Blaney McMurtry LLP

PUBLICATION

Ninth Circuit finds No Coverage under Crime Policy for Client Funds lost in Social Engineering Fraud, 35 Can. J. Ins. L. 119 (July 2017)

Date: July 2017

LexisNexis Canadian Journal of Insurance Law

This article originally appeared on Blaneys Fidelity Blog, and was republished in the Canadian Journal of Insurance Law (2017) vol. 35, no. 4.

In the March 9, 2017 decision of Taylor & Lieberman v. Federal Insurance Company,[1] the Ninth Circuit Court of Appeals affirmed a decision of the U.S. District Court for the Central District of California holding that a business management firm did not have coverage in respect of client funds which it was fraudulently induced to wire overseas.

While the District Court had held that the insured had failed to establish that it had sustained any "direct" loss at all,[2] the Ninth Circuit affirmed the result on other grounds, holding that the insured had also failed to establish that the loss came within the substantive requirements of any of the Forgery, Computer Fraud or Funds Transfer Fraud insuring agreements.

The Facts

Taylor & Lieberman ("T&L") was an accounting firm which also performed business management and account oversight services for various clients, including the client in issue. Clients' funds were held in separate bank accounts maintained with City National Bank. Clients granted Powers of Attorney over their accounts to a designated individual at T&L, permitting transactions to be made in the accounts.

A fraudster obtained access to the client's email account and sent two emails from that account to a T&L employee, as follows:

- The first email directed the employee to wire $94,280 to an account in Malaysia. The employee did so, and then sent a confirming email to the client's email account.

- The next day, the employee received another email from the client's account directing her to wire $98,485 to an account in Singapore. The employee again complied, and again sent a confirming email to the client's email account.

The employee then received a third email, purportedly from the client, but sent from a different email address. The employee contacted the client by phone, and discovered that all three emails were fraudulent. T&L was able to recover some of the funds, but had to reimburse its client and incurred a net loss of nearly $100,000.

T&L submitted a claim under each of its Forgery Coverage, its Computer Fraud Coverage and its Funds Transfer Fraud Coverage. The District Court held that each of these coverages required "direct loss sustained by an Insured" and that, as a matter of law, no direct loss had been sustained.

On appeal, the Ninth Circuit did not disturb the finding with respect to direct loss, but affirmed the result on the basis that T&L had failed to establish that the loss came within the scope of any of the insuring agreements.

The Forgery Coverage

The Ninth Circuit quickly dismissed T&L's contention that this insuring agreement's requirement of a "Forgery or alteration of a financial instrument" did not require proof of a "Forgery" of a financial instrument, because the insuring agreement required only proof of an alteration of a financial instrument or a free-standing "Forgery" of any document, of any type. The Court held that the insuring agreement plainly required either a "Forgery" or an alteration of a financial instrument.

More substantively, the Court rejected T&L's contention that the emails to T&L were financial instruments:

Here, the emails instructing T&L to wire money were not financial instruments, like checks, drafts, or the like. See Vons Cos., Inc. v. Fed. Ins. Co. … (C.D. Cal. 1998) (holding that wire instructions, invoices, and purchase orders were not "documents of the same type and effect as checks and drafts."). And even if the emails were considered equivalent to checks or drafts, they were not "made, drawn by, or drawn upon" T&L, the insured. Rather, they simply directed T&L to wire money from T&L's client's account. In sum, there is no forgery coverage.

The Computer Fraud Coverage

The Computer Fraud insuring agreement required T&L to demonstrate "an unauthorized (1) "entry into" its computer system, and (2) "introduction of instructions" that "propogate[d] themselves" through its computer system." The Court held that the sending of an email, without more, did not constitute an unauthorized entry into T&L's computer system. Further, the emails were not an unauthorized introduction of instructions that propagated themselves through T&L's computer system:

The emails instructed T&L to effectuate certain wire transfers. However, under a common sense reading of the policy, these are not the type of instructions that the policy was designed to cover, like the introduction of malicious computer code. … Additionally, the instructions did not, as in the case of a virus, propagate themselves throughout T&L's computer system; rather, they were simply part of the text of three emails.

The Funds Transfer Fraud Coverage

The Funds Transfer Fraud insuring agreement indemnified against:

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 Organization at such Institution, without an Insured Organization's knowledge or consent.

The Court held that the requirements of the insuring agreement were not met:

This coverage is inapplicable because T&L requested and knew about the wire transfers. After receiving the fraudulent emails, T&L directed its client's bank to wire the funds. T&L then sent emails confirming the transfers to its client's email address. Although T&L did not know that the emailed instructions were fraudulent, it did know about the wire transfers.

Moreover, T&L's receipt of the emails from its client's account does not trigger coverage because T&L is not a financial institution.

As a result, there was no coverage available under the Federal policy.

Conclusion

Following the Fifth Circuit's decision in Apache,[3] the Ninth Circuit's decision in Taylor & Lieberman provides another example of a clear trend on the part of the courts to refuse to find coverage for social engineering fraud losses under the "traditional" crime policy coverages (typically, computer fraud and funds transfer fraud coverages, but occasionally, as here, other coverages as well). The proliferation of social engineering frauds has created a new exposure for insureds, and fidelity insurers have responded by creating discrete social engineering fraud coverages. Like Apache, Taylor & Lieberman serves as a cautionary tale to businesses (and to their brokers) of how a business may be exposed to an uninsured loss in the event that it does not maintain such coverage.

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

David S. Wilson and Chris McKibbin are partners with the Fidelity Practice Group of Blaney McMurtry LLP in Toronto. Their fidelity insurance practice encompasses all aspects of coverage analysis and litigation involving fidelity bonds, commercial crime policies and financial

institution bonds, as well as fraud subrogation work against employees, co-conspirators, auditors and financial institutions. David and Chris are co-editors of Blaneys Fidelity Blog [https://blaneysfidelityblog.com/].

---

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

[2] Taylor & Lieberman v. Federal Insurance Company, 2015 WL 3824130 (C.D. Cal.).

[3] Apache Corporation v. Great American Insurance Company, 2016 WL 6090901 (5th Cir.).