



Battling Payment Fraud: The Never Ending Story

Presented by:
Peter Tristani, Vice President,
Payments and Remittance

Agenda

- Overview
- Fraud: The Big Picture
- Evolving Fraud
- Impact of Fraud on Corporations
- Impact of Economic Downturn on Fraud
- Corporate Actions to Prevent & Combat Fraud
- Framework for Fraud Management
- Payment Fraud Statistics & Strategies
 - *Cheques*
 - *Cards and Commercial Cards*
 - *Electronic payments*
- Fraud Prevention Practices & Tools
- Closing Remarks



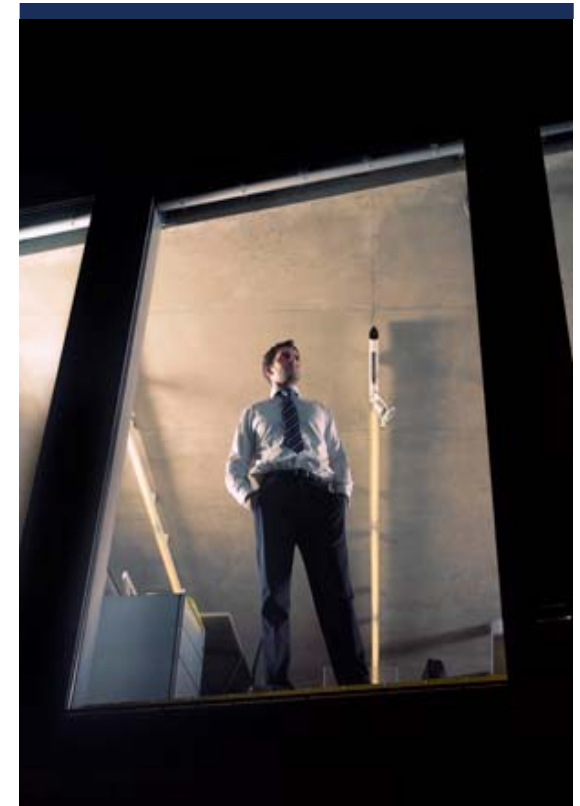
Overview of the Presentation

Today we will cover the following:

- How the economic downturn may impact fraud, and in particular, fraud threats within your organization
- How and why fraud threats are changing – the shifting landscape of fraud
- What you can do to protect your organization
- What you can learn from financial institutions as key partners in fighting fraud

Fraud: The Big Picture

- Fraud is the intentional deception or misrepresentation made for unlawful or unfair personal gain or to damage another individual.
- Fraud is ubiquitous, almost all organizations have been victims at one time or another, even if they don't formally admit it.
- Fraud is increasing every year, and declining economic environments create unique risk management challenges for businesses. Criminal organizations that profit from fraud view the current economic conditions as an opportunity, not a threat.
- Thieves are sophisticated and evolve with technology quickly. They are very entrepreneurial and stick with old cons and incorporate new ones as needed.
- Organizations do not get much sympathy from boards, senior management, investors, law enforcement and other stakeholders, who expect companies to take the offensive against fraud, corruption and abuse.



Fraud: The Big Picture

The good news:

By tightening your own internal controls, improving information security and adopting fraud control services offered by financial institutions and other partners, you can avoid or at least contain fraud losses, while also contributing to the “greater good” – driving down the ability of criminals to profit from fraud and protecting consumer confidence in the payments industry.



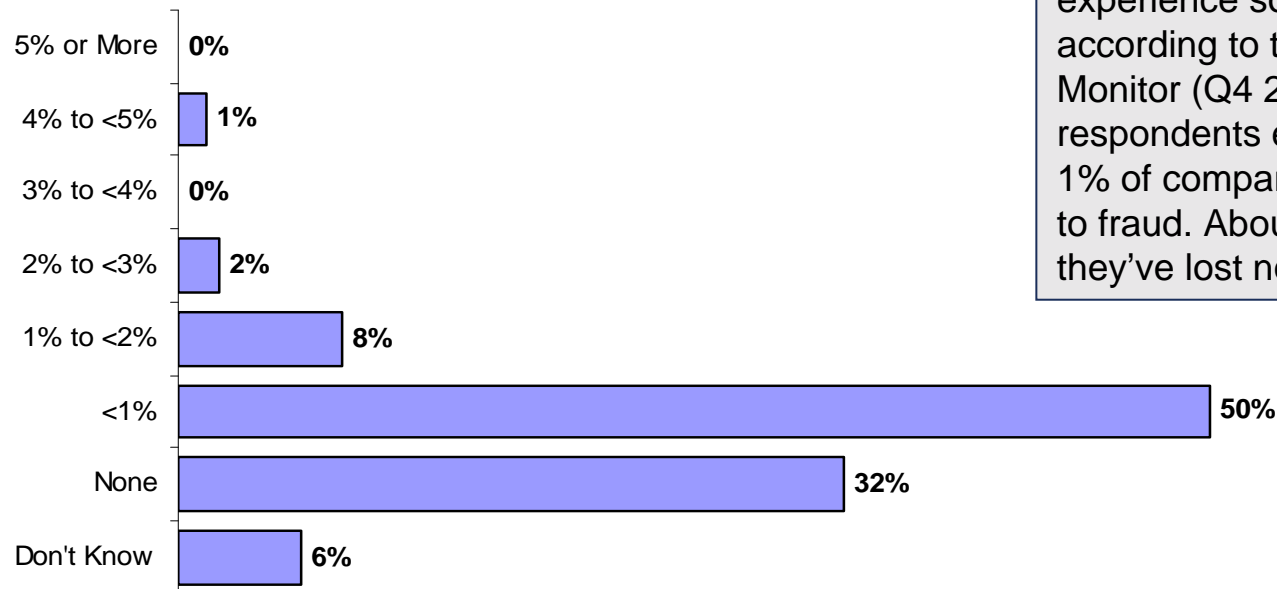
Evolving Fraud

Fraud threats are growing and evolving, and affect all kinds of companies, as seen in these examples

- Corporate Account Takeovers
 - Criminals are targeting cash management customers
 - Use clever social-engineering techniques in their phishing e-mails to get consumers to sign up
 - Transfers funds, for example in the US, using ACH fund transfer facilities
 - Strong customer authentication, fraud detection and transaction verification can significantly, if not dramatically, reduce the threat and damage caused by these crimes
- Phishing Using Stolen Corporate Logo
 - A letter on vendor letterhead asking that their account number for EFT credit deposits be amended to a new number.
 - The corporate client updated their A/P system, began sending EFT payments to the new account (5 payments in a 9 day period).
 - Vendor tells corporate client that they had not received payment, and upon investigation it was determined the letter received to amend the account was false.
 - The other FI was contacted and froze the funds in the account. \$4M had been withdrawn of the total \$720M that had been transferred at the time the account was frozen.

Impact of Fraud on Corporations

Percentage of Company Revenues Lost to Fraud 1



Over two-thirds of companies experience some fraud losses, according to the CICA / RBC Business Monitor (Q4 2008). One-half of respondents estimate that less than 1% of company revenues are lost due to fraud. About one-third believe they've lost no revenue due to fraud.

Research indicates few organizations really understand what fraud is actually costing their business. Some commentators put the estimate of losses from fraud at 7% of revenue². Others consider 7% high as an impact of fraud on businesses in general but recognize that some companies will experience significant frauds that will result in losses at this level, particularly in high risk frontier and emerging markets³. They see continuing opportunity for significant fraud losses as many organizations continue to underestimate avoidable fraud losses and fail to develop adequate controls.

¹ CICA/RBC Business Monitor (Q4 2008)

² Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse

³ PricewaterhouseCooper, Fraud in a downturn, 2009

Impact of Economic Downturn on Fraud

Employee Misconduct

The Corporate Executive Board¹ has seen startling trends internal fraud, including:

- A 20% increase in observations of misconduct from the first to the second half of 2008;
- A 5% decline in frontline employee perceptions of senior management's commitment to integrity;
- An increase in the number of disengaged employees, from one in ten to one in five, causing declines in companywide productivity of up to 5%.

When employees perceive a weak ethical culture, misconduct significantly rises.

¹ Corporate Executive Board/Business Week, How to deal with Employee Fraud and Misconduct, 12 June 2009

Impact of Economic Downturn on Fraud - Internal

Criminal organizations thrive during economic downturn:

- it becomes easier to infiltrate organizations and recruit insiders to help with fraud schemes as employees are more vulnerable due to family hardships.
- they can exploit greater weaknesses as companies are cutting oversight positions and reducing spending or resources devoted to internal controls

According to a 2009 PWC report, “Fraud in a Downturn”, they see increased opportunity for rogue traders to operate undetected as control environments weaken.

- There are also significant influences that will provide pressure or incentives for some staff to trade beyond the limit of their authority. In tough economic times, it becomes easier for people to rationalize fraud and corruption increases. Employees become cynical about the ethical culture of the typical corporation.

Rogue traders are not a threat faced only by investment bankers

- Many organizations use hedging strategies in their treasury function of trade commodities.
- The losses reported by Societe Generale in 2008 were an early warning of the impact of a declining economy on the heightened risk of fraud and irregularity.

Additionally, PWC believe that as companies whose revenues are dropping sail ever closer to breaching their banking covenants, the temptation to ‘massage the numbers’ will increase.

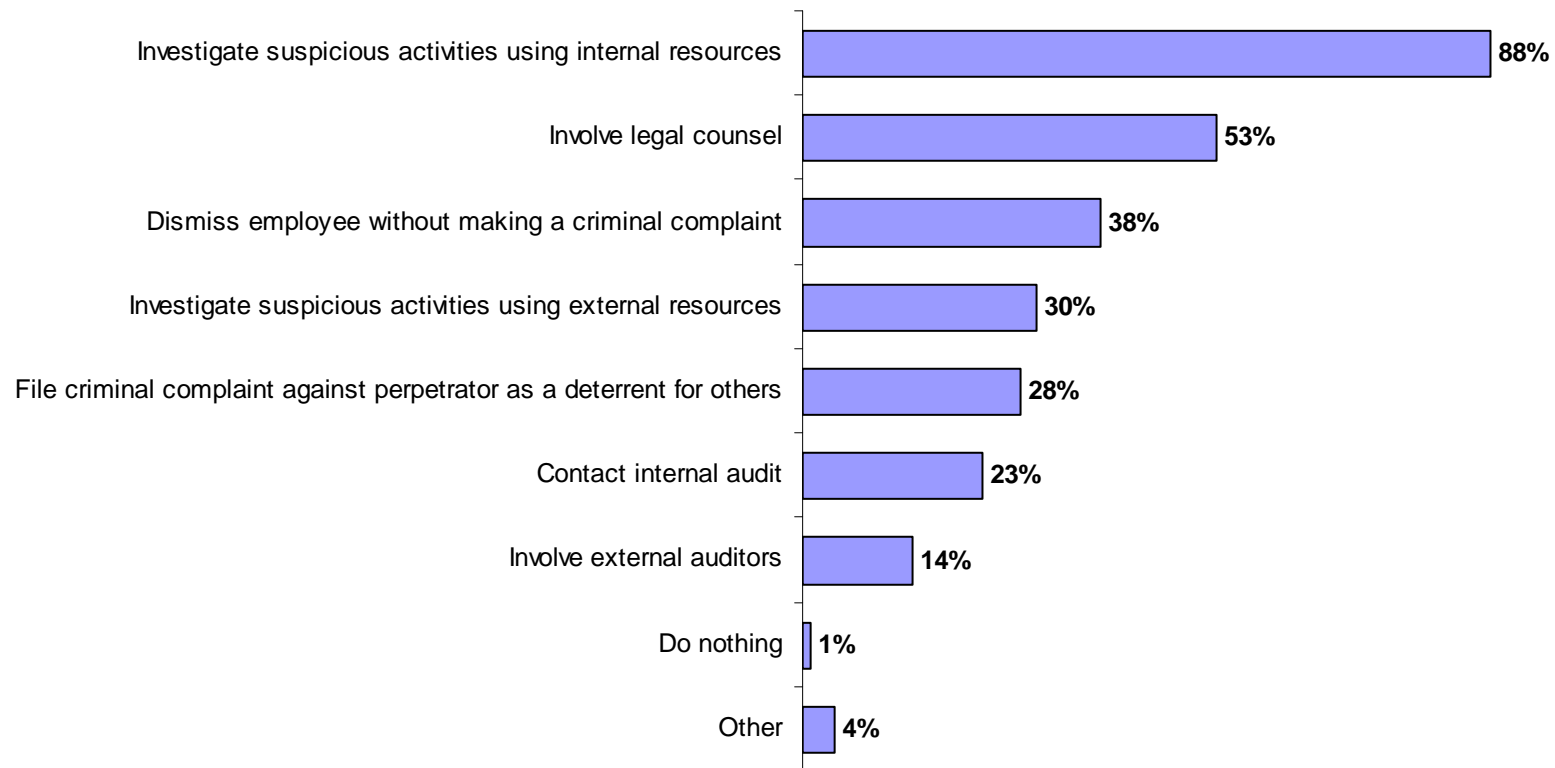


Corporate Actions Taken to Prevent Fraud⁴



⁴ CICA/RBC Business Monitor (Q4 2008)

Corporate Actions Taken to Combat Fraud⁵



⁵ CICA/RBC Business Monitor (Q4 2008)

Corporate Actions Taken to Prevent and Combat Fraud

Mitigating Fraud Risk via a Culture of Integrity

The key to corporate integrity and reduced misconduct is "organizational justice"

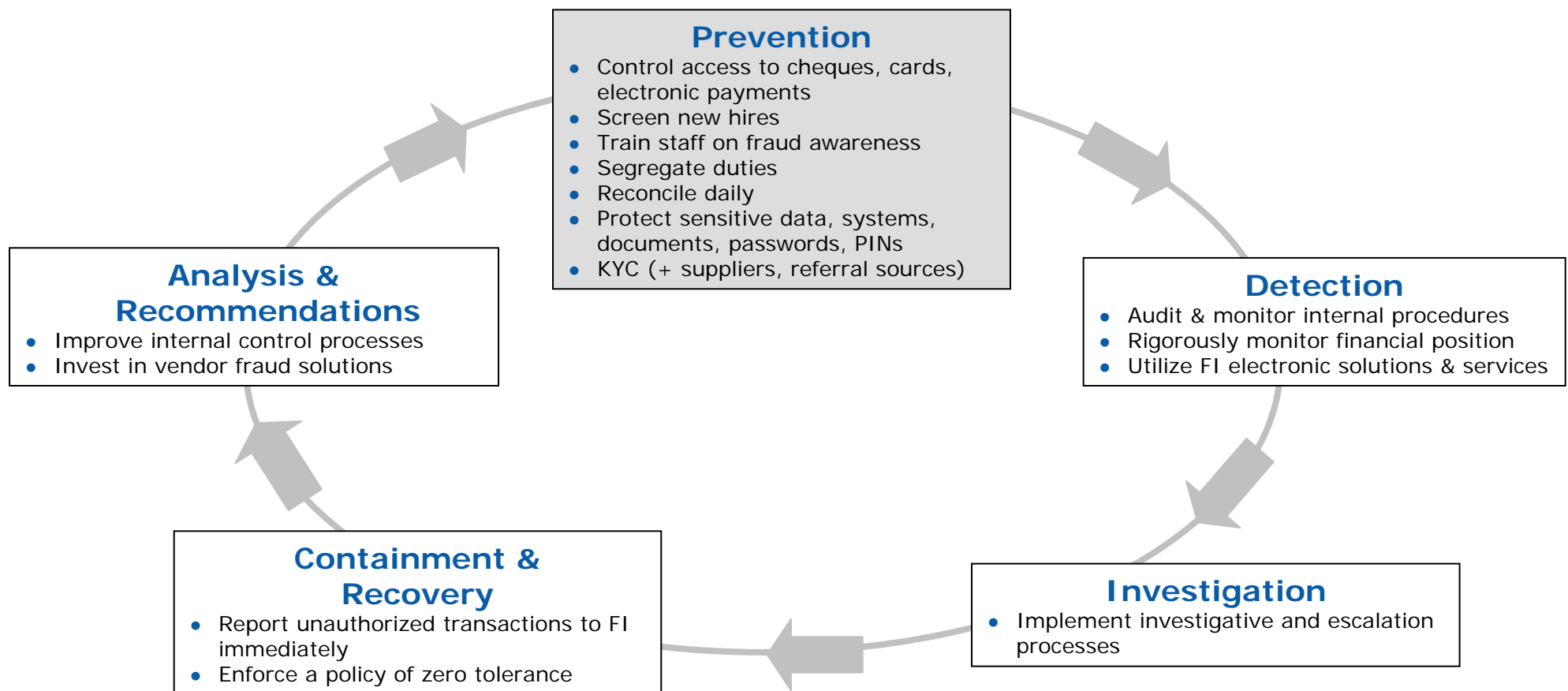
- When employees believe their company has strong organizational justice, the company's overall commitment to integrity rises and misconduct drops.

To create a culture of organizational justice, companies should start by following these three simple guidelines:

1. Equip managers to deal decisively and consistently with instances of misconduct or unethical behaviour;
2. Show the whole employee population how the company deals with misconduct; and
3. Close the loop with employees who report misconduct, so they know that appropriate actions were taken.

Framework for Fraud Management

There are five key components to the fraud management framework – **prevention, detection, investigation, containment & recovery, and analysis & recommendations**. This successful approach can be implemented in organizations of any size to effectively mitigate the risk of fraud. Some example activities are listed below and can be refined based on your own corporate needs.



Payment Fraud Statistics & Strategies

The results of the 2009 AFP Payments Fraud and Control Survey* indicate that payment fraud is rampant and growing, as a majority of organizations experienced attempted fraud or actual payment fraud in 2008.

Key findings include:

- 71% of organizations experienced attempted or actual payments fraud in 2008.
- 30% of organizations reported that incidents of fraud increased in 2008 over previous year
- Cheques continue to be the preferred target of thieves – 91% of organizations were victims of attempted or actual cheque fraud in 2008
- Other targeted payment types for fraud included:
 - ACH (AFT) debits (28%) or credits (7%)
 - Consumer credit / debit cards (18%)
 - Corporate / commercial cards (14%)
 - Wire transfers (6%)

Payment Fraud Statistics & Strategies – Cheques

While cheques are losing ground to credit & debit cards and electronic payments, they remain a leading payment vehicle across North America.

- Approximately 5 million cheques and money orders are cashed on a daily basis in Canada.
- In 2008, the amount of money being exchanged in Canada in the form of cheques represented close to 1 trillion dollars.

Forged signatures and endorsements, counterfeit cheques, kiting, physically altered amounts and / or payees are a few of the methods criminals exploit when attempting to pocket your business' money.

According to the 2009 AFP Payment Fraud and Control Survey*:

- Cheques continue to be the preferred target of fraudsters. E.g:
 - Counterfeit cheques using the organization's MICR line data (72%)
 - Altered payee names on cheques issued by organizations (59%)
 - Altered employee pay cheques (27%)
- 47% of organizations that were victims of at least one attempt of cheque fraud in 2008 suffered a financial loss resulting from cheque fraud

*2009 Association for Financial Professionals Payments Fraud and Control Survey

Payment Fraud Statistics & Strategies – Cheques

How to Protect Against Cheque Fraud:

- 1) **Internal controls** are crucial and are one of your best lines of defence against cheque fraud. Best practices include:
 - Reconcile your accounts daily
 - Separate the accounts payable and receivable roles
 - Periodically change cheque stock, destroy your old, unused cheques, and always lock up blank cheques. Ensure all cheques issued from a single account look and feel the same.
 - Minimize the number of manual or rush cheques and closely examining those that are issued
 - When using a laser printer to print cheques, ensure access is password-protected and that cheque paper has toner anchorage features
 - Place stop payments on cheques not cashed in a timely manner
 - Monitor payment activity carefully and conduct surprise and scheduled audits
- 2) Leverage **cheque security features**
- 3) Reduce the use of risk-prone cheques in favour of electronic payments
- 4) Take advantage of **corporate card payment services** to replace many cheque payments
- 5) Utilize **fraud control / security services** offered by your financial institution (e.g. Positive Pay, Enhanced Positive Pay)

With strong internal controls, electronic and card payment solutions, and fraud services, your company can reduce the risk of cheque fraud

Payment Fraud Statistics & Strategies – Card Fraud

While card payments are subject to greater controls than cheques, they can be vulnerable to particular types of attacks. Some common types include:

- Lost and stolen card fraud
- Non-receipt fraud – Cards intercepted in mail before customer ever receives card
- Counterfeit cards (skimming) – Magnetic stripe data on cards can be copied at tampered POS device or ABM and transferred onto a counterfeit card
- Card-not-present (CNP) fraud – Stolen or compromised card data used to commit fraud online or by phone
- Data breaches (i.e., “account data compromises”)

Rollout of Chip Technology in Canada

Enhanced security is coming for card users in Canada, as Chip cards and terminals will be rolled out over the next several years. Chip-based credit cards will require the use of a PIN as well.

- Security is improved as data on Chip is extremely difficult to copy or change
- Counterfeiting (skimming) of credit and debit cards should be reduced, but will take some time.
- Customer confidence should improve, along with less need to report / dispute unauthorized transactions or obtain replacement cards

Payment Fraud Statistics & Strategies – Card Fraud

How to Protect Against Card Fraud:

- Use Chip cards as soon as they are available
- Ensure your card users always check their statements regularly, verify that all transactions are legitimate and report any unauthorized transactions to your financial institution as quickly as possible
- Always memorize and protect your PIN; don't allow corporate card users to share cards / PINs
- Treat the card like cash - - keep it in secure place
- For internet purchases, ensure your users are registered for Verified by Visa and MasterCard SecureCode
- Determine access rules for who can be issued a corporate card and enforce control procedures when adding or changing employees
- Take advantage of corporate card control features, such as the ability to set merchant types where corporate cards can be used, reduce spending limits, disallow out-of-the country transactions, etc.



Payment Fraud Statistics & Strategies – Electronic Fraud

Criminals attack Internet users in a variety of ways, including:

Phishing

- Emails that pretend to be from your bank or other financial institution, urging you to click on a link that takes you to a fake website that appears to be identical to that of your bank or FI. You are then asked to verify your personal security and account information. If acted upon, the criminal may now have the required information (e.g., account number and password) to commit fraud on your account.

Trojans

- Types of computer viruses which can be installed on your computer without your knowledge. They are capable of logging your keystrokes thereby capturing your passwords and other personal or account information that allow the criminal to then complete fraud on your accounts.

Data Breaches (Account Data Compromises)

- In 2008 there were a reported 285 million compromised data records including payment transactions information.
- Although the revenue impact and operating expense impact were mainly suffered by card issuers and financial institutions, the impact to corporate clients is inconvenience - fraud on accounts, cards being preventatively blocked and reissued.

Payment Fraud Statistics & Strategies – Electronic Fraud

How to Protect Against Electronic Fraud:

1. Just as you protect your business with locks on doors and burglar alarms, it is vital that you take steps to ensure that your **computers are protected against the latest threats**.
 - Use anti-virus software and keep it up-to-date on a regular basis
 - Use a firewall
 - Download the latest security updates (or patches) for your web browser and operating system
 - Engage experts to stress test systems
2. Improve your **customer authentication** processes for both online and telephone transactions.
 - Combination of user ID and password
 - Multifactor Authentication (MFA)
 - New processes which leverage Chip technology are now being explored in Canada, after being used with success in Europe and other parts of the world.
3. If applicable to your business, **PCI Compliance Standards** should be followed:
 - Build and maintain a secure network
 - Protect cardholder data
 - Maintain a Vulnerability Management Program
 - Implement strong access control measures
 - Regularly monitor and test networks
 - Maintain an Information Security Policy

Fraud Prevention Practices & Tools

Strategic Framework

- Develop board and audit committee oversight
- Establish code of conduct
- Endorse board approved reporting structure
- Rigorously monitor financial position
- Align audit with regulatory mandates
- Consider implementing Committee of Sponsoring Organizations (COSO) framework
- Consider insuring employees with access to electronic payments

People and Processes

- Attract and hire professional staff
- Perform employee background checks
- Conduct fraud awareness training and ensure consequences are understood
- Segregate duties
- Make vacations mandatory
- Limit authority to initiate / originate movement of funds
- Report unauthorized transactions to your FI immediately
- Establish account and transaction controls

Physical and Virtual Environment

- Secure your floor, department, office, files and data
- Maintain tight controls over cheque stock and cheque printing processes
- Use cheques with a variety of security features
- Implement stringent controls around electronic payment initiation: password, session and user management, payment authentication
- Establish and automate transaction approval thresholds
- Utilize systems with built in controls
- Maximize automation and straight-through processing
- Segregate and back up sensitive data

Secure Your Corporate Identities

- Reconcile daily if possible
- Monitor wire and EFT activity
- Structure accounts to facilitate early fraud detection
- Protect documents containing corporate identity – statements, cheques, reports
- Protect PINs and passwords
- Keep financial documents secure at all times and shred when disposing
- Understand rights and privileges that you provide to your partners and vendors
- Designate a compliance officer
- Pay companies to monitor your websites

Fraud Prevention Practices & Tools

Strategic Framework

Develop board and audit committee oversight

Establish code of conduct

Endorse board approved reporting structure

Rigorously monitor financial position

Align audit with regulatory mandates

Consider implementing Committee of Sponsoring Organizations (COSO) framework

Consider insuring employees with access to electronic payments

Fraud Prevention Practices & Tools

People and Processes

Attract and hire professional staff

Perform employee background checks

Conduct fraud awareness training and ensure consequences are understood

Segregate duties

Make vacations mandatory

Limit authority to initiate / originate movement of funds

Report unauthorized transactions to your FI immediately

Establish account and transaction controls

Fraud Prevention Practices & Tools

Physical and Virtual Environment

Secure your floor, department, office, files and data

Maintain tight controls over cheque stock and cheque printing processes

Use cheques with a variety of security features

Implement stringent controls around electronic payment initiation: password, session and user management, payment authentication

Establish and automate transaction approval thresholds

Utilize systems with built in controls

Maximize automation and straight-through processing

Segregate and back up sensitive data

Fraud Prevention Practices & Tools

Secure Your Corporate Identities

Reconcile daily if possible

Monitor wire and EFT activity

Structure accounts to facilitate early fraud detection

Protect documents containing corporate identity – statements, cheques, reports

Protect PINs and passwords

Keep financial documents secure at all times and shred when disposing

Understand rights and privileges that you provide to your partners and vendors

Designate a compliance officer

Pay companies to monitor your websites

Final Thoughts

- As seen with the longevity of cheque fraud, payment fraud continues to be a never ending story.
- Payment fraud will continue to evolve as new payment types become available such as wireless mobile payments which launched in Canada in June 2009.
- Criminals will continue to switch their attack methods away from the more secure payment types e.g. Chip cards to other types of payment fraud such as international card fraud in non-Chip countries like the US.
- Criminals' sophistication and nimbleness will continue to increase. They will constantly be looking for ways to take advantage of any gaps in the system to perpetrate fraudulent activities. It's important to stay vigilant and on top of emerging trends.

Questions?

