DEMYSTIFYING SOCIAL ENGINEERING FRAUD
- UNDERWRITING, LEGAL AND CLAIMS PERSPECTIVES
Presenters

Joshua Laycock
National Fidelity Product Manager
Guarantee Company of North America

Brett Stephenson
Associate- Dolden Wallace Folick

Linda Van Den Brink
2 VP Specialty Claim- Travelers
Canada
• **What is Social Engineering Fraud (SEF)**
  ➢ Tactics, Trends, Why is it successful?

• **Coverage**
  ➢ Crime policy, Other insurance?

• **Reverse Social Engineering**
  ➢ What is it? Cases

• **Response and Recovery**

• **Risk Management**
  ➢ Prevention, Key Takeaways

• **Questions?**

• **Networking session**
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
Impersonation Fraud (Executive / Client / Vendor) is the main approach.

Examples include:

- **Email Spoofing** (look-alike email addresses designed to mislead)
  - employee@ProfessionalLiability.com vs. employee@ProfessionalLiability.com
  - Intent is to provide recipient with instructions that are not genuine
Common Tactics

- **Phishing / Spear Phishing / Whale Phishing**
  - Intent is to get the recipient to click on links or open malicious attachments

- **Unauthorized Access / Compromised Email Address**
  - An actual hack of a Computer System so fraudster can gain access to information a/o actual email application
What Do Fraudsters Want?

Money! But different ways of getting it:

- **Insured’s Money Directly** – business email compromise trying to induce fraudulent transfers or to induce Insured to change vendor bank info

- **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)
Common & Trending Scams

Fraudulently Induced Transfer Fraud Scams
- Vendor Impersonation
- Gift Card Scams
- Payroll Diversion

SEF Used For Other Purposes
- Credential harvesting
- Reputation Surfing
Why Does SEF Work So Well?

Fraudulent requests have similar, predictable traits:

• Create a sense of **urgency**

• Promise a **consequence** (good or bad)

• Expect **confidentiality** (executive impersonation)
Why Does SEF Work So Well?

• **Knowledge** of internal controls / deal info / personnel / vendor relationships

• Introduction of (sometimes very well-crafted) **third party participants** like fake “banker” or “lawyer”

• Involve **unusual transactions** (e.g. mergers, offshore acquisitions) that don’t have SOPs
Why Does SEF Work So Well?

- Trust that the person you are emailing is legitimate
- Comfort in the company’s controls
- Fear of annoying or upsetting the person you’re calling to verify

Professional Liability Underwriting Society
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
So where is the Coverage?

- Social Engineering Fraud as a broad concept takes advantage of natural tendencies and emotional reactions
- Classic non-computer example is a “tailgating attack”
- **Vendor Impersonation Frauds** and **CEO/Executive Impersonation Fraud**
- Potential coverage under a number of policies:
  - Crime, Fidelity, Cyber, CGL, Property, Professional Liability and Director and Officers
So where is the Coverage?

• Terminology
  – The names of Crime definitions can vary by jurisdiction, insurer, and even policy type
  – However, the underlying definitions are generally consistent
  – Can cause confusion when reading case law or summaries as the term “Computer Violation” in one case may or may not be equivalent to a “Computer Fraud” in another case
  – Check the language of the underlying policy
Coverage under Crime?

• History of the Fidelity/Crime Policy
  – 1900s – Fidelity Coverage for 1 employee
  – 1920s – Fidelity Coverage for multiple named employees
  – Fidelity / Crime coverage expanded over time to include corporate, forgery, theft in transit, etc
  – 2000s Funds Transfer Fraud and Computer Fraud introduced into Crime policies
    • Social Engineering Fraud using computers starts to gain attention of Insurers and Academics
Coverage Under Crime?

• **Computer Crime Insuring Agreement** *(typical)*:
  – Insurer will pay for **direct** loss … **directly** caused by ***Computer Fraud***

• **“Computer Fraud”** *(typical)*
  – Fraudulent entry of data or computer instructions into or within a Computer System by a third party **that causes the transfer** of property to a place outside the “premises”

Example: Hacker accesses corporate server to transfer money from Insured’s bank account.
Coverage under Crime?

- Not covered under **Computer Fraud**
  - *Apache Corporation v. Great American Insurance Company* (US Court of Appeal 5th Circuit)
    - Common Vendor Impersonation Fraud – money transferred in response to a fraudulent email
    - No direct causal link between the fraudulent emails and the transfer of funds
    - Computer use (i.e. email) was merely *incidental* to the scheme
    - Computer Fraud Insuring Agreement is not intended to cover all frauds
  - “*To interpret the computer-fraud Insuring Agreement as reaching any fraudulent scheme in which an email communication was part of the process would . . . convert the computer-fraud provision to one for general fraud.*”
Coverage under the Computer Fraud IA

- *Medidata Solutions, Inc. v. Federal Insurance Ins.* (US Court of Appeals for the 2nd Circuit)
- Fake Officer/CEO Impersonation Fraud
  - Transfer based on email of imposter company president
  - Fraudster embedded computer PHP script in spoof email
- The computer fraud IA
  - “the unlawful taking or the fraudulently induced transfer of Money . . . resulting from a Computer Violation.”
- Case turns on: (a) specific facts; and, (b) wording of the policy
Funds Transfer Fraud

- Funds Transfer Fraud IA:
  - *Insurer will pay the Insured Organization for the direct loss of Money contained in a Transfer Account* directly caused by *Funds Transfer Fraud*.

- Funds Transfer Fraud
  - losses caused by fraudulent instructions sent by a third party, *without* the Insured’s knowledge or consent.

- Example: Hacker cracks Insured’s system (e.g. Trojan) to obtain banking intel, and then independently sends wiring instructions
Coverage under Crime?

Not Covered under the Funds Transfer Fraud

The Brick Warehouse LP v. Chubb Insurance Company of Canada

• Vendor impersonation fraud
• Insured *knew* about the wire transfers, even if they were not aware of the fraud
• Court found in favour of the Insurer, confirming:
  – “fraudulent instructions” to a financial institution must be instructions which are fraudulent; rather than mistaken instructions
  – “Fraudulent instructions” must be caused by a third party/bad actor.
Coverage under Cyber

• History of **Cyber** Policy
  – Four typical components:
    • errors and omissions
    • media liability
    • network security
    • privacy.
  – Typical scenarios covered:
    • hacking and stolen Personal Identifying Information (PII)
    • hacking and encryption/destruction of data
    • third party privacy claims for lost PII
Coverage under Cyber

• **Notice** of an Impersonation Fraud under the Cyber potential coverage
  – Breach Coach and/or Forensic Investigators

• Theft of funds fraudulently transferred are generally **not** covered under the Cyber
  – Exclusion: the giving or surrendering of Money, Securities, or other Property…whether fraudulent or not.

• Computer Funds and Funds Transfer Fraud wording may be included in both the Cyber and Crime policies

- Lawyer victim of SEF.
- Duped into transferring $2.5 million to clear a mortgage on a client’s property to a fraudster’s account in Hong Kong.
- Application by Dentons for coverage for $1.7 million of firm’s net losses under the computer fraud rider (“CFR”) of its fidelity policy with Trisura.
CFR provides coverage for:

“Loss resulting from the wrongful abstraction of Money, Securities or other property which follows and is related to the use of any computer to fraudulently cause the transfer of such property from inside the Premises or a Banking Premises or similar recognized places of safe deposit to a person (other than a Messenger) or to a place outside those Premises.”
Condition XIII of the CFR:

“If there is any other valid and collectible insurance which would apply in the absence of such insuring agreement, the insurance under this bond shall apply only as excess insurance over such other insurance, provided the insurance shall not apply:

• to property which is separately described and enumerated and specifically insured in whole or in part by any other insurance, or

• to property otherwise insured unless such property is owned by the insured.”
Position of the parties

- **Dentons**: coverage based on the plain language of the CFR.
- **Trisura**: denied coverage:
  - Transfer of funds was not fraudulent; Dentons had declined SEF coverage;
  - Condition XIII not met:
    - Other insurance policies existed;
    - Funds were not “owned” by Dentons;
  - Exclusion (1)(f) applied.
Decision

• Procedural determination, no substantial issues decided on the motion.
• The court agreed with Trisura and ordered the application be converted into an declaratory action because a full factual matrix was required to make determination of all coverage issues for all insurers.
D&O Liability

- Allegations by shareholders/stakeholders of failure to adequately protect money or data.
- Compare shareholders derivative actions against boards involving high profile data security breaches:
  - Target (2014)
  - Wyndham Hotels (2014)
SEF Endorsements

• History: Social Engineering Coverage introduced US (2013) and CAN (2014)
• Various Insuring Agreement or Endorsement Wording – Typical:
  – The Insurer will pay the Insured Organization for the Insured Organization’s direct loss from the transferring, paying, or delivering of **Money** or **Securities**, directly caused by **Social Engineering Fraud**; …”
  – **Social Engineering Fraud** means the intentional misleading of an **Employee** by a person purporting to be: 1. a Vendor; 2. a Client; 3. an employee; or 4. an authorized Person, through the use of a **Communication**.
  – **Social Engineering Fraud** does not include **Computer Fraud** or **Funds Transfer Fraud**.
• A new risk and coverage issue for insurers
Reverse Social Engineering
Reverse Social Engineering

Concept

- Reverse Social Engineering ("RSE")
- In this technique, the attacker attempts to convince the victim to initiate the contact.
Posco Daewoo America Corp. v. Allnex USA, Inc. and Travelers Casualty and Surety Company of America (2018)

- Interesting twist on the usual SEF claim – in this case, it was the intended payee of the funds not the payor, which asserted a claim under its own crime policy (RSE).

- Facts
- Decision
- Take home
SEF Response and Recovery

• The likelihood of the recovery of funds lost to SEF is remote.
• Usually, by the time the fraud is discovered, the funds have disappeared and are not traceable.
• In such cases, victims of SEF must rely on insurance to recover or mitigate their losses.
• Critical to any recovery efforts is the immediate reporting by the Insured of the SEF to leverage resources of carriers.
• **Police:** in some cases, funds can be frozen by law enforcement and recovered.

• **Courts:** if identity of fraudster is known, legal remedies exist for recovery efforts:
  - **Mareva Injunction:** “freezing order” or “asset preservation order”.
  - Is there is a real risk of removal or dissipation of assets by the fraudster?
  - **Sibley & Associates LP v. Ross** – Court ordered the financial institutions to surrender information regarding the transactions of the account pertaining to the fraud.
• **World-Wide Mareva Injunction:**

• **Anton Pillar Order:** “search order” or “evidence preservation order”. Akin to a civil search warrant. Eg) to gain entry to a fraudster’s premises (without notice) to search and seize evidence.
Legal remedies also exist if identity of fraudster is unknown:

- **Norwich Order**: pre-action discovery order – when critical information is unknown but necessary to determine whether litigation should be commenced.

- Eg) when you have some information that might enable a TP to provide information to identify the fraudster (bank is in receipt of funds procured by fraud).
How Can Insureds Prevent SEF?

- Technology can leave a false sense of security
- Awareness
- Set the correct tone from the top
- Educate and empower employees
- Stay current
• Active dialogue with customers/vendors/underwriters about fraud risks
• Implement mandatory “out of channel” verification protocols
• Create a blend of rules-based and principles-based protections
• Don’t be nostalgic about the way business “used to be” conducted
Key Takeaways

• The threat is real – not a “flavour of the month”

• A robust risk-transfer portfolio is necessary

• The threat is preventable

• Communication is key
PLUSB Canada Social Engineering Seminar in Vancouver
Demystifying Social Engineering - Underwriting, Legal and Claims perspectives

Wednesday, May 22, 2019 | 3:30 - 7:00 p.m.
3:30 - Registration / Check-in, 4:00 - 5:30 - Social Engineering Seminar,
5:30 - 7:00 - Mixer with hors d’oeuvres & drinks

Gain a deeper understanding of Social Engineering exposures from the underwriting, claims, legal and risk management perspectives. CE pending approval in British Columbia.

Terminal City Club
837 West Hastings Street, Vancouver | BC

SPEAKERS

Joshua Laycock, GCNA
Jill Shore TBC, Dolden Wallace Folick LLP
Linda Van Den Brink, Travelers

Your Investment: Member $35 | Non-member $65

REGISTER ONLINE

Thank You
2019
Annual Sponsors

NATIONAL

Allianz Global Corporate & Specialty Americas
Aon
AXA XL
AXIS Reinsurance Company (Canada)
Beazley Canada Ltd.
Berkshire Hathaway Specialty Insurance
Charles Taylor Adjusting
Chubb
Clyde & Co Canada LLP
CNA

ENCON Group Inc.
FCL LLP
Gowling WLG (Canada) LLP
Intact
Liberty Mutual Canada
Sovereign Insurance
Strategic Underwriting Managers Inc.
The Guarantee Company of North America
Travelers Bond & Financial Products
Trisura Guarantee Insurance Company

GOLD

Brownlee LLP
Dolden Wallace Folick LLP
Merlin Underwriting Inc.

Norton Rose Fulbright
Zurich
Chapter C.E. Filing Form
(Send to PLUS at least 75 days prior to the program.)

PLUS Chapter: Western Canada Submitted: March 25\textsuperscript{th}, 2019
Event Coordinator: Ian Breheny Course Date: May 22\textsuperscript{nd}, 2019
Course Title: Demystifying Social Engineering- Underwriting, Legal and Claims perspectives
List States in which to File:
British Columbia, Canada

Course Objectives: Give a deep understanding of Social Engineering exposures. Presentations from a claim and underwriting perspective as well as panel discussion that will also bring in a legal and risk management perspective.

Brief Description:
25-30 minute Underwriting Presentation- Joshua Laycock- Crime Product Lead, Guarantee Company Canada

25-30 minute Claim Presentation- Linda Van Den Brink- Specialty Insurance Claim Lead Travelers Canada

30 minute Panel Discussion- Moderator- Ian Breheny Vice President Specialty Insurance, Travelers Canada. Panel Participants- Joshua Layock (Guarantee), Linda Van Den Brink (Travelers), Jill Shore (DWF).