Mitigating the Growth of Fraud Risk in Banking

GARP Toronto Chapter

July 2014

GARP | Global Association of Risk Professionals

Fraud Risk in Retail Banking

Dan McKenzie
Head of Enterprise Fraud

Agenda

What is Fraud

Canada is Unique

Where we are

- History
- Chip and PIN
- Move from Detection to Prevention
- Social Network Analysis

Current Threats

Questions

What is Fraud?

Fraud is a **deception** deliberately practiced in order to secure unfair or unlawful gain . As a legal construct, fraud is both a civil wrong (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud and/or recover monetary compensation) and a criminal wrong (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities). Defrauding people or organizations of money or valuables is the usual purpose of fraud, but it sometimes instead involves obtaining benefits without actually depriving anyone of money or valuables, such as obtaining a drivers license by way of false statements made in an application for the same

Canada is Unique

"Canada is a unique environment for fraud, we are fraud friendly

Rich social services

Privacy laws are strict

minimal deterrents"

– Craig Hannaford, Executive consultant Fraud Squad TV, Ex RCMP

History

Automated detection born in the Credit Card space

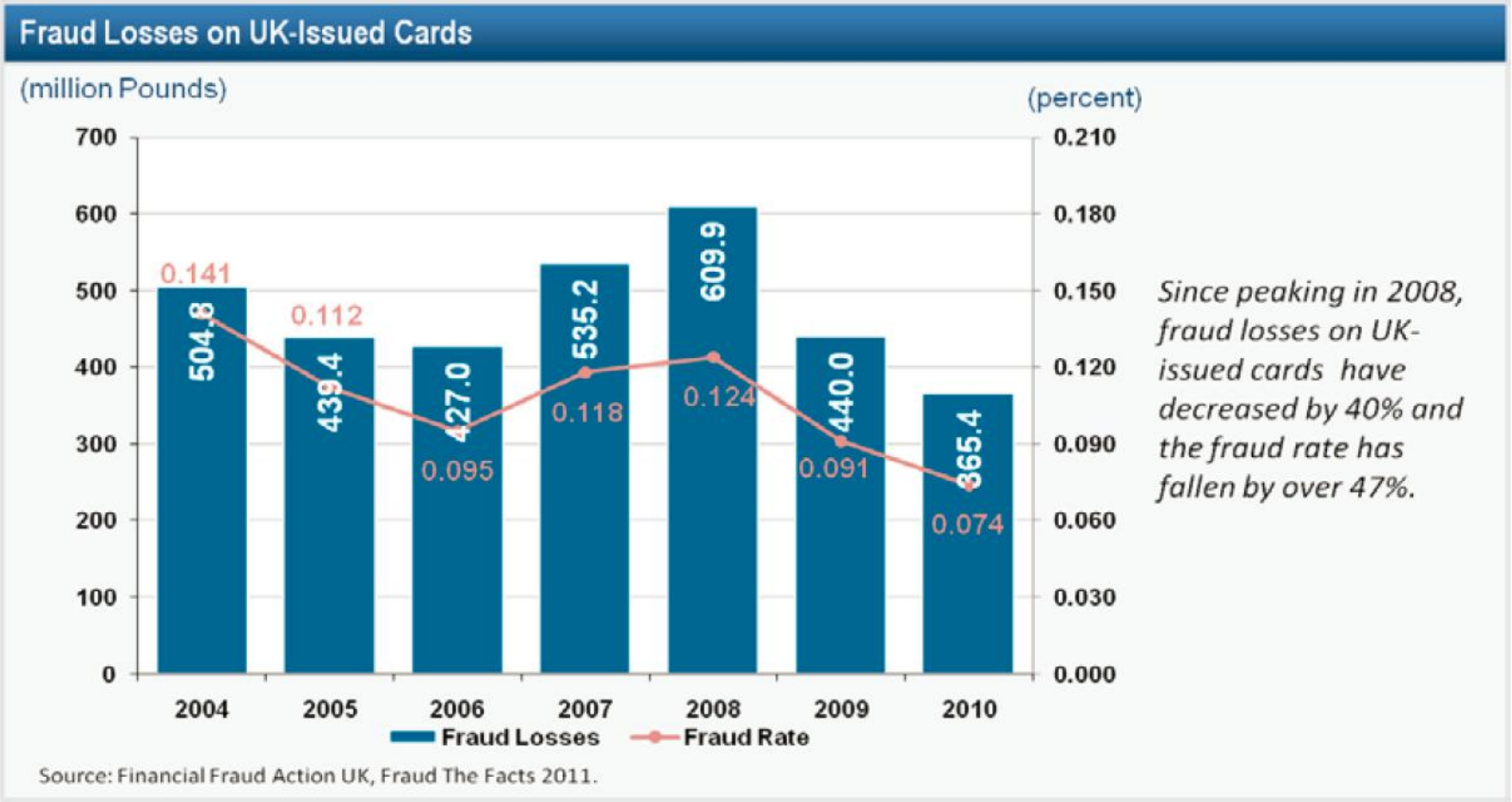
- Real-time detection
- Analytics
- Large call centers to handle alerts
- Mature systems and process

Cheques still a problem

- Altered cheques
- Stolen

Chip and PIN

Chart 1: Fraud Losses on UK-Issued Cards



Chip and PIN continued…

- Lost and stolen down
- Counterfeit down
- Card not Present Up
- Cross boarder up
- 1st Party up (hidden in PCL)

Move from Detection to Prevention

1st Party Fraud

- Hidden in PCL
- Manipulated credit files
- Standard detection systems fall down (except bustout)
- Same fraudsters over and over again

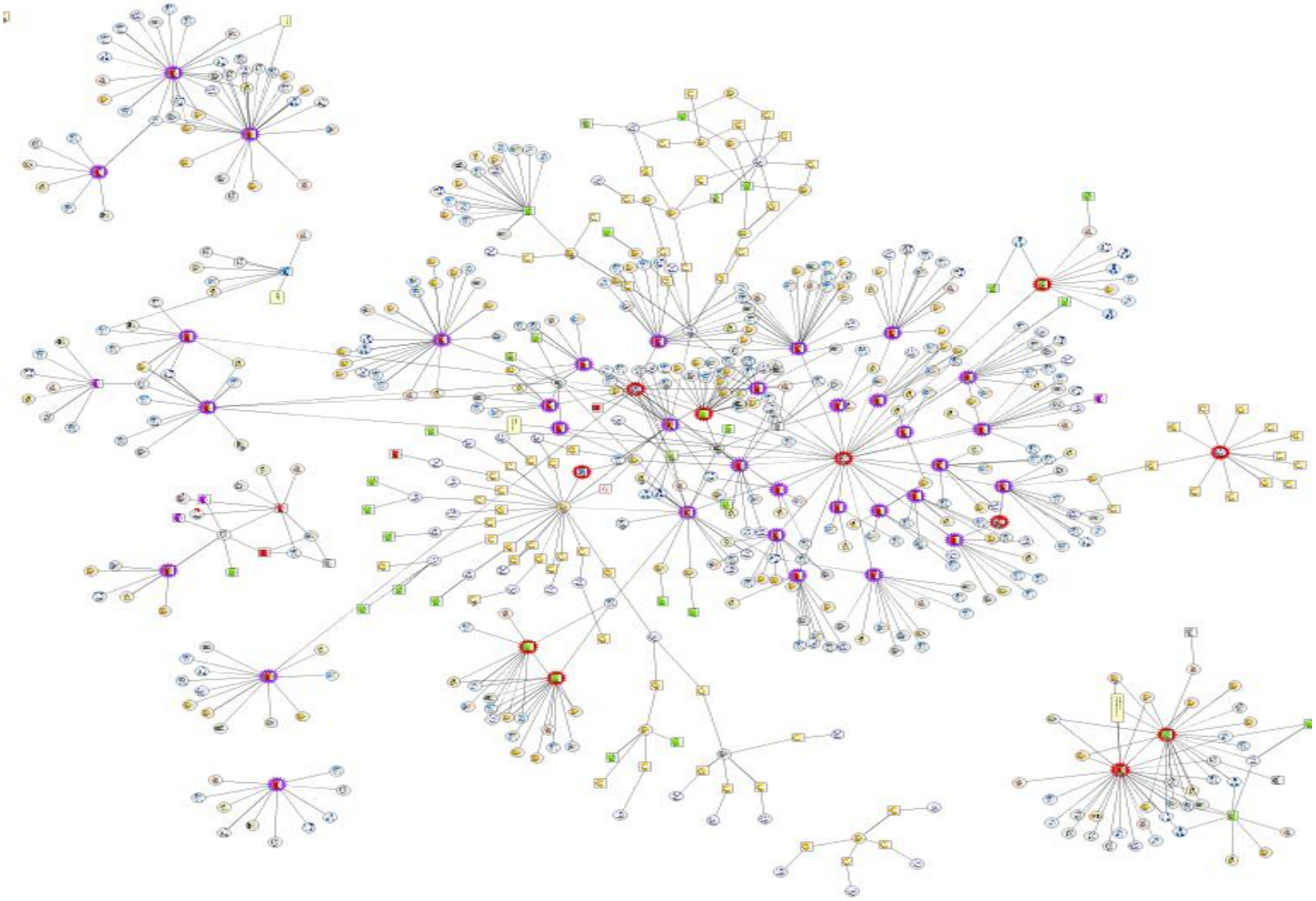
Requires consortium solution

- Citadel
- LinkView

Prevention

Social Network Analysis

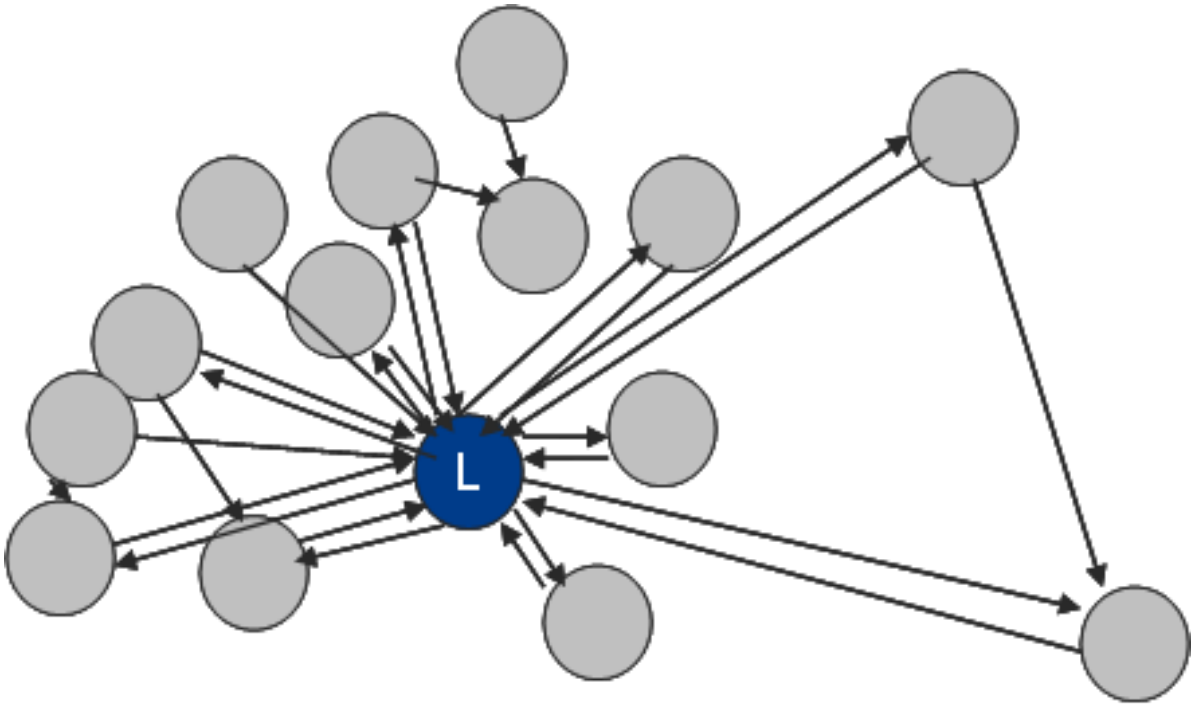
Social Network Analysis



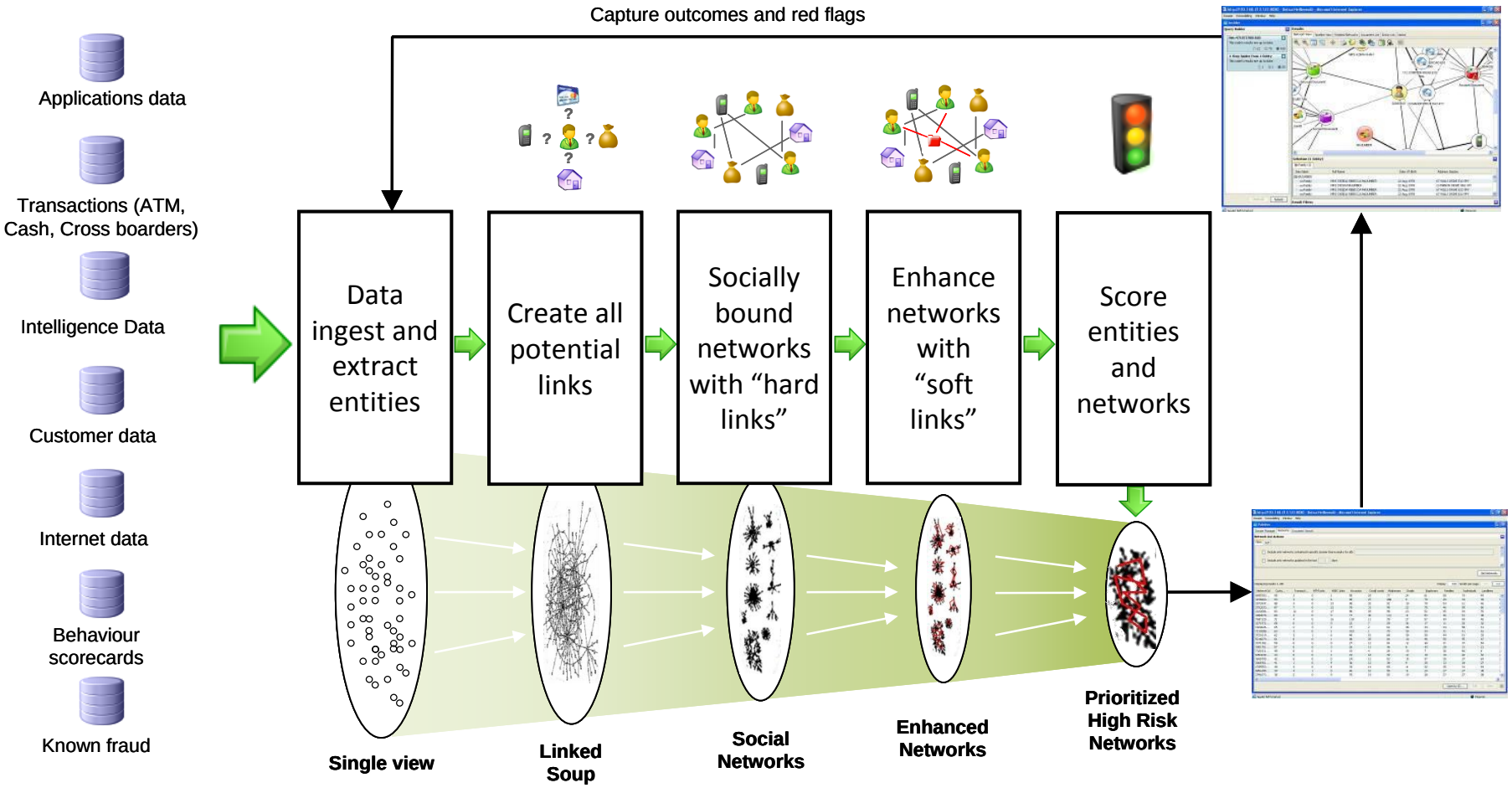
What is *"Social Network Analysis"* ?

Definition:

The practice of linking individuals and measuring the strength of their relationships



Network Build Approach



Current Threats

As new products and channels are developed to make is easier and faster for customers – faster and easier for criminals

Identity theft

- More elaborate
- Make and sell kits
- Must monitor new customers and changes to customer's profiles

Mobile Fraud

- Simulators
- They find the holes

Phishing, Phishing, Phishing

- Wealth Management
- Wires
- ACH

What keeps me awake at night

Fraud where bank is used as vehicle but no losses

Ponzi

- Court settlements
- Difficult to detect

Book Keeper Fraud

- Hits small business

Elderly Abuse

Fraud by Employees against clients

Wires

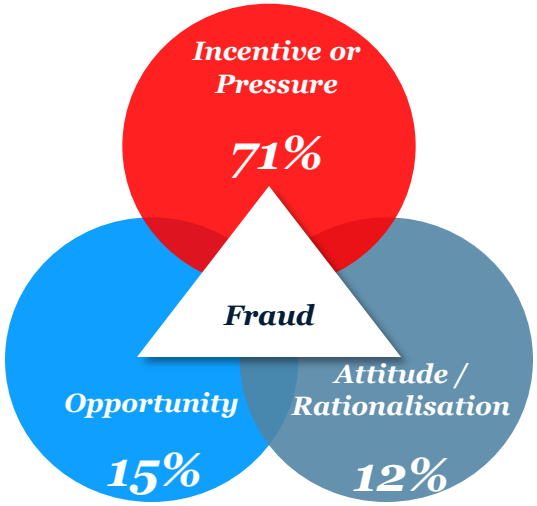
Fraud Risk in Capital Market

Maurits Bakker
Director FS Risk Consulting
PwC

Table of Contents

What is Fraud Risk in Capital Markets?

- Fraud Risk is the risk of someone defrauding the institution through an **intentional act committed to secure an unfair or unlawful gain**.
- Understanding fraud risk is about understanding who and why people commit fraud (the Fraud Triangle on the right illustrates 3 elements needed for someone to commit fraud).



Source: PwC Global economic survey

Who could be the perpetrator?

- Employee
- Customer
- 3rd Party Vendor
- Other External Party (e.g. market participant, cyber criminal)

What type of fraud could be perpetrated?

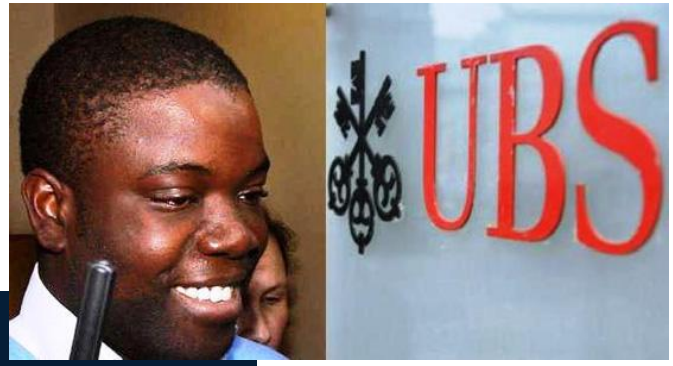
- Asset misappropriation
- Misrepresentation of information
- Intentional mi…g
- Unauthori…ivities
- Market …ulation
- Mis… confidential in…ion
- Bri…ery and corruption
- Anti-trust

Who are the victims of the perpetrated fraud?

- The Bank
- Customer
- External Parties

Fraud Example (1/3)
Unauthorized Trading

UBS lost $2.3 billion (2011) and Societe General lost $7.2 billion (2008) due to "rogue traders".



The traders found ways to conceal their positions or offset their P&L through fictitious trades, amending or cancelling trades, suppressing breaks in reconciliations and other means.

Fraud Example (2/3)
Market Manipulation

The accusations on manipulation of LIBOR and other rate setting mechanisms (e.g.) have resulted in significant internal and regulatory investigations into market manipulation for the banking industry. In relation to LIBOR, a number of banks have received fines which total in excess of $3.5 billion and there are still several banks under investigation.

Fraud Example (3/3)
Intentional Misselling

JPMorgan was fined a record fine of $13 billion in 2013 for being accused of misleading investors during the housing crisis due to alleged misrepresentations.

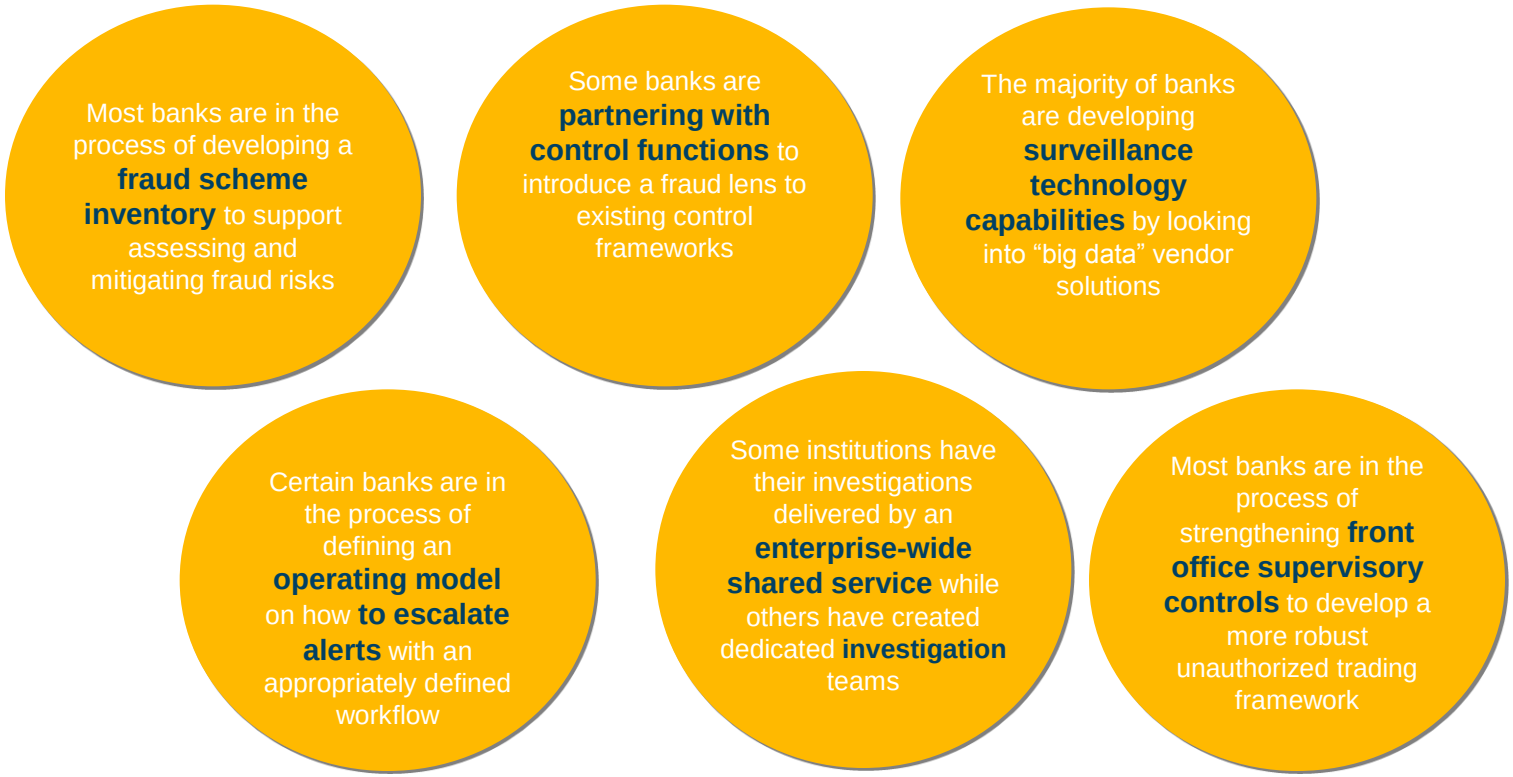
Lessons Learned

What went wrong and what can we learn from it?

Industry Trends: Enhancement of Fraud Risk Capabilities

Banks have responded by developing tailored fraud strategies for their platforms and by strengthening their analytics capacity.

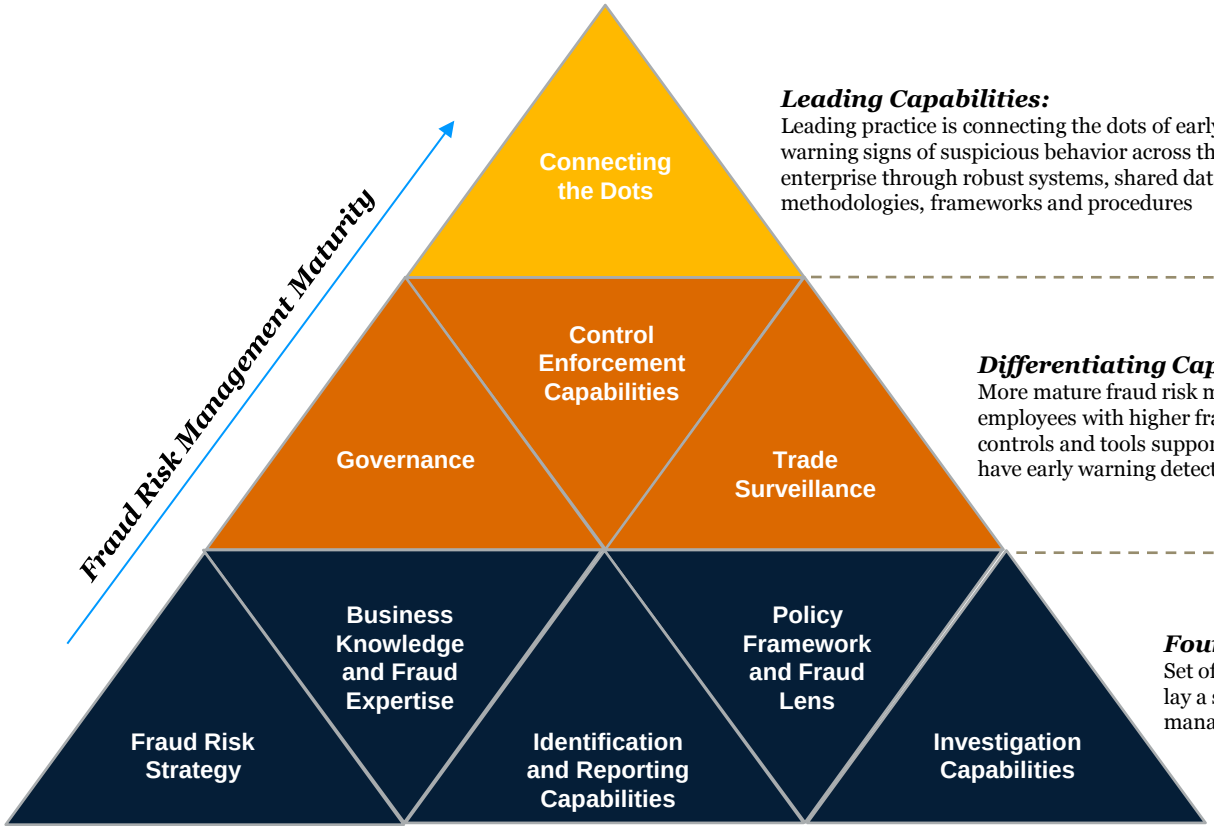
Examples of Fraud Risk Capabilities Developed



A Framework for Response

We have developed a structured framework to support the enhancement of an institutions' Fraud Risk Management Capabilities

Fraud Risk Management Capabilities and Maturity Framework

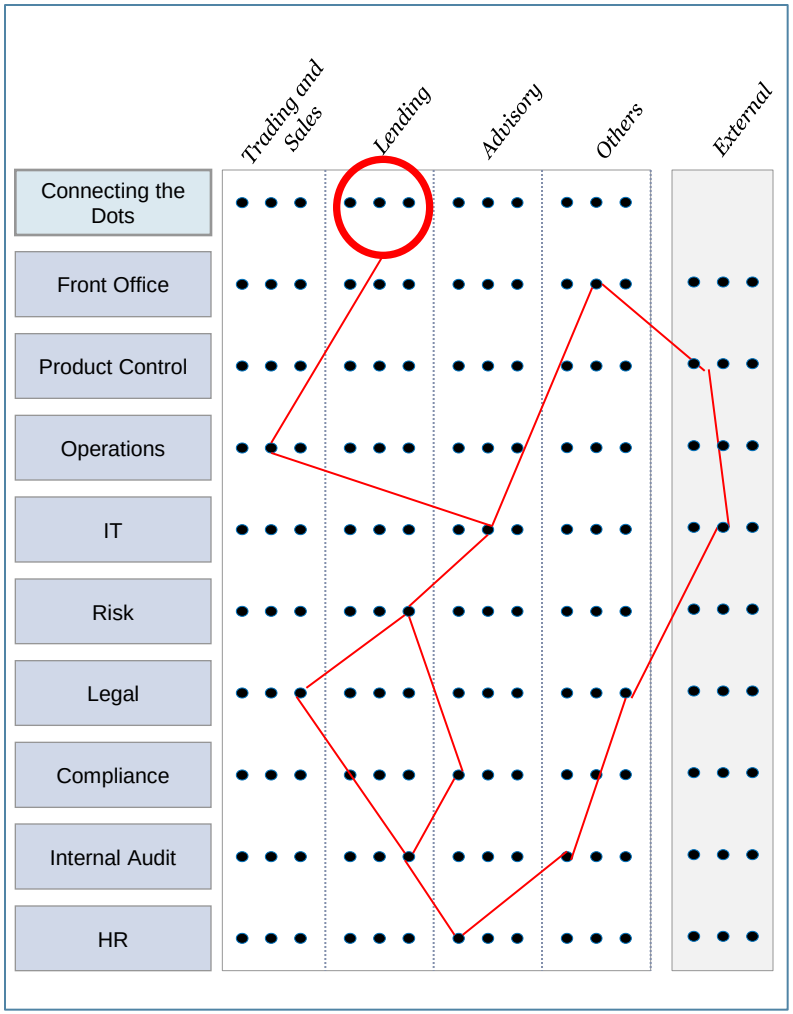


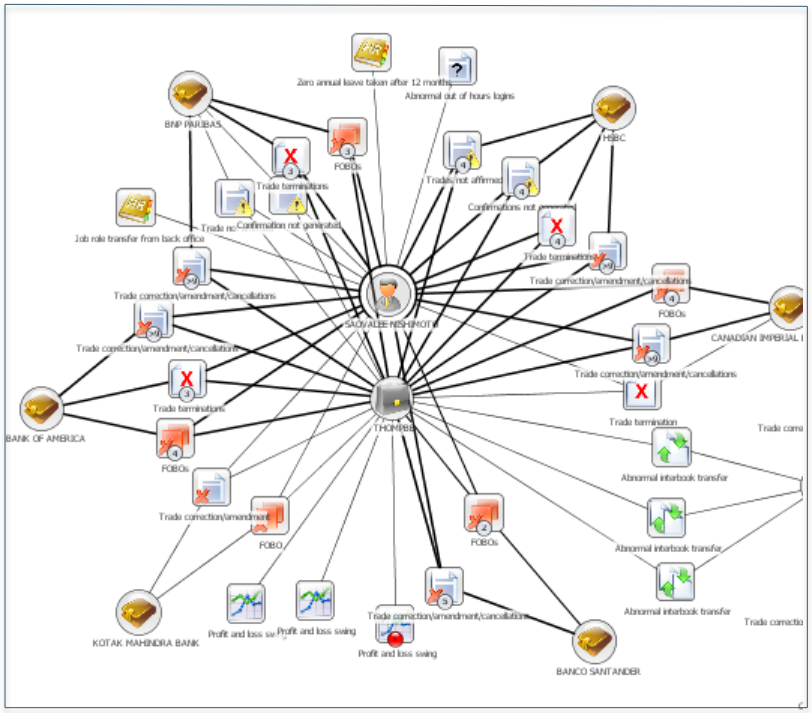
Leading Capabilities:
Leading practice is connecting the dots of early warning signs of suspicious behavior across the enterprise through robust systems, shared data, methodologies, frameworks and procedures

Differentiating Capabilities:
More mature fraud risk management practices have employees with higher fraud detection skills, integrated controls and tools supported by advanced analytics to have early warning detection of potential frauds

Foundational Capabilities:
Set of capabilities that banks should develop to lay a strong foundation for fraud risk management

Connecting the Dots through Social Network Analysis
Leading Capabilities





GARP Global Association of Risk Professionals

Contact details

Maurits Bakker

+1 647 801 2209

Maurits.r.bakker@ca.pwc.com

Fraud Risk – Data Breach

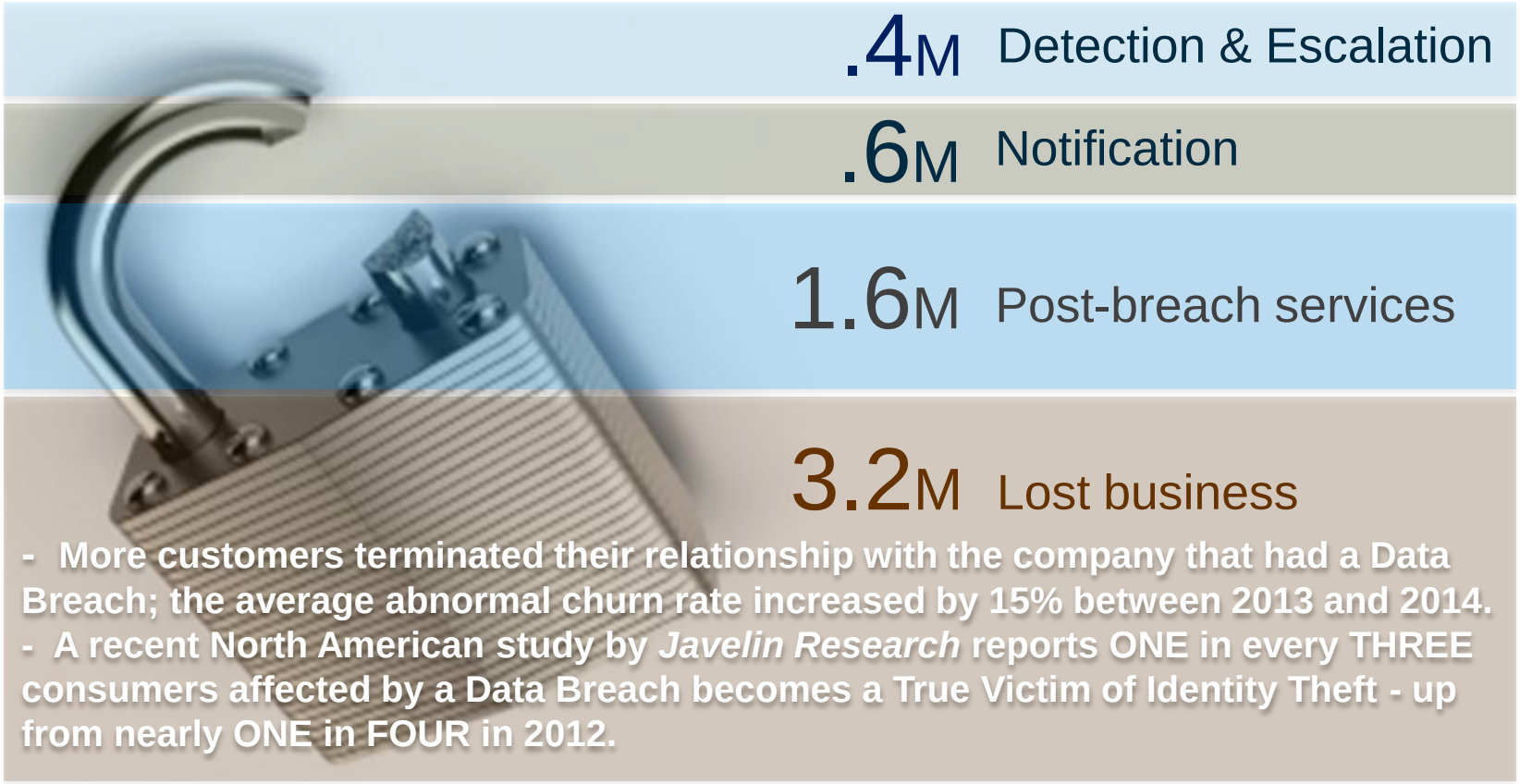
John Russo
VP, Legal and Chief Privacy Officer
Equifax Canada Co.

Agenda

1. Today's Breach Facts and Figures…somebody get the Popcorn…Please!!!
2. Impacts and Costs of a Data Breach
3. True Fraud Victims in Canada (Equifax Canada Statistics) and Victim Assistance
4. What the Hack…we've been Breached!?!?!
5. Fraud Management Checklist and Criminal Creativity
6. Tri-partite Relationship between Consumers,
   Data Custodians and Credit Bureaus
7. Contacts

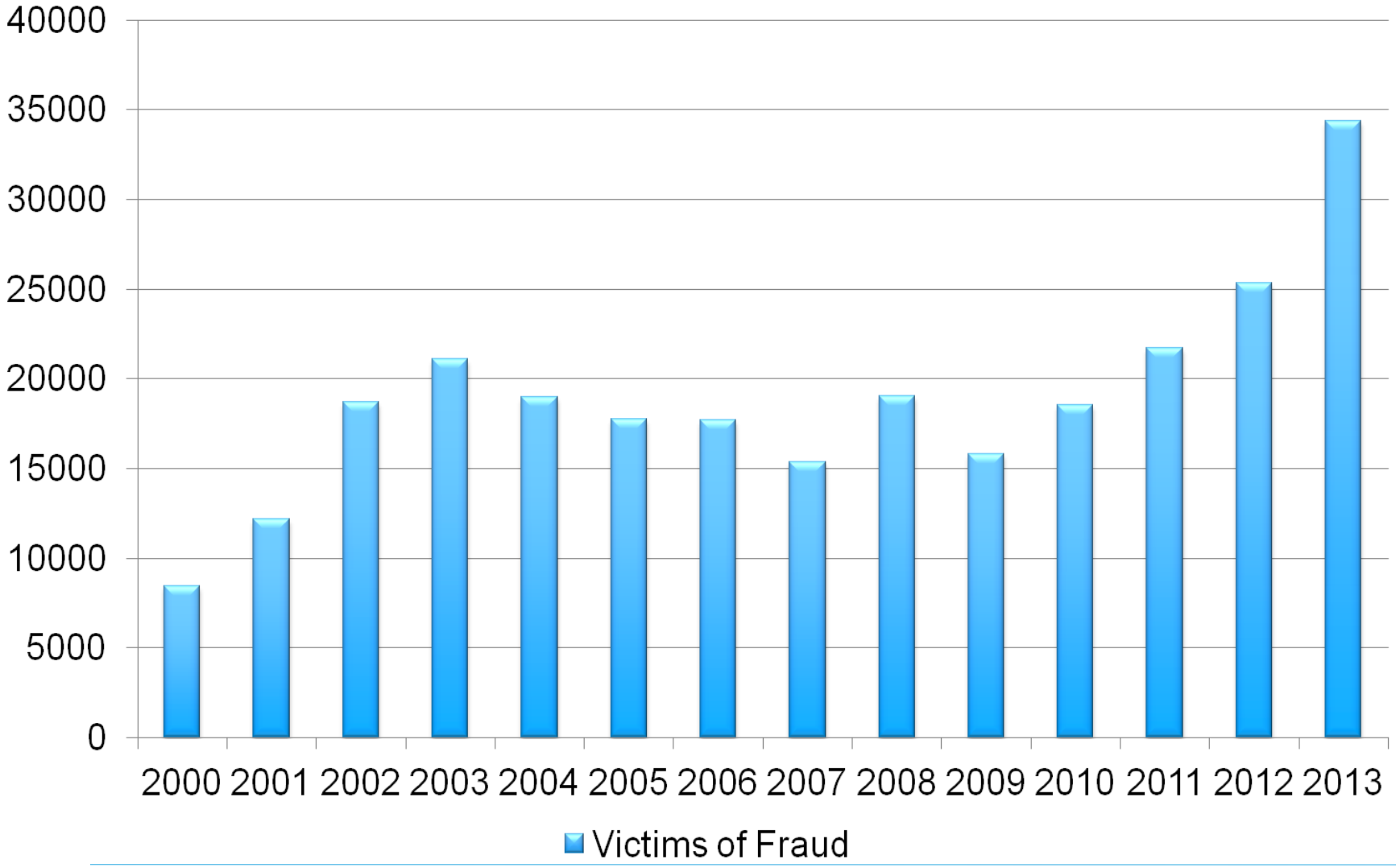
Impact and Costs of a Data Breach

- **42%** of incidents involved a malicious/criminal attack
- Average cost of a breach **5.9M** or **$201** per record



The Ponemon Institute's "2014 Cost of Data Breach Study: Global Analysis"

Protected Consumers
(True Fraud Victims as of Dec. 31, 2013)



GARP Global Association of Risk Professionals

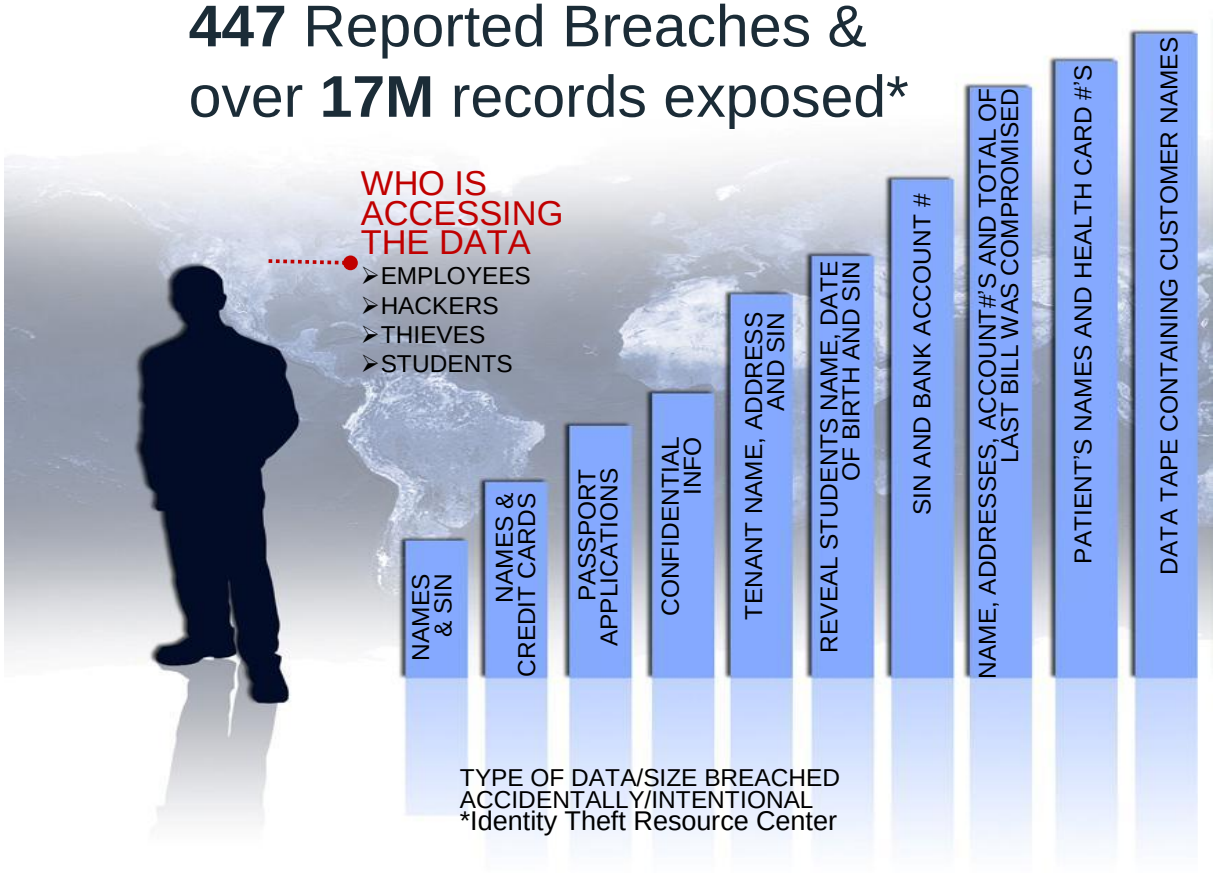
Fraud Victim Assistance

Equifax Canada Handling Process:

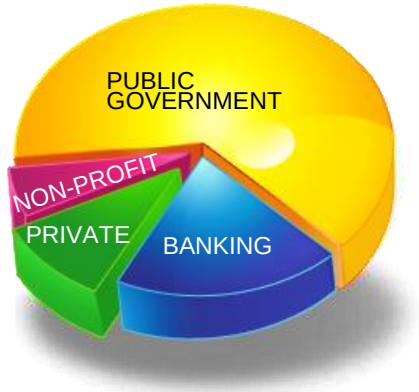
- ✓ Confirm identification;
- ✓ Review content of file and alert credit grantor(s);
- ✓ Provide consumer with credit grantor information;
- ✓ Obtain consent to notify Canadian Anti-Fraud Centre (formerly *Phone Busters*);
- ✓ Place Fraud or Identity Alerts on consumer's credit file; or
- ✓ Assist in Credit Monitoring

"What the Hack?!?!?!...we've been breached!!!"

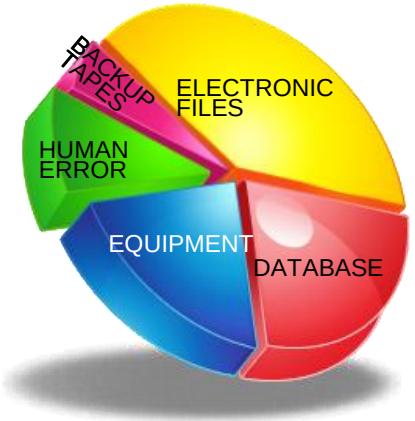
447 Reported Breaches & over **17M** records exposed*



INSTITUTION BREACHED



SOURCE OF DATA BREACH



CANADA

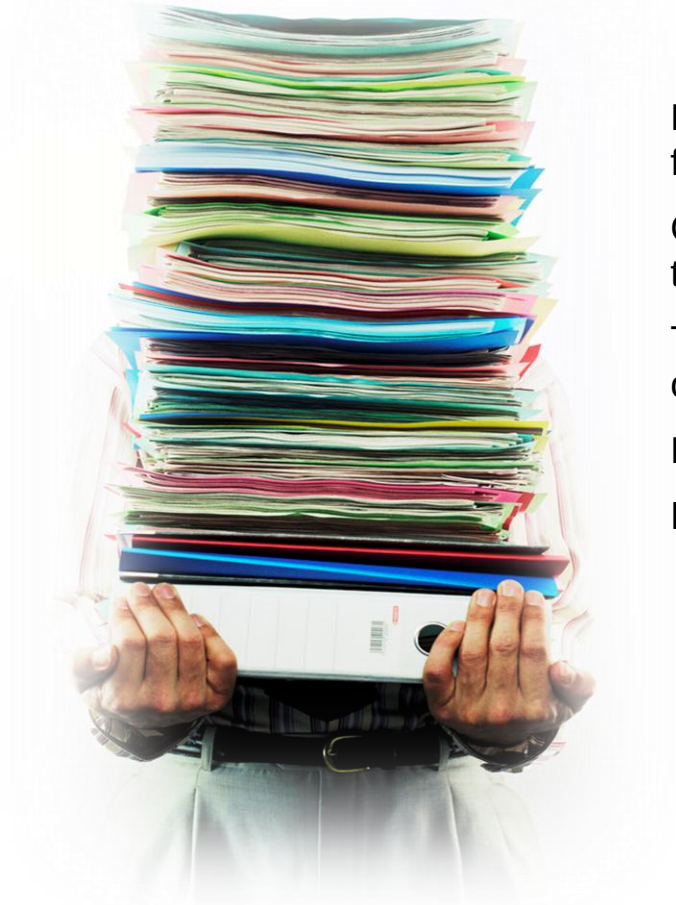
GARP Global Association of Risk Professionals

Fraud Management Checklist for your Team in a Breach - Friendly World

Things to think about

- What are your fraud prevention capabilities & procedures?
- What are your fraud detection capabilities?
- Do you have strong fraud management policies?
- Do you have tools to investigate/analyze suspected fraud?
- How do you track your fraud losses? Are they hiding somewhere else?
- Do you have strong internal fraud controls & monitoring?
- Do you have a fraud prevention education program for your staff?

Criminal *Creativity* - Fraud Crimes - *What* to look for on the Credit File



Applications typically start with a 'no hit' scenario

Fraudsters use a variety of **online** credit applications to build the fictitious ID

Online credit file creation dates tend to be from **2002** to the **present** time

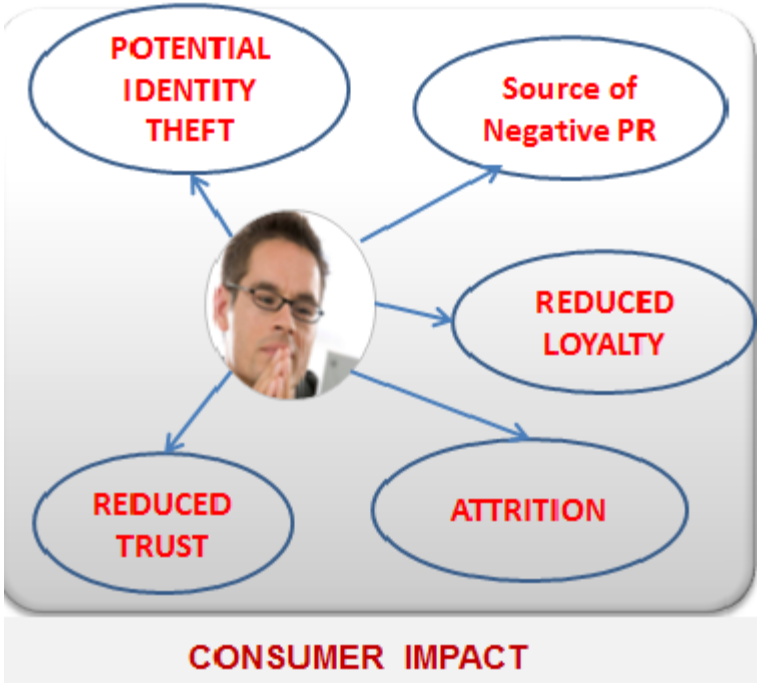
Their goal is to make it look like a **real ID** – spreading out inquiries over time

Fraudster maintains **good credit standing** on existing products

Files tend to have "**too much available credit**" (i.e., under-utilization)

The Consumer's Perspective: What are their pain points?

- When a cybercrime or data breach happens, the consumer is often, overwhelmed, concerned, confused and feeling powerless
- Consumer expects transparent communication, protection and resolution
- Educating and empowering the consumer will lessen the risk to the consumer and to your business
- In every data breach there is risk, but also **Opportunity**



The Data Custodian's Perspective

- Having a robust data breach plan in place that is quick to implement and reliable is essential to mitigating organizational impacts of cybercrimes or data breaches
- Implementing proactive self-regulation will help protect the consumer, mitigate business risks, and lessen the need for government regulation

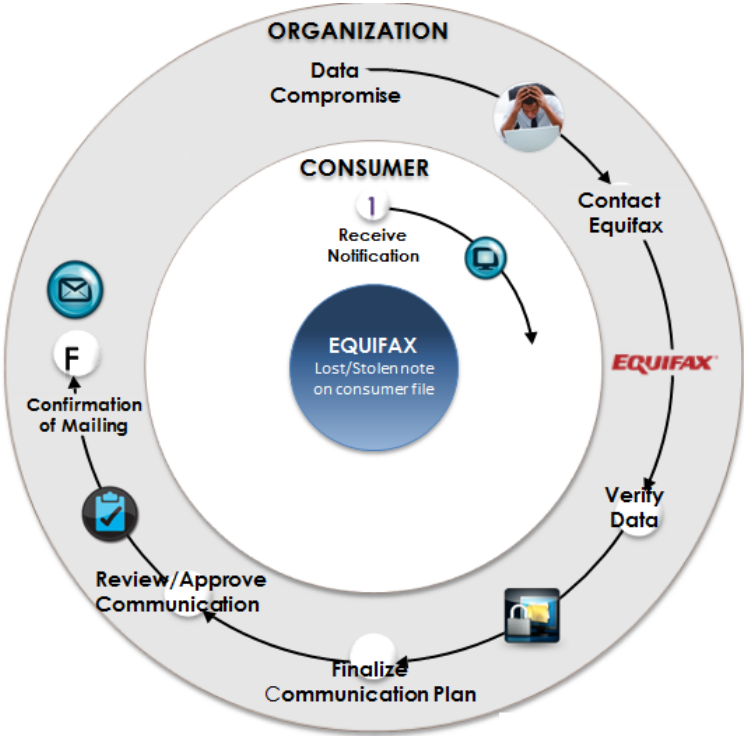
The Credit Bureau's Perspective:

Protect Consumer's valuable credit information

Promote fair consumer handling as a best practice; it's a "win-win" for all

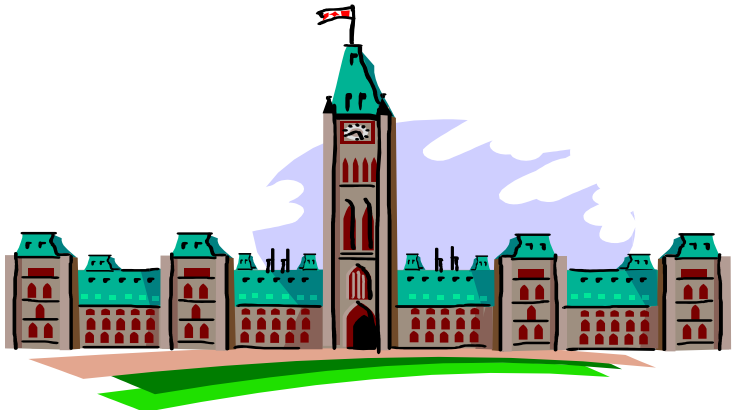
Consumer Support: empower, educate, assist and comfort

- Credit Alert Flags
- File Notations
- 24/7 Monitoring
- Identifying consumers at risk
- Consumer notification
- Reporting
- Incidence response checklists



Contacts

John Russo | Tel: (416) 227-5253| E-mail: john.russo@equifax.com



Equifax National Consumer Relations
1-800-465-7166

equifaxprotect.com or equifax.ca

Creating a culture of risk awareness®

Global Association of Risk Professionals

111 Town Square Place
14th Floor
Jersey City, New Jersey 07310
U.S.A.
+ 1 201.719.7210

2nd Floor
Bengal Wing
9A Devonshire Square
London, EC2M 4YN
U.K.
+ 44 (0) 20 7397 9630

www.garp.org

About GARP | *The Global Association of Risk Professionals (GARP) is a not-for-profit global membership organization dedicated to preparing professionals and organizations to make better informed risk decisions. Membership represents over 150,000 risk management practitioners and researchers from banks, investment management firms, government agencies, academic institutions, and corporations from more than 195 countries and territories. GARP administers the Financial Risk Manager (FRM®) and the Energy Risk Professional (ERP®) Exams; certifications recognized by risk professionals worldwide. GARP also helps advance the role of risk management via comprehensive professional education and training for professionals of all levels. www.garp.org.*

GARP | Global Association of Risk Professionals