SOCIAL ENGINEERING FRAUD

KNOW AND UNDERSTAND THE THREAT TO BETTER PROTECT YOUR ORGANIZATION

THE CYBER EXCHANGE
Hamilton, May 22, 2019

Mark Abbott, Senior Fidelity Claims Analyst,
The Guarantee Company of North America

Chris McKibbin, Partner, Fidelity Practice Group
Blaney McMurtry LLP

Please note that this presentation is for educational purposes only. Excerpts of policies or insuring agreement paraphrasing may be used for simplicity and to assist with presenting the concepts at a macro level.

This document is not to be relied upon for any coverage or policy language interpretation. At all times, the specific issued policy in its entirety including all definitions, conditions and exclusions is to be used when determining the scope of potential coverage under all Guarantee insurance products.

WHY ARE WE HERE ?

SOCIAL ENGINEERING

Impersonation Fraud

Business Email Compromise (BEC)

Executive Impersonation

Not a type of loss

WHAT ARE THEIR OBJECTIVES?

STRATEGIES

STRATEGIES

Transferring Money

Changing Key Information in the System

Sharing Corporate Confidential Information

Revealing details of Internal Processes or Protocols

Bypassing Established Internal Controls

Business Email Compromise (BEC)

TACTICS

TACTICS

- Urgency
- Consequences
- Internal Knowledge
- Confidentiality

- Email Spoofing

  @theguarantee.com vs. @theguarentee.com

  or Compromised Email Accounts

ACTORS IMPERSONATED

- Executive / Owners
- Vendors
- Customers

OTHER COMMON THEMES

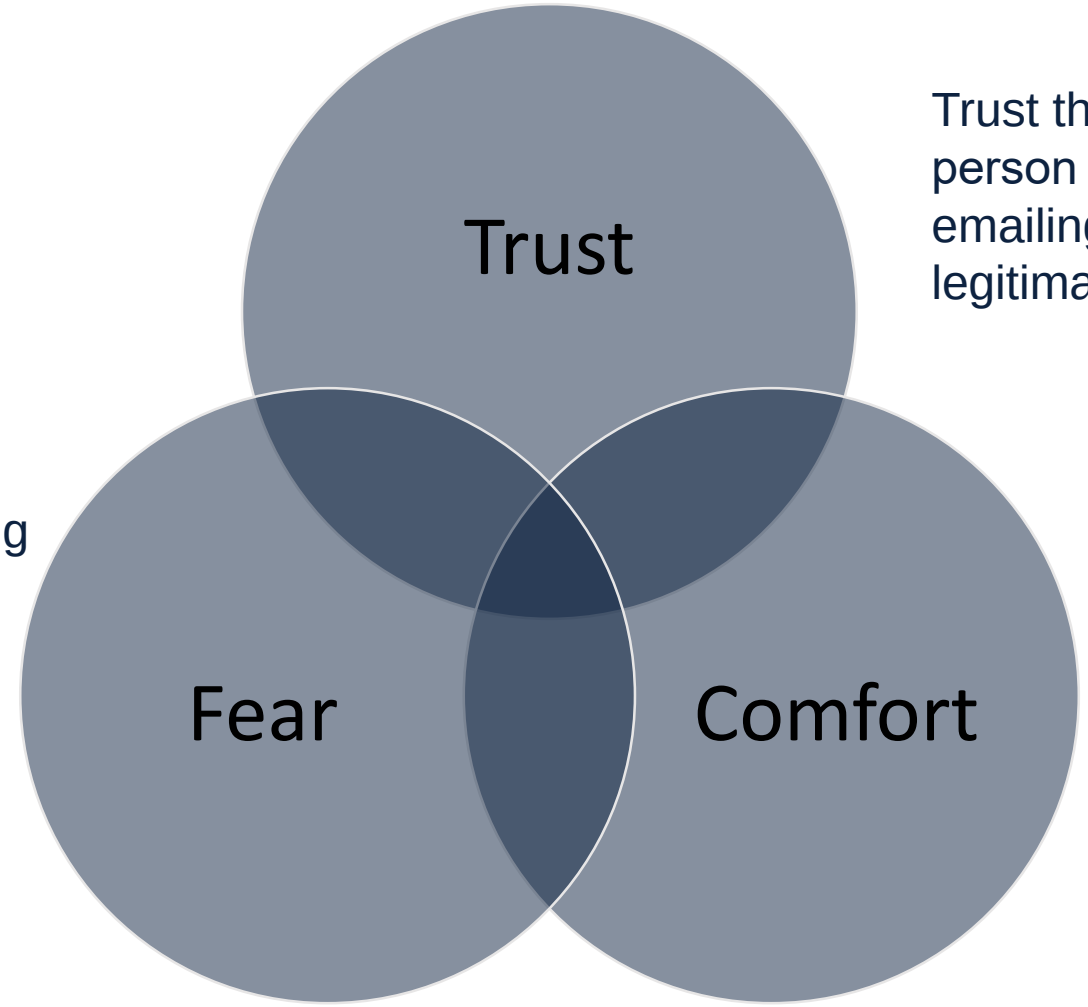
- Usually deals with an acquisition or large purchase order
- Executive being impersonated is usually travelling
- Target geography is usually Southeast Asia or Eastern Europe
- Organization typically has good financial controls

WHERE WE SEE COMPANIES GO WRONG

- Tight process for vetting new customers / vendors – stops there
- Over-reliance on dual-signature controls
- Lack of employee-empowering transfer protocols

An email will never suffice as adequate evidence to move money. You will never be asked to transfer funds without proper documentation. No employee will ever be reprimanded for requiring this documentation. Everyone who signs or approves a transfer is expected to have full knowledge of the reason for the transfer.

FRAUDSTERS' PARADISE

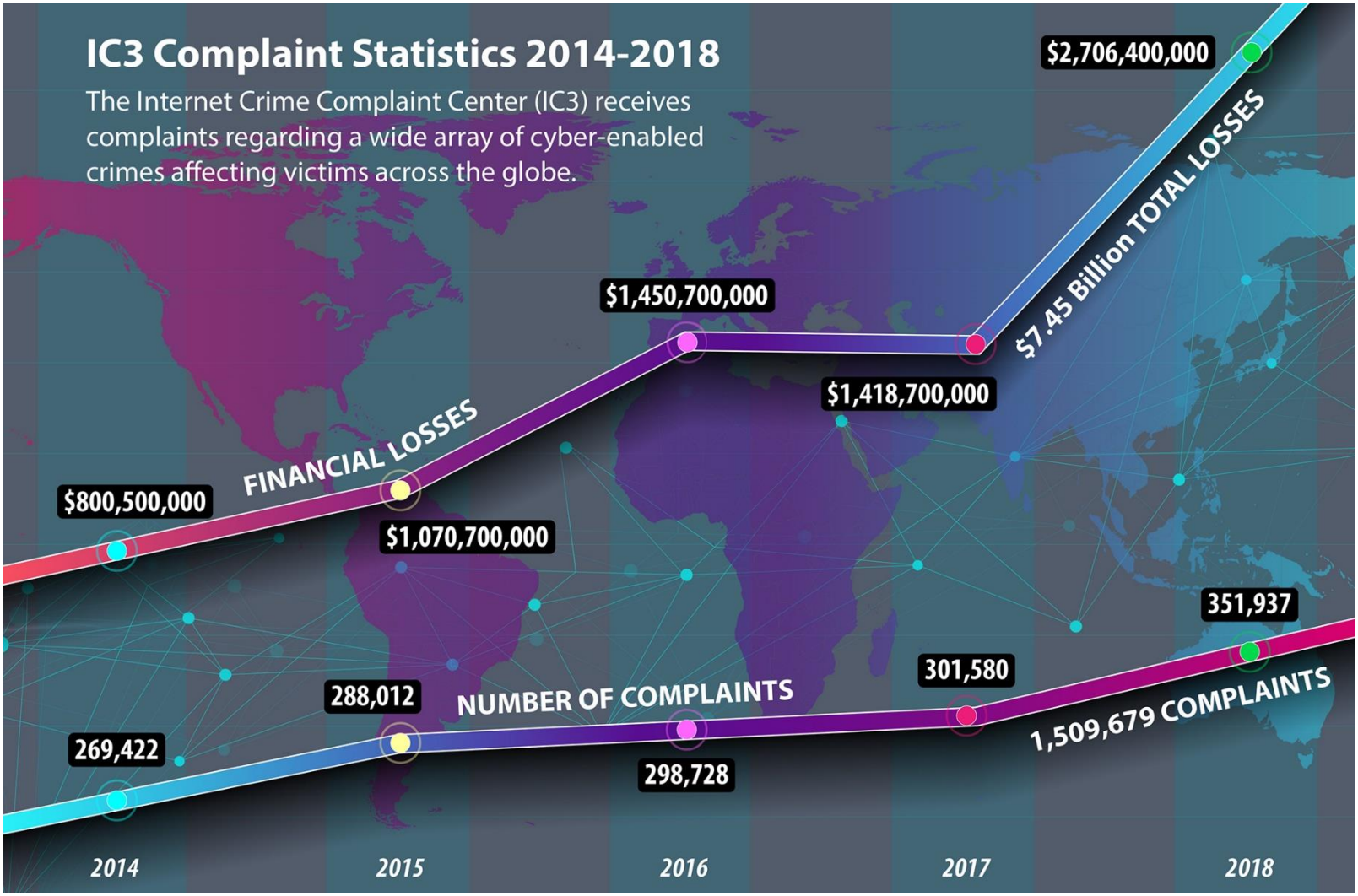


Trust that the person you're emailing is legitimate

Fear of annoying or upsetting the person you're emailing

Comfort in the company's controls

FBI STATS from Internet Crime Complaint Center (IC3)



FBI STATS from Internet Crime Complaint Center (IC3)

- USD $1.2 billion lost to Business Email Compromise in 2018, up from USD $675 million in 2017
- IC3 received 351,936 complaints in 2018 – an average of more than 900 every day.
- “Internet-enabled theft, fraud, and exploitation” financial losses in 2018 totaled USD $2.7 billion (USD $7.45 billion since 2014)
- Reports from every U.S. State and at least 131 countries
- Average losses are around $60K but the new “payroll diversion” scams causing average losses closer to $1MM

https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219

CLAIMS EXAMPLES

Please note that the types of claims we've seen with respect to SEF style events for the most part follow a very prescribed format – so there is a very good chance that some of the examples to follow will be familiar to you or may even sound like something you've experienced.

Any resemblance to scenarios you are aware of or you may have experienced is entirely coincidental. ALL of the figures and timing elements (if applicable) are fictional, but reflective of the size and scope of claims we've been seeing directly or have taken place in the industry.

CLAIMS EXAMPLES - 1

CFO receives an email from the CEO who is overseas on a business trip (legitimate trip)

Email states that the CEO has just become aware of a very serious problem and that they need to hire local counsel to start to address it

Instructs the CFO to wire $600K to a bank in Hong Kong for their counsel's retainer and advises that it needs to be kept top secret so that a formal press release can be made after consultation with their regulator – the CEO will stop by the CFO's office when he's back in the office next week

CLAIMS EXAMPLES - 2

A mid-level employee in the AP department receives a call from someone purporting to be from one of the company's largest suppliers. They quote the account number and ask that their banking information be updated as they've recently changed financial institutions.

Two months later the supplier calls to ask why their account is currently in arrears nearly $200K

The supplier confirms that they haven't changed financial institutions in over 10 years

CLAIMS EXAMPLES - 3

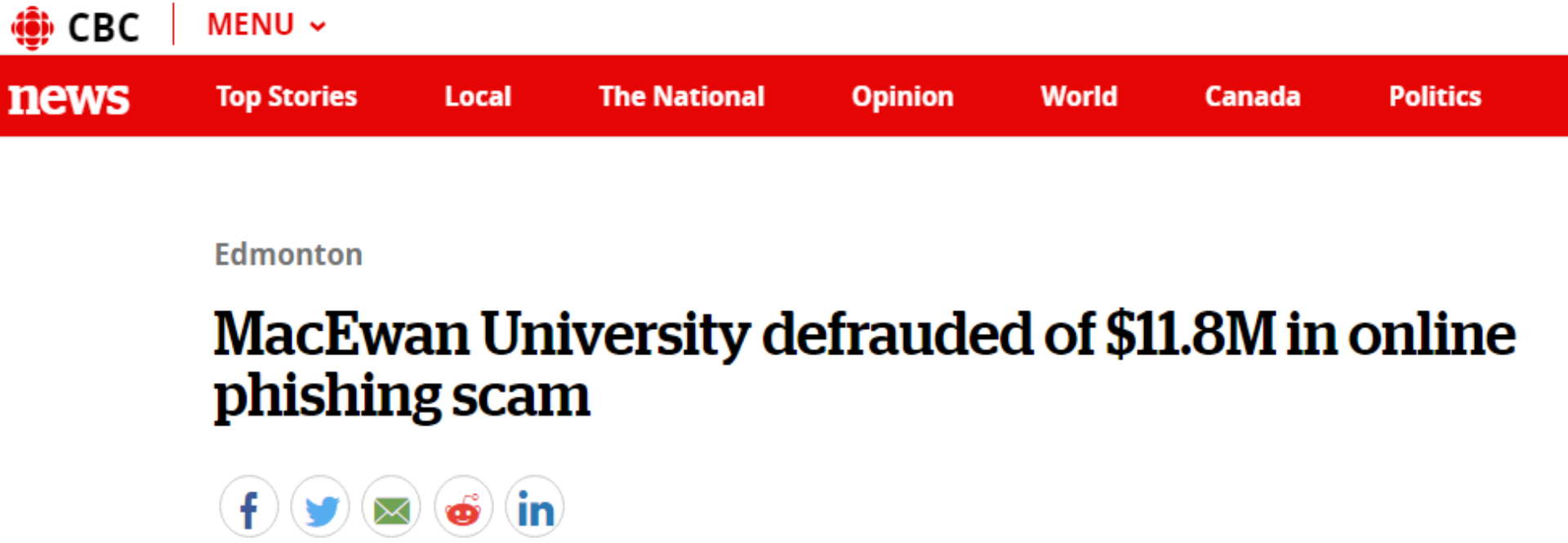
A lawyer acting on behalf of an offshore seller in a real estate deal closes a very challenging transaction

The lawyer gets an email from the client thanking them for their work, asks how their most recent family trip was, and asks that the proceeds be distributed slightly differently than what was originally laid out

The first $1.5MM are to be wired to a bank offshore (where the client is) and the balance is to be sent to the Canadian bank on file (they quote the account number)

When the client follows up for the remaining $1.5MM in three weeks, the fraud is uncovered

RIPPED FROM THE HEADLINES

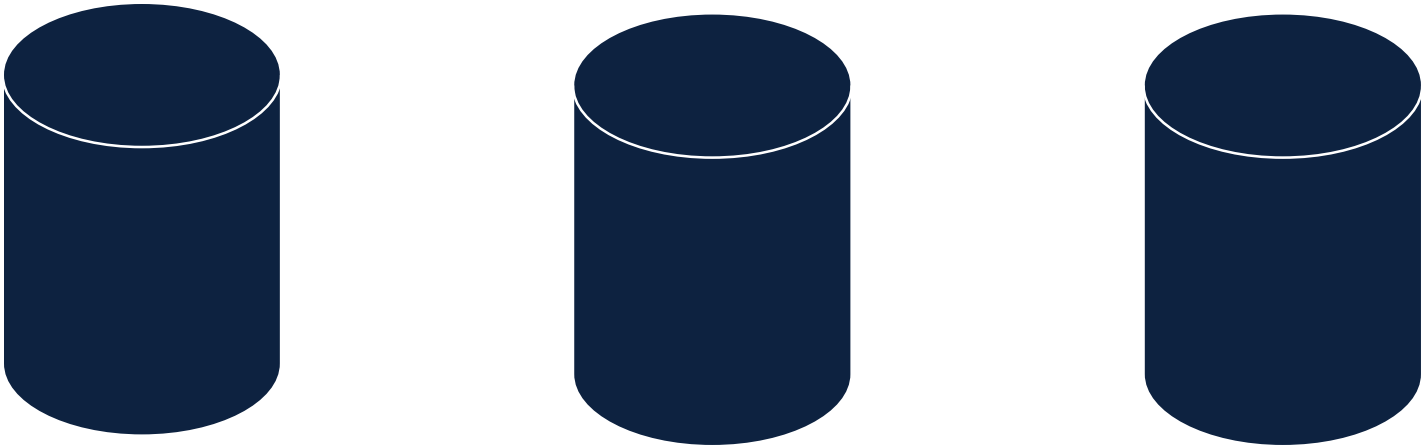


RIPPED FROM THE HEADLINES

SO WHAT NOW?

The Solution

AWARENESS PROTOCOLS TRAINING



COVERAGE CONCEPTS
AND
CASE LAW UPDATE

COMMON COVERAGE MISPERCEPTIONS

1. What does each Insuring Agreement cover (and not cover)?

- Computer Fraud
- Funds Transfer Fraud
- Social Engineering Fraud

2. Other Important Concepts

- Crime Coverage is Defined Perils Coverage
- Covered Property / Ownership Condition vs. Legal Liability
- Crime Coverage vs. Cyber Coverage

CASE LAW UPDATE

Computer Fraud

- No case law in Canada; intent is to cover hacking only

Funds Transfer Fraud

- *The Brick v. Chubb* (2017): supports insurers' interpretation on FTF, lends support on CF

Social Engineering Fraud / Fraudulently Induced Transfers

- *Dentons Canada LLP v. Trisura* (2018)
- *Posco Daewoo* (2018) – "reverse" SEF

QUESTIONS?

THANK YOU

theguarantee.com

Mark Abbott, Senior Fidelity Claims Analyst

mark.abbott@theguarantee.com

416-223-9880 ext. 11203

Chris McKibbin, Partner, Fidelity Practice Group, Blaney McMurtry LLP

cmckibbin@blaney.com

416.596.2899