

We provide effective solutions to **protect the assets** of our Insureds.



Crime Insurance 101: The ABCs of Fidelity

Why Crime Insurance?

- **Organizations lose 5% of their annual revenues to fraud**
- **Projected total global fraud loss of nearly \$4.0 trillion**



The Victims of Fraud

- **Small organizations (fewer than 100 employees) are disproportionately victimized by fraud**
 - These organizations typically have fewer resources to both prevent and recover from a fraud
 - They often require an increased level of trust in employees due to a lower ability to implement robust anti-fraud controls
- **Industries most commonly victimized include:**
 - Banking and Financial Services
 - Manufacturing
 - Government and Public Administration Sectors
- **Classifications of Organizations**
 - Private Companies Victimized More Frequently And Are Victim To The Most Costliest Schemes



Profile of a Fraudster – Fraud Triangle

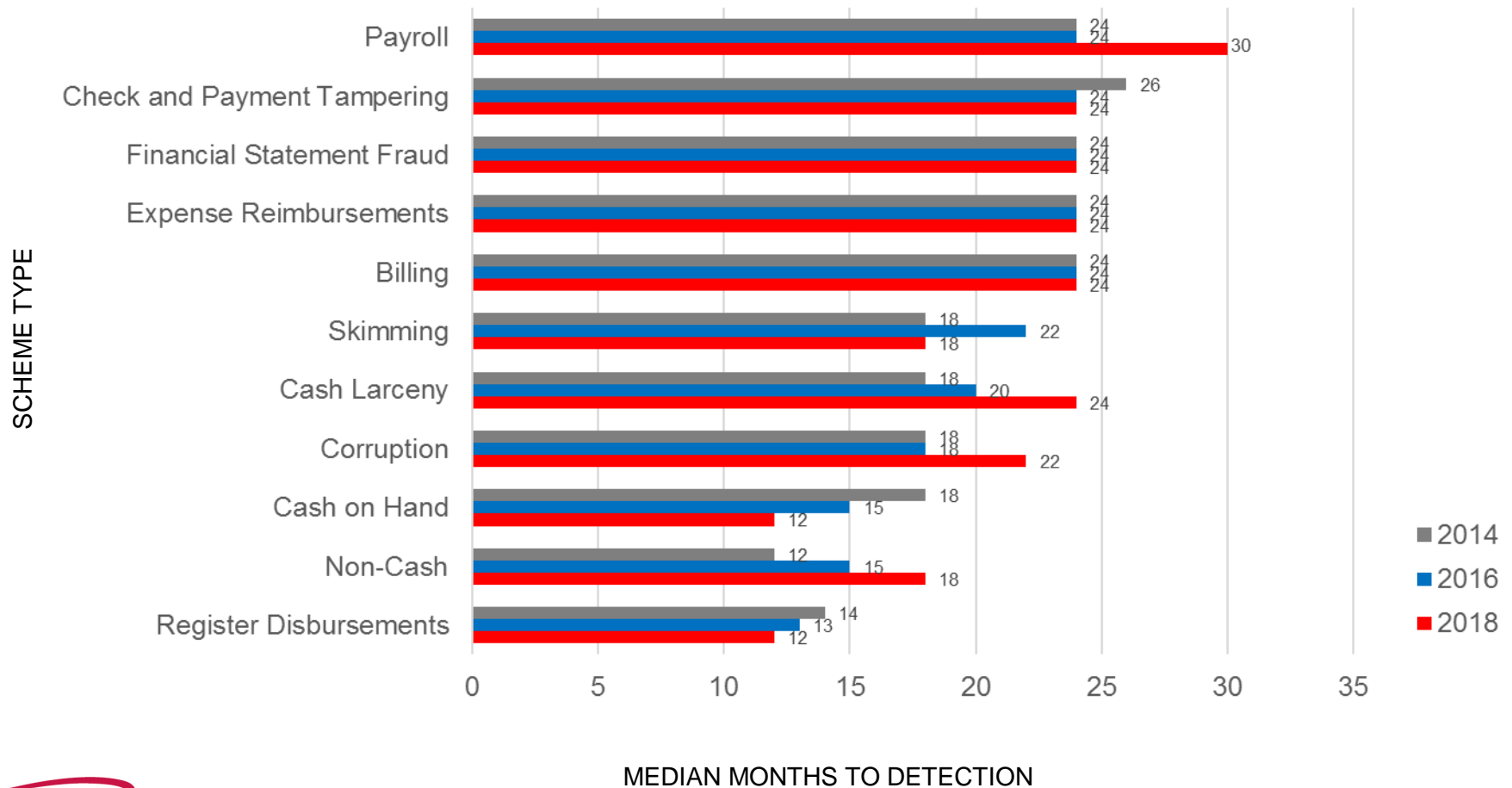


Profile of a Fraudster

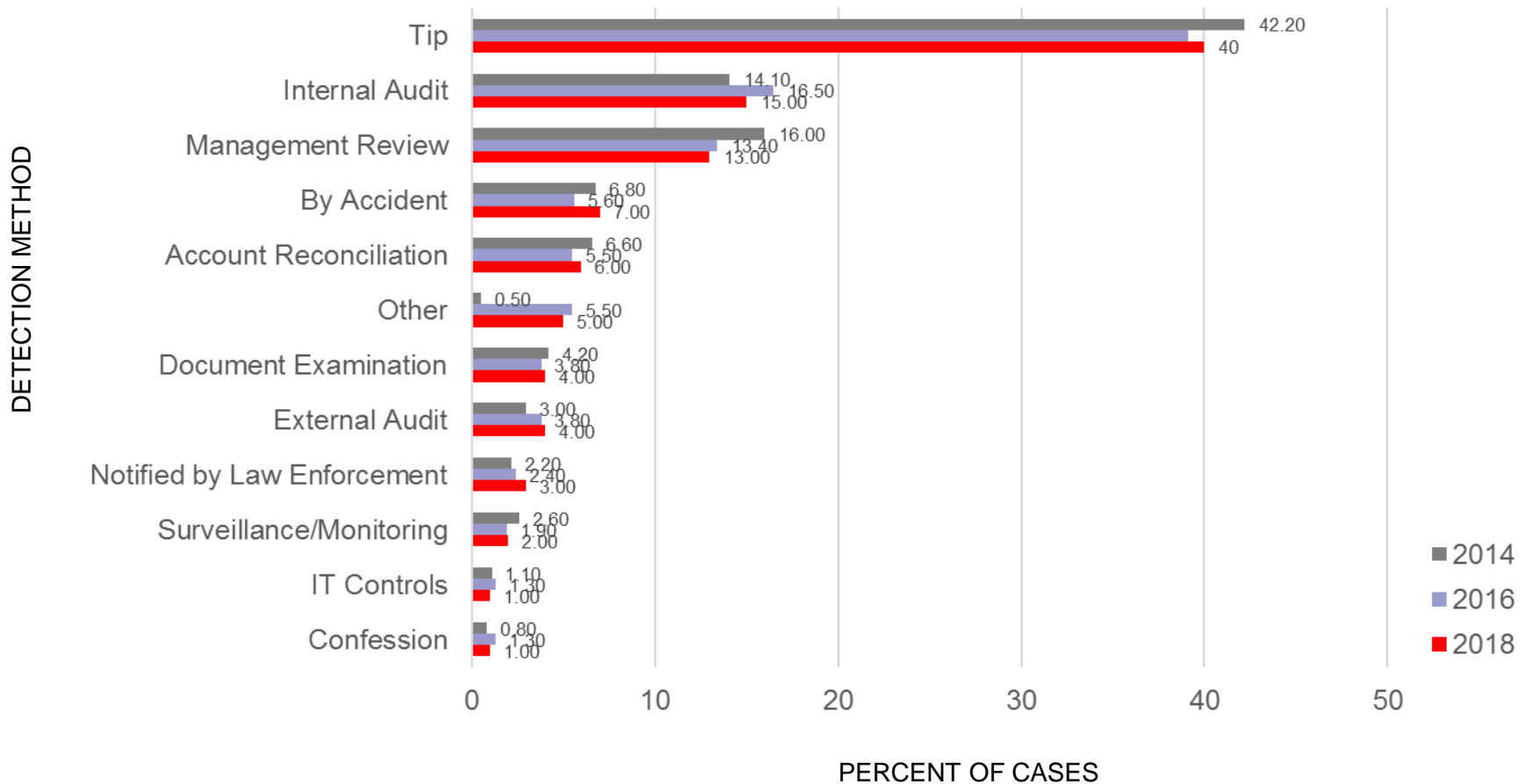
By the Numbers...

- **53% of perpetrators hold the position of Manager or Owner/Executive**
- **Employees with 10 or more years of tenure caused the costliest losses**
- **89% have never been charged or convicted of a prior offense**
- **69% are male and 31% are female**
- **47% possess at least a bachelor's degree**
- **61% possess a bachelor's degree or postgraduate degree**
- **The largest median losses were caused by fraudsters in the oldest age ranges (56 years and older)**
- **Largest number of cases come from members of both the Accounting (14%) and Operations (14%) Departments, while the largest median loss comes from members of Executive/Upper Management (\$729,000)**
- **Most are risk takers, extroverts, decisive, career or success-oriented individuals**
- **Most act alone and are motivated by need, greed, addiction problems, revenge, or debt/financial issues**

Median Duration of Fraud Based on Scheme Type



Initial Detection of Occupational Frauds



Common Types of Losses

■ Vendor Fraud

- ☐ Billing Schemes
- ☐ Ghost Vendors
- ☐ Kickbacks
- ☐ Largest and Longest
Current Running Trend in
Crime Losses

■ Foreign Losses

■ Social Engineering

■ Check Schemes

■ Payroll Schemes

- ☐ Ghost Employees
- ☐ Improper Overtime

■ Expense Reimbursements

■ Valuable Metals

- ☐ Copper Wire & Piping
- ☐ Catalytic Converters

Control Weaknesses That Contribute to Fraud

- **Lack of Internal Controls**
- **Override of Existing Internal Controls**
- **Lack of Management Review**
- **Poor Tone at the Top**
- **Lack of Competent Personnel in Oversight Roles**
- **Lack Independent Checks/Audits**
- **Lack of Employee Fraud Education**
- **Lack of Clear Lines of Authority**
- **Lack of Fraud Reporting Mechanisms**

Suggested Corrective Measures to Mitigate Fraud

- **Code of Conduct**
- **External audit of Financial Statements**
- **Internal Audit Department**
- **Management certification of Financial Statements**
- **External Audit of internal controls over financial reporting**
- **Management Review**
- **Hotline**
- **Anti-Fraud Policy**
- **Fraud Training for Employees**
- **Fraud Training for managers/executives**
- **Dedicated fraud department, function, or team**
- **Surprise Audits**
- **Job rotation/mandatory vacation**

Key Thoughts

- **Remember most fraudsters have done this before**
 - ☐ **Pre-employment Screening is critical**
 - ☐ **Vendor due diligence is essential**
- **Remember many frauds go unreported**
 - ☐ **Fear of bad publicity**
 - ☐ **Internal discipline sufficient**
 - ☐ **Costliness**
- **Most criminals have more time & money than we do to combat the problems**
- **Complacency is one of our biggest enemies**

Commercial Crime Coverage

SFAA Crime Protection Policy (Ed. 04/12)

- **Insuring Agreement 1 – Employee Dishonesty**
- **Insuring Agreement 2 – Forgery or Alteration**
- **Insuring Agreement 3 – Inside the Premises**
- **Insuring Agreement 4 – Outside the Premises**
- **Insuring Agreement 5 – Computer Fraud**
- **Insuring Agreement 6 – Money Orders & Counterfeit Paper Currency**
- **Insuring Agreement 7 – Loss of Clients' Property**
- **Insuring Agreement 8 – Funds Transfer Fraud**

(1) Employee Dishonesty

Property Covered

- **Money, Securities and Other Property**



Causes of Loss Insured Against

- **Dishonest acts committed by an employee with the manifest intent to:**
 - ☐ **Cause you to sustain loss**
and
 - ☐ **Obtain financial benefit**

(2) Forgery or Alteration

Property Covered

- Negotiable instruments such as checks, drafts, promissory notes, or similar written promises, orders or directions to pay a sum certain in money that are made by you or someone acting on your behalf
- This coverage applies only to your checks, not incoming checks

Causes of Loss Insured Against

- Forgery or alteration of covered instruments
- Suit against the insured for sums the insured becomes legally obligated to pay





(3) Inside the Premises

Property Covered

- Money and securities inside the premises or banking premises
- Other property inside the premises
- Other property inside the premises in a safe or vault
- Damage to the premises or its exterior, or, damage to a locked safe, vault, cash register, cash box or cash drawer located in the premises



Causes of Loss Insured Against

- Theft, disappearance or destruction
- Actual or attempted robbery of a custodian
- Actual or attempted safe burglary
- Actual or attempted theft, robbery or safe burglary, if you are the owner of the premises or are liable for damage to it

(4) Outside the Premises

Property Covered

- Money and securities outside the premises while in the care and custody of a messenger or armored motor vehicle company
- Other property outside the premises while in the care and custody of a messenger or armored motor vehicle company



Causes of Loss Insured Against

- Theft, disappearance or destruction
- Actual or attempted robbery



(5) Computer Fraud

Property Covered

- Money and securities and other property

Causes of Loss Insured Against

- Fraudulent use of a computer to transfer property from inside the premises or banking premises to a person outside those premises or to a place outside those premises



(6) Money Orders and Counterfeit Paper Currency

Property Covered

- Invalid money orders
- Counterfeit U.S. or Canadian paper currency

Causes of Loss Insured Against

- Acceptance in good faith, in exchange for merchandise, invalid money orders or counterfeit paper currency



(7) Loss of Clients' Property

Property Covered

- Money, securities and other property belonging to clients

Causes of Loss Insured Against

- Dishonest acts committed by an identified employee with the manifest intent to:
 - ☐ Cause your client to sustain loss
 - ☐ Obtain financial benefit



(8) Funds Transfer Fraud

Property Covered

- Funds (money and securities)



Causes of Loss Insured Against

- Fraudulent instruction directing financial institution to transfer, pay, or deliver funds from your transfer account

Policy Exclusions

- **Acts of Owners**
- **Acts of Employees (except for Insuring Agreement 1)**
- **Indirect Loss**
- **Inventory Shortages (Applies to Insuring Agreements 1 and 5)**

Common Policy Extensions

- **Credit Card Forgery**
 - **Part of Insuring Agreement 2 – Forgery or Alteration**
 - **Credit, Debit and Charge Cards issued to the Insured or any employee(s)**
 - **Does not cover customer credit cards**
- **Definition of Employee**
 - **Non-Compensated Officers, Directors & Trustees, Volunteer Workers Other Than Funds Solicitors, Students and Interns**
- **Omnibus Named Insured Wording**
 - **Majority-owned corporate entities (greater than 50%) & Employee Benefit Plans subject to ERISA Bonding Requirements**
- **Terminated Employees**
 - **Allows the Insured time to “Close the windows and lock the doors” after an employee leaves the company under any circumstances**
- **Revision to Inventory Shortage**

Common Questions & Issues

- **Manifest Intent (Employee Dishonesty) vs. Employee Theft**
 - ☐ Is there really a significant difference between the two?
- **Loss of Clients' Property (Third Party Coverage)**
 - ☐ Does my client need this coverage and what does it cover?
- **Is Electronic Data or Customer Information Covered?**
 - ☐ My clients' customer's credit card numbers were stolen and used, is there coverage available for this?
- **Employee Benefit Plans ERISA Coverage Requirements**
 - ☐ Where's the coverage and what limit does my client need to carry?

Evaluating a Risk

■ What we consider when underwriting a risk:

- ☐ Mainform Application vs Renewal Application
- ☐ Employee Screening – credit, background checks, prior acts of dishonesty
- ☐ Authorized Vendor List & Vendor Background Checks
- ☐ Separation of Duties
- ☐ Countersignature of Checks
- ☐ CPA Audit
- ☐ Internal Audit
- ☐ Are foreign operations/locations subject to the same controls as domestic operations/locations?
- ☐ Is there a valuable metals exposure?
- ☐ Loss History

Evaluating a Risk – Loss History

- **Loss details including size of loss, length of occurrence and details of how the loss occurred and how it was discovered**
- **Corrective measures**
 - ☐ **The Insured terminated the employee. Problem solved, right?**
 - ☐ **What did the Insured do to prevent this from happening again?**
 - ☐ **Were internal controls scrutinized and improved across the entire organization?**

Loss Examples

- **Lack of Internal Controls at a Hospital**

A hospital with revenues of over \$200 million per year could have afforded to develop good internal controls but did not do so. When the accounting office issued checks, the first two checks placed into the printer were used only to start the runs. They were blank when they came out of the printer. The accounting manager took those two checks, typed his name as payee, wrote the checks for several thousand dollars, and deposited the checks into this personal account. He then ran the checks through the check-signing machine, which would place one officer's name on the checks. The amounts were small enough that two signatures were not required. The accounting manager voided the check numbers in the accounts payable check log.

The manager was also in charge of reconciling the hospital's bank statement. He could remove the canceled checks, discard them, and make journal entries to cover the amount of the checks and the reconciliation balance to the general ledger. The amounts were small compared to the hospital's revenues to make it unlikely that an audit could trace the money. This continued for nine years with the loss exceeding \$2,000,000.

Loss Examples

■ Dual Controls Must Be Enforced

A twenty-year hospital employee stole \$2,400,000 over two years by creating false accounts payable checks to fictitious hospital patients. She created fictitious patient names for accounts payable forms for patient refunds. She requested that the checks be brought back to her. She forged the patients' names on the back of the check, signed her own name, and deposited the checks in a bank account. The investigation found that a supervisor reviewed the checks. Some of the checks were initialed by the supervisor, but the supervisor never questioned the employee, who was well liked in the hospital's accounting and finance office.

■ A Case for Mandatory Vacations

One employee successfully "lapped" cash receipts for twenty-nine years at a cost of over \$9,500,000. Extending over the employee's entire career with the company, the scheme was discovered only when the employee retired. The employee had access both to cash receipts and to the records establishing accountability for the receipts. The employee withheld checks from accounts receivable collections. He then took cash from later collections and covered the theft by crediting the previously withheld checks to the accounts of the customers who had paid cash. Later receipts were credited to the accounts of the customers who had sent in the first batch of checks, and so on.

Lapping requires continuous close attention. If misapplied receipts are not covered quickly, the customer receives a past-due notice and complains, and the scheme is undone. The thief must keep track of normal delinquencies and be prepared to deal with plant closings, strikes, market problems, and business disruptions of all kinds. This trusted employee was noted for his diligence. He never required help and never took a long vacation.

Loss Examples

■ Billing Scheme

A warehouse foreman and a parts ordering clerk conspired to purchase approximately \$3,000,000 of nonexistent supplies. The parts ordering clerk would initiate the false transactions by obtaining approval to place orders for parts he claimed were needed. The orders were then sent to a vendor who, acting in conjunction with the two employee fraudsters, prepared false invoices that were sent to the victim company. Meanwhile, the warehouse foreman verifies receipt of the fictitious shipments of the incoming supplies. The perpetrators were therefore able to compile complete vouchers for the fraudulent purchases without overstepping their normal duties.

■ Vendor Fraud Scheme

A department director was in charge of purchasing computer equipment. Because of his expertise on the subject and his high standing within the company, he was unsupervised in this task. The director set up a shell company in another state and bought used computers through the shell company. He then turned around and sold them to his employer at a greatly exaggerated price. The money from the victim company's first installment on the computers was used to pay the shell company's debts to the real vendors. Subsequent payments were profits for the bogus company. The scheme cost the victim company over \$5 million.



Social Engineering Fundamentals

In the context of information security, human-based SE, otherwise known as “human hacking” is defined as the art of influencing people to disclose information and to get them to act inappropriately.

Various forms of communication used:

1. **Email**
2. **Internet**
3. **Telephone**
4. **Face-to-Face interaction**

SE can take many different forms but security experts have recognized that most scams follow a four-stage method, **Information Gathering, Relationship Development, Exploitation, and Execution.**



Social Engineering Fundamentals

Strategies social engineers use for gathering information from their targets:

1. **Impersonation:** very common form of deception may involve an attacker using a believable reason to impersonate an authority, pretend to be a fellow employee, IT rep, or vendor in order to gather sensitive info.
2. **Phishing/Spearphishing:** This form can come in the form of a phone call or email from someone claiming to be in a position of authority asking for sensitive info. This method can include sending emails to organizational contacts that contain malware designed to compromise computer systems to capture private credentials.



Psychology of Social Engineering

- 1. Motivation behind Social Engineering Attack**
- 2. Exploitation**
- 3. The Art of Deception**



Combating SE/Countermeasures

- 1. Awareness**
- 2. Data Security Risk Assessment**
- 3. Be suspicious of unsolicited emails**
- 4. Avoid responding to any offers made of phone or via email**
- 5. Call Backs or out of band communication**



Case Study #1 – Vendor Email Hacked

Private Company, less than 250 employees, less than \$250M annual revenue:

The controller of a private distributor of component parts was responsible for making regular payments to overseas vendors from which the company purchased product for resale in the United States. After many months of working with the vendor and receiving regular shipments, the controller received an email which appeared to come from his contact, indicating that the vendor's bank was having issues with accepting payments, and asked if the next payment could be made to a new bank. The vendor was located overseas, making verification a challenge. After some pressure was applied by the supposed vendor, the invoice was paid by wire transfer. The following month, when the real vendor realized that their best customer was late on their payment, an investigation determined that the vendor's email was hacked, and an imposter had been socially engineering the company into believing that the change in bank information was authentic. In the end, almost \$250,000 was handed over to the fraudster.

Case Study #2 – Fake President Scam

Public Company, more than 250 employees, more than \$150M annual revenue:

The regional CFO of a subsidiary of a large, publically traded company received an email purporting to be from the assistant to the CEO in the United States. The email requested that the CFO transfer a large sum of money immediately to facilitate covering a tax payment in China. When the CFO questioned the request, a follow up phone call was made to the CFO, assuring him that the proper authority was granted, and that it had come "from the highest levels" within the organization . With intimate knowledge of company policies, and an official looking letter "authorizing"; the transfer on company letterhead, the CFO wire transferred the money. The scam was detected after another attempt made at transferring funds was stopped by the company's bank. After recovering only a portion of the original wire transfer, the customer suffered a \$1,000,000 loss.

Case Study #3 – Illegitimate Client

Private Company, less than 50 employees, less than \$100M annual revenue:

A business manager handling bill payment and book keeping services for a client received an email purportedly from their customer, inquiring about her balance and availability of funds for a wire transfer. The email included details regarding the scope of services that were provided, as well as information about other transactions that had recently been performed. The wire was to go to an offshore account, purportedly for the purchase of a new piece of real estate. After answering his client's questions, the client purportedly authorized the wire of funds to the account requested. After noticing some activity in the client's spam account, the client grew suspicious and contacted their bank, requesting the wire to be stopped. Unfortunately, no part of the wire could be, and all \$100,000 was lost.



Social Engineering Source: Lowers Risk Group