CYBERCRIME INSURANCE COVERAGE CASELAW: WELCOME TO CANADA?

Posted on August 21, 2017

Categories: Insights, Publications

Although several high profile cybercrime insurance cases have recently made headlines in the US, Canadian companies have been left wondering whether or not Canadian courts would follow the line of caselaw developing across the border. That wait is now over.

The first decision in Canada with respect to cybercrime insurance coverage was decided by the Alberta Court of Queen's Bench on June 29, 2017. The case highlights the need for robust cyber coverage, coupled with internal training and cross checks with external parties. In *The Brick Warehouse LP v Chubb Insurance Company of Canada*[1] the Court held that the Brick's insurance coverage for 'funds transfer fraud' under its crime coverage policy was not enough to protect the company from its losses of just over $200,000 due to social engineering fraud.

Background

In August 2010, the Brick accounts payable department received a series of calls from an individual claiming to represent Toshiba, one of the Brick's suppliers. The imposter asked for information clarifying the payment process, and an employee helpfully provided the requested information. These calls were followed up by an e-mail, from an account that appeared to come from Toshiba (silbers_toshiba@eml.cc), and an additional call informing the Brick of a change to the account where payments should be directed. The employee proceeded by following the standard internal practice on changing account information, had the paperwork reviewed by another employee, and satisfied the imposter's request. Ten invoices totalling $338,322.22 were then transferred into the "new" account.

This fraud may have gone on for several months if two things hadn't happened: the fraudsters got greedy, and Toshiba wondered why it wasn't being paid. On September 3, 2010 the Brick was contacted by someone claiming to represent Sealy Canada making the same request and asking to have the account information changed to match the same RBC account as Toshiba, with the explanation that Sealy and Toshiba were merging. Fortunately, before this transaction was completed, the Brick was contacted by a real representative of Toshiba inquiring why Toshiba hadn't been paid for several recent invoices. This call finally set off alarm bells,

which prompted the Brick to undertake an investigation that uncovered the fraud.

The fraud was immediately reported to police, and the Brick was able to recover a portion of the fraudulently transferred funds. The Brick then followed up with their insurer, Chubb Insurance, to make a claim for the remainder of the lost funds under its crime coverage policy (as it did not have a cybersecurity insurance policy in place). However, Chubb determined that the loss was not covered by the policy; specifically that it did not fall under the 'fund transfer fraud' coverage.

Decision

The Court determined that the losses suffered by the Brick as a result of social engineering fraud were not covered under the Chubb insurance policy. The decision hinged on the interpretation of the 'fund transfer fraud' clause and the words 'knowledge' and 'consent'. The Court found that under the wording of the clause, unless the fraudsters initiated the transfer themselves, there was no coverage. Absent clear definitions of the words 'knowledge' and 'consent' in the policy, the plain meaning of the terms prevailed. Based on such plain meanings, it was held that the employee who initiated the transfer had sufficient knowledge and consent to render the clause inoperative. The Court followed the reasoning from many recent decisions out of the United States, that in order for 'fund transfer fraud' coverage to apply, the fraudster must use a computer to initiate the transfer themselves. This results in limited coverage for companies manipulated by skilled social engineering fraudsters.

This case however stands in stark contrast to the *Medidata* decision that was issued less than three weeks later by the New York District Court.[2] In that case, the plaintiff was dealing with a similar situation to the Brick, except that the fraudster posed as the president of the company, rather than a supplier. The fraudster had manipulated emails sent to the employee to make them appear with the president's picture and contact information, which made it a convincing fake of an internal email. The company lost $4.8 million as a result of this fraud, and were denied coverage because the fraudster had used an employee to initiate the transfer. While the employee did knowingly carry out the transfer in this case, the Court found that the 'funds transfer fraud' insurance still applied. In the Court's opinion, stealing through a trick is still stealing, and the fraudster being a step removed from the actual transfer was not sufficient to deny coverage. Given that cybercoverage caselaw is relatively new, it remains to be seen whether or not the reasoning in *Medidata* will eventually prevail.

The Brick case highlights the importance of ensuring that risks, such as those stemming from social engineering fraud are mitigated, to the extent possible, through mandated employee training and strong internal policies which include cross-checks of other employees' decision-making. For example, companies should perform cybersecurity health checks to ensure that they are aware of any existing loss or exposure of

sensitive data and have identified and prioritized critical assets.[3] The Brick case also reminds us that even large companies are vulnerable to that one element we can mitigate but never fully control - human error. Given this, it is incumbent upon companies to ensure they have robust cyber insurance coverage which can respond to the various creative and always-evolving cyber threats that continue to plague our daily lives.

by Darcy Ammerman and Bob Bell, Student-at-Law

[1] *The Brick Warehouse LP v Chubb Insurance Company of Canada*, 2017 ABQB 413.[ps2id id='1' target='/]
[2] *Medidata Solutions Inc v Federal Ins Co*, Case No 15-CV-907 (SDNY July 21, 2017).[ps2id id='2' target='/]
[3] Cyber Security in Canada: Practical Solutions to a Growing Problem, by the Canadian Chamber of Commerce, April 2017.[ps2id id='3' target='/]

A Cautionary Note