SOCIAL ENGINEERING FRAUD

KNOW AND UNDERSTAND THE THREAT TO BETTER PROTECT YOUR ORGANIZATION

THE CYBER EXCHANGE
Kitchener, October 2, 2018

Joshua Laycock, National Fidelity Product Manager,
The Guarantee Co. 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 ?

Impersonation Fraud

Business Email Compromise (BEC)

CEO | Executive Impersonation

NOT A TYPE OF LOSS

What Social Engineering Fraud is and is not:

- Social Engineering Fraud is the fraudulent manipulation of an individual to induce them to say or do something they wouldn't otherwise say or do

- It is the *method* by which a fraud is initiated and executed, not the fraud itself

WHAT ARE THEIR OBJECTIVES?

Money! But different ways of getting it:

- **Information** – for the purposes of targeting Insured's money (*e.g.* Insured's banking credentials)
- **Information** – for the purposes of extracting value from it (*e.g.* selling it to third party)
- **Insured's Money Directly** –trying to induce fraudulent transfers, get or to induce Insured to change vendor bank info

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
  Compromised Email Accounts

ACTORS IMPERSONATED

Executives / Owners

Vendors

Customers / Clients

Third Party Intermediaries (Law Firms etc.)

OTHER COMMON THEMES

Often deals with an acquisition or large purchase order

Executive being impersonated is usually travelling

Destination account is usually China, East Asia or Eastern Europe

Organization typically has strong traditional financial controls

WHERE WE SEE COMPANIES GO WRONG

Tight process for vetting new customers / vendors – stops there

Over-reliance on dual-signature controls

Over-reliance on “Concentration of Authority”

Lack of employee-empowering transfer protocols

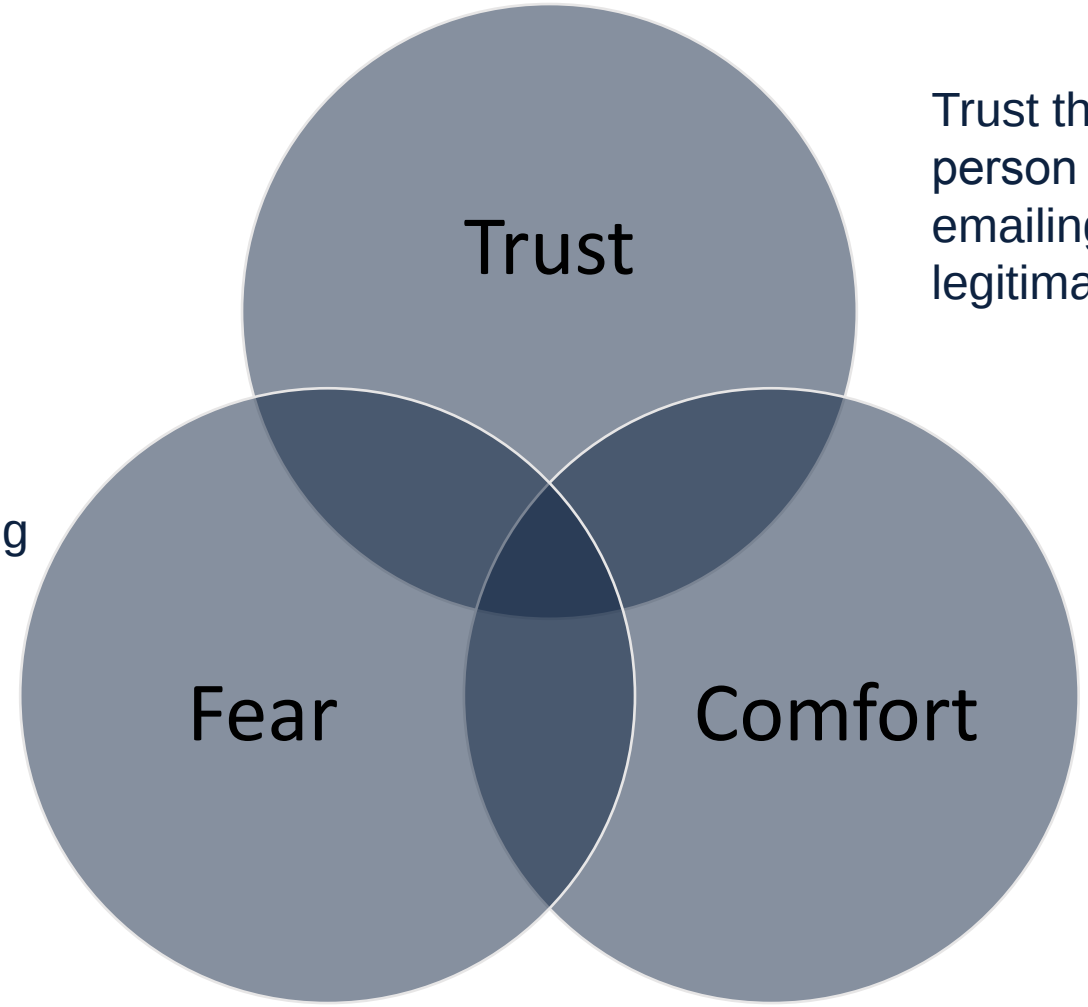
An email will never suffice as adequate evidence to move money.

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

FRAUSTERS' 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

+$5B worldwide lost to SEF e-mail scams – Oct 2013 to Dec 2016

Increase in activity of 2,370% Jan 2015 to Dec 2016

Reports from every U.S. State and at least 131 countries

Average losses are increasing every year – now around $90K

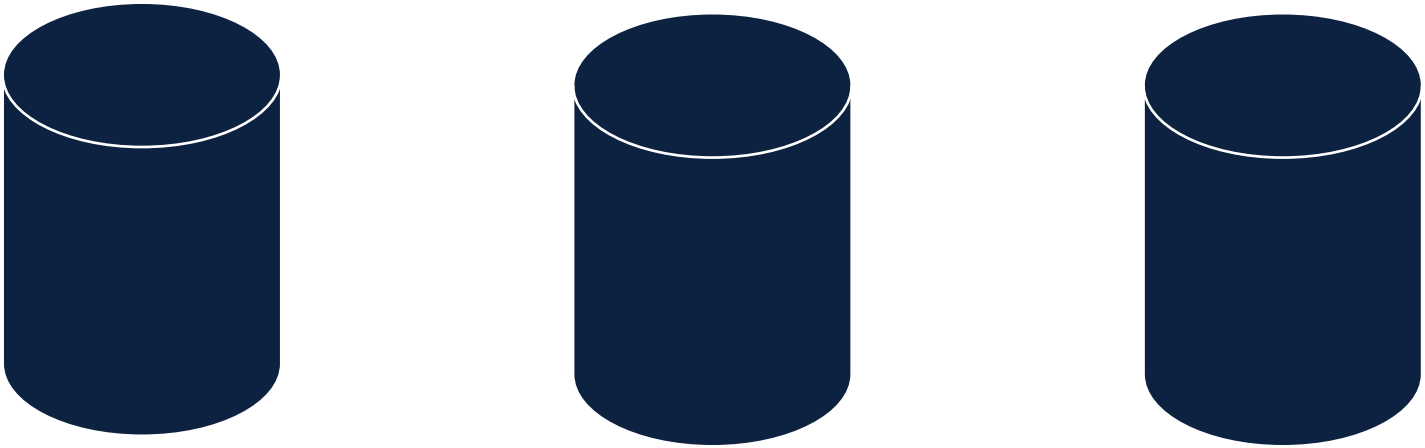
Source: https://www.ic3.gov/media/2017/170504.aspx

A VERY EFFICIENT FRAUD

- **Speed** – funds are typically cleared out of initial destination account within minutes
- **Anonymity** – attacks are carried out via email or phone, often from overseas
- **High ROI for fraudsters** – one successful attack can be worth millions of dollars

NEXT STEPS

AWARENESS PROTOCOLS TRAINING



RISK TRANSFER?

CRIME / FIDELITY POLICY

Depending on what happens, there may be coverage for you under a crime policy

“Computer Fraud” is intended to respond to situations where the direct fraudulent use of a computer (no human interaction) transfers money out of the Insured’s account (ie. a hacking event)

“Funds Transfer Fraud” is intended to respond when someone impersonates the Insured and causes their bank to transfer funds

“Fraudulently Induced Transfers” (formerly Social Engineering Fraud) is intended to respond when someone purports to be an authorized Vendor, Client or Employee and instructs an Employee of the Insured to transfer Money.

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 reflect the size and scope of claims we've been seeing directly or which 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

WHERE DOES THIS LEAVE US?

YOU ARE IN CONTROL

QUESTIONS?

Joshua Laycock, National Fidelity Product Manager

joshua.laycock@theguarantee.com

416-223-9880 ext. 11321

www.linkedin.com/in/joshualaycock

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

cmckibbin@blaney.com

416.596.2899

www.blaney.com

THANK YOU

theguarantee.com