Association of Corporate Counsel

Presented by: Lisa Majeau Gordon, CPA, CA•IFA, CFE, CFF, CICA
Partner, Investigative and Forensic Services

Date: April 25, 2019

Who Are We?

- Chartered Professional Accountants (CPAs)
- Specialists in Investigative and Forensic Accounting (CA•IFA)
- Chartered Business Valuators (CBV)
- Licensed Insolvency Trustee's and Canadian Insolvency and Restructuring Professionals
- Accredited Senior Appraisers (ASA), American Society of Appraisers
- Accredited Appraiser of the Canadian Institute (AACI) Senior Designation of the Appraisal Institute of Canada or Professional Appraiser (P. App)
- Former Police Officers – Commercial Crime, Proceeds of Crime, Stock Market Enforcement backgrounds
- Certified Fraud Examiners and Certified Forensic Investigators
- Computer Forensic Specialists and Cyber Security Experts
- Industry experts: Oilfield Services, Mining, Forestry, Agriculture, etc.

What Rules Govern Our Work?

- Rules of Professional Conduct of CPA Canada/Alberta
- Canadian Business Corporations Act (Court-Appointed Inspectorship)
- Alberta Rules of Court, 2010
- Court of Queen's Bench of Alberta, Civil Practice Note 5 (formerly Note 10) (Format of Expert Evidence of Economic Loss or Damages)
- Court of Queen's Bench of Alberta, Civil Practice Note 4 (formerly Note14) (Guidelines for use of technology in civil litigation matters)
- Investigator licensing guidelines in Alberta
- CPA Canada Standards for Investigative and Forensic Engagements

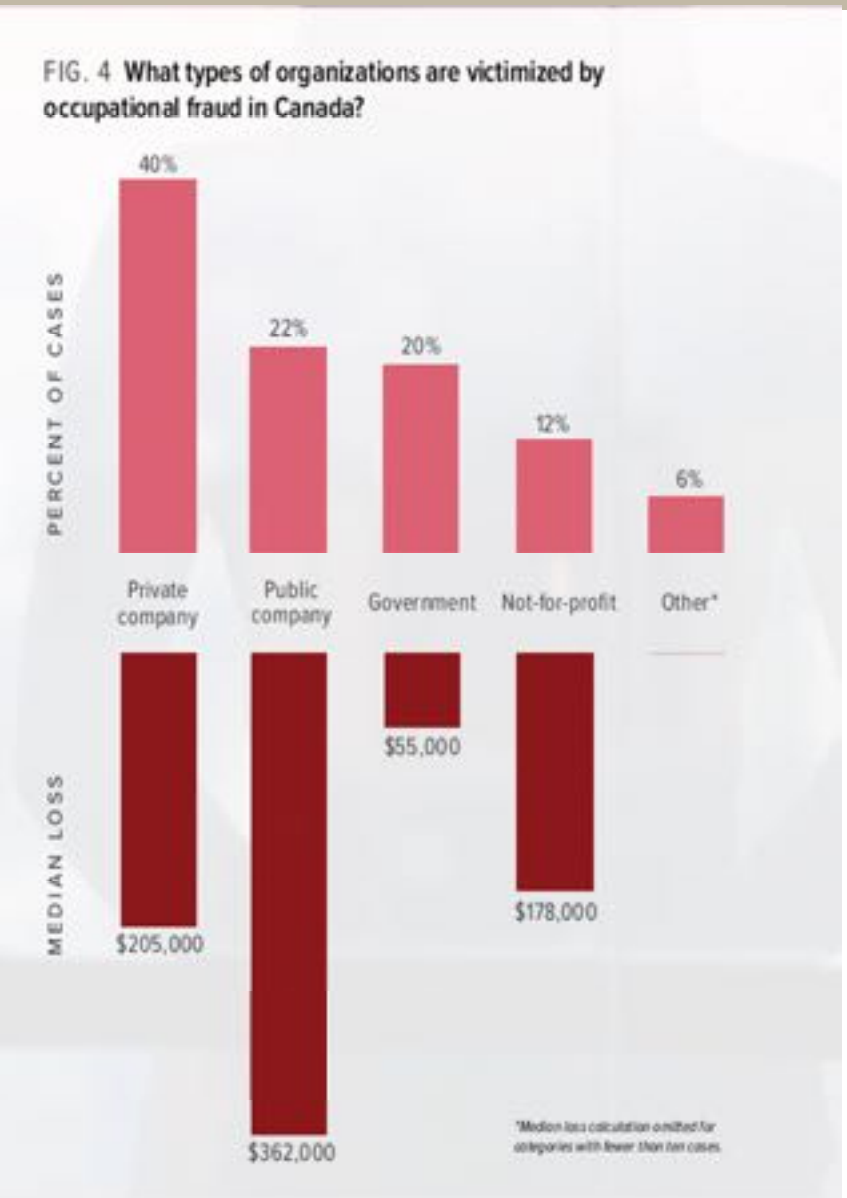
Fraud is alive and well in Canada …

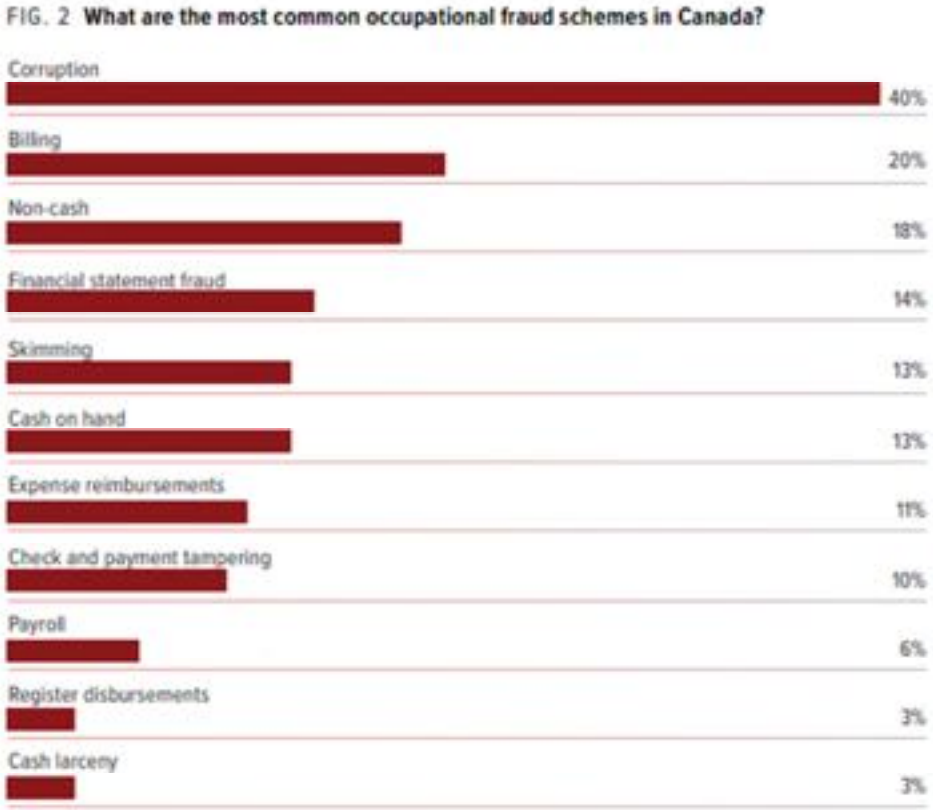
- 33% of Canadian organizations surveyed reported being victims of economic crime in 2018
- Canada's private sector has experienced the highest fraud levels in six years. Median losses are >$250,000 CDN
- Fraud trends anticipated for 2018 include an upswing in employee fraud, breach of contracts, corruption, and conflict of interest
- **The smaller the organization, the bigger the risk**

Think fraud is just a cost of doing business?

Just remember that, assuming a 10% planned surplus, an additional $1 Million in revenues is required to make up every $100,000 fraud loss!

ACFE Report to Nations 2018: Canada Edition





What is Fraud?

Any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair

Including:

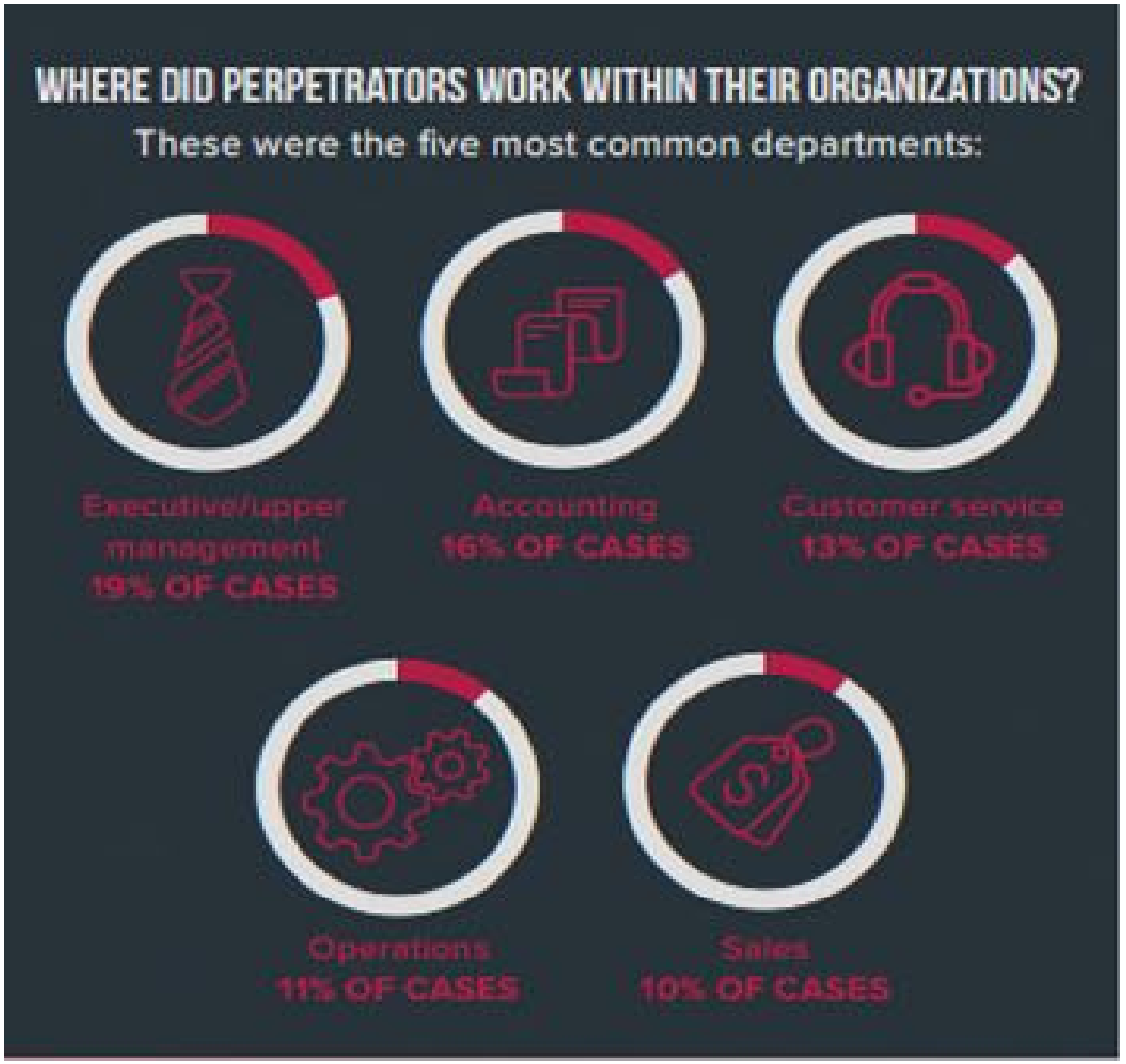
- ✓ Theft by lying or cheating
- ✓ Using acts of forgery and false documents
- ✓ Engaging in deceptive behaviour; and
- ✓ Manipulating information

FRAUD IS PERPETRATED BY A PERSON IN A POSITION OF TRUST

ACFE Report to Nations 2018: Canada Edition

Median age for all fraudsters in the region was

45



Behavioural Red Flags

- Addictions are a factor in a significant percentage of employee investigations undertaken in the past five years
- Gambling in particular is a powerful addiction that has led to many large frauds/financial crimes

How Frauds are Committed

Financial Reporting

- Understatement or withholding expenses
- Overstatement of results
- Related party transactions
- Shareholder loan accounts

Misappropriation

- Payroll fraud
- Procurement and payment fraud
- Employee expenses
- Theft of assets

Other Misconduct/Corruption

- Bid rigging
- Conflict of interest
- Acceptance of bribes
- Intellectual property

Employee Fraud

- Office employees defraud “field” employees
- Payroll fraud
- Fraudulent vendors
- Diversion of revenues
- Theft or misappropriation of assets
- Fraudulent bonuses
- Accounting malfeasance
- Too much trust on employees without monitor or review
- Suspicious activity or “red flags” often overlooked or ignored
- **Same people responsible for payroll, accounting, banking, and financial reporting**
- Conflict of interest

Joint Venture and Contracts

- Joint ventures are often not subject to rigorous operational contracts
- Service contracts are ignored in act execution and billing of work
- Contract terms and conditions are n monitored, and delivery of service is not secured before payment is mad
- Inappropriate allocation of revenues expenses, and assets in joint ventur operations
- Little to no due diligence regarding new business partners

Intellectual Property

- Theft of intellectual property rapidly increasing
- Often perpetrated by outside hackers, but increasingly in this market by internal disgruntled employees
- R&D, scientific data, client lists, personal information, databanks: downloaded, emailed, printed, hacked, removed
- Most organizations do not monitor internet, social media, or email usage of their employees
- Often stolen for use in a new company or for a new employer – or simply to hurt the company

Remote Locations

- Decreasing controls with distance from central office or senior management
- “Wild West” mentality
- Lack of management review and infrequent audit
- Lack of segregation of duty
- “Off the Radar”

Fraudulent Investment Vehicles

- Primarily real estate or resort or commercial development projects
- Offering Memorandums appear comprehensive - but language of OMs allow for manipulation of use of funds
- Funds invested are used for a completely different reason th expected
- Financial reporting fraudulentl overstates Capital and results

Helping Organizations

- Minor Sports Clubs, charities, churches, medical professionals, healthcare organizations, and NPOs are commonly victimized
- Volunteers and employees are main perpetrators
- Unwillingness to investigate, reluctance to take action
- More than money at stake.
- Organizations with a “culture of care” are uniquely vulnerable to fraud

What is Fraud Risk Management?

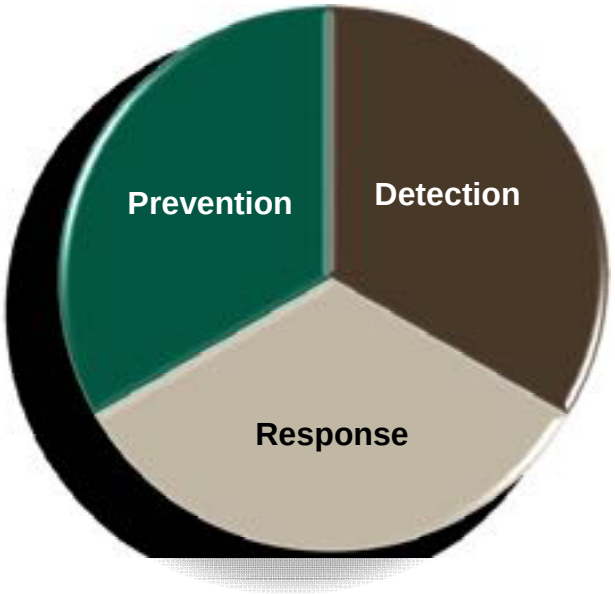
Effective anti-fraud programs provide an organization with tools to manage risk in a manner consistent with its stewardship requirements as well as its business needs. Such an approach has four phases:

- **Assess Risks** to the Organization
- **Design** an Anti-Fraud Program to Mitigate R
- **Implement** the Program
- **Evaluate** and Update the Program Periodic

Fraud Risk Management

Anti-Fraud Programs and Controls are focused on:

- **Prevention**: controls designed to reduce the risk of fraud and misconduct from occurring in the first place
- **Detection**: controls designed to discover fraud and misconduct when it occurs
- **Response**: controls designed to take corrective action and remedy the harm caused by fraud or misconduct



Fraud Risk Management

Prevention	• Fraud and misconduct risk assessment • Code of conduct and “tone at the top” • Human Resource practices • Fraud Awareness training • Process-specific fraud risk controls • Delegated Authority limits	Governance oversight CEO and Executive review Internal audit, external audit, and monitoring activities
Detection	• Testing of controls and documented policy • Auditing and monitoring • Proactive forensic data analysis • Ethics lines and reporting mechanisms	
Response	• Critical incident response protocols • Governance reporting • Disclosure protocols • Remediation of control weaknesses	

Prevention Questions

Executives should ask the following questions regarding preventative controls:

- Have we performed a fraud risk assessment?
- Are our HR policies and Code of Conduct defined and documented?
- Have we defined and documented transaction-level controls?
- How do we delegate financial authorities?
- Do we have an appropriate tone from the top?
- Do we have fraud awareness training for staff?
- Who has responsibility for the anti-fraud program, and how often will they provide reporting to the Board?

Detection Questions

Executives should ask the following questions regarding detective controls:

- How do we know our controls are working?
- How often do we test and report on our anti-fraud controls?
- Do we have a mechanism to receive complaints anonymously? Do we track complaints we receive?
- Do we take into account feedback from auditors in our anti-fraud progra[illegible]?
- Have we trained our employees

Fraud Response Questions

- Does the Company have insurance that will cover a financial loss or costs of an investigation?
- Who should conduct the investigation?
- What impact will our decisions have on internal controls, company policies and procedures, and morale?
- Is the alleged misconduct culpable or non-culpable? (legal consideration)
- Will we require an external media communication strategy?
- What should we say to employees?
- Do we have a critical incident response plan?

Fraud Response Considerations

A structured critical incident or fraud response plan provides those people within your organization who may receive reports of alleged fraud and misconduct with guidance on how to respond.

It addresses such matters as:

- Containment, control, and chain or custody of records/data
- Responsibility and protocol for investigations
- Need to consult with internal and external legal counsel
- When to involve outside parties
- Consideration of avenues of recovery
- Remediation of control weaknesses
- Reporting to the Board and Executive

Employee(s) Under Suspicion

- How serious is the alleged incident or crime?
- How credible is the initial detection method?
  - Tips, internal/external call, flags in IT system, attempts to access records, accounting or banking irregularities, etc.
- Is the employee in a position to harm the organization?
  - Access to accounting data, bank accounts, server files, IT, physical records, email, etc.
- Should the employee be suspended with p
  Otherwise removed from current job dutie
- Where is the evidence? Is it contained an
- Are there potential witnesses?

Common Weaknesses

Weaknesses We See in Anti-Fraud Programs:

- Ineffective Code of Conduct
- Deficient design and poor communication of Ethics Line or other reporting mechanism
- Contradictory or vague policies and procedures
- Lack of fraud risk assessment/identification
- Lack of fraud reporting and response plan
- Management override of controls is not addre
- Senior Management not held accountable for prevention in contracts, evaluations, and compensation

Top 10 Fraud Prevention Measures

10. Control Access to What Makes You Money

- Do you have a patent? Lucrative customer list? Uniquely modified equipment? Special techniques?
- Intellectual property fraud is relatively easy to commit and tough to litigate. Protect your knowledge assets with access limitations and user alerts

Top 10 Fraud Prevention Measures

9. Regular financial reporting package

- A regular financial reporting package should be prepared and provided to the Executive/Board for review (monthly or quarterly)
- Packages should include standard reports (such as budget variance reporting) and financial statements
- The package should be designed by Executive or Board – “top down”

Top 10 Fraud Prevention Measures

8. User access controls

- Unique user names and passwords should be created for all individuals with access to the organization's systems. Passwords should never be shared
- Passwords need to be changed on a regular schedule
- Limit access to payroll and cheque production
- Online banking or accounting software access needs to have unique access identifiers for each user

Top 10 Fraud Prevention Measures

7. Control Access to Funds

- Limit access to credit cards, p-cards, and bank accounts. Develop and follow policies on employee expenses submitted for reimbursement. Monitor overtime claims
- Reimbursement should not be processed without a review of receipts or supporting documentation
- Establish a relationship with your banker that does not involve your employees

Top 10 Fraud Prevention Measures

6. Implement a Fraud and Ethics policy

- A policy should be developed and implemented regarding the expectations for employees and volunteers, including consequences of violation
- Increasing the perceived likelihood of detection and consequences is an effective deterrence method

Top 10 Fraud Prevention Measures

5. Conduct background checks

- Background checks should be conducted on all employees. All references provided should be contacted and a check for known criminal activity performed. Academic achievements should be verified

Top 10 Fraud Prevention Measures

4. Reconcile bank statements monthly

- Bank statements should be sent directly to the person responsible for reconciling them. All reconciling items should be listed and investigated. Bank reconciliations should be reviewed by another individual once completed
- Reconciliation should not be performed by anyone with direct access to banking activity

Top 10 Fraud Prevention Measures

3. Documented procedures

- Day-to-day procedures for:
  - cash handling and banking
  - accepting donations
  - creating cheques
  - accounting entries
  - reconciliation
  - Processing payroll
- Must be documented and tested for compliance from time to time

Top 10 Fraud Prevention Measures

2. Dual signing authorities

- Implement two signing authorities for all cheques/electronic payments if you can. Reconcile all payments with a vendor invoice or other paper supporting document. Do not sign cheques without appropriate support
- Do not, under any circumstances, sign blank cheques.
- Cheque creators cannot be cheque signers

Top 10 Fraud Prevention Measures

1. Segregation of duties

- Ensure no single individual is responsible for handling cash, issuing cheques, and reconciling the bank statement
- Wherever possible, segregate banking activities from accounting/financial reporting activities. When it is not possible, add a layer of peer or management review

Protect Yourselves Externally Too

- Insurance over fraud losses and the co investigations
- “Right to Audit” clauses in agreements a contracts
- Universal Shareholder Agreements (US
- Joint Venture Contracts
- Qualified and Experienced Accountants Lawyers, Bankers, and Insurers

Botched Investigations

- Mishandling of computers and technological devices, rendering data inadmissible to a Court
- Accusations without sufficient proof, and making threats
- Unreliable evidence collection
- Conclusions drawn without consideration of sufficiency of evidence or alternate theories
- Biased investigators
- Ignorance of fraud investigation and forensic accounting standards

You Suspect a Fraud – Now What?

"I don't appreciate you questioning my integrity. Especially since I've skipped town and can't be there to defend it."

Thank you!

Lisa Majeau Gordon, CPA, CA•IFA CFE, CICA, CFF
Partner, Investigative and Forensics Services
MNP LLP
☎ 780.453.5375
✉ Lisa.MajeauGordon@mnp.ca
www.MNPForensics.ca and www.MNP.ca

Questions