Grant Thornton

An instinct for growth™

Knowledge is power: PROTECT your business through fraud awareness

Every business, regardless of size or industry, is at risk of fraud. In fact, according to the Association of Certified Fraud Examiners (ACFE), the average organization loses five percent of its revenue annually to fraud—amounting to a median loss of USD $130,000 per case.[1] This type of criminal activity not only takes a tremendous toll on a company's bottom line, it can dramatically impact overall culture, reputation and the continuity of the business.

Fortunately, there are things you can do to protect yourself against fraudulent activity—starting with boosting your organization's level of fraud awareness. At Grant Thornton, we work alongside Canadian businesses of all sizes, and across all industries, to help them identify--and mitigate--the fraud risks that are most pertinent to them.

A closer look

Since a fraudster's only limit is his or her imagination, it's impossible to protect your company from every type of fraudulent act or predict accurately how fraud typologies will morph in the future. That said, raising the level of fraud awareness within your organization can help you identify risky behaviour down the road.

Broadly speaking, you need to be aware on both the external and internal fronts, as businesses are vulnerable to fraudsters both outside and from within. Below, we explore a number of common fraud trends and scenarios that can occur both externally and internally.

External

Cyber fraud

While there are countless types of external fraud, at present, the most common is cyber fraud which according to the Canadian Anti-Fraud Centre (CAFC), is considered "any false, deceptive, misleading or fraudulent act that potential victims may come across while using the internet."[2]

Ransomware: Also known as "cyber extortion", ransomware penetrates a company's computer systems and encrypts a company's data. The fraudsters then demand a ransom from the affected company in exchange for access to its computer systems. Sometimes, the criminals will threaten to release the data to the public if the company fails to comply.

Data theft: Beyond stealing actual cash, fraudsters also target your data. This data can include

1. financial information they can use to commit secondary fraud;
2. proprietary data they can sell to a competitor; or
3. personal confidential information (e.g. health records, social insurance numbers of your customers or employees, financial accounts, passwords) which they can sell on the dark web to identity thieves.

Banking malware: This type of fraud occurs when sophisticated cyber criminals target your bank's online banking facilities—essentially hijacking the connection between an online banking user and the bank. After logging into your banking portal, you'll come across a page that looks like your bank's website when, in fact, it's a replica being managed by criminals on the back end—allowing them to steal your passwords and information.

Business email compromise (BEC): Also known as CEO or CFO email scams, this type of fraud usually targets senior employees of a company—and it's growing in prevalence. In fact, the FBI reports that BEC scams cost companies more than $1 billion in losses in 2016.[3] Hiding behind a fake—but very real-looking—email, thieves request an urgent wire payment from the user. More recently, they have even begun claiming that a known supplier has changed its banking information—and then inserting their own account details instead. When the next payment is sent it goes to the thieves rather than supplier.

RED FLAGS:
If you receive an email request including payment instructions ensure the details are verified independently. An email/ instructions is not sufficient authority on its own to support payment, processing and protect you from fraud.

RED FLAGS:
If you receive a request from a vendor to change their payment details and you notice an increase in change orders; or if vendors you don't recognize are submitting invoices, verify the activity with the actual company—either over the phone or face-to-face—as soon as possible. Review your internal controls and payment processes regularly and make sure they rigorously protect your business and allow you to confirm that you receive the value from your vendors that you expect.

There are a number of things you can do to protect your company from cyber fraud:

1. **Install and maintain a robust, commercially-available anti-virus, anti-malware software program.** While it won't cover everything, it should catch at least a reasonable number of threats.
2. **Boost staff and management awareness.** All of your staff should learn how to identify common forms of cyber fraud—such as phishing, link baiting and BEC—and protect the personal information they share on social media.
3. **Password protect everything.** Your servers, VPNs, email accounts, routers—virtually everything connected to the internet—should be protected with a secure password, not the default password which came with the product when purchased.
4. **Patch your software.** Make sure your system is set to install all critical updates as they become available.
5. **Secure your critical data.** Take time to identify which data is critical to your organization—such as financial data, personal information and client information—and secure it. You can't protect everything, but you can protect the higher priority assets.
6. **Back it up.** The best protection against ransomware is a reliable backup program, one that's not easily accessible from your existing systems.

Of course, external fraudsters aren't restricted to the internet. Below are some examples of other types of external threats you need to be wary of:

Business partnership fraud: When setting up a business overseas, many Canadian companies choose to form business partnerships with foreign service providers. Recognizing this, criminals have started impersonating legitimate companies—like collection agents—and using their position to access information and defraud their "clients". Protect yourself by making sure you complete due diligence (i.e. background checks) on both the entity and individual.

Vendor fraud: Without upfront and ongoing diligence, many companies fall victim to vendor fraud—which can include overbilling, billing for incomplete work, price fixing, duplicating invoices or product substitution. In some cases, fraudsters will set themselves up to look like a real vendor—perhaps creating a similar name to a well-known legitimate vendor—and issuing fake invoices used to misdirect funds.

Bid rigging: This type of fraud involves any violation of a vendor bidding process, that your business runs to select and secure vendor relationships. In this type of fraud, two vendors collude to "scam" the bidding process, with one vendor intentionally outbidding the other to allow the lower bid to win. The roles reverse upon the next project.

Personal scams exist too

External fraud against corporations is rising, but companies are not the only targets. Individuals—including business owners and managers—often fall prey to a wide range of fraud schemes, including:

CRA impersonation: Since January 2014, Canadians have paid over $6.2 million[4] to overseas fraudsters posing as CRA representatives in search of outstanding tax dollars or looking to resolve financial immigration matters.

Investment fraud: If an investment opportunity sounds too good to be true, it usually is. This type of fraud typically presents an opportunity to make cash fast but doesn't offer many details and requires you to make your decision quickly. It can include anything from a new Initial Coin Offering (ICO) that's expected to blow Bitcoin out of the water, or a Ponzi scheme which, while promising high returns investment deals, in reality has the fraudster using money from subsequent victims to pay off early victims in an attempt to keep the scheme afloat.

Internal

On the internal front, our awareness also needs to be high. "Occupational fraud," is fraud that is committed from within an organization's walls—either by its managers, directors or employees. According to the ACFE, occupational fraud can be divided into three primary categories: asset misappropriations, corruption and financial statement fraud.

Asset misappropriation:
Asset misappropriation accounts for 89 percent of internal fraud that's been reported,[5] and occurs when individuals responsible for managing valuable business assets choose to steal them. In this instance, "assets" refers to either cash or inventory.

Cash misappropriation typically includes an employee or manager stealing cash-on-hand or cash receipts that never make it to internal documentation, but can also include more schemes. For example, someone could create a ghost employee, add them to the payroll and pocket the new employee's salary. Or, similarly, a manager could add a phantom vendor into the system—and collect tens of thousands of dollars if the company pays the vendor without confirming its existence or having payment processing controls. Inventory misappropriation could include someone in the shipping and receiving department failing to scan an item as it comes in—and opting to steal it instead. In many cases, the company may just assume it was lost in transit.

RED FLAGS:
If an employee or manager never takes a vacation, bullies other employees, appears to be living beyond their means and/or is experiencing a massive lifestyle change, they could be in financial distress and fraud awareness levels should be higher.

Corruption: Corruption is a term which broadly covers many types of fraud. Most commonly, it refers to employees or managers who form personal alliances with external parties and then put those relationships ahead of the best interests of the company. This type of fraud occurs in 38 percent of occupational fraud cases, according to the ACFE, and costs companies a median loss of USD $250,000.[6] It can include conflicts of interest (e.g. purchasing and sales schemes); illegal gratuities; and bribery, such as vendor kickbacks. Bribery occurs when a vendor offers an employee or manager a personal incentive in exchange for a specific benefit. The incentive can be cash-related—such as a percentage of the overall project payment—or it can be offered in the form of a service, or other personal benefit.

A clear, transparent code of conduct should draw the line for your employees. Are sports tickets from a vendor okay? Up to what dollar amount? What if the sports tickets are for an event in a different location and all the travel costs are being covered as well? The answers to these questions will depend on your business, the nature of relationships and what you are willing to allow.

RED FLAGS:
Consider whether an employee or manager appears to have an unusually close relationship with a specific vendor—for instance, they're going on trips that are completely covered by a vendor.

Financial statement fraud: Overstating an organization's net worth/net income typically involves falsifying the records surrounding revenues, liabilities, expenses and asset valuations. While there are numerous motives for this type of fraud, it's often done for personal gain—for instance, to inflate organizational performance to receive a larger bonus, to make the organization look better in the eyes of investors or lenders, or to cover up other types of fraud/risk.

There are a number of things you can do to protect your company from internal fraud:

1. **Implement a whistleblower hotline.** According to the ACFE, 40 percent of frauds are discovered through tips—and, of those tips, 53 percent originate from employees or other individuals inside the company. A properly-managed—and well-communicated—whistleblower hotline is an effective and inexpensive way to encourage fraud reporting within your organization and reduce the amount of time it takes to identify incidences of occupational fraud.

2. **Conduct a fraud risk assessment.** A fraud risk assessment can be a detailed, involved exercise – but it doesn't have to be. A phased approach with a few initial steps can strongly support and increase the level of fraud awareness for yourself and your employees to help protect your future.

3. **Provide your employees with fraud awareness training.** Once employees have a channel to report fraudulent behaviour, it's important to educate them on how to leverage it. Fraud awareness training is about flipping the switch on your workforce so that they can be your eyes and ears as you grow; you can't do it all.

4. **Put in place and communicate a code of conduct. Set a strong tone from the top.** To create a fraud-savvy organization, awareness must be embedded into your organizational culture. This will inevitably require buy-in from the C-suite—and the implementation of a clear, well-communicated code of conduct.

5. **Implement checks and balances.** Taking steps to segregate duties and control access to sensitive information, inventory, cash and other assets either through password protection or another form of sign-in method—will make it more difficult for individuals to commit fraudulent acts under the radar.

Understand existing fraud risk

Both internally and externally, Canadian businesses are vulnerable to fraud. That's why it's important to take steps now to protect your company, your people and your reputation. We know from years of experience that raising the level of fraud awareness within your business can really have a huge impact.

To defend your business from fraudsters, you first need to know your vulnerabilities. A fraud risk assessment can help you understand prevalent market risks, your most at-risk assets, and the current state of your processes and controls. It can also help you to identify glaring gaps and establish a plan to strengthen your anti-fraud controls. This could include anything from implementing a more robust fraud awareness training program to investing in fraud insurance.

Know how to respond—and recover

Should the unthinkable happen, you can't afford to be caught off-guard. Having a response and recovery plan in place can not only shorten the duration of a fraudulent act and save money in the process, but it can help your company get back on its feet faster. Knowing how to preserve the evidence of a fraud can also give investigators a decent opportunity to catch the perpetrator and help you strengthen your defenses to prevent history from repeating itself.

1 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
2 Canadian Anti-Fraud Centre. April 27, 2017. "Fraud Types". Government of Canada. http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/index-eng.htm
3 Better Business Bureau. November 9, 2017. "FBI Says Business Email Compromise Scams Continue to Grow in U.S., Cost Companies More Than $1 Billion". https://www.bbb.org/stlouis/news-events/news-releases/2017/11/cftf-bec/
4 Hermann, Penny. January 23, 2017. "CRA scam continues, but with a new twist". Royal Canadian Mounted Police. http://www.rcmp-grc.gc.ca/en/news/2017/23/cra-scam-continues-a-new-twist
5 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
6 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 10. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
7 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

To learn more about how we can help protect your organization against fraud, contact us:

Jennifer Fiddian-Green
Partner, National Forensics and Dispute Services Leader
T +1 416 360 495 7957
E Jennifer.Fiddian-Green@ca.gt.com

Atlantic Canada:

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

Jeff Merrick
Senior Manager
T +1 902 420 7197
E Jeff.Merrick@ca.gt.com

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

Central Canada

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

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

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

Eric Au
Senior Manager
T + 1 416 369 7069
E Eric.Au@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 4988
E Robert.Osbourne@ca.gt.com

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

Western Canada

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 +1 604 687 2711
E Mohammad.Pahrbod@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.