Fraudulently Induced Transfer Social Engineering Fraud

Fraudulently Induced Transfer (also referred to as Social Engineering Fraud) is a recent adaptation of an old fashioned scam to trick an employee into voluntarily parting with their employer's money or valuable information. The scam is simple in nature and usually involves a third party impersonating a key trusted individual – an executive, customer, or supplier, to trick the victim. It is done with a targeted approach that shows a startling sophistication and research on the victim, their relationships and business operations. The end goal is to have money or securities transferred to the criminal by relying on the victim to voluntarily perform the transaction.

Recent Fraudulently Induced Transfer/Social Engineering Claim Examples:

1. The Calgary Herald (Feb. 24, 2017) published an article detailing an email scam that defrauded Calgary's McKnight Hockey Association of almost $100,000. The Association's vice-president went public with their story to spread awareness that smaller volunteer organizations are also targets of fraudulent scammers.

   The McKnight Hockey's treasurer received a fraudulent email regarding an investment transaction. The treasurer, believing that the investment transaction was approved by McKnight Hockey's board and the email communications were from the president and vice-president, approved and released a wire transfer for $98,000. The fraud is now being investigated by the police and the association's financial institution. This email was also sent to a number of other hockey associations but they were able to identify the email as fraudulent.

2. An employee in the finance department of an insurance brokerage received an email on a Friday afternoon from the brokerage's president. The president was travelling on business and stated in the email that a wire transfer for $55,000 was to be sent to a new US vendor before the end of the day and the paperwork would follow on Monday morning.

   The insurance brokerage had strict protocols on cheque and wire transfers. The protocols mandated 2nd authorization and that all documents pertaining to the payment had to be included with the payment requisition. The 2nd authorizer called the president and said payment couldn't be enacted on the basis of the email that was sent and payment would have to wait

until the following week. The president's response: "I didn't send an email to anyone in finance". A closer review of the email showed that the fraudster had set-up a fake email address that replicated that of the brokerage, but was slightly different.

3. An employee changed a contractor's banking information based on an email that was sent from what appeared to be the contractor's firm. The employee did not verify the banking change with anyone from the contracting firm. Shortly after the change was made, the organization issued a priority payment in the amount of $650,000 by means of an electronic funds transfer to the new bank account. The fraud was uncovered when the legitimate contractor followed up on the outstanding receivable. The contracting firm had not changed banks. The funds were never recovered.

Is Fraudulently Induced Transfer Covered by Cyber Policies?

A Cyber Policy typically covers loss from unauthorized breaches into your system. With fraudulently induced transfer losses, the system is working well and has not been breached. Very few Cyber Policies respond to a loss of money or securities. These types of losses need to be covered under a Crime Policy.

Is Fraudulently Induced Transfer Covered by Crime Policies?

A Crime Policy typically covers loss from theft and employee dishonesty. There is no dishonest intent on the part of your employee here – your employee is taking action because they believe what they are doing is correct and they are doing so voluntarily.

Is Fraudulently Induced Transfer Covered by Frank Cowan Company?

In a Frank Cowan Company package we are pleased to offer our new Fraudulently Induced Transfer Endorsement to the Crime Policy with **limits of up to $100,000. Higher limits may be available upon request.**

Are There Other Ways to Protect my Organization?

Yes – Frank Cowan Company's Risk Management department has put together some excellent resources to help prevent these losses. They are available on our Risk Management Centre of Excellence for registered customers and brokers. Access the site at: **www.frankcowan.com**.

Risk Management Tips:

1. Implement and follow strong financial controls, such as 2nd authorization; no payment of invoice until the invoice is approved by whoever ordered the goods or contracted for the service; never pay on the basis of a rushed email; never pay from a statement – always ask for the original invoice from the vendor and proof of authorization for the service/goods.
2. Fraudsters can easily setup a fake email address that resembles yours. Always double check the email address.
3. Never make any changes to a vendor's or client's banking information based on an email or telephone call. Always verify the change with the vendor by calling them on the number/emailing them on the address in your file. Ignore the telephone number or email address they've used in the email request.
4. If you receive a request for a rush payment especially on a Friday afternoon or first thing in the morning, check the email very carefully and follow your established protocols. Rushed requests are common when perpetrating fraud.
5. If an email is received from a senior executive of your firm asking for a payment to be made, verify with finance before you pay. If no one is available, call the executive on their cellphone. They will appreciate the call.
6. Create an environment that promotes caution and have established financial protocols.
7. Train all employees on your financial protocols.
8. Purchase the appropriate insurance coverage.