

BRIEFING NOTE

Social Engineering Fraud & Crime Policy Coverage – The Latest Chapter?

In the last few years there have been a number of decisions considering insurance coverage under crime policies for Corporations whose employees have sent money to fraudsters, as a result of e-mail instructions. Such instructions have masqueraded as being from company officers (e.g. *Medidata Solutions, Inc. v. Federal Insurance Company*), vendors (e.g. *American Tooling Center Inc. v. Travelers Casualty and Surety Co., & The Brick Warehouse LP v. Chubb Insurance Company of Canada*), and clients (e.g. *Taylor and Lieberman v Federal Insurance Company*). In the latest iteration, a United States District Court (New Jersey), has considered whether a corporation's crime policy covered funds that were due to the company from a vendor, but paid to a fraudster as a result of fake e-mails sent to the vendor.

In *Posco Daewoo America Corp. v. Allnex USA Inc. and Travelers Casualty and Surety Company of America*, 2017 WL 4922014 (D.N.J.) PD had supplied product to Allnex, for which Allnex owed payment. An impostor, posing as an employee of PD's accounts receivable department sent fraudulent e-mails to Allnex, instructing payment to be made to his/her own account. Approximately \$US650,000 was transferred, of which Allnex recovered approximately \$US260,000 once the fraud was uncovered. PD sued it for the balance. Allnex alleged that the unrecovered payments satisfied the balance it owed to PD.

PD also sued Travelers for coverage under its "Wrap and Crime" insurance policy. Travelers brought a motion to dismiss. In order to successfully defend the motion, all PD had to show was *inter alia* that the pleaded claim contained "*sufficient factual matter that is plausible on its face*".

The court allowed Travelers application, finding that the following provision was dispositive:

The property covered under this Crime Policy ... is limited to property:

i. that the Insured owns or leases;

ii. that the Insured holds for others:

*(a) on the Insured's Premises or the Insured's Financial Institution Premises;
or*

(b) while in transit and in the care and custody of a Messenger; or

Guild Yule LLP

BARRISTERS AND SOLICITORS

2100 – 1075 Georgia Street

Vancouver, BC V6E 3C9

www.guildyule.com

P 604 688 1221

F 604 688 1315

E feedback@guildyule.com

iii. for which the Insured is legally liable, except for property located inside the Insured's Client's Premises or the Insured's Client's Financial Institution Premises.

The court found that PD did not own the money that Allnex transferred to the fraudster. The monies at issue did not fall within the “*property covered*”, until received by PD; while it had a right to collect payment and a cause of action to enforce that right, it did not own the funds at the time they were diverted.

As the court's analysis rested solely on this provision, it felt it did not need to address at all, other issues raised, including whether the fraud amounted to a “... *direct loss of ... Money, ... directly caused by Computer Fraud*”.

The parties agreed that an intervening event took place between the impostor sending Allnex an e-mail and the money appearing in the fraudster's bank accounts. Travelers had argued that “direct loss” required the absence of intervening events, however PD and Allnex both argued that a loss resulting from a chain of events qualified as a “direct loss”. The meaning attributed to this phrase is the subject of divergent case authority; with the *Medidata* trial decision siding with PD's position (the decision was upheld on appeal, but on other grounds), and *American Tooling Centre*, siding with Travelers position. Whether a further (obiter) decision here, would have assisted in clarity is debatable. Given the *American Tooling Centre* decision appears to have considered an identical Travelers policy, that would seem the more likely precedent to follow, however if the Court had followed *Medidata*, that also would not have assisted in predictability of decisions in this area.

It is also of interest that it was PD and not Allnex who brought this action against their insurer. Perhaps it was because Allnex not only had no cyber cover, but also no crime coverage? At first brush, that would seem surprising given they appear to be a large, multinational company.

Finally, it is doubtful that, even if PD had a cyber-liability policy, it would provide coverage for what is in essence a loss suffered by its customer. However, the following common social engineering fraud extension, would have provided coverage to Allnex (if it had had such a policy):

We agree to reimburse you for loss first discovered and notified to us during the period of the policy as a direct result of any third party committing:

...any phishing, vishing or other social engineering attack against an employee or a senior executive officer that results in the inadvertent transfer of funds to an unintended third party.



Adam Howden-Duke
Email: ahd@guildyule.com
Direct Line: 604-844-5505

Guild Yule LLP

BARRISTERS AND SOLICITORS

2100 – 1075 Georgia Street

Vancouver, BC V6E 3C9

www.guildyule.com

P 604 688 1221

F 604 688 1315

E feedback@guildyule.com