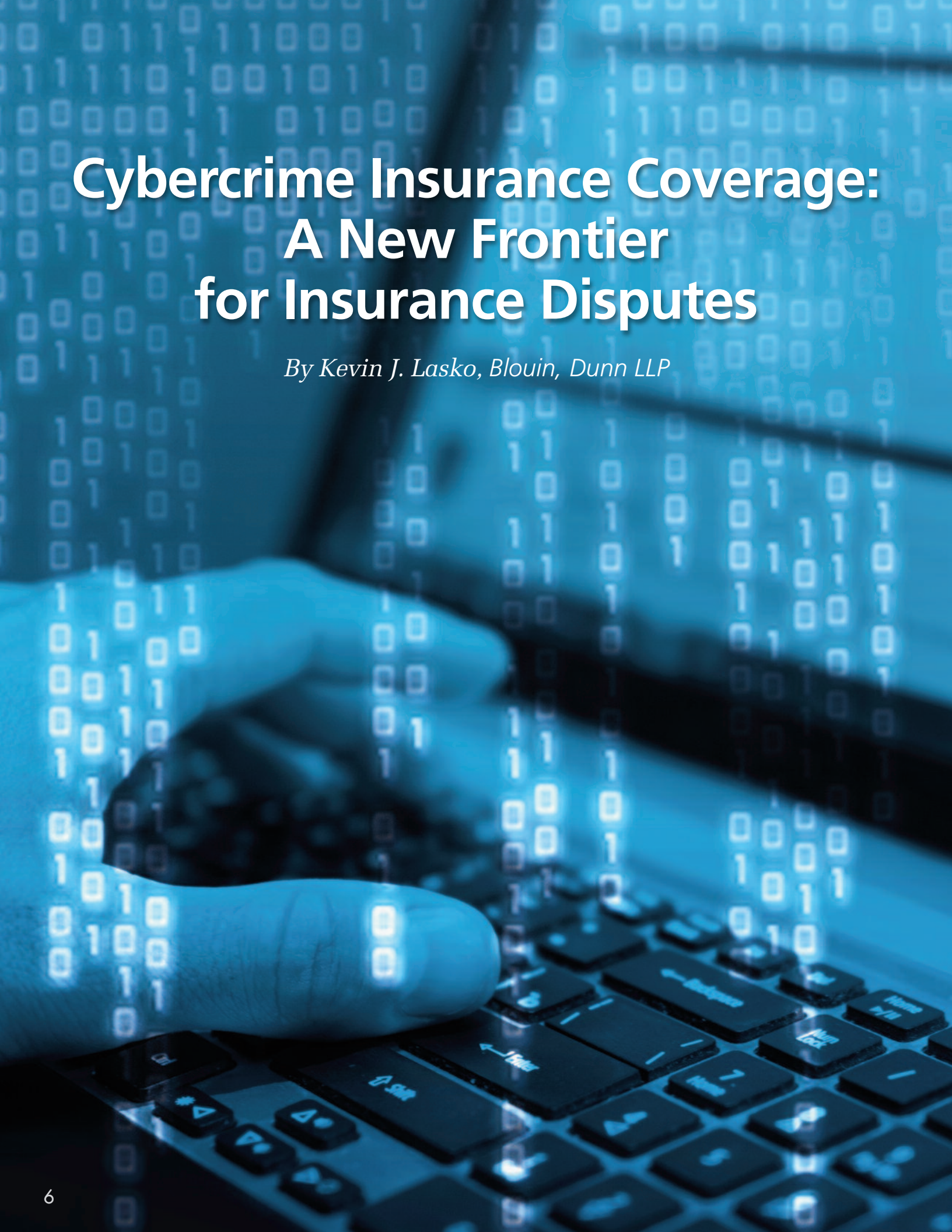

Cybercrime Insurance Coverage: A New Frontier for Insurance Disputes

By Kevin J. Lasko, Blouin, Dunn LLP

The world of cybercrime

is an ever evolving enterprise which is having an increasing impact on business across the globe. As a result, corporations have sought out insurance coverage in order to protect against these transgressions. Insurance companies have catered to the demand by underwriting policies that cover a variety of situations including forgery, social engineering fraud and funds transfer fraud.

Not surprisingly, insurance coverage disputes have arisen over new and innovative policy wordings drafted to address the wrongdoing that caused damage. Policy wording is at the center of these disputes and courts are left to interpret insurance policies to determine whether coverage is available for specific losses.

A recent spate of cases in the United States has highlighted a number of issues pertaining to cybercrime policy coverage, or lack thereof. The first cybercrime coverage case in Canada is *The Brick Warehouse LP v. Chubb Insurance Company of Canada*[1]. It is anticipated that more cases will follow in the near future.

Below is a summary of the recent approaches taken by courts in interpreting cybercrime policies and dealing with the potential ramifications in circumstances where there is no insurance coverage.

THE U.S. DECISIONS

2017 has proven to be a busy year for American courts in terms of analyzing cybercrime insurance policy wording. As many as four decisions have been reported in the first half of 2017 and there are many more on the horizon.

In reviewing the American jurisprudence, it appears that the courts have enforced a strict interpretation to the application of policy wording.

Take for example the case of T*aylor & Lieberman v. Federal Insurance Company*[2]. Here, the insured accounting firm brought an action against its insurer based on its denial of coverage for "funds transfer fraud". The damages occurred when funds were transferred in response to emails from an imposter who had fraudulently taken over an email account.

The policy provided coverage for the insured's direct loss "*resulting from forgery or alteration of a **financial instrument** of a third party*".

In interpreting the policy wording, the court ruled that there was no coverage despite allegations of forgery, computer fraud and funds transfer fraud. Forgery was not applicable because email was not considered to be a "financial instrument" as per the plain reading of the policy. The emails were not an unauthorized introduction of instructions propagated through the insured's computer system (such as malicious code) and there was no finding of computer fraud. The court also did not find coverage pursuant to funds transfer

fraud because the insured was not a financial institution and it had authorized the wire transfers without vetting the email instructions.

Coverage was also denied by the court in *InComm Holdings Inc. v. The Great American Insurance Co.*[3] This case involved an insurance coverage dispute over fraudulent debit card transactions. In short, a "code error" occurred in a telephone voice system which interfaced with a computer system allowing funds to fraudulently be added to debit cards.

The insured had a policy covering a variety of risks. The court considered some specific parts of the policy including the following:

> *The insurer 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 denying coverage, the court reasoned that the loss did not result from the use of any computer, but rather, from the use of the telephone system. Therefore, there was no loss "*resulting directly*" from computer fraud even though the telephone system was ultimately communicating with a computer system in applying the debit card funds.

In *American Tooling Center Inc. v. Travelers Casualty and Surety Company of America*[4], the insured received fraudulent emails from someone purporting to be one of the insured's vendors. As a result, payments were authorized to a fraudulent bank account. The insured made a claim arguing that the loss was covered under the "*computer fraud*" provision of the insurance policy. The policy wording was as follows:

> *The Company will pay the Insured for the Insured's* ***direct loss of****, or* ***direct loss from****, damage to, Money, Securities and Other Property directly caused by Computer Fraud.*
>
> *"Computer Fraud" is defined as 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.*

The court commented that the insured did not attempt to independently verify the bank account change with the vendor in response to the emails requesting the change. Ultimately, there was an authorized transfer of funds which did not result in a "*direct loss*" or a "*directly caused*" loss by use of a computer. Impersonation fraud was therefore deemed to fall outside of the terms of the computer fraud coverage.

The denial of coverage trend was not followed in *Medidata Solutions Inc. v. Federal Insurance Co.*[5]. This was yet another fraudulent email case. The scam started with a spoofed email to an accounts payable employee purportedly from the insured's president, directing the employee to await an attorney's wire transfer instructions to pay for an impending acquisition. The wire transfers were ultimately made resulting in damages.

The insured's policy contained a "*Crime Coverage Section*" addressing loss caused by various criminal acts, including forgery, computer fraud and funds transfer fraud. The Policy's Computer Fraud Coverage protected the "*direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party*".

The insured argued that the policy's computer fraud clause covered the losses because a thief had entered and changed data in the insured's computer system. The court agreed. The court found a direct nexus between the fraudulent use of the computer and the insured's loss which was consistent with the policy wording and was deemed to be the "direct cause" of the loss.

CANADIAN APPLICATION

The lone Canadian case to date follows the denial of coverage pattern established in the American jurisprudence. The facts of *The Brick Warehouse LP v. Chubb Insurance Company of Canada* are similar to the facts set out in *Taylor*. An imposter contacted an employee at the Brick to advise of new payment directions concerning one of The Brick's vendors. A follow up email was also sent with information concerning a new bank account and this information was never verified by The Brick. Funds were transferred in accordance with the fraudulent instructions and damages resulted. The insurance claim was denied.

The insurance policy provided for indemnity for "*Funds Transfer Fraud by a Third Party*". Funds Transfer Fraud was defined as follows:

> *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.

The court ruled that the policy wording should be given its "*plain, ordinary and popular*" meaning, "*such as the average policy holder of ordinary intelligence, as well as insurer, would attach to it*". Here, the court reasoned that the Brick employee provided instructions to the bank to transfer funds, and therefore, the transfer was done with The Brick's consent and was not itself a fraudulent act.

THE NEW FRONTIER

The *Brick* decision is the first in Canada to address policy interpretation involving cybercrime. It surely will not be the last decision on this point. The ramifications of this decision are significant.

Giving effect to the plain meaning of policy wording appears to be the overall theme when examining the jurisprudence. This can have far ranging consequences, as experienced firsthand by The Brick. Transparency is an absolute must when it comes to insurance coverage in the form of niche policies. Depending on the facts, the case law differentiates between specific fraudulent activities. The result is that there may be cybercrime activities that general "*cybercrime*" policies do not cover.

What may sound all-encompassing to the average person may not necessarily be consistent with the actual wording of the policy. If the policies are not properly explained, there is potential for litigation that may result in a finding of no coverage.

Courts will not indulge a forced construction where the policy wording is plain[6]. Communication seems to be the key in terms of understanding what policy coverage is available and whether the policy coverage is sufficient for its intended purpose.

Brokers and insureds should be encouraged to consider all potential risks within a corporation when addressing cybercrime coverage. This is a new and innovative niche in the insurance market that will continually evolve to keep pace with (or catch up to) the imaginations of cybercriminals.

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

2 *Taylor & Lieberman v. Federal Insurance Company*, 2017 WL 929211 (9th Cir.) [*Taylor*].

3 *InComm Holdings, Inc. v. Great American Insurance Company*, 2017 WL 1021749 (N.D. Ga.).

4 *American Tooling Center, Inc. v. Travelers Casualty & Surety Company of America*, 2017 WL 3263356 (E.D. Mich.).

5 *Medidata Solutions, Inc. v. Federal Insurance Co.*, 2017 WL 3268529 (2nd Cir.).

6 *Taylor*, supra note 3 at para 3.

Kevin Lasko is a lawyer at Blouin, Dunn LLP. He acts as lead counsel in numerous cases involving complex insurance defence related issues. Kevin is a graduate of Western University and was called to the Ontario Bar in 2005. For the last decade, Kevin's practice has focused exclusively on civil litigation with an emphasis on auto insurance, property and product liability claims. Kevin spent several years working directly for one of North America's pre-eminent home and auto insurance companies. Since 2012 he has been providing legal services to a variety of insurers at Blouin, Dunn LLP. Kevin's experience includes both trial and appeal work.

This paper could not have been written without the contribution of our articling student Paul Gill.

WP