



## Tell Them The North Remembers: Canadian Courts Follow American Courts' Lead In Interpreting Social Engineering Fraud Coverage



**Chris McKibbin and  
Devra Charney**  
FCL LLP

*Chris McKibbin is a partner and  
Devra Charney is an associate with  
FCL LLP in Toronto.*

### 1. Introduction

The proliferation of social engineering fraud losses in the 2010s resulted in American and Canadian insurers introducing social engineering fraud coverages by endorsement to fidelity and crime policies and, in some cases, to base policy insuring agreements. Social engineering fraud losses have now generated a significant body of American jurisprudence.

Canadian courts, by contrast, have only had occasion to render two decisions on social engineering fraud losses, consistent with the significantly smaller body of Canadian case law on fidelity coverage issues generally. This can be explained by several factors, including Canada's much smaller population; different summary judgment rules, which make summary judgment motions less common; and perhaps more use of ADR, resulting from mandatory mediation requirements in many jurisdictions. Nevertheless, when called upon, Canadian courts have affirmed the approach taken by most American courts that social engineering fraud losses are distinct from the types of losses covered under "traditional" Computer Fraud and Funds Transfer Fraud insuring agreements.

### 2. Coverage for Social Engineering Fraud Losses

Generally speaking, commercial crime policies in Canada are fairly similar to their American counterparts. This is due both to the use of standard wordings across the border, as well as the fact that many of Canada's crime insurers are subsidiaries of American parents. Canadian courts have held that, where there is little or no Canadian authority interpreting language commonly used in standard form insurance contracts in both Canada and the United States, they will look to American authorities to ensure uniformity in the construction of insurance contracts in use in both countries.<sup>1</sup>

In *The Brick Warehouse LP v. Chubb Insurance Co. of Canada*,<sup>2</sup> the Court of Queen's Bench of Alberta considered whether a social engineering fraud was

[Read more on page 18](#)

<sup>1</sup> *Halifax Ins. Co. of Canada v. Innopex Ltd.* (2004), 72 O.R. 3d 522, para. 56 (C.A.); *Zurich Ins. v. 686234 Ontario Ltd.* (2002), 62 O.R. 3d 447, 461 (C.A.).

<sup>2</sup> *The Brick Warehouse LP v. Chubb Insurance Co. of Canada*, 2017 ABQB 413 (Can.).



*Tell Them... continued from page 7*

covered under a crime insurance policy held by The Brick Warehouse LP (“The Brick”). Funds were transferred out of The Brick’s account by an employee of The Brick as a result of fraudulent faxes directed to the employee, which induced the employee to change a legitimate vendor’s banking information. The Brick asserted that its loss was covered under the Funds Transfer Fraud insuring agreement, which indemnified for “*Funds Transfer Fraud by a Third Party*,” and defined Funds Transfer Fraud as:

[T]he 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.<sup>3</sup>

The court held that, in order for The Brick to be successful, it must show that its bank transferred funds out of The Brick’s account pursuant to instructions from a third party impersonating The Brick. The loss would not be covered if The Brick knew about or consented to the instructions given to its bank. The court held that the insurer was not liable because the transfer was done with The Brick’s consent, and even if The Brick did not consent, the third party did not affect the transfer. Although the emails containing the fraudulent instructions were from a third party, the actual transfer instructions were issued by an employee of The Brick.

In *Future Electronics Inc. (Distribution) Pte Ltd. v. Chubb Insurance Co. of Canada*,<sup>4</sup> the Québec Superior Court relied on the decision in *The Brick* in deciding the substantive coverage issue on a common law analysis rather than a Civil Code analysis.<sup>5</sup> The fraudsters, masquerading as representatives of a legitimate supplier of Future Electronics Inc. (Distribution) Pte Ltd. (“Future”), induced employees of Future’s accounting department to transfer funds to accounts that the perpetrators maintained with various overseas banks rather than to the account of the rightful supplier. All communications between Future’s employees and the perpetrators occurred by email or telephone. Future asserted that its loss was covered under both the Computer Fraud and the Funds Transfer Fraud insuring agreements.

---

<sup>3</sup> *Id.* at para. 18.

<sup>4</sup> *Future Electronics Inc. (Distribution) Pte Ltd. v. Chubb Insurance Co. of Canada*, 2020 QCCS 3042 (Can.).

<sup>5</sup> Québec uses a civil law system somewhat similar to that of Louisiana. However, it is not uncommon for Québec courts to consider common law jurisprudence from the rest of Canada (or the United States) in interpreting standard-form insurance contracts.



The court concluded that the loss was not covered under the Computer Fraud insuring agreement because the fraudsters did not unlawfully take any funds from Future by the means of their computer system. Rather, the fraudsters unlawfully caused Future to voluntarily relinquish its funds to the fraudsters through the intentional misleading of Future's employees, during communications held by email and, on one or two occasions, by phone.

The court also declined to find coverage under the Funds Transfer Fraud insuring agreement. Although Future's employees did not know that the perpetrators' instructions were fraudulent, they expressly authorized and consented to the monetary transfers out of Future's bank account. As in *The Brick*, there were no direct communications between the fraudsters and the insured's bank.

The decisions in *The Brick* and *Future Electronics* are consistent with American case law. The court in *The Brick* relied on *Taylor & Lieberman v. Federal Insurance Co.*<sup>6</sup> In *Taylor and Lieberman*, 2015 WL 3824130, emails were sent to the insured's employee, who then acted upon them, transferring money out of the insured's account. The emails were fraudulent. The court held that the insurer was not liable because the employee requested and knew about the transfers, even though the email instructions inducing the employee to authorize the transfers were fraudulent.

In *Future Electronics*, the court was guided by *Apache Corp. v. Great American Insurance Co.*,<sup>7</sup> a decision of the Fifth Circuit Court of Appeals. In *Apache Corporation*, 662 F. App'x 252, the Fifth Circuit concluded that a loss, which had occurred under similar circumstances to the loss in *Future Electronics*, was not covered under the insurance policy's Computer Fraud insuring agreement. The Fifth Circuit stated that the fraudulent email at issue was part of the scheme, but that the email was merely incidental to the occurrence of the authorized transfer of money. The court observed that few, if any, modern fraudulent schemes would not involve some form of computer-facilitated communication:

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**

<sup>6</sup> *Taylor & Lieberman v. Fed. Ins. Co.*, No. CV 14-3608 RSWL SHX, 2015 WL 3824130 (C.D. Cal. June 18, 2015), *aff'd*, 681 F. App'x 627 (9th Cir. 2017).

<sup>7</sup> *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016).



**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.<sup>8</sup>

The court in *Future Electronics* also held that the Exchange or Purchase exclusion would apply to Future’s claimed loss. The form of exclusion at issue provided that:

Coverage hereunder does not apply to: ... loss due to an Insured knowingly having given or surrendered Money, Securities or Property in exchange or purchase to a Third Party, not in collusion with an Employee. This exclusion shall not apply to Money Orders and Counterfeit Currency Fraud;<sup>9</sup>

The court held that the language of the exclusion was unambiguous and applied to any voluntary parting of property by the insured, in exchange or purchase, to a third party. Thus, the exclusion would have applied to exclude the loss if the court had found that either the Computer Fraud or the Funds Transfer Fraud insuring agreements applied.<sup>10</sup>

### 3. Social Engineering Fraud and “Other Insurance” Provisions

A recent Ontario decision interpreting a commercial property policy raises the possibility that social engineering frauds might fall into coverage in policies other than crime policies. This raises the possibility that a crime insurer that has paid out on a social engineering fraud loss may look to other parties to recover part of its indemnity payment, whether through equitable contribution or subrogation.

First, a brief explanation on the Canadian law of equitable contribution among insurers is helpful. The Supreme Court of Canada has held that, where multiple policies, of any kind, are triggered by the same loss, the insurers are each equally liable to the insured<sup>11</sup> and are also, as a matter of equity, entitled to seek contribution amongst themselves.<sup>12</sup> In so holding, the Supreme Court of Canada expressly rejected the “closeness to the risk” or “Minnesota” approach adopted by some American courts.<sup>13</sup>

---

<sup>8</sup> *Id.* at 258 (emphasis added).

<sup>9</sup> *Future Electronics*, *supra* note 4, at para. 97.

<sup>10</sup> *Id.* at paras. 99-100.

<sup>11</sup> Net of their respective deductibles and up to their respective limits.

<sup>12</sup> *Family Insurance Corp. v. Lombard Canada Ltd.*, 2002 SCC 48 (Can.).

<sup>13</sup> *Id.* at paras. 24-27.



The recent decision of the Ontario Superior Court of Justice in *Heart Zap Services Inc. v. Lloyd's Underwriters*<sup>14</sup> raises the possibility that, if a crime insurer has paid out on a social engineering fraud loss under a social engineering fraud-specific coverage, the crime insurer may look for equitable contribution from the insured's commercial property insurer.

In *Heart Zap*, the insured was contacted by an individual who placed an order that turned out to be fake. Nevertheless, the ordered property was shipped, the perpetrator was never identified, and the shipped property was never located. The insured filed a claim under its all-risks commercial property policy with the insurer, which was ultimately denied. The court granted summary judgment in favor of the insured, holding that the property was lost from a location which was an insured location under the policy because the location of a loss from fraud or theft is suffered not where the fraudsters are, but rather, the location from which the goods are taken. The court held that the type of loss suffered by the insured was covered by the property policy because there was no consensus *ad idem* and therefore no contract of sale was formed, and so the insured did not voluntarily convey the ordered property. The court held that the lost property was not sold under a conditional sale because the vendor's consent to sell was obtained by fraud.

Most, but not all, social engineering fraud coverages in crime policies are limited in scope to Money or Securities, as defined, as the classes of covered property. These forms of the coverage are drafted so as to not cover the loss of tangible goods through fraudulent misrepresentation, as happened in *Heart Zap*. If the social engineering coverage does extend to tangible property, then the crime insurer is within its rights to ascertain whether the insured also maintained commercial property insurance which might respond. In such circumstances, the crime insurer may be able to seek equitable contribution from the commercial property insurer. Theoretically, the risks should dovetail; however, in practice, overlaps can occur. For this reason, it is essential for Canadian fidelity claims professionals to obtain copies of any other coverages which may potentially respond on behalf of common insureds. For example, where a social engineering fraud targets a law firm, the fidelity insurer might seek a copy of the law firm's errors and omissions policy to ascertain whether there is trust shortage coverage which might respond to the loss.

---

<sup>14</sup> *Heart Zap Services Inc. v. Lloyd's Underwriters*, 2019 ONSC 3667 (Can.).





Alternatively, if the social engineering coverage in issue does not extend to tangible goods, the crime insurer may nevertheless point to the commercial property insurer as the appropriate entity to deal with their common insured's loss.

#### 4. Conclusion

Canadian courts have provided helpful guidance for claims professionals in the analysis and adjustment of future claims. Courts have reinforced insurers' intent that Computer Fraud and Funds Transfer Fraud insuring agreements do not respond to these types of losses and should not be misinterpreted so as to fill a so-called "gap" in coverage caused by inadequate or missing social engineering fraud coverage. These cases also serve as a reminder to businesses (and to their brokers) of how a business may be exposed to an uninsured loss if it does not maintain appropriate social engineering fraud coverage. ➤

## DIVERSE SPEAKERS DIRECTORY

Open to both ABA and Non-ABA members.



The Directory allows you to create a customized Speaker Profile and market your experience and skillset to more than 3,500 ABA entities seeking speakers around the country and the world.

Please contact TIPS Staff **Norma Campos** if you are sourcing speakers or authors for your programs and publications

[norma.campos@americanbar.org](mailto:norma.campos@americanbar.org)