Crime Insurance

Employee Theft and Social Engineering Fraud

May 2, 2025

TRAVELERS

Important Note

Travelers Insurance Company of Canada , The Dominion of Canada General Insurance Company and St. Paul Fire and Marine Insurance Company (Canada Branch) are the Canadian licensed insurers known as Travelers Canada.

This material is only for the informational use of the reader. Information contained herein is not intended as, and does not constitute, legal or professional advice. Travelers Canada has shared this material with you solely to understand our perspectives and strategies so that you may better service our mutual customers and prospects. You may not use this material for any other purpose, share it with colleagues who are not working on or with Travelers Canada customers or prospects, or distribute to anyone outside your company without our advanced written consent. Under no circumstances may you share this material with any competitor of Travelers Canada or with anyone acting on behalf of a Travelers Canada competitor. As it respects this presentation, any materials or information (oral or written) provided either during the course of this presentation or subsequent, shall be kept confidential. Further, it does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers Canada. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and provincial regulations. In all cases, risk selection follows applicable provincial regulations. In Ontario and Newfoundland and Labrador, filed underwriting rules must be followed. The applicable provincial Take All Comers, Unfair or Deceptive Acts or Practices rules and regulations, as well as abstention from prohibited risk selection practices, must also be followed.

Your Hosts

Savannah Ferguson

Brayden Cline

Emily Dikranian

Today's Topics

- What is Crime insurance?
- Why does Employee Theft Occur?
- What is Social Engineering Fraud?
- Crime Insurance Policy Attributes
- Unique Exposures
- Sources of Loss from Employee Theft
- Sources of Loss from Social Engineering Fraud
- Loss Examples

What is Crime Insurance?

- A packaged insurance policy offering protection for loss arising directly from Fidelity, Burglary, Robbery, Forgery, Computer Crime, Funds Transfer Fraud.
- Employee dishonesty insurance is the main insuring agreement and the main criminal threat to organizations.
- “Third Party Crime”, or “Employee Theft of Client Property” is a subset of Fidelity Coverage that occurs when the loss is *sustained by a client* of the organization.

Crime Insurance Policy Attributes

- First party loss (except for Third Party Crime)
- Single Loss Limit versus Aggregate Limit
- Loss Discovered versus Loss Sustained
- Named perils, not “all risk” or “all perils”

Why Does Employee Theft Occur?

- Opportunity: too much access or control over money or financial systems
- Need or Greed: financial pressures
- False Sense of Entitlement: the feeling that an individual deserves more than the organization offers them

Sources of Loss from Employee Theft

- It is important to remember that large employee theft losses are more often a series of small related transactions (“death by a thousand cuts”) than single large transactions.
- Organizations with greater complexity have higher exposure. As do organizations with high volumes of transactions, employees, vendors, or clients.
- Some examples include: skimming, billing schemes / kickbacks, payroll schemes, expense reimbursement schemes, cheque tampering, inventory theft.
- Insurer application questions tell a lot about where the losses come from.

There are typically several questions relating to segregations of duties, dual authorizations, and regular reviews. If one individual has too much authority, he or she can perform transactions without secondary approval or oversight.

Invoicing Scheme

Two employees of a large municipality orchestrated a false invoicing scheme. Employee 1 led procurement. They directed city business to a private rental sign company owned by a relative. Employee 2 approved the false and unsupported invoices for payment by cheque. Employee 2 received “gifts” from the private company. Approximately $1.6M.

Source: Cook, D., 2020, City of Edmonton alleges $1.6 million stolen in invoicing scheme by two city employees

Stolen Products

An employee of a Canadian retailer stole $2M in laptops and electronics from his employer over a 5-year period. The employee stole the products and sold them online, making $750K-$1M in personal profit. It allegedly started because he was unhappy with the company.

Source: Proctor, J., 2024, 'Staggering' $2 million theft lands London Drugs employee in jail

Too Much Authority

Chief Administrative Officer of a Manitoba municipality allegedly made 33 fraudulent transfers of funds for a total of $515K, falsified bank statements, and faking a cyber attack to cover up the theft.

Source: Shebahkeget, O., 2003, Former CAO accused of faking cyberattack to cover theft of $500K from Manitoba municipality

Unique Exposures

- Art or valuable collectibles
- Care, custody, control of client property or assets
- Commission sales
- Commodities
- **Diversified businesses**
- High cash exposure
- High portable inventory
- Narcotics / opioids / cannabis / pharmaceutical products
- Precious metals/gemstones
- Proprietary trading activity
- Scrap metal
- Warehousing / storage
- **Many locations** or foreign locations
- Financial distress

What is Social Engineering?

- Broadly, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Sources of Losses for Social Engineering Fraud

- Unlike Employee Theft, Social Engineering Fraud originates from outside of the organization.
- Usually, perpetrators purport to be a client, vendor, employee, or person of authority. They attempt to exploit the human psychology to manipulate people to divulge sensitive information or perform unauthorized actions.
- Phishing emails, phone calls, physical infiltration
- Tailored attacks – impersonation of trusted individuals (mimic CEO, video impersonations, etc.)
- AI is poised to enhance capabilities of Cyber criminals
- Supply chain attacks – compromise a third party to gain access to a corporation's network or information

Banking Information Change

A tech company placed an order for approximately $200,000 in furniture for their new office. The original vendor provided the company with an invoice payable within 30 days of the sale, as well as their banking coordinates. A month later, the supposed vendor reached out to inform the company that their banking coordinates changed. They also attached the same invoice and requested the company pay 50% of the purchase price. The first payment was made. A week later, the company received another notice from the purported vendor with different banking instructions and their final account. The company paid the final invoice. A few weeks later, the actual vendor reached out to inquire on payment status as the original 30 days have passed. Once the company started investigating as to why the vendor did not receive payment, they noticed that the email address of the supposed vendor contained a small error. Payment was made to a threat actor, and the company fell victim to a social engineering fraud scheme.

Mock Invoice

A hardware store placed an order with a supplier they typically use. A few weeks after the order was placed, they received an invoice for payment by email. The email contained different banking instructions than the ones the company had on file, but the invoice was legitimate. An employee in the hardware store's finance department called the vendor at their known number to inquire about the change in banking information. The vendor supposedly confirmed that they did not change their banking information. Despite this confirmation, the employee sent the funds to the threat actor by mistake. Coverage was afforded under the SEF endorsement.

Imposter Manager

An employee in a municipality's accounts payable department received an email from his purported boss attaching an invoice for payment. The invoice came from a vendor the employee was not familiar with. The employee replied to the email asking for clarification, received a satisfactory response, and subsequently issued payment to this new vendor for approximately $100,000. Later that day, he ran into his boss in person and informed her that the payment was made, as requested. His boss was confused. They investigated and realized there was a slight change in the boss's email address that the employee did not catch before the funds were sent.

THANK YOU