SOCIAL ENGINEERING FRAUD

SO … IS IT COVERED?
Joshua Laycock
National Fidelity Product Manager
Guarantee Company of North America

Chris McKibbin
Partner, Fidelity Practice Group
Blaney McMurtry LLP

Greg Markell
President & CEO
Ridge Canada Cyber Solutions Inc.
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** a.k.a. Business Email Compromise (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

• Phony Client Scam vs. Lawyer
  – Intent is to trick lawyer into “recovering” fraudulent settlement and then wiring trust funds to fraudster

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

• Unauthorized Access
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).
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

Fear

Comfort

Trust that the person you are emailing is legitimate

Fear of annoying or upsetting the person you’re calling to verify

Comfort in the company’s controls
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
Coverage may be found in a few places:

**Commercial Crime Policy**

- **Fraudulent Instruction Coverage** (a.k.a. SEF coverage a.k.a. Fraudulently Induced Transfer coverage)
- **Not Computer Crime** (*Apache Corp. v. Great American Ins. Co.*)
- **Not Forgery or Alteration** (*Taylor & Lieberman v. Federal Ins. Co.*)
- **Typically not Funds Transfer Fraud**
So where is the Coverage?

Cyber Policy

- Sub-limits for SEF, along with an extension for Computer Fraud
- Cyber policy can respond in the event of a liability trigger... but what are the triggers under your Cyber policy???
- Difference between “dollars” and “data”
Professional Liability (E&O)
• Client Impersonation vs. professional

Directors’ and Officers’ Liability
• Allegations by shareholders/stakeholders of failure to adequately protect money or data
• Compare derivative actions involving data security breaches:
  • Target (2014)
  • Wyndham Hotels (2014)
  • Home Depot (2015)
How Can Insureds Prevent SEF?

- Technological solutions:
  - Advanced email screening, advanced attachment scanning, DMARC
- Technology can leave a false sense of security
- Awareness
- Set the correct tone from the top
- Educate and empower employees
- Stay current
How Can Insureds Prevent SEF?

- 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
Links to Case Studies

• Joshua’s article:  


• Taylor & Lieberman:  