**Aon Risk Solutions**
Financial Services Group

# At-a-Glance

Issue 70 July 2018

## In this Issue

1 U.S. appeal courts find social engineering coverage under commercial crime policies

2 Data breach D&O lawsuits on the rise?

3 Items of Note

4 Key Contacts

## U.S. appeal courts find social engineering coverage under commercial crime policies

In the first of two consecutive precedent setting decisions, the U.S. Second Circuit Court of Appeals in *Medidata Solutions Inc. v. Federal Insurance Co.* (Medidata Action) found that social engineering coverage existed under a commercial crime insurance policy. Medidata Solutions, Inc. (Medidata), the insured, was planning an acquisition in 2014, which it advised its finance department of at the time. Fraudsters targeted an accounts payable clerk at the company, who received a fraudulent email purportedly sent by Medidata's president advising that an attorney would contact the clerk. The clerk then received a phone call from the faux attorney who provided payment instructions in connection with the acquisition. A subsequent email from the imposter "president" confirmed the payment instructions, following which the clerk initiated a $4.77 million wire transfer to the fraudsters. Typically, when Medidata employees receive emails from internal colleagues, the sender's full name, email address and picture would appear, contrary to emails received from external third parties. One of the key facts of this case was that the emails received by the clerk contained the president's name, email address and picture in the "From" field. The fraudsters had entered the company's email system and introduced "spoofing code" to alter the email system's appearance to misleadingly indicate that the sender was a trusted internal party.

Medidata sued the insurer following a denial of coverage for the $4.77 million loss under its commercial crime policy. In affirming the Southern District of New York's ruling, the Second Circuit, applying New York law, found that both the Computer Fraud and Funds Transfer Fraud coverage sections provided coverage for Medidata's loss. Even though there was no hack into Medidata's systems, the court concluded that the attack on the company's email system (which the parties agreed constituted a "computer system" within the meaning of the policy) by way of the implantation of spoofing code amounted to a fraudulent entry of data into the insured's computer system. Also in accordance with the policy wording, there was a "change to a data element" as the code altered the appearance of the email system to disguise the identity of the sender. In perhaps the most significant aspect of the court's judgment, a causal and proximate relationship was found to exist between the social engineering fraud and the loss, thereby meeting the "direct loss" requirement of the policy. Other courts had previously denied coverage on the basis that the actions taken by company employees in effecting fund transfers in typical social engineering fraud cases sever the causal connection, thereby preventing a "direct loss" from occurring and precluding coverage.

In a second decision released shortly thereafter, the Sixth Circuit Court of Appeals similarly found that coverage applied to a social engineering loss under the Computer Fraud coverage section of the insured's commercial crime policy. In *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America* (ATC Action) the insured, American Tooling Center (ATC), received fraudulent emails appearing to be from one of ATC's legitimate vendors redirecting payment to a different bank account. ATC proceeded to make numerous transfers to the imposters, totaling approximately $830,000 before the fraud was discovered. After the insurer denied coverage, ATC filed a lawsuit. At the outset, the district court sided with the insurer and denied coverage. However, in overruling the decision, the Sixth Circuit's judgment both confirmed and clarified certain points initially addressed in the Medidata Action.

Like the ruling in the Medidata Action, the court found that the insured had incurred a "direct loss", irrespective of whether that phrase referred to either "proximate" or "immediate" causation. The court also found that the definition of "Computer Fraud" contained within the policy was met, and rejected the insurer's attempt to limit the definition to hacking or other penetrations of the insured's computer system. This finding is especially significant, as, in the Medidata Action, the "Computer Fraud" coverage found by the court was heavily dependent upon the facts pertaining to the loss – namely, a fraudster had accessed and altered Medidata's email system to make the fraudulent emails appear authentic. In this case, no such system penetration was present, making the ATC decision a broader, and potentially stronger, precedent for policyholders to leverage in future social engineering coverage disputes.

While these decisions may signal a change in the tide of judicial opinion regarding coverage for social engineering losses, it is important to note that the outcome of each case is highly dependent on the specific facts and circumstances surrounding the loss, and the policy wording at issue. Coverage was found to exist in these two cases, but it cannot be assumed that a commercial crime policy will definitively cover social engineering losses. Furthermore, U.S. decisions are not binding on courts in Canada, and, regardless of such, the legal landscape is littered with conflicting decisions in this area. It is prudent for those insureds seeking social engineering coverage to purchase a specialized social engineering endorsement to be added to their commercial crime policy. Typically sold for an extra premium, this endorsement is designed to respond to social engineering losses and can ensure a degree of certainty in the coverage provided. This certainty may be required in the near future as, in light of these decisions, it is anticipated that insurers may alter current policy language to clarify the intent to exclude social engineering coverage from the Computer Fraud insuring agreement.

# Data breach D&O lawsuits on the rise?

Akin to the canary in the mineshaft, litigation trends in the U.S. often serve as a precursor to those experienced in Canada. Several high-profile data breaches in the U.S. have led to shareholder D&O lawsuits, either in the form of a derivative action or a securities class action. Shareholder derivative lawsuits were filed in the U.S. against companies such as Wendy's, Wyndham Worldwide, Target and Home Depot. While some of these suits were dismissed and others were settled by way of non-monetary remedial measures, a couple have resulted in the payment of substantial plaintiffs' attorneys' fees. Namely, Wendy's agreed to pay $950,000 and Home Depot agreed to pay up to $1.25 million in plaintiffs' attorneys' fees.

In situations where the share price has declined after a data breach, a securities class action lawsuit could be the preferable forum for aggrieved shareholders seeking compensation. In January 2018 Yahoo settled a data breach-related securities class action lawsuit in the U.S. for $80 million. The litigation stemmed from two data breaches Yahoo experienced in 2016, which ultimately compromised PII associated with over 1 billion user accounts. Following the two data breaches, Yahoo's share price declined 3.06% and 6.11% respectively.

While Canada hasn't had the same history with respect to data breach D&O litigation, some legal and insurance experts predict that it's only a matter of time until aggrieved shareholders north of the border turn their attention to directors and officers for recovery. A directors' and officers' liability insurance policy can provide indemnification for settlements, judgments and defence costs should a board member or executive face allegations of wrongdoing stemming from a data breach. In the case of Wendy's, discussed above, the company's D&O policy responded to pay the $950,000 in plaintiffs' attorneys' fees. Where the corporate entity faces a securities lawsuit, it may also have coverage for the costs it incurs in defending or resolving these claims.

# Items of Note

- In June 2018, Bithumb, a South Korean cryptocurrency exchange, was hacked, resulting in the theft of approximately $31 million in cryptocurrency. Bithumb ranks as the sixth largest cryptocurrency trading exchange globally.
- On 17 May 2018, B.C.'s Bill 21, the Class Proceedings Amendment Act, 2018, received Royal Assent. Previously known as one of Canada's more favourable forums for class action proceedings, Bill 21 may increase B.C.'s appeal even further in this regard due to it's change from an "opt-in" regime to a voluntarily "opt-out" regime. As such, all non-residents of B.C. will be included as members of a lawsuit automatically unless they voluntarily opt-out. This change will simplify the creation of national classes, and, along with the other changes contained in Bill 21, will assist in bringing B.C.'s class action regime in line with other provinces such as Ontario, Alberta and Saskatchewan.
- Natural Resources Canada has released a revised Extractive Sector Transparency Measures Act (ESTMA) guidance document, reporting template and verification checklist after reviewing the first reporting cycle under the ESTMA. These documents are meant to be a resource for companies in helping to clarify the various reporting obligations under the legislation.
- On 11 June 2018, the Canadian Securities Administrators (CSA) published CSA Staff Notice 46-308- Securities Law Implications for Offerings of Tokens, which aims to provide practical guidance on the application of Canadian securities laws to initial coin/token offerings.

# Key Contacts

**Brian Rosenbaum LL.B**
Senior Vice President and National Director
Financial Services Group
Legal and Research Practice
t +1.416.868.2411
brian.rosenbaum@aon.ca

**Desiree Money, CAIB, CRM**
Senior Vice President and Regional Manager
Financial Services Group
t +1.403.267.7754
desiree.money@aon.ca

**Denise Hall**
Senior Vice President and National Broking Leader
Financial Services Group
t +1.416.868.5815
m +1.416.953.3280
denise.hall@aon.ca

**Catherine Richmond, LL.B., CRM**
Senior Vice President and Regional Manager
Financial Services Group
t +1.604.443.2429
m +1.604.318.5470
catherine.richmond@aon.ca

**Catherine Lanctôt B.A.**
Vice President and Manager
Financial Services Group
t +1.514.840.7008
catherine.lanctot@aon.ca

**Alexis Rivait**
Vice President and Team Leader
Financial Services Group
t +1.416.868.5597
alexis.rivait@aon.ca