percipience
cyber insurance law

schultz frost LLP

Welcome to Percipience

Schultz Frost's pulse on the state of cyber insurance law in Canada.

What is Schultz Frost doing in the cyber insurance market? As a disruptive litigation boutique specializing in coverage, defence, risk management and prosecution for a wide range of insurers and self-insured entities, our engagement with cyber resilience, cyber risk and cyber claims is a natural transition. Our advocacy and intellectual leadership in the areas of fraud, multi-party litigation, and complex coverage matters leave us well-positioned to address the many challenges of the burgeoning cyber insurance industry. Whether as breach coaches, coverage or defence counsel, our award-winning litigators have cyber covered.

Readers will quickly notice a lack of Canadian case law involving true cyber insurance policies. We predict that that this will change swiftly and exponentially in the near future. As policies increasingly make their way into mainstream Canadian insurance markets, coverage and claims-based disputes will inevitably follow. As it stands, cyber insurance has developed most rapidly in the U.S., so our first issue includes some American case law as an example of what to expect in the coming months and years.

Be sure to check back in with us for our quarterly issues of Percipience as the Canadian cyber insurance market goes from up-and-coming to abundant mainstay.

1 Must Know Background Cases

Jones v. Tsige,
2012 ONCA 32
(September 29, 2011)[1]

Evans v. the Bank of Nova Scotia,
2014 ONSC 2135
(February 13, 2014)[2]

The tort of "intrusion upon seclusion" in Ontario

The Court held that civil damages can result from an invasion of privacy. Given that most cyber breaches involve a violation of privacy on some level, don't be surprised if this relatively new tort becomes a key component of cyber insurance disputes going forward.

Plaintiffs were successful in certifying a class action relating to the improper transfer of confidential client information by a bank employee. The tort of intrusion upon seclusion was pled and accepted as a viable cause of action.

[1] https://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.html?resultIndex=1

[2] https://www.canlii.org/en/on/onsc/doc/2014/2014onsc2135/2014onsc2135.html?resultIndex=1

2 Coverage Cases: Almost (but not quite) Cyber

The following two cases involved commercial crime policies with cyber components. Many cyber policies contain similar wording to the paragraphs at issue, and we can expect similar disputes arising from cyber policies in the near future.

The Brick Warehouse LP v. Chubb Insurance Company of Canada,

Alberta Queen's Bench

(July 4, 2017)[3]

Coverage denied where policy did not specifically cover social engineering fraud

Facts

The Brick sold a number of household appliances manufactured by Toshiba. In August 2010, an individual in the Brick accounts payable department received an email from an individual using the email address silbers_toshiba@eml.cc. The person sending the email claimed to be the controller of Toshiba, and stated that Toshiba had changed banks from the Bank of Montreal (BMO) to the Royal Bank of Canada (RBC). The email provided direction to transfer all payments to the new RBC account, and provided the necessary account details. Various Brick employees also received follow-up phone calls from "Toshiba representatives" over the course of the month.

The Brick employee who received the email updated the bank information for Toshiba in the Brick's payment system with the fraudulent RBC account details. Of note, the employee followed the Brick's internal procedures on changing account information at every step of the way. However, these internal procedures were deficient – no one from the Brick took any independent steps to verify the change in bank accounts (i.e. no pre-existing Toshiba contacts were consulted to confirm the transfer of funds).

Thankfully, a real Toshiba representative eventually followed up on the outstanding receivables corresponding to the fraudulent transfers, which revealed the fraud. The Brick's net loss was $224,475.

Coverage

The policy indemnified "Funds Transfer Fraud by a Third Party," which 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."

Chubb's Argument

The Brick's instructions to its own bank had emanated from an authorized employee of the Brick, and that the instructions were not themselves fraudulent. Therefore, there was knowledge and consent.

The Brick's Argument

The focus should be on the fraud itself, rather than our employee's instructions. There was a crime involving electronics – it was reasonable to expect this would be covered.

Outcome

Coverage denied. The Brick was not entitled to recover from Chubb because the Brick's agent had knowledge and consent of the instructions being given. The transfer was not enacted by a third party, it was done by a Brick employee.

In reaching its decision, the Court cited U.S. jurisprudence at paras. 21-22, further confirming that U.S. case law will be of importance on both sides of the border in the nascent stage of cyber insurance markets.

[3] https://www.canlii.org/en/ab/abqb/doc/2017/2017abqb413/2017abqb413.html?autocompleteStr=the%20brick%20v.%20chubb&autocompletePos=1

2 Coverage Cases: Almost (but not quite) Cyber

Apache Corporation v. Great American Insurance Company,

5th Cir.

(October 18, 2016)[4]

Coverage denied where the loss was an indirect result of cyber activity

Facts

Apache is a multinational oil-production company. In March 2013, an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed Apache to change the bank account information for its payments to Petrofac.

The Apache employee instructed the caller to provide a formal request on Petrofac letterhead. A follow up email was sent, with an attached letter on Petrofac letterhead providing a phone number to verify the change in account.

The letter also included details of Petrofac's "old" (real) bank account. The only sign (in writing) that the request was fraudulent was that the Petrofac email domain name was "petrofacltd.com." The real Petrofac domain name was simply "petrofac.com."

The Apache employee called the phone number listed on the letter, and concluded from the call that the account change request was authentic. A second (supervising) Apache employee then approved and implemented the change. Funds were transferred to the fraudsters' account, and Apache lost about $2.4M USD.

Coverage

The policy covered a loss resulting directly from the use of any computer to fraudulently cause a transfer of property from inside the premises or banking premises to a person/place outside those premises.

GAIC's Arguments

The loss did not result directly from the use of a computer.

Nor did the use of a computer cause the transfer of funds.

Apache's Arguments

The incident is clearly covered if it is accepted that the policy was designed to cover a situation where "any computer was used to fraudulently cause the transfer of funds." This reading was Apache's reasonable understanding of the policy.

Any ambiguity in the policy terms should be resolved in favor of the insured's reasonable interpretation, even if the insurer's interpretation is more reasonable, objectively speaking.

Outcome

Judgment rendered for GAIC, as the email was found to be "merely incidental" to the transfer.

The computer use was viewed as a single small step in an unfortunate multi-step process that led to the authorized transfer of money. The computer use did not fraudulently cause the transfer. Rather, the transfer was initiated because Apache elected to pay its legitimate invoices to the wrong bank account.

The Court gave examples of ways that Apache could have handled the request in a safer manner. For instance, Apache could have investigated its own records with the information provided during the initial phone call. It could have also investigated the follow-up email/letter in a more prudent manner – it could have called an independent phone number for Petrofac instead of relying on the number from the letter.

[4] No hyperlink is available for our U.S. case law, but please feel free to contact Chris Macaulay (or any of our other cyber lawyers) for a copy of any case referenced in Percipience. Chris can be reached at cmacaulay@schultzfrost.com

3 Bona Fide Cyber Coverage

The below case involved a coverage dispute resulting from a true cyber policy.

P.F. Chang's China Bistro, Inc. v. Federal Insurance Company,

D. Ariz.,

May 26, 2016

Coverage denied where the insured did not directly suffer the loss

Facts

On June 10, 2014, P.F. Chang's learned that computer hackers had obtained and posted on the Internet approximately 60,000 credit card numbers belonging to its customers. Chang's notified Federal of the data breach on the same day.

Chang's had an agreement with BAMS, a credit processing entity who had its own agreements with all major credit issuers (e.g. VISA, MasterCard etc.). Whenever a credit card was used at a Chang's restaurant, Chang's delivered the customer's credit card info to BAMS, who then settled the transaction though an automated clearinghouse; BAMS then credited Chang's account for the amount of the payment.

MasterCard performed a "fraud recovery" investigation concerning the data breach, and billed BAMS almost $2M for the investigation. BAMS then sought to recover the costs from Chang's. The agreement between Chang's and BAMS clearly stipulated that Chang's would be responsible for payment resulting from this type of incident. Chang's paid for the investigation, but then sought indemnity for the expense from Federal under its cyber policy.

Federal brought a summary judgment motion and argued that the policy did not cover the expenses.

Coverage

The policy covered losses on behalf of an insured on account of any claim first made against the insured for injury (the term 'injury' explicitly encompassed 'privacy injuries'). The policy also covered 'privacy notification expenses' incurred by an insured resulting from a privacy injury. Finally, the policy was also broadly marketed as a "flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world."

Exclusions

There were multiple exclusions to support that there would be no coverage for contractual obligations that an insured assumed with a third party outside the policy.

Federal's Arguments

Neither Chang's nor BAMS sustained any privacy injury. The record of the issuing banks sustained the injury, not the BAMS record. Chang's was one step further removed than BAMS, and likewise suffered no privacy injury.

Chang's did not incur the privacy notification expenses, BAMS did.

Lastly, the policy exclusions should apply as per their plain meaning.

Chang's Arguments

A privacy injury existed and the associated costs were levied against them – the fact that it was not Chang's who directly suffered the injury was immaterial.

The fact that BAMS initially "incurred" the expenses was immaterial, because it was Chang's who was ultimately responsible for paying under their agreement with BAMS.

Finally, the broad policy marketing language would lead any insured to the reasonable expectation that the costs would be covered, even if they were technically excluded by the policy.

Outcome

The Court agreed with Chang's that they were the party to ultimately "incur" the costs of the MasterCard investigations. However, the Court disagreed that Chang's was the party to sustain injury, and also disagreed that the reasonable expectation doctrine could be used to overrule the clear policy exclusions. Summary judgment motion granted for Federal.

In upholding the policy exclusions, the Court noted (at page 15): "In reaching this decision, the Court turned to cases analyzing commercial general liability insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same."

The Court made a point of noting that Chang's was a sophisticated party who could have bargained for extra coverage to protect themselves from third party investigation costs at the time of policy inception with Federal. Chang's reasonable expectation doctrine arguments fell flat on this basis.

4 Looking Ahead – Cases We are Watching

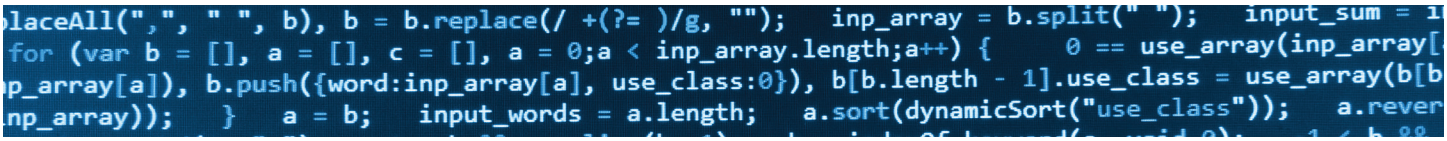
Agnew-Americano v. Equifax Canada,

2018 ONSC 275

(December 19, 2017)

Cyber breaches in the news

The Ontario litigation resulting from the well-publicized Equifax breach. In this case, the court determined which law firm would have carriage of the Ontario class action. The case law will likely clarify the standards which business owners, directors and officers are expected to adhere to when responding to a breach.



Closing Thoughts and Acknowledgments

Ransomware is on the rise. The general consensus amongst cyber security professionals is that the malicious software has overtaken social engineering fraud as cyber criminals' preferred entry method as of late. A good way to defend against ransomware is to ensure you have installed account lock-out measures after a number of failed password attempts. If you don't have a minimum of 10 characters for your own password, make the change today!

The Canadian federal government recently announced that the mandatory breach reporting requirements of the Digital Privacy Act will come into force on November 1, 2018. Stay tuned for our take on the new requirements.

Schultz Frost would like to extend a warm thank you to Kivu Consulting for giving a dynamic and engaging presentation on cyber security issues to our team on April 18, 2018. If you need a Pen Test or an External Vulnerability Assessment, be sure to consider Kivu's world-class services.

schultz frost LLP

www.schultzfrost.com

151 Yonge Street, Suite 1302 Toronto, ON M5C 2W7 • t 416-969-3434 • f 416-949-3435

Schultz Frost Cyber Contacts

Kadey B.J. Schultz | Chris Macaulay | Marija Tasevska | Adrita Shah Noor | Amar Ramasamy