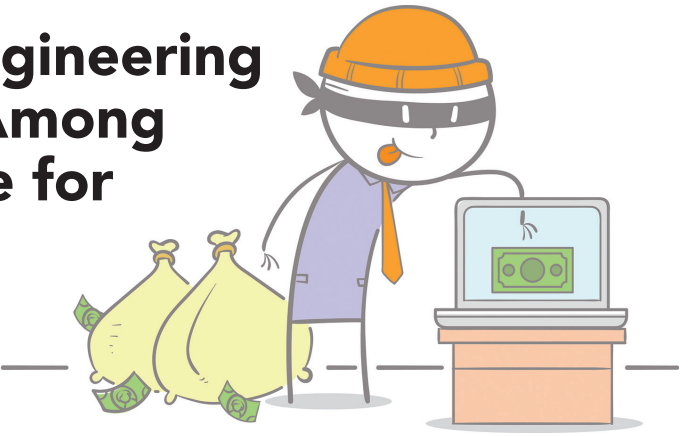
Coverage for Social Engineering Fraud Takes its Place Among the Required Coverage for Canadian Business



BY DAVID S. WILSON, CHRIS MCKIBBIN AND ZACK GARCIA, BLANEY MCMURTRY LLP

Insurance for loss resulting from the use of technology to commit fraud has existed for decades. Since the 1980s, commercial crime policies have included various forms of computer fraud and funds transfer fraud coverage. Similar coverage has been available in financial institution bonds since the 1990s.

New forms of fraud have emerged in recent years that do not fit neatly into the existing coverages. Social engineering fraud is the most significant of these new frauds, and occurs when an employee of a business is duped by a fraudster into voluntarily parting with the assets of the business. Some examples include:

1. **Phony Client Scams:** The victims or targets of these scams are financial institutions or other entities that handle client funds. The target's employee is induced by email, phone or fax to wire client funds to a "new" account. Verification procedures are either absent or not followed, and the funds are typically unrecoverable. The target must reimburse its client for the lost funds, and then looks to its crime insurer for indemnity.
2. **Vendor Impersonation Scams:** The fraudster purports to be a legitimate vendor of the target, and contacts the target's employee to request that the vendor's banking information be changed. The victim wires funds to the "new" account. By the time the legitimate vendor follows up with the victim on its outstanding receivables, the funds are gone.
3. **Executive Impersonation Scams:** The fraudster, posing as the target's "CEO" or other high-ranking executive, contacts its finance department using a spoof email or similar-domain email, under the pretext of needing an emergency payment relating to a "top secret" acquisition, merger or other situation. The fraudster directs the finance department employee to wire funds to a "special" account. The lost funds are typically unrecoverable, and the victim turns to its crime insurer for indemnity.
4. **Law Firm Collection Scams:** The fraudster poses as a foreign "client" in a debt collection matter. The "debtor" is in collusion with the "client". As soon as the lawyer demands payment, the "debtor" promptly issues a (counterfeit) cheque payable to the lawyer's trust account. The lawyer is instructed to wire the funds (less his or her fee) to the "client"—invariably, on an urgent basis. Once the debtor's cheque is returned as counterfeit, the lawyer's trust account is in deficit. Given the limited scope of trust account overdraft coverage under most lawyers' E&O policies, the lawyer often looks to his or her crime insurer for indemnity.

Standard crime insurance policies are not intended to cover social engineering fraud:

- Computer Fraud insuring agreements typically only indemnify for unauthorized entries (or "hacks") into an insured's computer system. Social engineering incidents typically involve payments initiated by the insured's employee, albeit on the basis of an inaccurate understanding of the facts.
- Funds Transfer Fraud insuring agreements are intended to cover fraudulent transfers caused by a third party directing an insured's financial institution to transfer the insured's funds without the insured's knowledge or consent. Social engineering incidents typically involve payment instructions authorized and voluntarily initiated by the insured's employee and, as such, they usually do not meet the requirements of the insuring agreement.
- Crime policies generally contain exclusions for losses resulting from an insured's voluntarily parting with money, or for losses resulting from authorized entries into an insured's computer system.

In response, the first discrete social engineering fraud coverages were introduced in Canada in 2014. Unfortunately, some victims of social engineering fraud have not obtained this coverage and, after incurring a loss, seek indemnity under the computer fraud or funds transfer fraud insuring agreements of their policies.

The October 18, 2016 decision of the U.S. Court of Appeals for the Fifth Circuit, *Apache Corporation v. Great American Insurance Company*,[1] is one of the first American appellate decisions to consider coverage for a vendor impersonation scam under "traditional" commercial crime policy wording since the widespread introduction of social engineering fraud coverage. In holding that the resulting loss did not trigger indemnity under the computer fraud coverage, the Fifth Circuit adopted the interpretive approach to computer fraud coverage taken by most other American courts, such as the Ninth Circuit in *Pestmaster Services v. Travelers*,[2] and applied it in the context of social engineering fraud.

Apache is an oil production company headquartered in Texas and operates internationally. In March 2013, an Apache employee in Scotland received a call from a person claiming to be a represen-

tative of Petrofac, a legitimate vendor of Apache. The caller instructed the employee to change the bank account information which Apache had on record for Petrofac. The Apache employee advised that such a change request would not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts payable department received an email from a @petrofacltd.com email address. Petrofac's legitimate email domain name is @petrofac.com. The email advised that Petrofac's bank account details had changed, and included as an attachment a signed letter on Petrofac letterhead setting out the old and new account numbers and requesting that Apache *"use the new account with immediate effect."*

An Apache employee called the telephone number on the letterhead and confirmed the authenticity of the change request. A different Apache employee then approved and implemented the change. One week later, Apache began transferring funds for payment of Petrofac's invoices to the new bank account. Within a month, Petrofac advised Apache that it had not received payment of approximately $7 million which Apache had transferred to the new account. Apache recovered some of the funds, but still incurred a net loss of approximately $2.4 million.

Apache maintained a Crime Protection Policy with Great American. The policy does not appear to have included social engineering fraud coverage. Apache asserted a claim under its Computer Fraud coverage, which provided that:

> The Court observed that prior courts had generally refused to extend the scope of the computer fraud coverage to situations where the fraudulent transfer is not a direct result of computer use, but rather a result from other events.

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or
>
> b. to a place outside those premises.

In Great American's view, this coverage applies when an individual improperly accesses, or "hacks", into the insured's computer system and fraudulently causes a transfer of funds, either from the insured's premises or the insured's bank's premises. Thus, no indemnity was available to Apache because the @petrofacltd.com email did not cause the transfers in issue; the loss was not the direct result of unauthorized computer use, but rather the subsequent acts of Apache's employees.

The Fifth Circuit accepted Great American's position. The Court engaged in what it described as a "detailed—but numbing—analysis" of the authorities interpreting the Computer Fraud coverage. Chief among these was the Ninth Circuit's recent decision in *Pestmaster*, in which that Court interpreted the computer fraud coverage to require an *unauthorized* transfer of funds, rather than simply any transfer which involved both a computer and a fraud at some point.

The Court observed that prior courts had generally refused to extend the scope

of the computer fraud coverage to situations where the fraudulent transfer is not a direct result of computer use, but rather a result from other events. In concluding that no indemnity was available under the computer fraud coverage, the Court held that:

> 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…, 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. [emphasis added]

Apache is significant to the insurance industry not only because, like *Pestmaster*, it reaffirms the intended scope of the computer fraud coverage, but also because it reinforces the purpose behind insurers' recent introduction of discrete social engineering fraud coverage.

In our view, a Canadian court should reach the same conclusion if it were to consider similar facts. As the Court of Appeal for Ontario has held, where there is little or no Canadian authority interpreting language used in standard-form policies in both Canada and the United States, resort may be had to American authorities to ensure uniformity in construction in both countries.[3]

While insurers have responded by creating discrete social engineering fraud coverages, *Apache* serves as a cautionary tale of how a business may be exposed to an uninsured loss in the event that it does not maintain such coverage.

The proliferation of social engineering frauds has created a new exposure for Canadian business. While insurers have responded by creating discrete social engineering fraud coverages, *Apache* serves as a cautionary tale of how a business may be exposed to an uninsured loss in the event that it does not maintain such coverage.

David S. Wilson and Chris McKibbin are partners, and Zack Garcia is an associate with the Fidelity Practice Group of Blaney McMurtry LLP in Toronto. The Group's practice encompasses all aspects of coverage analysis and litigation involving fidelity bonds, commercial crime policies and financial institution bonds, as well as fraud subrogation work against employees, co-conspirators, auditors and financial institutions.

1 *Apache Corporation v. Great American Insurance Company, 2016 WL 6090901 (5th Cir.).*

2 *Pestmaster Services, Inc. v. Travelers Casualty and Surety Company of America, 2016 WL 4056068 (9th Cir.).*

3 *Halifax Insurance Co. of Canada v. Innopex Ltd. (2004), 72 O.R. (3d) 522 (C.A.) at para. 56, citing Zurich Insurance v. 686234 Ontario Ltd. (2002), 62 O.R. (3d) 447 (C.A.) at 461.*