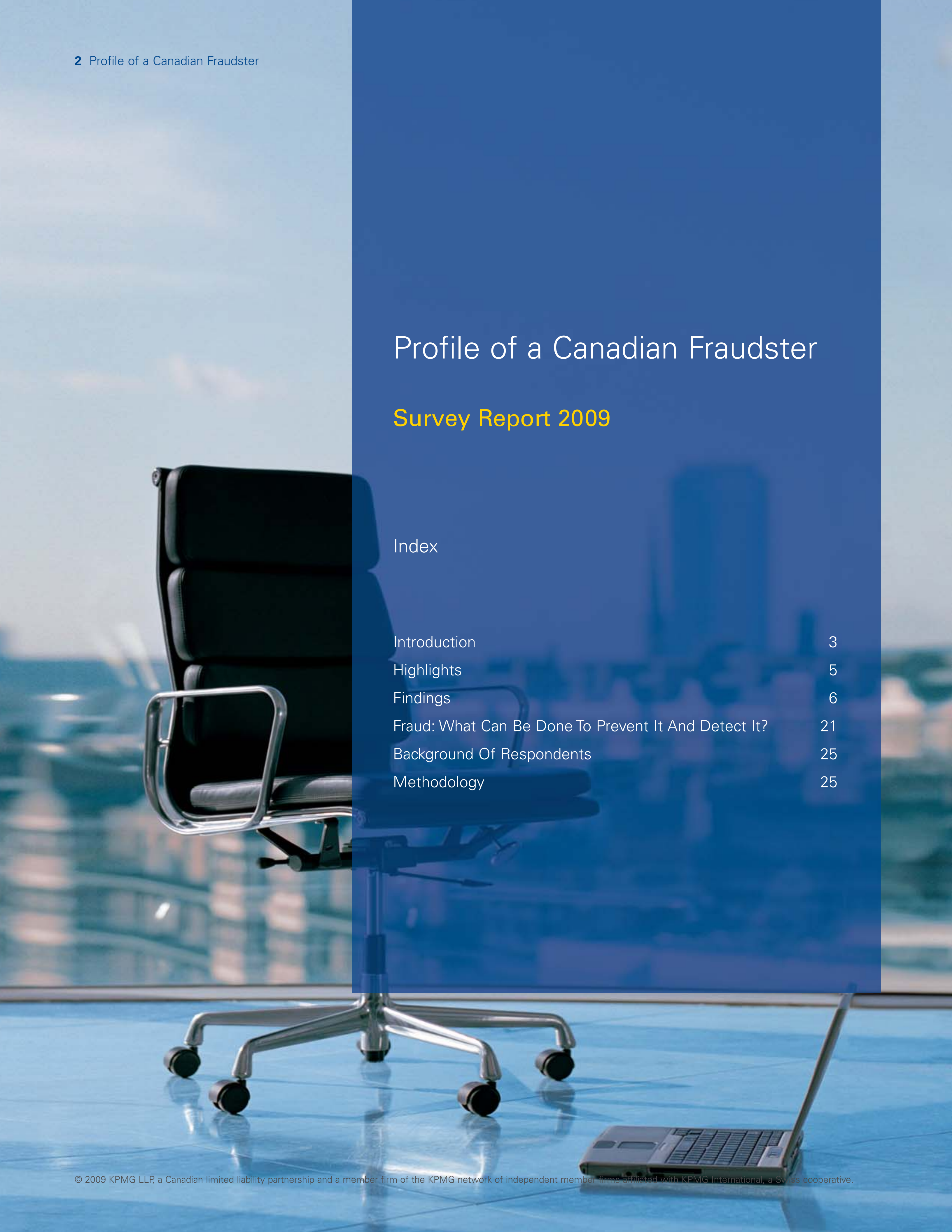
FORENSIC

Profile of a Canadian Fraudster

Survey Report 2009

KPMG LLP

AUDIT ▪ TAX ▪ ADVISORY



Profile of a Canadian Fraudster

Survey Report 2009

Index

Introduction

Fraud and deceit are topics of perennial human interest. If anything, this interest has increased since 2001 after Enron collapsed. Fraud and malfeasance in corporations is a topic that receives significant and growing attention and press coverage. In early 2009 there was a further resurgence of tales of fraud and greed in the press. For example, we have all read about the alleged loss of a reported $50 billion through an investment Ponzi scheme in the United States, an admitted billion dollar fraud in India and any number of other perhaps smaller but still significant frauds. Canada is not immune to fraud and we have seen our own made-in-Canada fraud problems, both large and small.

At KPMG Forensic we know that fraud will not decline in the foreseeable future. With the recession causing significant corporate and personal economic pain, there will be motivation for certain individuals and companies to take improper advantage of opportunities they may find or create. In addition, fraud that may have been ongoing for some period of time may only now be discovered as a direct result of the tightening of credit and the overall cash crunch.

In these unusual economic times, it is therefore reasonable to revisit one of the most basic questions concerning fraud: who commits fraud? For many years, KPMG Forensic carried out a fraud survey in Canada, which in the past has asked executives of Canada's largest companies to comment on the incidence of fraud within their company. In this, our most recent fraud survey, we explore the profile of the people who defraud Canadian companies:

- What are their characteristics and background?

- Why did they commit fraud?

Overall, we wanted to obtain information to support or refute the stereotypical profile of the fraudster.

On the surface, the typical fraudster may appear to be not all that different from an average person, which is confirmed in our survey. However, below the surface, a fraudster is not typical. He (most fraudsters are men) takes advantage of situations for personal and illicit gain. A fraudster identifies and exploits opportunities to carry out a scheme to steal. The factor most difficult to accept, however, is the fact that people who commit fraud are our friends and colleagues. They generally have trust placed in them by their co-workers and employers, and through their fraudulent activities, this trust is severely betrayed.

The un-masking of the fraudster is usually a surprise to co-workers; the façade of normality and the trust reposed in the fraudster are shattered. In most cases, there will be a sense of anger or betrayal. Workers will often reflect that, in hindsight, there were telltale signs of the fraud (or the risk of fraud) while it was occurring, and had they been more aware of the issues that lead people to commit fraud, they might have been able to prevent it or detect it earlier.

This report will assist the reader in obtaining a better understanding of who commits fraud in Canada today. When combined with an enhanced awareness of the risk of fraud, it should also help companies take tangible steps to protect themselves from exposure to fraud and from those who commit it.

Highlights

KPMG surveyed executives of Canada's largest companies on the topic of people who had defrauded their company.

Respondents told us:

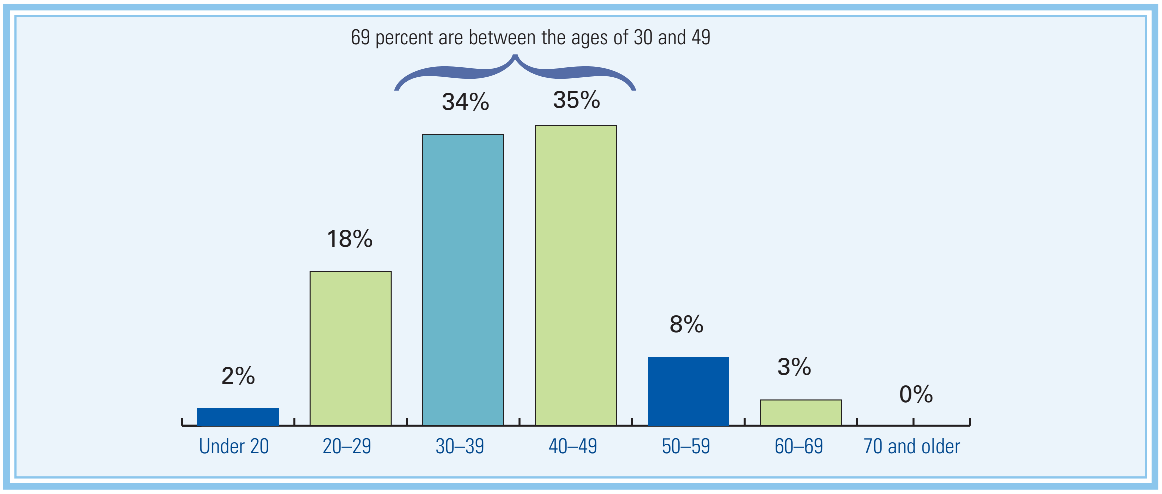
- Almost three-quarters of frauds were carried out by men.
- Most fraudsters (69 percent) were between the ages of 30 and 49.
- In terms of seniority, 62 percent of frauds were carried out by people below the level of management, and 22 percent were carried out by senior management.
- In terms of years of service, it appears that the most common time for a fraud to be carried out is when the fraudster has been with his or her company for between 3 and 5 years (31 percent).
- The education of those committing fraud was spread through all levels: 40 percent had no post-secondary school education, 30 percent had some post-secondary school education, and 26 percent either had a university degree or a professional designation.
- 69 percent of frauds were inside jobs, 20 percent were perpetrated by external fraudsters, and 11 percent involved collusion between insiders and outsiders.
- In the majority of cases, the fraudster acted alone. Respondents reported that 73 percent of frauds were carried out by one person and in only 7 percent of cases were there more than 5 people involved.
- Fraudsters were employed most often in operations (45 percent), accounting (14 percent), and procurement (7 percent) groups within their company.
- The three main factors reported as leading to fraud were personal need (28 percent), opportunity (19 percent), and greed (14 percent).
- "Bad habits," which include alcohol, drug abuse, and gambling, were a factor in 11 percent of cases reported.

Findings

Who Is Committing Fraud in Canada?

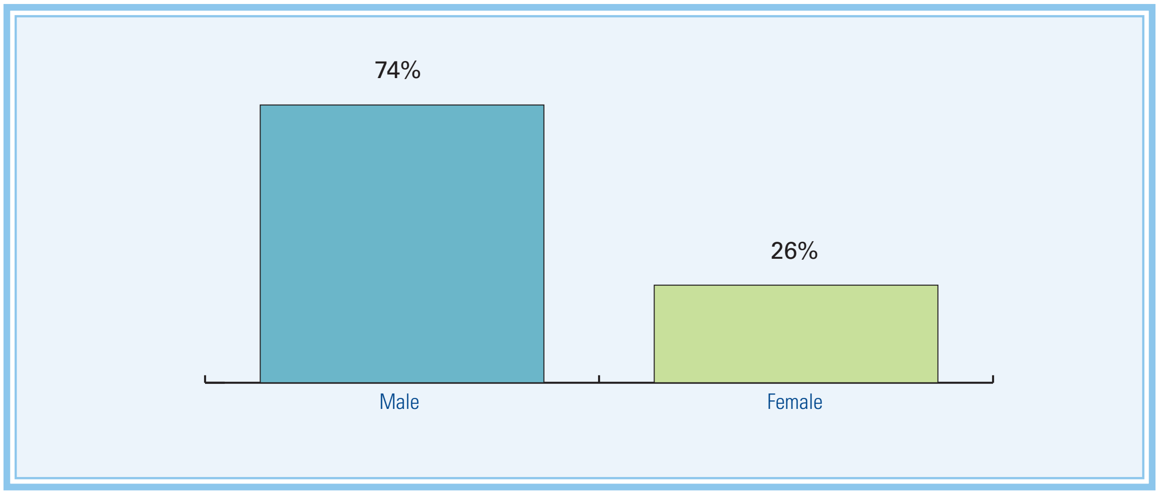
Based on the responses received regarding the attributes of the Canadian fraudster, the typical fraudster is a man, acting alone, who has been with his employer for 3 to 5 years, and who is between the ages of 30 and 49. He has at least some post-secondary school education and is not a member of management; however, certain exceptions to this pattern were reported by the respondents as set out in this survey.

Age of the Main Fraudster



The prime age for fraudsters was reported to be between 30 and 49 years (69 percent). It is in this age range that individuals will have gained a thorough understanding of the company and may be in a better position to recognize opportunities for fraud. Also, this is the general age when an individual will often have the greatest financial concerns or needs, which is a common motivating factor that drives some people to initiate or participate in fraudulent schemes.

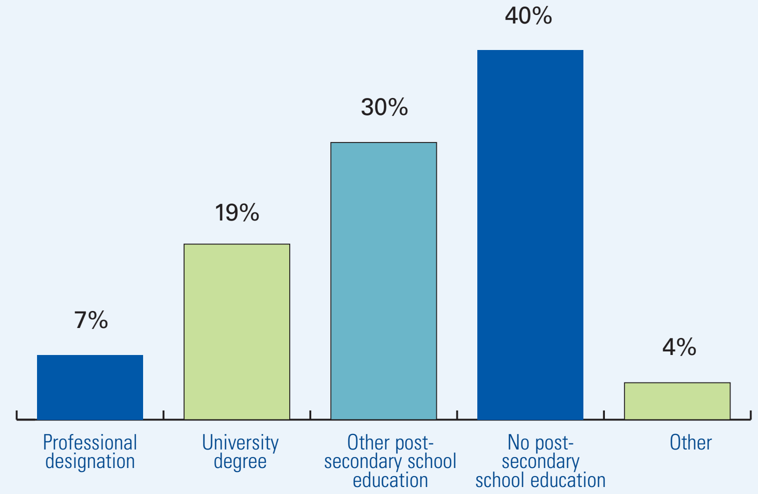
Gender of the Perpetrator



One should not be surprised that it was reported that almost three-quarters of fraudsters were men. Recent and high profile frauds in Canada and around the globe attest to this finding. It is also interesting that KPMG International's *Profile of a Fraudster Survey 2007* conducted in Europe, Middle East, and Africa found that 85 percent of fraud perpetrators were men—this is indeed a global phenomenon.

This statistic does not mean, however, that men are three times as dishonest as women. This result may well be reflective of a continuing reality in Canada that men still hold a higher percentage of the more senior positions within many organizations and therefore may well have greater opportunities to commit fraud. Whether this statistic will become more balanced with the changing demographic composition of senior roles in Canadian organizations will be of future interest.

Education of the Fraudster

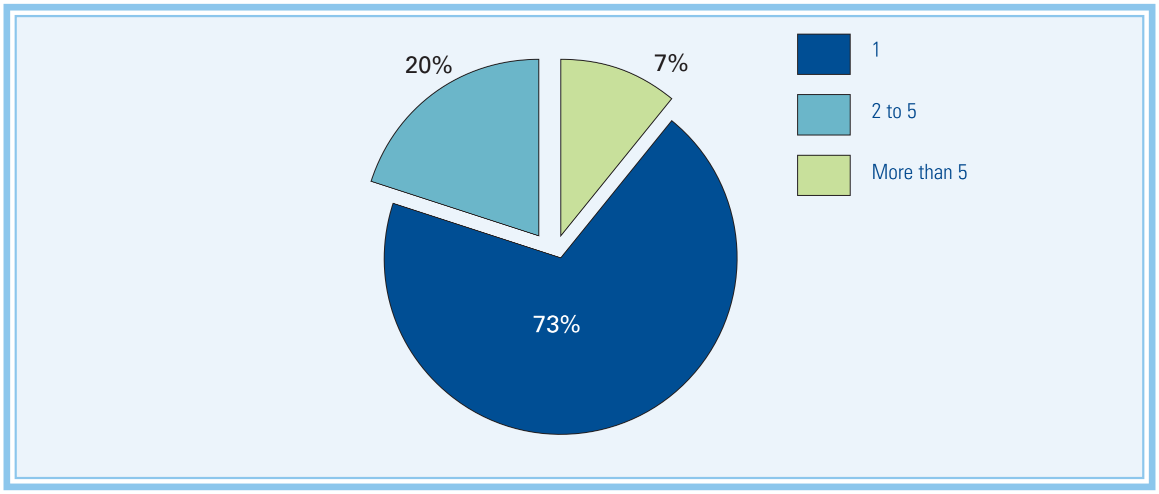


In cases where the education of the fraudster was known, only 26 percent of the reported frauds were committed by individuals holding either a professional designation or a university degree. A further 30 percent of frauds were committed by people with some post-secondary school education and 40 percent of the reported frauds were carried out by someone with no post-secondary school education.

This finding may be a somewhat surprising result if one assumes that persons with a higher education would have more opportunities to commit fraud on the basis that they held more senior positions in an organization. This finding, however, is consistent with other findings related to the seniority of fraudsters, where it was found that only 22 percent of fraudsters internal to the company held management positions.

A further factor potentially influencing this finding is that persons with professional designations (7 percent of fraudsters) may well have more to lose if caught committing fraud, such as higher salaries and loss of professional designations and reputation.

Number of Fraudsters

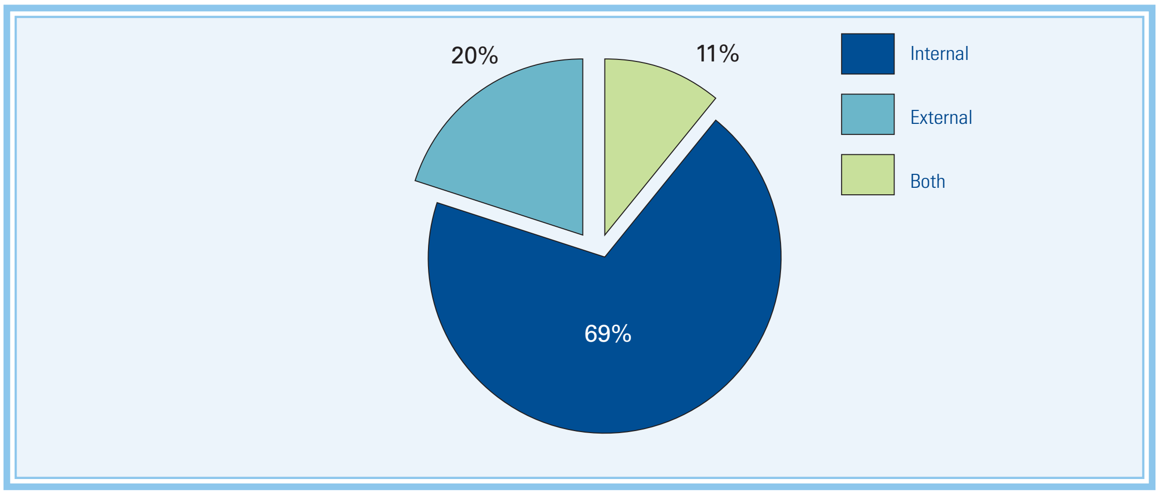


In the majority of cases the fraudster acted independently (73 percent). Individuals committing fraudulent acts do tend to act alone as the involvement of and reliance on others increases the risk of the fraud being exposed.

In a sizeable number of cases (27 percent), however, more than one person was involved in the fraud, which creates an enormous problem for those concerned with preventing fraud. One of the most important overall internal controls to prevent and detect fraud is a segregation of duties, which would result in more than one person being involved in initiating, reviewing, authorizing, and recording a transaction. When people collude to override or circumvent these controls, errors, whether accidental or fraudulent, are more likely to be undetected for longer periods of time.

In addition, some frauds are only possible when a number of people with different responsibilities in a company conspire to commit or facilitate the fraudulent act. For example, the fraudulent misstatement of accounting records and financial statements usually requires the involvement (and likely informed knowledge) of many people to initiate accounting transactions and prepare and approve financial statements.

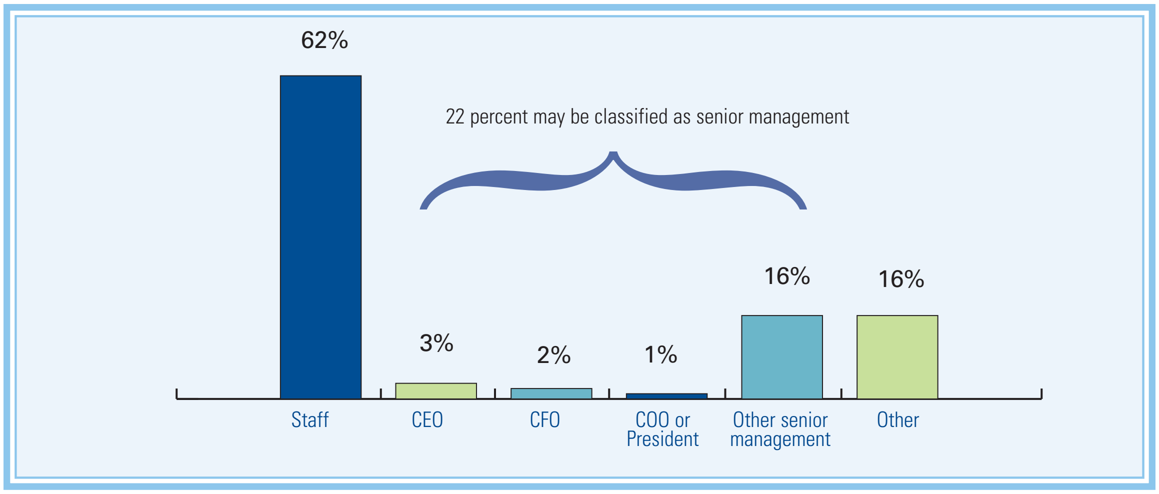
Internal or External Fraudster



Sixty-nine percent of frauds were committed internally and 20 percent were committed by someone outside the company; however, in 11 percent of reported cases, both an insider and an outsider were involved.

Kickbacks (sometimes referred to as secret commissions) are the most common example of a fraud where insiders conspire with external parties. In these situations, it is often the case that individuals in the sales or procurement groups are involved as these functions have influence over customers and suppliers. Similar to other forms of multi-party fraud, kickbacks can be difficult to prevent and detect. In such cases, much of the evidence required to prove the fraud lies beyond the control of the company. The best protection against kickback schemes are strong processes and internal controls over relationships with the external parties.

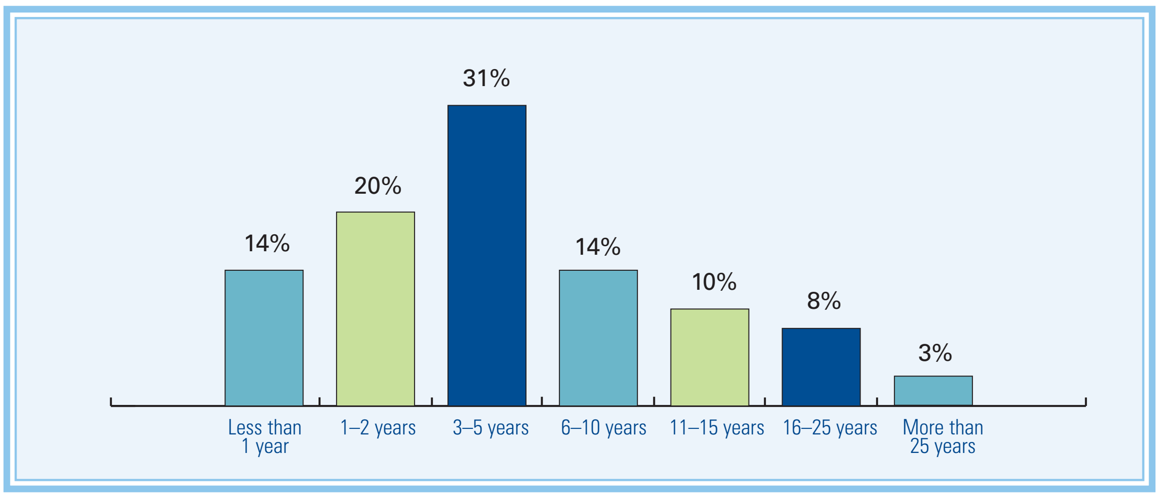
Level of Seniority within the Company



Fraud was most common at the staff level (62 percent), while 22 percent of fraud was committed by senior management. There was less fraud activity by the most senior people, including the CEO (3 percent), CFO (2 percent), and COO and President (1 percent), which is perhaps reassuring given the trust placed in and responsibilities of the most senior executives of a company.

On the other hand, some of the largest and most serious frauds in Canada and elsewhere have occurred as a result of the manipulation of financial statements by a conspiracy of senior people. Inherent in the role of senior executives is the ability to override internal controls, internal knowledge, and access to confidential information, which, while critical to managing the success of a company, creates a risk that fraudulent acts may occur. Such high impact frauds are perpetrated for many reasons, including the concealment of a diversion of assets, obtaining or maintaining financing, or the manipulation of the share prices. Therefore, while the number of serious frauds in Canada may be low, should a company face a large and pervasive fraud involving senior people its impact will be significant and perhaps fatal for an organization.

How Long Was the Fraudster Working at the Defrauded Company?

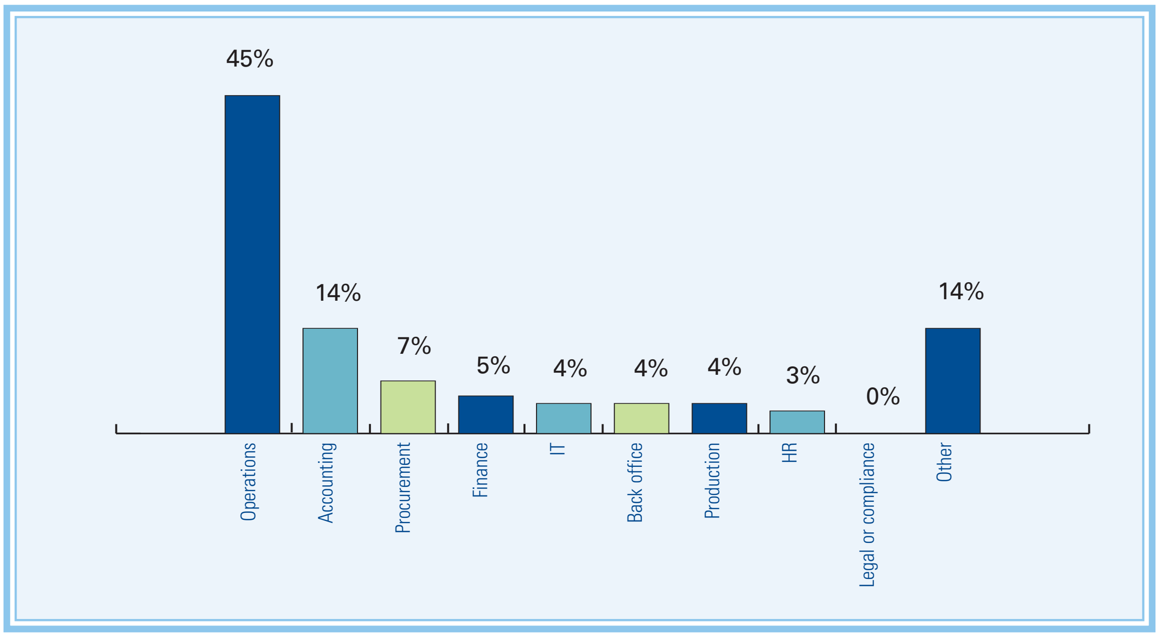


The prime time for frauds to be perpetrated is when employees have been at the company for 3 to 5 years. In fact, 66 percent of all reported internal fraud involved employees who had been with the company for more than 2 years.

The impact of an individual's tenure with a company before a fraud is committed is understandable as it takes time for an individual to understand a company and its systems. This correlation is important as it allows for the recognition of the internal control and process vulnerabilities that may facilitate fraud or allow fraud to be concealed. Also, the trust placed in an employee generally grows over time, making it easier to commit and hide fraud. It may also be the case that frauds develop over time and may not be discovered until the fraudster has been employed for years.

The survey results also indicate that the likelihood of someone committing fraud consistently diminishes after being employed for more than 5 years with a company. Does this suggest that employees with longer service are more honest or ethical? This declining trend in fraudulent activity may relate, in part, to the age of the employee (older employees are less likely to commit fraud) and perhaps achieving more senior positions (through promotions) with the length of employment. However, another very likely explanation relates to the mobility of employees and the resulting fact that there are increasingly fewer employees with lengthy terms of service at any company.

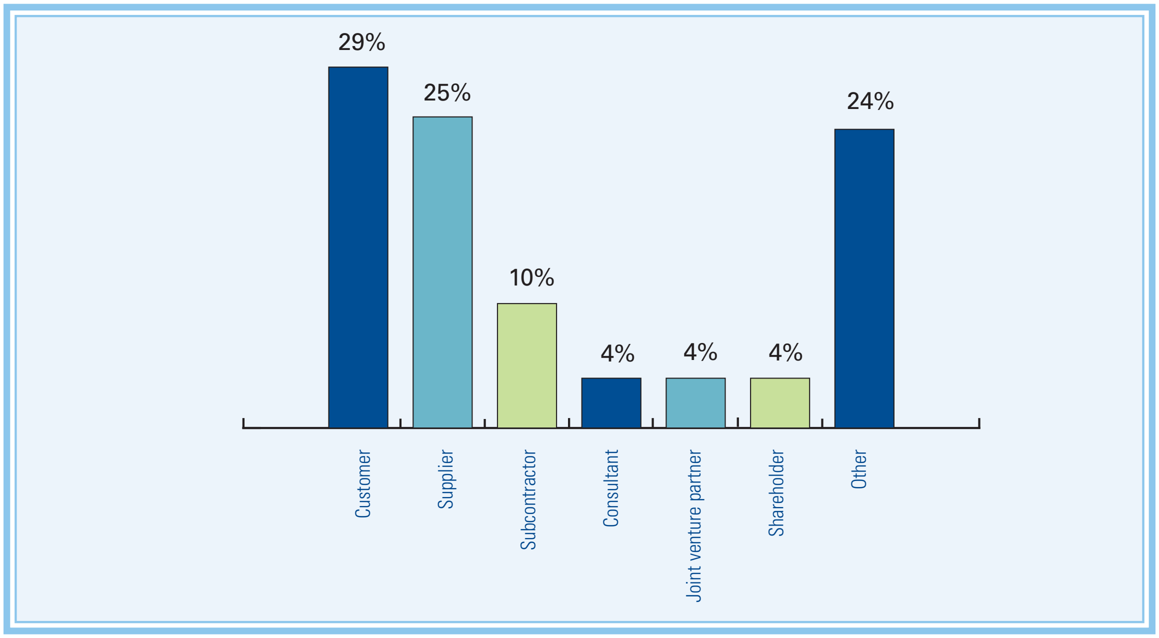
What Department Is the Fraudster Working In?



The majority of respondents (45 percent) indicated that frauds occurred in the operational departments, while only 14 percent of frauds occurred in accounting and 5 percent in finance functions. These results may be surprising to some as many believe that individuals who work in the accounting or finance departments have the greatest opportunity to commit fraud. While this may be true for certain types of fraud, the majority of reported frauds (theft or diversion of cash), especially those frauds that might be smaller (less than $100,000), do not necessarily require the involvement of those who work in the finance and accounting areas.

It is a fact that responsibility for and access to financial information and assets does impact the ability to commit fraud in many cases. Most large frauds require access to accounting records and the ability to authorize or change the recording of transactions if this fraud is to be successful and concealed. Therefore, care must be taken when establishing and monitoring internal controls over financial reporting, financial assets, accounting records, and cheques.

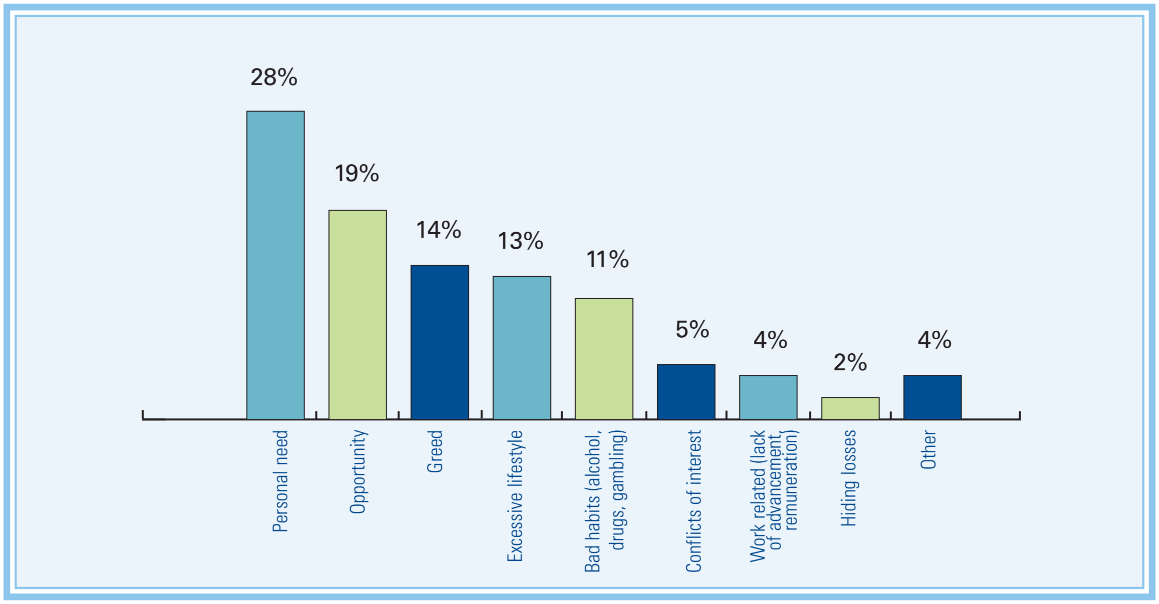
Who Externally Is Defrauding the Company?



Where the identity of the external fraudster was known by the survey respondents, customers (29 percent) and suppliers (25 percent) were the two groups most often involved in the fraud. This result is expected as these groups generally have the most opportunities to defraud corporations. Customers can make false claims on a company while suppliers can submit false invoices for faulty or non-existent goods and services. These two groups are also generally in the best position to offer or receive secret commissions or kickbacks. It is clearly important that corporations are vigilant when dealing with its customers and suppliers, through appropriate monitoring, policies, procedures, and internal controls.

Over one-half of the survey's respondents could not identify who, externally, had defrauded them; this is a surprising result that leads to questions about the quality and extent of investigations following the discovery of a loss. The ability to take appropriate remedial and protective actions following a fraud will be negatively impacted when the identity of the fraudster or even the nature of the perpetrator's connection with the company is not known.

Motivating Factors



What leads a person to commit a crime, betray the trust instilled in him or her, and jeopardize one's job, career, and future? Is this only the result of education, upbringing, and character, or are there other factors that influence this behaviour? Victimized companies should question if their culture and ethics are appropriate or, rather, whether this culture may have contributed to the factors that led to fraud.

It is important to understand that in most cases of fraud there will be more than one motivating factor. An individual will likely have a personal need (perhaps as a result of an excessive lifestyle or bad habits), which, when combined with opportunity and greed, will create a perfect storm for fraud to occur.

Through their collective answers, the respondents confirmed a common theory of fraud that suggests three factors lead to it:

- Need (28 percent) – Fraudsters' needs are the most important single motivating factor. These needs may be financial or work-related and they may be caused by an "excessive" lifestyle (13 percent) or "bad habits" (11 percent).

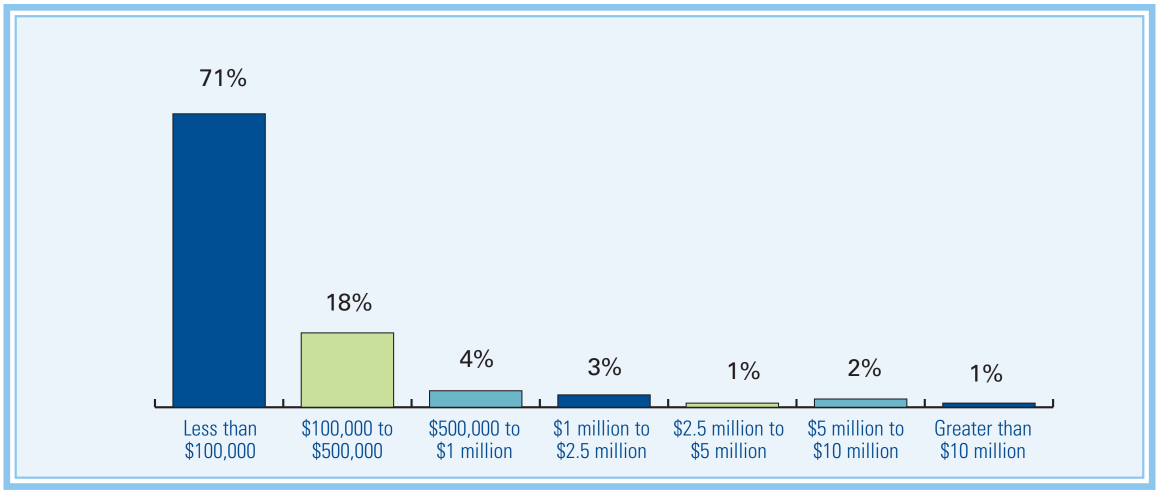
- Opportunity (19 percent) – Without opportunity a person will not have the means to defraud a company, which is why companies rightfully spend much time and money on internal controls and other preventative steps that reduce the risk of fraud.

- A character defect in the fraudster (14 percent) – Greed is one important character trait of many fraudsters. In the end, many people would never consider committing a fraud; however, others seem to be predisposed to seek out opportunities to obtain personal benefit using dishonest means and deception to satisfy their greed.

Fraudsters do not expect to be discovered and very often have rationalized what they do: "Everybody does it," "I am underpaid," "I deserve to be acknowledged," or "I owe it to my family to enhance our lifestyle."

What Were the Frauds?

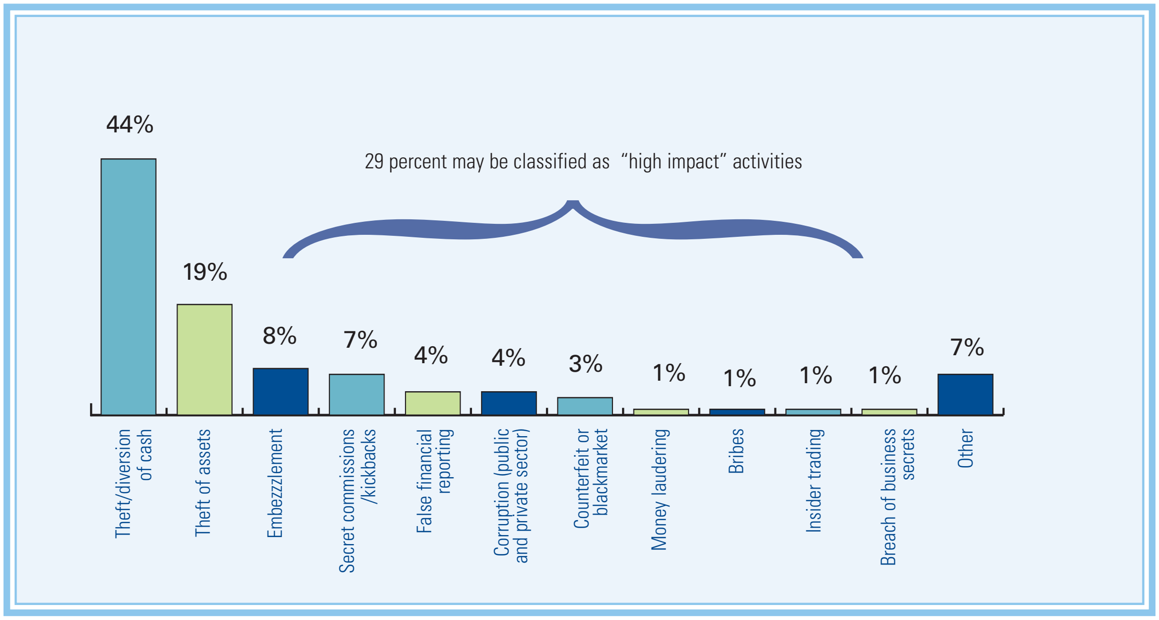
How Much Did the Fraudsters Get Away With?



Most individual frauds in Canada are small; where reported, 71 percent of respondents said losses were less than $100,000. While this may not be a significant amount for the large companies that were surveyed, the impact of the fraud likely exceeds the pure dollar value. For example, there will likely be an investigation, with its associated costs; Human Resources may become involved; and senior management will have to spend time conferring about the issue and determining the appropriate response. An intangible but potentially significant cost is the potential damage to a company's reputation if the fraud becomes public. Another important intangible cost is the effect of the fraud on the morale of the fraudster's co-workers and supervisors. There will be feelings of anger and betrayal and some in a supervisory position may be subject to criticism or disciplinary sanctions.

While less prevalent, larger frauds present companies with increasingly complex issues and risks, and often more senior and trusted employees are involved with the fraud. These situations often require more direction by senior management as the matter is reviewed and investigated. Such situations also commonly become an issue for the company's audit committee, board of directors, and external auditor. In addition, larger frauds will likely require retaining external legal counsel and possibly external investigators. Public exposure is more likely in these cases and may be required if the loss is significant to the organization. This public disclosure will likely attract the interest and scrutiny of regulatory authorities, shareholders, and the media.

What Did the Fraudsters Do?



Sixty-three percent of respondents indicated that the fraud involved a theft or a diversion of cash or other assets.

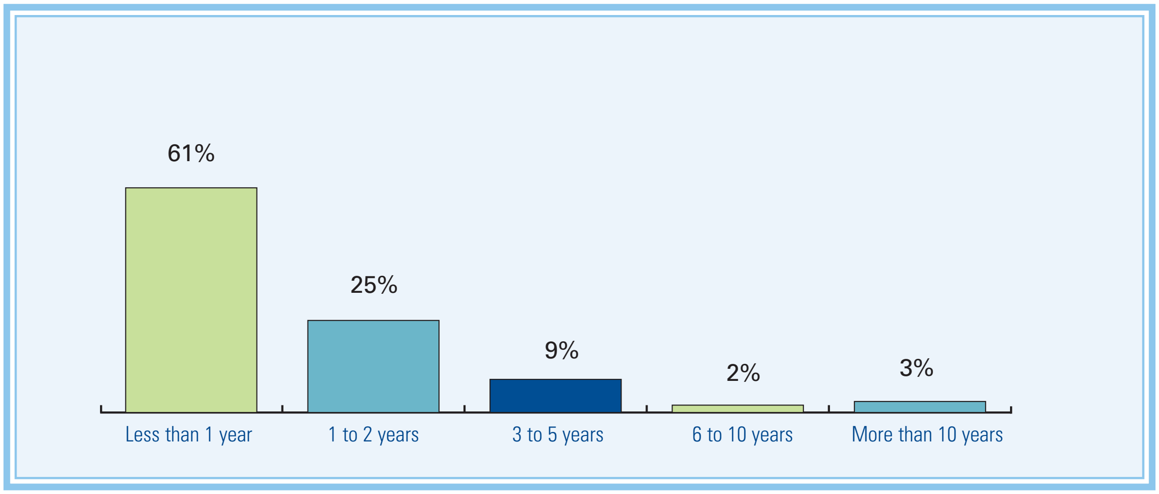
While individually less prevalent, various "high impact" fraudulent activities collectively account for 29 percent of the reported fraud. These high impact frauds can be significant in both size and impact to a company. The range of these illicit activities also readily illustrates the wide variety of frauds that occur with some regularity.

As mentioned elsewhere in this report, false financial reporting (4 percent) is of particular concern. In many cases, this form of fraud requires the active involvement of a number of trusted people with important responsibilities. False financial reporting, when detected, usually creates significant stress on a company and there is often a need to restate past financial statements, which will usually spur an internal investigation under the supervision of the audit committee or a special committee of the board. These situations usually lead to the involvement of external parties, such as legal counsel, auditors, and financial regulators.

Four percent of reported incidents were classified as involving corruption. Corruption differs from other types of fraud in that it involves the compromising of an official, often someone in government, who is offered and accepts a bribe to perform some unauthorized activity as a result of his or her position. In some ways this is a reassuring finding as it suggests that we live in a relatively non-corrupt country. Canada's position as a relatively corruption-free country has been corroborated by Transparency International's *2008 Corruption Perceptions Index*. This Index, which measures the perceived levels of public sector corruption in 180 countries, indicates that Canada is considered as one of the 10 least corrupt countries.

In comparison, KPMG International's *Profile of a Fraudster Survey 2007* conducted in Europe, Middle East, and Africa, found that 23 percent of frauds in that region were related to corruption.

How Long Did the Fraud Continue Before It Was Discovered?



The good news is that most frauds are nipped in the bud early; over 60 percent of respondents indicated that the fraud was discovered within 1 year of its start. Relatively few frauds continued for more than 3 years and only 3 percent of frauds continued for more than 10 years.

Of course, there may be frauds that continue for many years that are never discovered. In our experience, this is generally not common in larger frauds. As the dollar amount of the fraud grows, it becomes increasingly difficult to conceal the fraud's existence and impact. In these cases, the fraudster can spend an increasing amount of time working to cover up the fraud-induced losses, but ultimately the weight of the fraud causes the scheme to collapse. At some point, senior management will note a discrepancy, a whistleblower may speak up, or the fraud will be uncovered by the internal or external auditors.

This general observation, however, has been brought into question by recent events. Some newly exposed multi-billion frauds reportedly had their genesis many years ago and have only now been uncovered as a result of current economic conditions. These cases appear to be unusual and pervasive frauds, and one hopes they are only exceptional and isolated ones.

Fraud: What Can be Done to Prevent It and Detect It?

Canadian companies spend a great deal of time and effort looking at internal controls—the system of checks and balances that are supposed to deter wrongdoing and fraud, among other things, and ensure that any wrongdoing is brought to light as soon as possible.

However, a determined individual or group that decides to defraud a large company will generally be able to find a way to subvert the existing system of controls, which is particularly the case with collusion or a conspiracy. One of the most effective mechanisms of internal control is the segregation of duties where more than one person is involved in making, checking, approving, and recording a transaction or series of transactions. However, if these people—who are entrusted with stewardship or supervision—decide to collude, then the key control of segregation of duties will be ineffective.

What Can be Done?

As a result of the *Sarbanes-Oxley* legislation, which was introduced in 2002 in the United States as a result of large corporate frauds, companies are looking at entity-level controls to help prevent and detect fraud.

Three entity-level controls can collectively have a major impact in the detection and prevention of fraud:

1. An effective whistleblower hotline

2. A robust and properly implemented code of business conduct

3. A consistently applied and thorough system to pre-screen new hires.

Whistleblower Hotlines

A properly organized and internally publicized whistleblower line is one of the best mechanisms to shed light on a financial irregularity at an early stage. A whistleblower line cannot replace effective internal controls, an effective audit department, and other mechanisms designed to avoid and mitigate losses arising from fraud and misconduct, but it can be critical to discouraging and detecting fraud.

It is important to recognize that, regardless of how robust a company's system of internal controls is, a conspiracy among trusted employees will usually defeat internal controls. However, where people in a position of responsibility are working together to promote a scheme of financial irregularity, many other people within the company may know or suspect wrongdoing.

A whistleblower line provides an avenue for a concerned employee to anonymously voice his or her concerns. The protection provided to the whistleblowers through a confidential reporting mechanism is important, as generally such concerned employees are not appropriately protected. Far from being regarded as ethical heroes, they are often regarded as individuals who have betrayed their colleagues and the company. More often than not, those who speak up are sanctioned rather than rewarded, which is why one of the central features of a robust whistle-blowing regime is the assurance given to employees that they can speak up anonymously and confidentially.

The implementation of a whistleblower line is not something that should be done hastily and on short notice; common implementation pitfalls can be avoided with proper planning, guidance, and counsel.

Code of Business Conduct

A well-constructed and robust Code of Business Conduct sets the expected standard of behaviour at a company. The Code of Business Conduct should establish the ethical tone of the company and should be a document that guides the moral framework for business decisions. In the end, it will not be worth the paper it is written on if the most senior executives of a company do not embrace and adhere to the letter and spirit of the Code of Business Conduct. It is the visible and vocal support from the top of an organization that will make a Code of Business Conduct an important document that establishes the high expectations for day-to-day conduct in a company.

Best practice suggests at least an annual form of written acknowledgement that employees subject to a company's Code of Business Conduct have adhered to it throughout the year (or, if not, any infringements are to be disclosed), and that they are not aware of others not adhering to it. If there is no requirement for annual compliance, at best, employees will forget the terms of the Code of Business Conduct or, at worst, if they did not read it when they were first hired, they will have no knowledge of its contents.

A System to Pre-Screen New Hires

A comprehensive system of background checks on new hires is important to help reduce the potential losses arising from fraud and misconduct. Potential new hires who have a history of fraudulent conduct are at a very high risk to repeat this type of behaviour at a new employer, should the opportunity arise. Unfortunately, such individuals commonly have no compunction about falsifying résumés or otherwise providing incomplete information during an interview.

Organizations should develop policies and procedures regarding the level of background checks required for individuals coming in at different levels of responsibility. For example, at a minimum, checks of the following should be carried out with the knowledge and consent of the applicant:

- Credit checks
- Bankruptcy history
- Criminal records checks
- Verification of education and professional designations
- Reference checks
- Media checks.

By being diligent in assessing the qualifications, characteristics, and qualities of those being invited to join a company, there is a greater opportunity of keeping potential fraudsters from gaining positions of trust and, ultimately, defrauding a company.

Other Fraud Prevention and Detection Actions

In addition to the above, there are other important steps that can be taken to prevent and detect fraud in a company:

- Comprehensive fraud and misconduct risk assessment – A fraud risk assessment helps management to understand a company's business risks, identify gaps or weaknesses in internal controls, and develop a plan for any required remedial actions. Internal controls—the prime system to avoid errors and mistakes (whether intentional or accidental)—are complex and a risk assessment can provide a balanced review of the controls central to preventing fraud and misconduct.

- Third party due diligence – As with a process of pre-screening new hires, due diligence on third parties is a prudent course of action both from a business and fraud risk perspective. Knowing who your company is doing business with has never been more important.

- Fraud and misconduct awareness training – Providing fraud awareness training to employees is an important step to help ensure they are aware of the nature of fraud in corporations, the risks that the company faces, and fraud prevention approaches. This awareness is important if employees are to be of assistance in deterring and detecting fraud.

- Appropriate communications – Recognition of an organization's ethical tone and the importance placed on appropriate business practices is best communicated from the top down. Such communications will help ensure that employees understand they have a role to play and an obligation to ensure that the company is protected from fraud and misconduct.

- Auditing and monitoring plans – Active auditing and monitoring can build upon the company's fraud and misconduct risk assessment. Auditing and monitoring plans can give the higher risk issues priority and facilitate the detention of fraud and misconduct.

- Proactive data analysis tools – Data analytic tools consist of computer-based cross matching and non-obvious relationship identification. Such tools can help to identify potential fraud and misconduct that otherwise might remain unnoticed by management, possibly for years.

Background of Respondents

We received a total of 72 responses from across Canada with two-thirds of respondents coming from BC, Alberta and Ontario. Over one-half of the respondents were CFOs (54 percent) and one-fifth coming from Vice Presidents. Our respondents covered a wide-range of industry sectors including: Energy and Natural Resources, Financial Services, Consumer Markets and Industrial Markets. One-quarter of respondents had revenues of over $1 billion, with another quarter having less than $100 million in revenues.

Methodology

From our extensive experience of carrying out these types of surveys we know that respondents are concerned about the confidentiality of their information. Corporate victims of fraud are understandably displeased that they have been victimized in this way and therefore are usually reticent to talk about their experiences. A high response to such surveys is not generally achieved.

KPMG Forensic mailed out hard-copy surveys and e-mailed links to an online survey to companies listed on the combined *Financial Post 800*, *Report on Business* Public 1,000, and Report on Business Private 350 lists. Responses were received between February and August 2008.

We received a total of 72 responses; respondents were asked to answer a set of questions for up to three different cases of fraud they had experienced. Based on the 72 responses received, 142 individual cases of fraud were reported, an average of about two reported frauds for each respondent.

This report provides some benchmarking information that helps us better understand the profile of fraudsters in Canada.

Partners and Associate Partners of KPMG Forensic in Canada

Calgary

Suzanne Schulz
eMail: saschulz@kpmg.ca
Tel: 403 691 8077

John Williams
eMail: johnlwilliams@kpmg.ca
Tel: 403 691 8180

Halifax

Mary Jane Andrews
eMail: mjandrews@kpmg.ca
Tel: 902 492 6050

Montréal

Stéphan Drolet
eMail: sdrolet@kpmg.ca
Tel: 514 840 2202

Robert Castonguay
eMail: rcastonguay@kpmg.ca
Tel: 514 840 2422

Ottawa

Victor Duret
eMail: vduret@kpmg.ca
Tel: 613 212 2881

Jocelyne Lafreniere
eMail: jlafreniere@kpmg.ca
Tel: 613 212 2861

S.W. Ontario

Paul Ross
eMail: pross1@kpmg.ca
Tel: 519 747 8255

Toronto

James Hunter
eMail: jameshunter@kpmg.ca
Tel: 416 777 3193

James McAuley
eMail: jmcauley@kpmg.ca
Tel: 416 777 3607

Derek Rostant
eMail: drostant@kpmg.ca
Tel: 416 777 3685

Vancouver

Peter Armstrong
eMail: perarmstrong@kpmg.ca
Tel: 604 691 3589

kpmg.ca