Harper Grey LLP

Social Engineering and Cyber Fraud: Prevention, Response, and Recovery

Jonathan Meadows, Daniel Reid and Paul Saunders
Harper Grey LLP

A September 2016 lawsuit filed by Tillage Commodities Fund, L.P. in the New York Supreme Court illustrates the threat posed by an evolving species of cybercrime known as "social engineering" fraud. In its complaint, Tillage alleged that a third party fund administrator, financial services firm SS&C Technologies, was tricked into sending nearly $6 million dollars of investor money to fraudsters in China.[1] Tillage's complaint describes a relatively low tech scheme that seems almost comically amateur, yet allegedly tricked a firm hired in part for its expertise in cyber-security. Similar social engineering frauds of varying degrees of sophistication are resulting in major losses for organizations around the world.

The Tillage fraudsters allegedly sent a series of emails to SS&C staff impersonating investors and asking that increasingly more funds be transferred to a Hong Kong bank account, supposedly that of a technology company. These emails were sent from the domain "@tilllagecapital.com", which mimicked Tillage's email domain name "@tillagecapital.com", but with the addition of a third "l". No one noticed the change in spelling. The email requests made little sense given Tillage's normal operations and came from parties who were not investors in the Tillage fund. The emails were also awkward in grammar and syntax. Even more bizarrely, Tillage alleges that SS&C employees actually helped the fraudsters correct flawed wire instructions on multiple occasions over the course of the almost month-long fraud.

The complaint seems unbelievable and remains unproven, but sophisticated organizations have fallen victim to similar frauds. Although the Tillage complaint describes a fraud that might easily have been prevented, it also illustrates what makes social engineering different from other forms of cybercrime, and potentially more difficult to prevent: human error. Social engineering fraudsters, or "social engineers", do not so much attack computer systems but exploit the weaknesses of human beings.[2] Employees can be convinced to bend the rules or disregard procedure, and security

[1] *Tillage Commodities Fund, L.P. v SS&C Technologies, Inc*., Supreme Court of the State of New York, County of New York, Index No. 654765/2016.

[2] The Tillage complaint pauses to observe the human element that make social engineering fraud difficult to control: "Even more disturbing is that email evidence provided to Tillage shows that SS&C employees were not just following clearly fraudulent instructions but that they were actually responding and engaging in a two way dialogue with the criminal…" (at para. 69).

systems are of little value when doors are voluntarily opened. Even more unnerving, cybercrime insurance policies may not respond to this kind of fraud since deliberate employee action may not fall within the usual definition of a cyber-attack. Potential losses can be massive, and coverage is not a given. The Tillage complaint is a reminder that any system with human actors is inherently vulnerable – something well known to social engineers.

This paper examines the nature of social engineering fraud, how it can be prevented, how it has been treated in Canadian and United States insurance coverage litigation, and how the insurance industry is responding to the ubiquitous risk of loss from social engineering fraud faced by today's organizations.

What is Social Engineering Fraud?

Social engineers generally rely on deception to "engineer" situations in which persons inside organizations are fooled into disclosing information, providing access to networks, or transferring funds under false pretenses. Social engineering is different from "hacking" in that the vulnerabilities of human beings are exploited rather than the vulnerabilities of computer systems. Social engineers may have sophisticated technical skills, but rely primarily on deceptive interactions which cannot necessarily be controlled by conventional cyber security.

The Office of the Chief Information Officer of British Columbia provides the following definition:

> Social engineering is a collection of techniques that can be used to manipulate people into revealing sensitive or personal information. Social Engineering is a non-technical kind of intrusion that relies on human interaction and can be done using the Internet, the telephone or in person…[3]

Social engineering could be described as the application of timeless fraud techniques in the context of technology that can enhance their effectiveness and greatly increase their potential cost. Somewhat counter-intuitively, it is the "non-technical" nature of social engineering that can make it inherently difficult to control. A foolproof password, for example, does nothing when it is given away under false pretenses. Social engineering has aptly been described as hacking the "Human Operating System".[4]

[3] British Columbia, Office of the Chief Information Officer. "Social Engineering" (October 2014).
[4] https://www.hackread.com/simple-tips-manage-prevent-social-engineering-attacks/

Social engineering fraud often takes the form of attacks similar to the kind orchestrated on larger scale by malware, but with an adaptive human element that permits infinite versatility.[5] Interpol has identified four steps to a typical social engineering fraud:

1. gathering information;

2. developing a relationship;

3. exploiting any identified vulnerabilities; and

4. execution.[6]

Social engineers may put in a considerable amount of time in the preliminary steps learning about an organization and attempting to establish trust with someone inside, usually an employee. In the execution stage, a situation is "engineered", permitting the fraudster to use the employee to achieve his or her ends.

Generally, the more sophisticated the fraud, the more time will go into the initial phases and the more difficult it will be detect the fraud before it is too late. The spectrum spans all the way from unsophisticated mass frauds such as the classic "Nigerian Prince" email scheme to sophisticated and targeted impersonation attacks.

Social engineering fraud is an ever-growing security concern and is responsible for massive losses. The FBI reported that a worldwide increase in wire fraud scams alone resulted in domestic losses of $179,755,367.08 and global losses of $214,972,503.30 from 2013 to 2014.[7] From June to December of 2016, wire fraud victims reported domestic losses of $346,160,957 and global losses of $448,464,415, roughly doubling the 2013-2014 estimates.[8] Between January 2015 and December 2016, there was a remarkable 2,370% increase in exposed losses.[9] The FBI reports that these scams continue to grow, evolve, and target small, medium, and large businesses in every country in the world. They have become an unavoidable liability for anyone with an email account.

[5] https://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

[6] https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud

[7] Federal Bureau of Investigation, Public Service Announcement, Alert No. I-012215-PSA (Jan 22, 2015).

[8] Federal Bureau of Investigation, Public Service Announcement, Alert No. I-050417-PSA (May 4, 2017).

[9] Exposed dollar loss includes actual and attempted loss.

Types of Social Engineering Fraud

Phishing

Generally speaking, “phishing” is a form of cyber-attack that involves the use of deception to extract information that can be used in a later attack or fraudulent transaction.[10] In the context of electronic communications, phishing can be defined as the practice of sending emails or other communications appearing to be from reputable sources with the goal of influencing people or gaining personal information.[11] The fishing analogy arises from the way illegitimate communications and websites are often used as “lures” or “bait” in phishing attacks to invite the input of information.

A typical phishing attack involves sending an email tailored to appear as if coming from within an organization or from a trusted third party, such as a service provider or supplier. In the information gathering stage, fraudsters may access publicly available information to clone the appearance of institutional communications or impersonate employees. Fraudsters may create email addresses that mimic organizational addresses, or even hijack legitimate addresses so that only tone, content, or context can alert recipients. The ultimate goal is to fool people who are not paying close attention into disclosing information.

The techniques used in phishing attacks can also be executed over the phone (“Vishing”) or by text message (“SMishing). Anyone with access to communications technology is a potential victim.

In social engineering attacks, the “spoofing” associated with malware is introduced in the context of what appears, through manipulation, to be an interaction with a trusted party.[12] This kind of attack combines elements of social engineering and traditional phishing, which can also be conducted *en masse* using malware. Social engineers spend considerable time setting up their phishing attacks by gathering information in the initial stages and using deceptive interactions, resulting in targeted attacks that are more difficult to detect. The term “spearphishing” is sometimes used to connote these sophisticated attacks.

[10] One sophisticated example of the latter involved sending invites to Gmail addresses to collaborate on Google Docs. The invites came from familiar addresses and, though in many cases would have seemed out of context, were virtually indistinguishable from legitimate invites. Opening the document gave the perpetrator access to the victim’s entire Gmail account. See: http://fortune.com/2017/05/03/google-docs-scam/

[11] Christopher Hadnagy and Michele Fincher. *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails*. Indianapolis: John Wiley & Sons, 2015.

[12] “Spoofing” refers to a wide range of impersonation techniques, including the creation of cloned websites.

The threat is not limited to the workplace. One scheme, for example, targets frequent corporate travelers with phony but convincing flight confirmations that activate malware when accessed. The goal is to steal corporate credentials in order to access corporate networks and gather information for attacks. The scheme is highly effective because the fraudsters do a significant amount of preliminary research; emails are tailored with travel destinations, airlines, and prices specific to each mark.[13] Even persons who are trained not to open suspicious attachments may be caught off guard. Researchers studying the scam found a success rate of over 90%.[14] This is likely because targeted information gathering puts the spoofed emails in a credible context and reduces the chance that suspicions will be raised.

Wire Fraud

"Wire Fraud" describes a number of similar scams that involve gathering information about an organization and using that information to convince employees to transfer funds to a supposed client, supplier, or other third party.

Social engineers attempting a variant of wire fraud termed "Business Email Compromise" (or "BEC") usually gather information about a high ranking employee with authorization to approve the transfer of funds, such as a CEO or manager. A pretext, such as a high pressure situation involving an "urgent" or "secret" deal, is then engineered to coerce another employee into making a wire transfer. Believing they are dealing with an authority within their organization, even well-trained employees may be convinced to breach company protocols or otherwise go along with something unusual. Fraudsters have also been known to create contact information for phony points of contact, such as lawyers, who can "verify their identity", thus frustrating employees' attempts at due diligence.

In a characteristic example of BEC fraud, the corporate controller of Scoular – a grain-trading and storage company that ranks among the largest private companies in the U.S. – transferred $17.2 million to an offshore bank account at the request of the "CEO". The fraudsters sent the controller a "top-secret" email instructing him that Scoular had closed a deal to acquire a Chinese company. He was to liaise with a lawyer at KMPG who would provide instructions to wire the funds to a bank account in Shanghai. The fraudsters had set up contact information in the name of a real KMPG partner using the fake but convincing domain name "@kpmg-office.com". The controller later told the FBI he was not suspicious of the transfers because Scoular was discussing an expansion to China and had been working with KMPG, facts which were likely known to the

[13] https://www.pindrop.com/blog/highly-effective-phishing-attack-targets-corporate-travelers/
[14] https://blog.barracuda.com/2017/03/30/threat-spotlight-the-airline-phishing-attack/

fraudsters. Investigations revealed that the fraudulent communications were linked to a server in Moscow and a Skype account registered in Israel.[15]

Fraudsters also perpetrate targeted attacks against small organizations. In 2015, the Law Society of B.C. warned practitioners that a B.C. law firm had fallen victim to a variant of wire fraud. The perpetrators hacked the firm's computers, then monitored email traffic for some time. When the lawyer went on holiday, the fraudsters sent an email from the lawyer's own account urgently requesting that an assistant transfer funds to a "client's" bank account. Although the assistant tried to contact the lawyer to confirm the instructions over the phone, the fraudsters blocked the calls and responded to the assistant's urgent emails advising they were busy and unable to speak over the phone.[16]

Another variant of wire fraud involves impersonating a trusted partner or supplier. This is sometimes termed a "supplier swindle". A business with a longstanding relationship with a supplier is requested to wire funds to an alternate account. If the scam is conducted over email, spoofed accounts or websites are used to make the request look legitimate. Fraudsters may also impersonate a supplier claiming to have changed certain information, including banking information.[17] These frauds are usually discovered only when the real supplier calls asking why its invoices have gone unpaid.

Staff at McEwan University in Edmonton, for example, were convinced by social engineers to change the banking information of one of McEwan's major vendors, a construction company. The emails requesting the change used a realistic replica of the vendor's logo. Over several transactions, McEwan staff proceeded to transfer almost $12 million to the fraudulent account. As is often the case, the University was alerted to the fraud only when the real vendor called, asking why it had not yet been paid. It was subsequently discovered that fraudsters had produced fake emails for 14 other construction firms in the area. This example is unusual only in that most of the funds were frozen and recovered before disappearing.[18]

[15] https://www.ft.com/content/19ade924-d0a5-11e5-831d-09f7778e7377#axzz41IFeKIyw

[16] https://www.lawsociety.bc.ca/support-and-resources-for-lawyers/lawyers-insurance-fund/fraud-prevention/fraud-alerts/fraud-alert-december-15,-2017/

[17] In a particularly bizarre example of such phony information change, a Chicago man actually managed to reroute all of UPS's deliveries to his one bedroom apartment simply by changing the company address with the U.S. Postal service: https://www.washingtonpost.com/news/business/wp/2018/05/11/a-rare-time-change-of-address-actually-worked-a-chicago-man-redirects-all-of-upss-mail-to-his-one-bedroom-apartment/?utm_term=.c3c30431b335

[18] http://www.cbc.ca/news/canada/edmonton/macewan-university-phishing-scam-edmonton-1.4270689

Other Examples

While phishing and wire fraud represent the majority of social engineering attacks, the variants are practically limitless.

Some variants rely on impersonation to gain physical access to network computers, for example by impersonating a tech support worker. Another involves leaving a USB drive in the common area of an office, thus inviting a well-intentioned employee to access the data and determine to whom the USB belongs; the USB is in fact loaded with malware that will allow the social engineer to gain access.

The common thread linking social engineering frauds is that human beings are manipulated into facilitating access to networks, disclosing sensitive information, or transferring funds. In the rest of this paper, we focus on wire fraud because it represents a massive liability but often involves no direct cyber-attack that would be covered under typical cyber-crime policies. As we discuss below, the distinction between "pure" social engineering fraud and hacking is of legal significance and has resulted in much litigation.

Mitigating the Risk of Social Engineering Fraud

The primary methods of mitigating the risk of social engineering fraud before it occurs are internal policies and employee training.

Some of the policies recommended by law enforcement and risk management analysts include multiple party sign-off requirements and multiple form authentications for all significant transactions.

However, organizations should not over-rely on internal policies because social engineers are adept at convincing employees to ignore them. In the Scoular case, for instance, the company controller was convinced to bypass standard channels of communication by a "secret" transaction. Similarly, in the Tillage complaint it is alleged that SS&C had internal policies that prohibited the conduct described in the complaint, but that SS&C's employees, for whatever reason, did not follow them. We do not focus on internal policies here – suffice to say they must be supplemented to be effective.

Because social engineers generally target employees, employee training is probably the best method of mitigating the risk of social engineering fraud. Employees should be trained to be wary of:

- “urgent” requests;
- spoofed domain names and email addresses;
- any requests for sensitive information;
- sudden changes in business practices;
- changes in contact or banking information;
- unsolicited tech support or offers of services;
- communications displaying unusual tone or content;
- invitations to access embedded links or attachments.

Employees should generally be advised to slow down and pay close attention to details such as the spelling of email and web addresses, especially when circumstances are unusual or pressure is applied. Other channels of communication should always be used to verify the legitimacy of sensitive communications. “Reply to” should not be used until the identity of a sender has been confirmed, and never via information provided by the sender.

Employers should also make sure to update employees on the latest frauds and reward those employees who are proactive in reporting suspicious activity.

One commentator encourages fostering an organizational “culture of doubt” that will increase the chances that employees will spot signs of social engineering and react accordingly. However, it is also cautioned that the inherent nature of these attacks is that they cannot be prevented entirely.[19] If you have human workers, social engineering attacks are an inevitable liability.

This fact of inevitable liability makes adequate insurance coverage very important. However, coverage under standard commercial insurance policies cannot be assumed. Companies that have sustained losses due to social engineering may look to their commercial general liability policy (“CGL policy”) or cybercrime policy only to find out that their policies apply, for instance, only when computer networks are hacked allowing a transaction to be initiated directly by the hacker. In the case of social engineering

[19] Kevin Baird, “How to Prevent Social Engineering… You Can’t” (January 16, 2016) (PheonixTS blog post). See: https://phoenixts.com/blog/how-to-prevent-social-engineering-you-cant/

fraud, losses that are incurred as a result of the voluntary release of information or funds may not be covered at all.

Coverage Issues: Case Law on Social Engineering Fraud

The chance of recovering funds lost to social engineering fraud is usually remote to non-existent. It is only in exceptional cases that funds can be frozen by law enforcement and recovered. Usually by the time a fraud is discovered, the funds have disappeared forever. In such cases, victims of social engineering must rely on insurance to recover or mitigate their losses. The case law on social engineering fraud deals primarily with the coverage litigation that can ensue when insurance is the only means of recovering losses. Some relevant cases are discussed below.

Taylor & Lieberman v. Federal Insurance Company

In one of the first U.S. cases to consider social engineering fraud, *Taylor & Lieberman v. Federal Insurance Company*, the Ninth Circuit Court of Appeals took a restrictive approach to insurance policy language that might have been read to cover social engineering fraud.[20]

In that case, the complainant, Taylor & Lieberman, had power of attorney over its clients' accounts. A fraudster hijacked the email account of one of Taylor & Lieberman's clients and sent wire transfer instructions to the email address of one of Taylor & Lieberman's employees. The email was signed with the client's name typed at the bottom. The requested transfer was to a bank in Malaysia in the amount of $94,280.00. The employee completed that transfer and a second requested transfer of $98,485.90. When a third request for a transfer of $128,101.00 came in from a different email address, the employee was tipped off and called the real client to confirm. Taylor & Lieberman reimbursed the client and was able to recover most of the first transfer. It then attempted to recover the second under the crime coverage of its insurance policy.

The relevant policy language was as follows:

> Forgery Coverage: The Company shall pay the Parent Corporation for direct loss sustained by an Insured resulting from Forgery or alteration of a Financial Instrument committed by a Third Party.

[20] *Taylor & Lieberman v. Federal Insurance Company*, Court of Appeals, 9th Circuit 2017. Also see: *American Tooling Center Inc. v. Travelers Casualty and Surety Co*., Case No. 5:16-cv-12108, 2017 U.S. Dist. (E.D. Mich. Aug. 1, 2017).

> Computer Fraud Coverage: The Company shall pay the Parent Corporation for direct loss sustained by an Insured resulting from Computer Fraud committed by a Third Party.
>
> Funds Transfer Fraud Coverage: The Company shall pay the Parent Corporation for direct loss sustained by an Insured resulting from Funds Transfer Fraud committed by a Third Party.

The Federal Insurance Company refused coverage on the basis that none of the above terms of coverage applied.

At the trial level, the United *States* District Court, C.D. California, held that Taylor & Lieberman's losses did not constitute a "direct loss" of its funds, as defined by the policy, since it was the client's funds that were lost. The Court made the following comments on this point:

> The Court finds Defendant's reasoning more persuasive. If the funds had been held in an account owned or attributed to Plaintiff, such as an escrow account … and a hacker had entered into Plaintiff's computer system and been able to withdraw funds such that Plaintiff's accounts were immediately depleted, then Plaintiff would be correct in asserting coverage from the Policy. Here, however, a series of far more remote circumstances occurred: Client gave Plaintiff power of attorney over Client's money held in Client's own account; a perpetrator of fraud motivated Plaintiff's agent to use the power of attorney to transfer funds out of Client's account; Plaintiff discovered this fraud and attempted to recover the funds; Client requested repayment of the lost funds and Plaintiff obliged; Plaintiff now requests Defendant indemnify it for the losses that were transferred from Client to Plaintiff. These are … not the circumstances … within the contemplation of the Policy.

On appeal, the Ninth Circuit of the United States Court of Appeals affirmed the trial decision on different grounds.

The Court of Appeals held that there was no "forgery" such that the policy language would be engaged, since there was no alteration of any financial instrument such as a cheque or bank draft. Instead, the fraudsters had simply directed Taylor & Lieberman's employee to transfer funds into an account.

There was also no "computer fraud" since sending a "normal" email to a business, without a virus or malware, could not constitute unauthorized entry into a computer system. The Court rejected Taylor & Lieberman's contention that the emails were akin to a computer virus in that they introduced “instructions” that propagated themselves through its computer systems. Put another way, they were simply emails that relied on fooling employees rather than introducing malicious code or otherwise attacking Taylor & Lieberman’s computer network per se.

Finally, the Court held that Taylor & Lieberman was not entitled to funds transfer fraud coverage, reasoning as follows:

> … Fraud transfer fraud encompasses:
>
> > fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by an Insured Organization at such Institution, without an Insured Organization's knowledge or consent.
>
> This coverage is inapplicable because T&L requested and knew about the wire transfers. After receiving the fraudulent emails, T&L directed its client's bank to wire the funds. T&L then sent emails confirming the transfers to its client's email address. Although T&L did not know that the emailed instructions were fraudulent, it did know about the wire transfers.

The Court of Appeals effectively held that the policy would have covered conventional cyber-attacks, but did not extend to social engineering attacks in which employees were tricked into transferring funds. From whichever angle the policy was interpreted, at both the trial and appellate level, it was held that social engineering fraud escaped the policy language because, essentially, it involved no hacking of a computer system.

Similarly, in *Apache Corporation v. Great American Insurance Company*, the Fifth Circuit of the United States Court of Appeals similarly held that supplier fraud was not captured by the wording of a traditional crime policy.[21] In that case, a fraudster claiming to be a vendor to an oil company convinced an employee to change vendor information and later contacted the company with a false phone number that was used for verification of subsequent payments of $2.4 million. The policy covered loss “resulting directly” from the use of any computer to fraudulently cause the transfer property from inside the premises or banking premises to an outside party. Great American argued that there was no coverage unless a criminal hacks into the insured’s computer system and directly causes a transfer of funds.

[21] *Apache Corporation v. Great American Insurance Company*, U.S. Court of Appeals, 5th Circuit 2016

The Court of Appeals, reversing the trial decision, agreed with Great American, holding that there was no coverage because the employee's action rather than the false emails caused the transfers.[22] Whereas the trial judge had held that the fraudulent email was the direct cause of the Apache's loss despite the intervening acts of employees, the Court of Appeals provided the following analysis:

> The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in *Pestmaster II*,[23] convert the computer-fraud provision to one for general fraud… We take judicial notice that, when the policy was issued in 2012, electronic communications were, as they are now, ubiquitous, and even the line between "computer" and "telephone" was already blurred. In short, few—if any—fraudulent schemes would not involve some form of computer-facilitated communication…
>
> …
>
> Moreover, viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache elected to pay legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers.

Taylor & Lieberman and *Apache* both demonstrate that conventional cybercrime policies may not apply when the "Human Operating System" is hacked.

The Brick v. Chubb

The Brick Warehouse LP v. Chubb Insurance Company of Canada, a Canadian decision of the Alberta Court of Queen's Bench, also illustrates the coverage issues that can arise when losses ensue from social engineering fraud rather than a conventional cyber-attack.[24]

Like Apache, the Brick was the victim of a "supplier swindle". A fraudster called the Brick's accounts payable department and spoke with an employee, indicating he was from Toshiba but was new to the company and was missing some payment details.

[22] For a detailed and illuminating discussion of this case see: https://www.claimscanada.ca/coverage-social-engineering-fraud-takes-place-among-required-coverage-canadian-business

[23] *Pestmaster Services, Inc. v. Travelers Cas. & Sur. Co. of Am*., U.S. Court of Appeals, 9th Circuit 2016.

[24] *The Brick Warehouse LP v. Chubb Insurance Company of Canada*, 2017 ABQB 413.

The employee, being helpful, faxed payment documentation to a number that the fraudster provided. The fraudster called again a few days later, and the same employee advised him to write to the Brick's lender to update contact information so he would receive electronic notification of payments.

A different employee later received an email from the fraudster using the spoofed "Toshiba" email address "silbers_toshiba@eml.cc". The email claimed to be from the controller of Toshiba Canada and advised that Toshiba had changed banks from the Bank of Montreal to the Royal Bank of Canada. The email indicated all payments should be made to the new account and provided wire transfer information. The employee changed Toshiba's bank information to reflect the new account information, and even followed the standard practice of having another employee review the paperwork.

The fraudster later contacted the Brick claiming to be from Sealy Canada and provided information for another phony change of account. However, because the same account number was given for Sealy as for the Brick, the information could not be entered into the payment system. The fraud was discovered shortly thereafter when a bona fide Toshiba representative called to inquire about why the company had not received payment for recent invoices. By that time, ten invoices totaling $338,322.22 had been paid to the fraudulent Toshiba account. A police investigation revealed that the fraudulent account belonged to an individual in Winnipeg who had been convinced by someone to receive the money as part of an investment scheme, then transfer it to Dubai. The Brick recovered $113,847.18 as a result of the investigation and turned to its insurer, the defendant Chubb, for the remaining $224,475.14.

Before considering the coverage litigation that ensured, it is worth pausing to note the oversights that enabled the fraud. Despite the unusual nature of the caller's request, which should have raised red flags, the employee who initially dealt with the fraudster did not take any steps to verify the caller's identity. He also faxed sensitive information to a phone number provided by the caller and not independently verified. The second employee should also have been on high alert faced with a request to change banking information, but did not contact Royal Bank, Toshiba, or the Bank of Montreal, nor did the employee who reviewed the transfer. This appears to have been a case in which employee training could potentially have prevented the fraud.

Chubb refused to cover the claim on the basis that it had no obligation to pay given the wording of the Brick's insurance policy, which covered "funds transfer fraud" but defined it as follows:

> Funds transfer fraud means the fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution

> directing such institution to transfer, pay or deliver money or securities from any account maintained by an insured at such institution without an insured's knowledge or consent.

Citing *Taylor & Lieberman*, the Court agreed that the above policy language excluded coverage because the Brick's employee had consented to the fraudulent transfers:

> There is no doubt that funds were transferred out of the Brick's account. The question really is whether the funds were transferred under instructions from an employee who did not know about or consent to the fraudulent transactions…
>
> The Brick contends that the policy provision states that Chubb will pay for direct loss resulting from funds transfer fraud by a third-party, and the focus should be on the fraud itself and not on the fraudulent instructions. [However]… There is no mention anywhere in the insurance policy of the term "informed consent". …
>
> One of the definitions of consent is "permission for something to happen, or agreement to do something. Examining the facts, a Brick employee did give instructions to the bank to transfer funds. The employee was permitting the bank to transfer funds out of the Brick's account. Consequently, the transfer was done with the Brick's consent. Even applying the *contra proferentem* rule, the Brick still consented to the funds transfer.
>
> Even if the Brick did not consent to the funds transfer, there is still the issue of whether the transfer was done by a third party. Certainly, the emails with the fraudulent instructions were from a third party. The actual transfer instructions; however, were issued by a Brick employee. There was no one forcing the employee to issue the instructions, there were no threats of violence or other harm. The employee was simply a pawn in the fraudster's scheme. Therefore, the transfer was not done by a third party.

Because of its finding that the policy wording excluded voluntary transfers, even under false presences, the Court held that the Brick was not entitled to recover the balance of its losses from Chubb.

Medidata Solutions Inc. v. Federal Insurance Co.

The Second Circuit Court of Appeals recently came down with a more policy-holder favorable decision in the case of *Medidata Solutions Inc. v. Federal Insurance Co*.[25]

Medidata concerned the availability of coverage for a typical BEC social engineering fraud. In the summer of 2014, Medidata, a company that provides cloud-based services to scientists conducting research in clinical trials, notified its finance department of a short-term business plan that included a possible acquisition (this notification was legitimate). Employees were instructed to be prepared to assist with transactions on an urgent basis.

Shortly thereafter, an employee in the finance department received an email purporting to be from the company president. Like all internal Medidata emails, the name, email address, and picture of the sender was populated and displayed by Gmail – however, the fraudster had embedded a computer code causing Gmail to populate the email with the president's information and hide the true origin of the email.

The email explained that Medidata was close to finalizing an acquisition and that an attorney named "Michael Meyer" would be in contact her with further details. The matter was to remain strictly confidential. The same day, a man purporting to be Michael Meyer called the employee and demanded that she process a wire transfer. The employee indicated that she would need an email from the president and confirmation from the vice-president to proceed. An email from the president followed in which the vice-president and director of revenue services were copied. The employee logged into an online banking system and initiated a wire transfer of almost $4.8 million dollars, which was then approved by the vice-president and director of revenue services on the basis of the false email.

The fraud was discovered when Michael Meyer contacted the employee two days later requesting a second transfer. The employee initiated the transfer and the director of revenue services approved. However, this time the vice-president became suspicious about the email address in the "Reply to" field and contacted the president directly to make inquiries. The president told her that he had not requested either of the transfers. Medidata then realized it had been defrauded and contacted the FBI, which was not able to recover the funds. Medidata therefore turned to its Federal Insurance Company crime policy, but coverage was denied on the basis that the wire transfer was authorized by Medidata employees and thus was made with the knowledge and consent of Medidata.

[25] *Medidata Solutions Inc. v. Federal Insurance Co.*, U.S. Court of Appeals, 2nd Circuit 2018.

The ensuing coverage litigation turned on the scope of "fraudulent entry" under the policy terms. Medidata's coverage for "computer fraud" extended to, among other things, the "fraudulent … entry of Data into ... a Computer System" and "change to Data elements or program logic of a Computer System".[26] Federal argued that there was no fraudulent entry since the emails were sent to an email address that was open to the public and there was no change to any data in Medidata's computer system.

At the trial level, the Court disagreed with Federal's position. The Court cited *Universal American Corp. v. National Union Fire Insurance Company of Pittsburgh*, a case of the New York Court of Appeals, which involved a health insurance company that was defrauded by healthcare providers who entered claims for reimbursement of services that were never rendered.[27] The policy in that case also defined computer fraud coverage in terms of fraudulent entry. In denying coverage, the Court of Appeals held that the language of that policy "applie[d] to losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users."

The Court distinguished *Medidata* from *Universal* on the basis that Medidata had experienced exactly the kind of unauthorized access contemplated by the Court of Appeals in *Universal*. Interestingly, the Court appeared to caution against making draconian distinctions between "hacking" and social engineering fraud:

> Federal's reading of *Universal* is overbroad. In this case, Federal focuses on the thief's construction of the spoofed emails and computer code before sending them to Gmail, arguing that, as a result, there was no entry or change of data to Medidata's computer system... Under this logic, *Universal* would require that a thief hack into a company's computer system and execute a bank transfer on their own in order to trigger insurance coverage. However, this reading of *Universal* incorrectly limits the coverage of the policy in this case. It is true that the Court of Appeals in *Universal* peppered its opinion with references to hacking as the example for a covered violation … But a hacking is one of many methods a thief can use, and "is an everyday term for unauthorized access to a computer system." … Thus, Universal is more appropriately read as finding coverage for fraud where the perpetrator violates the integrity of a

[26] A "Computer System" was defined in turn as "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned and operated by an Organization; (b) leased and operated by an Organization; or (c) utilized by an Organization."

[27] *Universal American Corp. v. National Union Fire Insurance Company of Pittsburgh*, (2015) 37 N.E. 3d 78 (Court of Appeals of New York).

> computer system through unauthorized access and denying coverage for fraud caused by the submission of fraudulent data by authorized users…

Accordingly, the Court held that there was coverage:

> In this case, it is undisputed that a third party masked themselves as an authorized representative, and directed Medidata's accounts payable employee to initiate the electronic bank transfer. It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties' manipulation of the emails. The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees' knowledge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny. Therefore, Medidata has demonstrated that the Funds Transfer Fraud clause covers the theft in 2014.

At the appellate level, the United States Court of Appeals affirmed the New York District Court's decision, holding that the plain and unambiguous language of the policy covered loss due to "fraudulent entry of data into a computer system", despite the fact that no actual hacking occurred.

This finding is consistent with the direction of recent developments in American jurisprudence, and may reflect a shift away from the restrictive policy interpretation found in earlier cases. For example, the Michigan District Court in *American Tooling Center Inc. v. Travelers Casualty and Surety Co*.[28] came to the exact opposite conclusion as *Medidata,* on similar facts, but was subsequently overruled on appeal days after the *Medidata* appellate decision was released.

American Tooling Center Inc. v. Travelers Casualty and Surety Co.

American Tooling was another "supplier swindle" with facts similar to those in *The Brick*. A fraudster had intercepted an email from an American Tooling employee asking a supplier to provide outstanding invoices and responded by informing the employee that its banking information had changed. The employee was not suspicious since this had happened, legitimately, in the past. The rest of the facts should be predictable at this point.

[28] *American Tooling Center Inc. v. Travelers Casualty and Surety Co*., 2017 U.S. Dist. Crt. (E.D. Mich. Aug. 1, 2017).

The District Court held that there was no coverage for American Tooling under its Traveler's computer fraud policy because the policy extended only to "direct loss" caused by computer fraud. "Computer fraud" was defined in turn as follows:

> The use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Financial Institution Premises:
>
> 1. to a person (other than a Messenger) outside the Premises or Financial Institution Premises; or
>
> 2. to a place outside the Premises or Financial Institution Premises.

In effect, the Michigan District Court would have required that the fraudster hack into a computer and fraudulently effect a wire transfer, the very thing the New York District Court in *Medidata* found "overbroad" and "incorrect" in principle when dealing with social engineering.[29]

The district court finding in *American Tooling* was subsequently overturned by the Sixth Circuit of the United States Court of Appeals.[30] The Court of Appeals, applying the plain meaning of the word "direct", held that American Tooling had suffered a "direct loss" in the sense that the transfer resulted immediately and proximately from the interception of the email and fraud. The Court of Appeals characterized its interpretation of "direct loss" as a matter of common sense:

> A simplified analogy demonstrates the weakness of Travelers' logic. Imagine Alex owes Blair five dollars. Alex reaches into her purse and pulls out a five-dollar bill. As she is about to hand Blair the money, Casey runs by and snatches the bill from Alex's fingers. Travelers' theory would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill. This interpretation defies common sense.

The Court of Appeals rejected Traveler's argument that policy definition of "computer fraud" required a computer to cause a fraudulent transfer as opposed to simply using a computer to facilitate a fraudulent transfer. If Traveler's intended to restrict coverage to "hacking" it could have done so with narrower language:

[29] https://www.insurancerecoveryreport.com/2017/08/two-court-rulings-show-coverage-difficulties-for-fake-president-fraud

[30] *American Tooling Center Inc. v. Travelers Casualty and Surety Co*., U.S. Court of Appeals, 6th Circuit 2018.

> Travelers' attempt to limit the definition of "Computer Fraud" to hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer is not well-founded. If Travelers had wished to limit the definition of computer fraud to such criminal behavior it could have done so … Because Travelers did not do so, the third party's fraudulent scheme in this case constitutes "Computer Fraud" per the Policy's definition.

Arguably, *American Tooling* goes even farther than *Medidata* in recognizing that the distinction between social engineering fraud and hacking upheld in previous decisions is artificial and out of step with the hybrid nature of modern cyber-attacks. However, the liberal approach was permitted by the relatively loose language of the policy at issue.[31]

It remains to be seen to what extent *Medidata* and *American Tooling* signal a departure from the restrictive approach to coverage for social engineering fraud exemplified in cases like *Taylor & Lieberman* and *The Brick*.[32] The specific wording of a policy will always be paramount. In this regard it is important to keep in mind that *Medidata* involved the introduction of malicious code and *American Tooling* involved the illicit "interception" of an email. It may be that future cases will hold that computer fraud coverage can apply to fraudulent transfers engineered without traditional "hacking", but at present the safest assumption is that Canadian Courts will not find that "pure" social engineering attacks are covered by cybercrime policies absent clear language or specific endorsements providing such coverage.

Industry Response: Endorsement for Social Engineering Fraud

In recognition of the risk that existing computer fraud or funds transfer fraud insurance policies may not cover social engineering fraud, insurers are beginning to market dedicated "social engineering fraud" coverage in addition to traditional crime insurance.[33]

Such policies can cover a range of types of fraud, including phishing, wire fraud and other forms of loss where the loss arises out of the perpetrator imitating legitimate vendors, suppliers, clients or staff in order to cause funds or information to be transferred.[34]

[31] The policy at issue in *Medidata*, notably, may not have permitted coverage on the same facts given the requirement of "fraudulent entry" in a computer system.

[32] The insurers in both *Medidata* and *American Tooling* have filed petitions for rehearing.

[33]See, for example: https://www.alignedinsuranceinc.com/social-engineering-fraud-coverage/

[34] See, for example: https://www2.chubb.com/ca-en/business-insurance/social-engineering-fraud-coverage-for-crime-insurance.aspx

Given the legal uncertainty regarding whether coverage will be found under existing cybercrime or fraud policies, organizations and businesses should explore whether such an endorsement should be added to their existing insurance coverage.

Conclusion

Social engineering fraud represents a massive and expanding area of risk that should be a concern for any organization or business. This risk can be mediated through understanding and deliberate risk prevention strategies, but not eliminated.

This paper has attempted to introduce readers to social engineering fraud as a first step towards understanding its unique threats to organizations. It has also attempted to inform readers of the unsettling disconnect between the realization that insurance coverage for social engineering fraud is necessary and the uncertainty that coverage will be found under traditional cyber or crime policies.

Given this state of affairs, it is recommended that companies looking to mitigate the risk of losses from social engineering fraud review their current insurance coverage with insurance professionals and coverage counsel. The insurance industry continues to respond with new policy options that can provide some peace of mind amidst the "culture of doubt."

For enquiries relating to this paper, please contact:

Jonathan Meadows
Partner
604.895.2809
jmeadows@harpergrey.com

Daniel Reid
Associate
604.895.2877
dreid@harpergrey.com

Paul Saunders
Associate
604.895.2832
psaunders@harpergrey.com

This paper is made available for educational purposes only as well as to give readers general information and a general understanding of the law, not to provide legal advice. Readers should not act on the basis of this paper without first consulting a lawyer for analysis and advice on a specific matter.