fei financial executives international dirigeants financiers internationaux canada

Private Company Committee Roundtable

Cheque Fraud

In association with: KPMG

KPMG ENTERPRISE

fei financial executives international dirigeants financiers internationaux canada

Introduction

Moderator:

Tim Zahavich, CFO, St. Joseph Communications Inc.

Presenters:

Peter Armstrong, Senior Vice President, KPMG Forensic Inc.
Sunil Mistry, Partner, KPMG Enterprise
Jasbir (Jas) Anand, Senior Director, Fraud Strategy, CIBC
Jennifer Hill, VP, Financial Institution Practice, Marsh Canada Ltd.

KPMG
cutting through complexity

Cheque Fraud

Peter Armstrong, KPMG Forensic Inc.
Sunil Mistry, KPMG Enterprise

Overview

- Introduction
- Statistics and Trends
- Schemes and Methods
- Fraud Triangle
- Internal Controls – Lessons Learned
- Detecting Cheque Fraud
- Conclusion

fei
financial executives international
dirigeants financiers internationaux
canada

Prepared by: KPMG LLP

Statistics

Payment Fraud Survey - US

- Respondent Organizations reporting attempted or actual payment fraud in 2008
  - 91%
- Fraud financial losses by payment method

Payment Method	Percentage of Respondents
Cheques	60%
ACH debits (automated clearing house)	20%
Consumer credit/debit cards	10%
Corporate purchasing cards	5%
Wire transfers	1%

- Source: JP Morgan Treasury Services Whitepaper on Payment Fraud, 2008

fei financial executives international dirigeants financiers internationaux canada

Prepared by: KPMG LLP

Statistics and Trends

- Cheques are the payment form most vulnerable to fraud attempts (JP Morgan Fraud Survey)
- Clustered attacks (alterations and counterfeits) are common over an extended period
- Large companies processing many cheques are the most common target

Schemes and Methods

- **Cheque kiting**
- **Cheques for cash – substitution schemes**
  - Personal cheques in the cash drawer
- **Unauthorized disbursement schemes**
  - Forged authorization
  - Authorized signatory
  - ‘Redirecting’ pre-signed cheques
- **Concealed cheques**
  - Relies on poor review by authorized signatory

Schemes and Methods

- **Cashing duplicate cheques**
- **Stealing and converting blank cheque stock**
- **Split deposit (or less cash deposit)**
- **Forged endorsement schemes**
- **Altered/counterfeit cheques**
  - Cheque 'washing'

– *For internal perpetrators to remain undetected in the long-run, they need access to the cheques, bank statements, financial books and records*

Schemes and Methods

Cheque Fraud Recent Example

- **Montreal, Quebec**
  - $195 million in counterfeit cheques
  - Schemes detected during Canada Post investigation into forged postmarks
  - Schemes (two examples):
    - Recipients were told they had won the lottery and needed to cash a cheque and wire the funds to the fraudsters to cover prize fees
    - Recipients were told they were performing market research by cashing the cheque and sending money via wire transfer - this was to help “evaluate the effectiveness and efficiency of a payment system”

      - Montreal Gazette, December 2007

Schemes and Methods

Cheque Fraud Recent Example

- **Kemptville, Ontario**
  - Construction firm book-keeper – theft of more than $1.2 million
  - Misappropriation over 6 years
  - Charged with theft over $5,000, fraud over $5,000, uttering forged documents, falsification of books and records, possession of property obtained by crime, and laundering money

    - Ottawa Citizen, February 2008

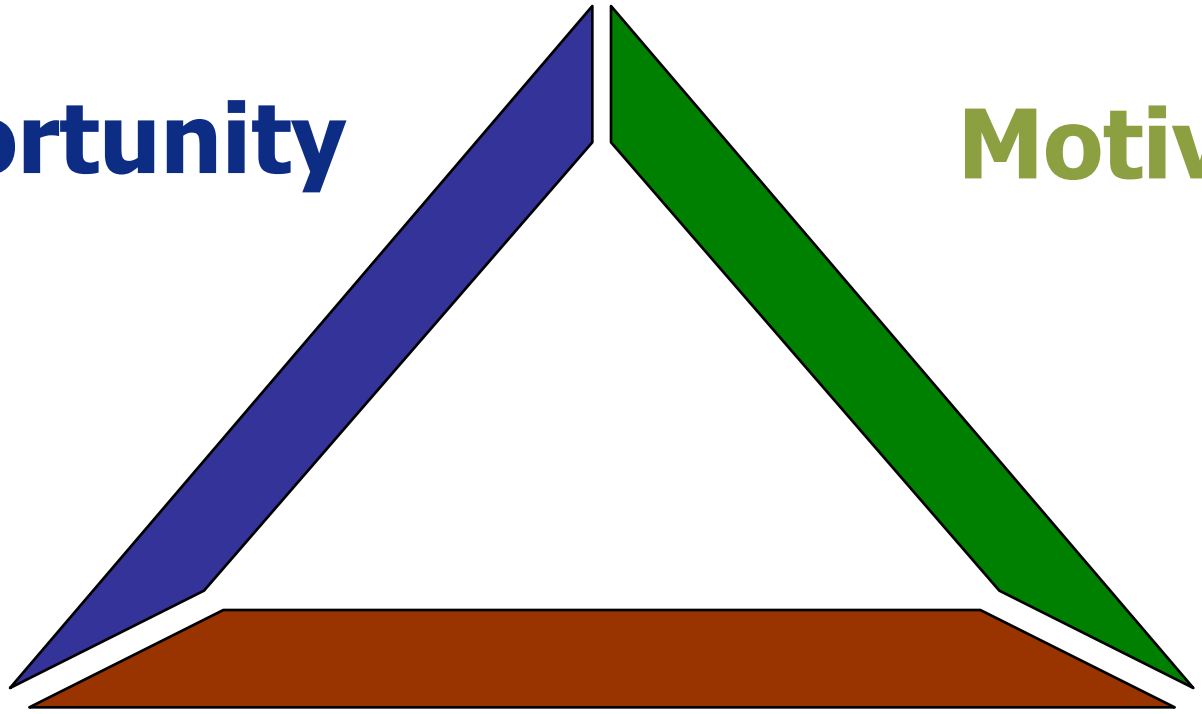
Schemes and Methods

Cheque Fraud Recent Example

- **Canada – KPMG Example #1**
  - Fraudster employed as a clerk at a public sector organization
  - Defrauded employees of more than $300,000 over a number of years
  - Scheme:
    - Deposited cheques payable to other staff into the fraudster's bank account

- **Ontario – KPMG Example #2**
  - Following an investigation, an employee admitted they provided blank cheque stock to a 'friend' who made a request – cheque stock was unsecured
  - 'Friend', or their 'friends' processed a series of larger dollar cheques and obtained payment on some while others were flagged

The Fraud Triangle



financial executives international
dirigeants financiers internationaux
canada

Prepared by: KPMG LLP

Internal Controls

Lessons Learned With Hindsight

- **Cheque security controls**
  - Purchase cheque stock from known vendors
  - Establish employee order/reorder policy for stock
  - Keep cheque stock and related equipment secure and establish custody procedures
  - Cashier's office should be in a room with a lock (not in an open plan area or with moveable partitions)
  - Strict rules on access to cashier's office and security/monitoring practices (physical, audit, etc.) consistent with the risks
  - Use cheque stock containing security features

Internal Controls

Lessons Learned With Hindsight

- **Cheque processing controls**
  - Segregation of duties between key functions
  - Avoid using cheques (however, alternatives are not perfect either)
  - Perform bank reconciliations on a timely basis
  - Stamp cheques on receipt “payable to XYZ only”
  - Payee details should never be abbreviated
  - Minimize manual or “rush” cheques

Internal Controls

Lessons Learned With Hindsight

- **Cheque processing controls (continued)**
  - Envelopes used to send cheques should not be separately identifiable
  - Cheques should require two signatures, be supported by original documentation
  - Never pre-sign blank cheques under any circumstances

Internal Controls

Lessons Learned With Hindsight

- **Post handling controls**
  - Contents of envelopes which contain cheques should not be visible through window
  - Envelopes containing cheques should not be left in an accessible location overnight
  - Secure incoming or outgoing post bags

Internal Controls

Lessons Learned With Hindsight

- **Other internal control issues**
  - "Clear desk" policy overnight – enforce
  - Access control over contractors' staff should be strict and always adhered to
  - Reasonable physical security over building should be maintained at all times
  - Timely investigation of vendor complaints
  - Monitor unusual spending patterns

Detecting Cheque Fraud

Red Flags

- **Unusual looking cheques**
- **Frequent cheques in the same amount**
- **Frequent cheques in round numbers**
- **Cheques to banks**
- **Deposits not made daily or intact**

fei
financial executives international
dirigeants financiers internationaux
canada

Prepared by: KPMG LLP

Detecting Cheque Fraud

Red Flags

- **Supporting documentation for cheques is not available or has been prematurely destroyed**
- **Irregular cheque endorsements**
- **Cheque numbers, payee, date and amount don’t agree with entries in the cheque register**

Detecting Cheque Fraud

Red Flags

- **Voided cheques are not retained**
- **Cheques issued to individuals for large, even dollar amounts**
- **Cheques clear the bank significantly out of order**
- **Variations on the name of the payee**

Conclusion

- **Cheque fraud continues to be a serious problem – smaller organizations are equally exposed**
- **Organizations have an important role in preventing and detecting cheque fraud**
- **Those without sufficient internal controls or who fail to follow their policies are exposed**
- **Organizations can have a significant impact on the risk of cheque fraud losses**

financial executives international
dirigeants financiers internationaux
canada

Prepared by: KPMG LLP

Restrictions

- This summary has been prepared for informational purposes only for participants at the presentation made by a representative of KPMG Forensic.
- This summary is no substitute for informed professional advice in each specific circumstance. This document should not be misconstrued as representing legal advice.
- KPMG Forensic Inc. assumes no liability whatsoever from any reader having relied on the information contained herein.
- Additional reproduction and distribution of this document must be approved in advance and in writing by KPMG Forensic Inc.

Prepared by: KPMG LLP

Reducing the Risk of Fraud

Jasbir (Jas) Anand
Senior Director, Fraud Strategy
CIBC

Agenda

1) Payment Fraud
2) Payment Fraud Prevention

Payment fraud types

Percent of organizations that reported payments fraud occurring through the corresponding methods:

93% - Cheque Fraud
25% - ACH Debits (EFT)
4% - ACH Credit (EFT)
23% - Consumer credit/debit cards
15% - Corporate/Commercial Cards
4% - Wire Transfers

Associate of Financial Professionals 2011 Fraud Survey (U.S.)

Percent of Organizations that reported cheque fraud occurring through the following techniques*:

61% - Payee Name Alteration on Issued Cheques

57% - Counterfeit Cheques with firm's MICR info and another firm's name

41% - Loss, theft and counterfeit of employee pay cheques

* Based on actual incidence of loss

www.checkfraud.com

fei financial executives international dirigeants financiers internationaux canada

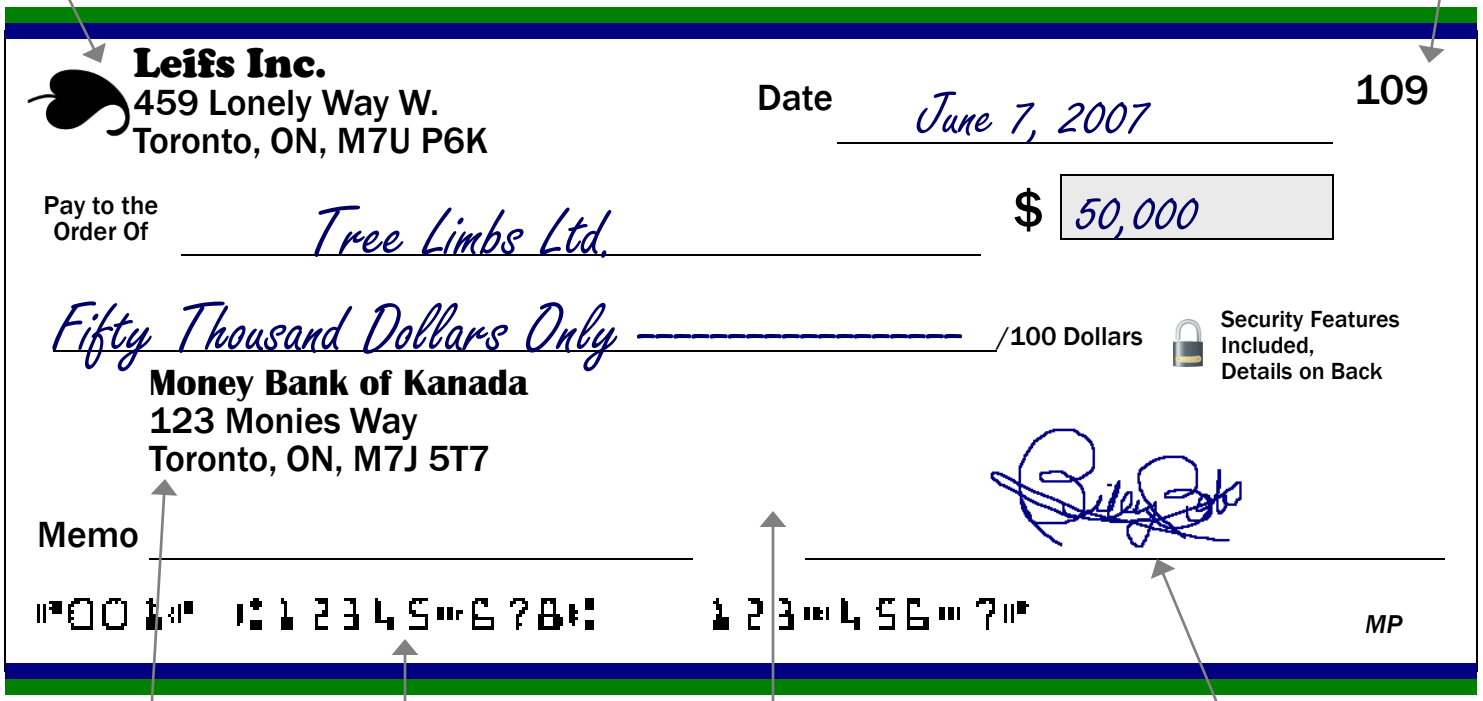
Common 3rd Party Cheque Fraud Techniques

- Altered Cheques
  - Cheques are intercepted
  - Payee name and amount are removed through chemical processes or through scraping the ink from the paper
  - New payee name and/or amount are applied to the cheque and the cheque is deposited
- Counterfeit Cheques
  - Cheques are intercepted
  - Copies of the cheque are produced, changing the cheque sequence numbers as needed
  - Copied blank cheques are filled out and deposited
- Forged Endorsements
  - Cheques are intercepted
  - Payee's signature is forged

Cheques – the preferred target

- Confidential information used for illegal activity
- Cheques are paper based and can be duplicated quite easily (low cost)
- Transportation of cheques (i.e. Canada Post) presents opportunities to intercept
- Criminals exploit the clearing process hoping to receive funds prior to fraud being detected through cheque reconciliation; physical items still travelling across the country to be negotiated
- Canadian landscape finally migrating to image but will be a long transition phase

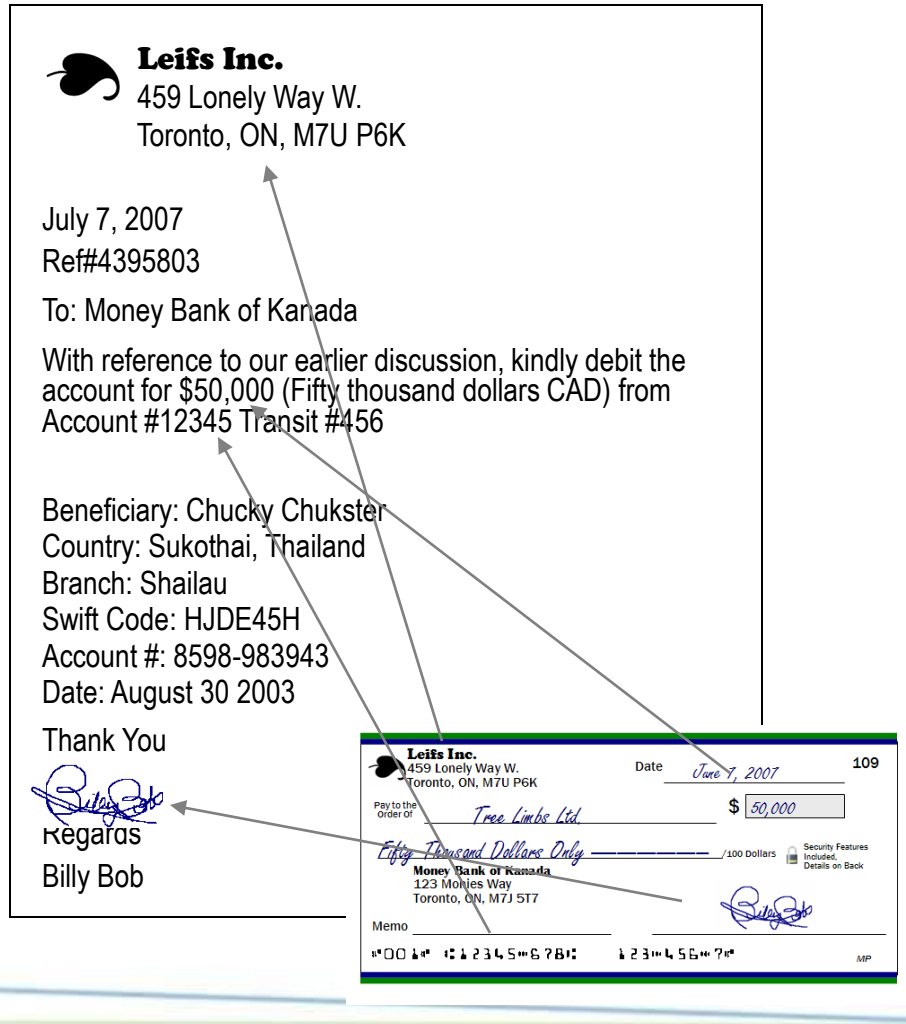
Cheques contain valuable information



fei financial executives international dirigeants financiers internationaux canada

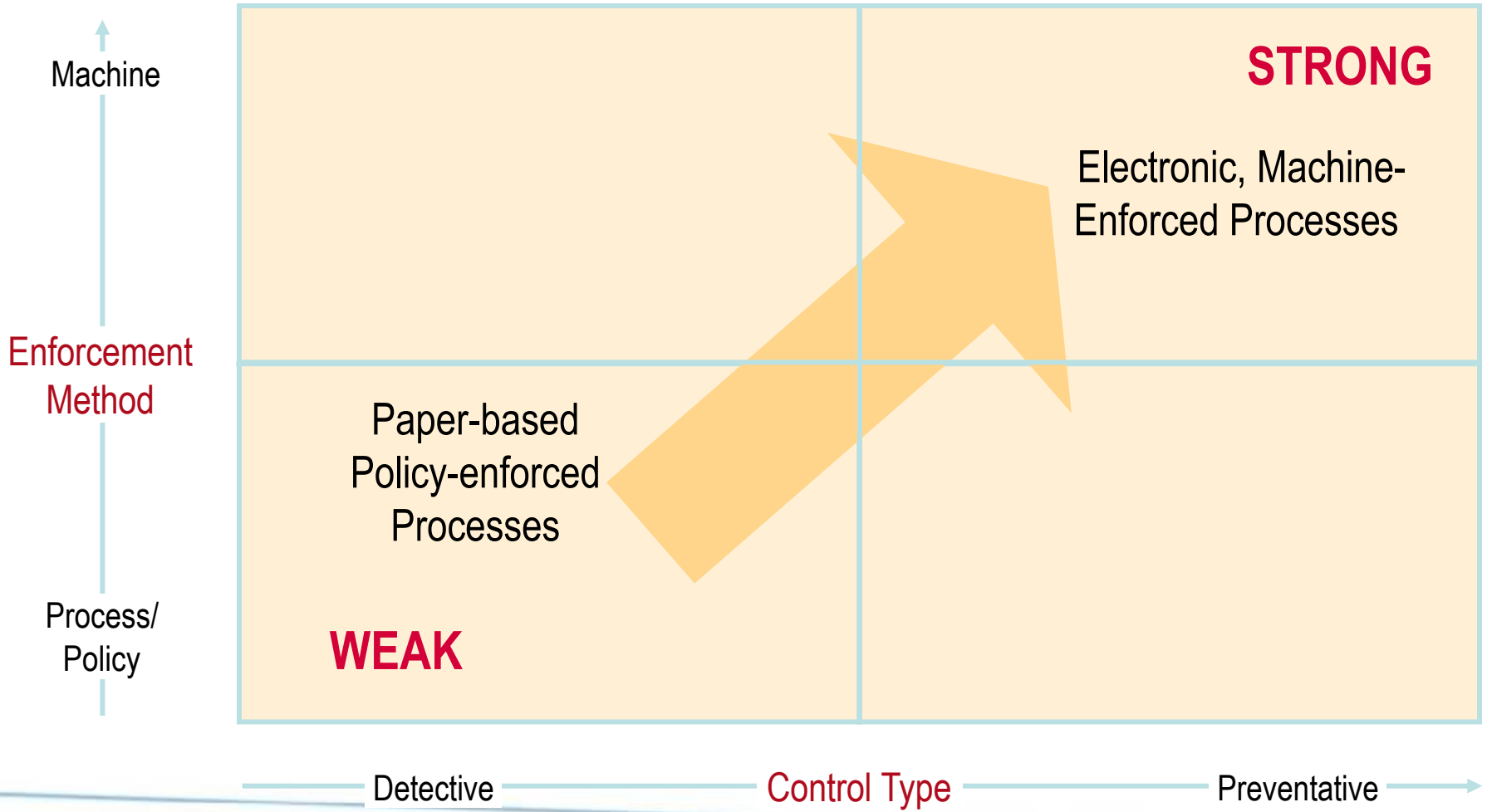
How information on cheques can be exploited

- Canadian banks continue to receive fraudulent wire instructions year over year
- $20MM in 2010 alone sent to China targeting North American business

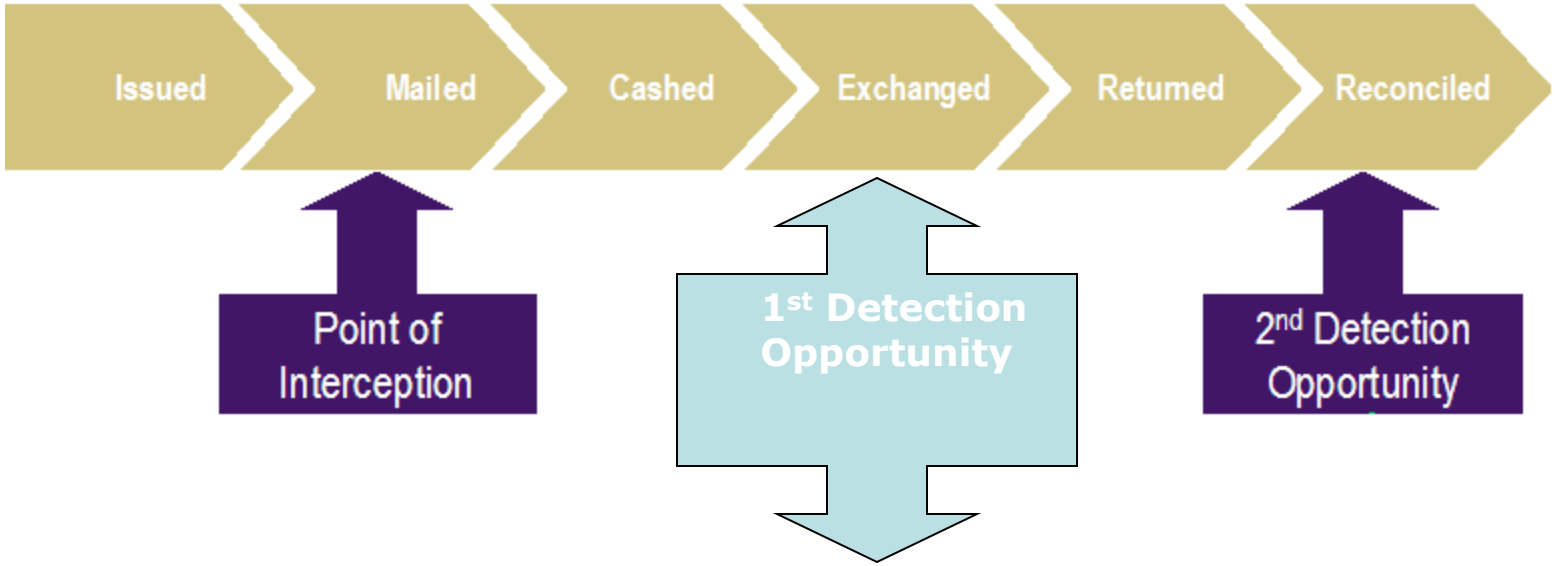


financial executives international
dirigeants financiers internationaux
canada

Improving Control Efficacy in Payments



Overview of cheque clearing process



What steps are CIBC taking to help ensure you as a Client are protected?

- CIBC clearing centres have installed with a Counterfeit Cheque Detection System
  - System identifies *suspect* items based on historical cheque writing patterns on a per account basis
  - Suspect items are subject to further scrutiny including physical inspection and as required, client contact for validation
- Continue to invest in the latest technology – migration to image based processing has begun

Overview of Electronic Payments

Transforms policies from process-enforced to machine-enforced

- Electronic payment processes eliminate risk of lost or stolen cheques in mail or transit
- Processes can be tailored to meet different risk needs
- Administration features enable user level transaction limits and authorities
- Authentication protocol moves from signature (poorly protected) to passwords (highly protected)
- Payment automatically sent to reoccurring payees, eliminating risk of non-payment
- Audit trail for all events

Transforms detective controls into preventative controls

- Controls cannot be readily circumvented
- Reduces social engineering risks

Reduces perception of opportunity and…Is more operationally efficient!

- Simplifies payment process, utilizing fewer resources and saving costs

Customizing your Accounts & Account Activity

Simple and cost effective suggestions:

- Multiple signing officers deters internal fraud
- Having collections or deposit only accounts
- Separate wire and cheque disbursement accounts; and low value and high value disbursement accounts to identify irregular activity with ease
- Use only one set of cheques per account
- Use a continuous set of serial numbers when re-ordering cheques
- Issue unique passwords to those responsible for laser-printing cheques
- Use plain envelopes instead of window envelopes when mailing out cheques

Controls are never one size fits all. Avoid stretching low value processes to serve high value needs.

MARSH

LEADERSHIP, KNOWLEDGE, SOLUTIONS...WORLDWIDE.

Managing the risk of cheque fraud

fei
financial executives international
dirigeants financiers internationaux
canada

Jennifer Hill

Vice President, Marsh Canada Limited

Crime Insurance

- Exposure
  - No company is immune from exposure to theft or fraud
    - Even the most robust internal controls are not “foolproof”
      - Experts estimate that 96% of all companies will experience some type of employee theft
        - » The average organization loses 5% of its total annual revenue to fraud and abuse committed by its own employees
      - It is estimated that it takes approximately $20 dollars in sales to recover each dollar of theft
      - The medium loss for Private companies in 2010 was $231,000
- Sources of Claims
  - Common crime claims allege employee dishonesty, embezzlement, forgery, robbery, safe burglary, computer fraud, wire transfer fraud, counterfeiting, and other criminal acts.

Crime Insurance

- Insurance Solutions
  - Crime policies have been developed to provide broad indemnity to organizations suffering loss from theft of fraud.
    - Prudent organizations will always have procedures in place to minimize the opportunity for loss a crime insurance policy provided an additional security safety net beyond internal risk management procedures
- Risks Covered
  - Loss of money or securities that have been embezzled by an employee through an act of fraud or dishonesty
  - Forgery or alteration of a financial instrument such as a cheque or draft issued by the company
    - Alteration includes washing and copying
  - Loss as a result of a financial institution transferring money or securities based on a fraudulent document purported to have been sent by the insured organization
  - Loss of money, securities or other property for which the insured company is legally liable

Crime Insurance

- Risks Covered (cont'd)
  - Extortion – some policies will extend to cover monies paid away as a result of a direct threat to inflict bodily injury on a director or an employee of the firm or to damage or destroy any property owned by the insured firm
  - Loss to money, securities and property (eg. stock) as a result of "hacker" activities
  - Many policies contain a very broad definition of employee which can include: any director or trustee; part time or temporary employees; students; volunteers; or any person provided to the insured by an employment agency
  - Coverage under some policies will extend to undiscovered acts committed before the insurance was purchased
    - Loss Discovered versus Loss Sustained
  - Provide cover without the requirement of identifying who caused the loss or where it occurred
  - No requirement to secure prosecution or conviction of employee who caused the loss

Crime Insurance

- Last thoughts
  - Crime losses are costly and difficult to detect
    - Many frauds can go on for years undetected leading to an enormous ultimate net impact
      - The most common method for detecting fraud in privately held companies is simply by accident
  - A well constructed Crime Policy can protect you from potentially serious financial consequences for relatively little cost

Disclaimer

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.
This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are intended solely for the entity identified as the recipient herein ("you"). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh's prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.

fei
financial executives international
dirigeants financiers internationaux
canada

Live Q&A

Tim Zahavich
Chief Financial Officer
St. Joseph Communications Inc.
tim.zahavich@stjoseph.com

Jasbir (Jas) Anand
Senior Director, Fraud Strategy
CIBC
jasbir.anand@cibc.com

Peter Armstrong
Senior Vice President
KPMG Forensic Inc.
pearmstrong@kpmg.ca

Jennifer Hill
VP, Financial Institution Practice
Marsh Canada Ltd.
jennifer.hill@marsh.com

Sunil Mistry
Partner
KPMG Enterprise
sunilmistry@kpmg.ca

KPMG ENTERPRISE

financial executives international
dirigeants financiers internationaux
canada