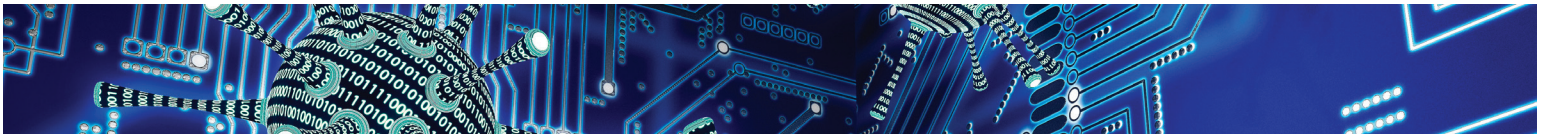

# DOES YOUR INSURANCE COVER PHISHING SCAM? IT MAY NOT.

**By: Imran Ahmad**

Cybersecurity incidents are a popular topic of coverage in the press. These incidents range from hacking into government elections such as the 2016 U.S. presidential election, to that of hacking into the computers of power utility plants to potentially interfere with power outlets as what occurred in Vermont and in Ontario. Cybersecurity is a top of mind issue for most organizations. From a risk management standpoint, organizations often purchase insurance coverage to mitigate the impacts of a cybersecurity incident. That said, sometimes there is a disconnect between the type of coverage the buyer thinks it is getting and what the policy actually covers.

This was a particularly important focus in *Apache Corp. v. Great American Insurance Company* decision, where the U.S. Court of Appeals for the 5th Circuit adopted a narrow interpretation of a crime insurance policy, finding that it did not cover a loss resulting from a fraudulent email directing funds to be sent electronically to the imposter's bank account because the scheme did not constitute "computer fraud" under the policy.

## Background

In 2013, an employee at Apache Corporation ("**Apache**") received a telephone call from an individual identifying herself as a representative of Petrofac, a vendor of Apache. The caller instructed Apache to change the bank-account information for its payments to Petrofac. The Apache employee replied that the change-request could 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" address advising that Petrofac's bank information had been changed and attached a fraudulent letter on Petrofac letterhead providing that this "new" bank information was to take "immediate effect." The Apache employee verified the number provided on the letterhead and concluded that the change-request was authentic which was followed by a formal approval and change. Shortly thereafter, Apache transferred funds to this "new" bank account, and was later notified that Petrofac had not received payments totally approximately $7 million. While Apache was able to recover a portion of the payments from its deductible, it also sought to recover the balance from its insurer.

While Apache was insured under a crime-protection insurance policy issued by Great American Insurance Company ("**GAIC**"), its claim under the policy's computer-fraud coverage was denied. GAIC claimed that the loss did not directly result from the use of a computer nor did the use of a computer cause the transfer of the funds.

The 5th Circuit reversed the district court's finding made in favor of Apache. It found that the loss was not the result of a "direct" use of a computer so as to be covered under the "computer-fraud" provision. The email was merely incidental to the authorized transfer of money and was one step in the multi-step scheme leading to the transfer of funds to the fraudulent account.

The Court also noted the fact that electronic communications are ubiquitous and that, as a result, it is difficult to envision a fraudulent scheme that would not involve some form of computer-facilitated communication (i.e., emails). However, it found that to interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would convert the computer-fraud provision to one for general fraud.

## Key Takeaways

This case underscores the narrow judicial interpretation that may be afforded to crime policy "computer fraud" provisions which effectively constrains the computer-fraud coverage to "hacking" type events. From a Canadian perspective, the question is whether Canadian courts and insurance companies would similarly interpret "computer fraud" provisions of insurance policies if faced with a similar set of facts as in Apache.

Cybersecurity threats are increasingly sophisticated and inventive. Rather than "hacking" computers in a traditional sense, hackers will often attempt to exploit individuals to obtain compromising information. The 5th Circuit recognized the ubiquitous nature of electronic communications, but declined to extend insurance coverage.

The Apache decision raises a number of questions and is particularly interesting given that many Canadian organizations are either purchasing cyber insurance coverage or relying on their existing insurance policy to cover losses flowing from a potential cybersecurity incident. It is recommended that organizations regularly conduct an internal cyber risk assessment, which will inform the adequacy of their existing insurance coverage vis-à-vis the actual risks the organization faces at an operational level.

## Contact

**Imran Ahmad**
Partner
416.597.6031
iahmad@millerthomson.com

MILLER THOMSON
AVOCATS | LAWYERS