Anil Roy
Partner
E Anil.Roy@in.gt.com

Raman Narasimhan
Director
E Raman.Narasimhan@in.gt.com

Nitin Talwar
Director
E Nitin.Talwar@in.gt.com

Hong kong

Barry Tong
Partner
E Barry.Tong@hk.gt.com

Star Chen
Associate Director
E Star.Chen@hk.gt.com

Kenneth Lam
Senior Manager
E Kenneth.Lam@hk.gt.com

Shanghai

Dr. Tim Klatte
Partner, Head of Shanghai Forensic Advisory Services
E Tim.Klatte@cn.gt.com

Local contacts

To learn more about how to protect your business from fraud, please visit **grantthornton.ca** or contact your local Grant Thornton advisor.

Jennifer Fiddian-Green
National Advisory Partner
T +1 416 360 4957
E Jennifer.Fiddian-Green@ca.gt.com

British Columbia

Shane Troyer
Partner
T +1 604 443 2148
E Shane.Troyer@ca.gt.com

Caroline Hillyard
Senior Manager
T +1 604 697 7941
E Caroline.Hillyard@ca.gt.com

Mohammad Pahrbod
Senior Manager
T +1 604 443 2174
E Mohammad.Pahrbod@ca.gt.com

Ontario

David Florio
Partner
T +1 416 369 6415
E David.Florio@ca.gt.com

David Malamed
Partner
T +1 416 360 3382
E David.Malamed@ca.gt.com

Eric Au
Senior Manager
T +1 416 369 7069
E Eric.Au@ca.gt.com

Sandy Boucher
Senior Manager
T +1 416 369 7027
E Sandy.Boucher@ca.gt.com

Mohamed Elghazouly
Senior Manager
T +1 416 607 8762
E Mohamed.Elghazouly@ca.gt.com

Ali Jaffer
Senior Manager
T +1 416 607 2612
E Ali.Jaffer@ca.gt.com

Dwayne King
Senior Manager
T +1 416 607 8717
E Dwayne.King@ca.gt.com

Robert Osbourne
Senior Manager
T +1 416 360 5031
E Robert.Osbourne@ca.gt.com

Jen Pavlov
Senior Manager
T +1 416 369 6421
E Jen.Pavlov@ca.gt.com

Nova Scotia

Leah White
Partner
T +1 902 491 7718
E Leah.White@ca.gt.com

Jeff Merrick
Senior Manager
T +1 902 448 0401
E Jeff.Merrick@ca.gt.com

Newfoundland and Labrador

Adam Lippa
Senior Manager
T +1 709 778 8842
E Adam.Lippa@ca.gt.com

Grant Thornton

An instinct for growth™

grantthornton.ca

Audit | Tax | Advisory

About Grant Thornton in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Together with the Quebec firm Raymond Chabot Grant Thornton LLP, Grant Thornton in Canada has approximately 4,000 people in offices across Canada. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member firms operate in over 130 countries worldwide.