HUNTON& WILLIAMS

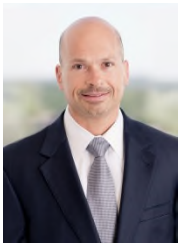
Lawyer Insights

November 1, 2017

Will Your Crime Insurance Cover Cyber?

by Michael Levine and Jennifer White

Published in Risk Management Magazine




Employees at four different businesses in four different states were tricked into wiring money to cybercriminals who used fraudulent emails to impersonate legitimate vendors, clients or company executives. Each business lost hundreds of thousands of dollars, and some lost millions. Each business sought coverage for its loss under similar crime insurance policies, but was denied. Ultimately, judges found coverage in Medidata Solutions, Inc. v. Federal Insurance Co. and Principal Solutions Group, LLC v. Ironshore Indemnity Inc., but did not in Apache v. Great American Ins. Co. and American Tooling Center, Inc. v. Travelers Casualty & Surety Company of America.

The similarities and differences among these four cases provide useful insight to businesses looking to recover money lost to social engineering scams and other types of fraudulent transfers. As courts continue to grapple with whether social engineering losses are covered under standard crime forms, policyholders should take steps to control what they can in anticipation of crime losses. While factors like jurisdiction cannot be controlled, others, such as policy terms, business protocol and vendor relations, can be and thus must be chosen carefully to ensure that the coverages obtained adequately match the risks.

Lesson One: Emails matter. The cybercriminals in each of the aforementioned cases used emails in their schemes. In Medidata and Principal Solutions, the criminals solicited payment from a high-level corporate officer for costs associated with a legitimate business acquisition. Preliminary emails were followed by subsequent emails from purported legal counsel (also fraudulent) and telephone calls from the same.

In American Tooling, it was the company that solicited payment from a legitimate vendor. Then, instead of receiving a response from the vendor, the company heard from an imposter who instructed the company to change its billing information. In Apache, however, the scheme started with a phone call by a purported vendor, followed by fraudulent emails instructing the accounts-payable department to change account details.

Ultimately, the rulings hinged in part on whether judges viewed the emails as critical to the loss. In Medidata and Principal, the courts viewed the emails as integral to the fraud, noting that the criminals would not have succeeded without these spoofed communications.

In American Tooling and Apache, however, the courts found the emails too attenuated from the loss; according to those courts, the emails did not cause the wire transfers, people did by failing in their processes and scrutiny.

The latter rulings are problematic for policyholders because they ignore or underestimate increasingly complex and authentic-looking cybercrime schemes. Money is seldom siphoned from a business through a single email. Instead, cybercriminals access systems, gather intelligence, lie in wait, and then use that intelligence to maximize credibility. In the Medidata incident, the cybercriminal was able to use the identities of critical personnel and confidential business information (e.g., an expected business acquisition) to convince multiple high-level employees that the funds transfer request was valid. Social engineering schemes also frequently rely on multiple forms of communication and may include multiple fabricated identities, including employees, outside legal counsel and vendors.

Crime policies must anticipate this type of complexity in the details of coverage. If they do not, social engineering endorsements may be necessary, but even those can be too narrow in terms of how fraudsters operate, especially since criminals are constantly developing new and more sophisticated tactics. Policyholders should aim for breadth and flexibility with respect to such coverage and remember that, while email is likely to be involved, it is unlikely to be the singular cause of loss.

Lesson Two: Policy definitions matter. The policy at issue in Medidata defined "computer system" broadly to include "communication facilities…utilized by" the insured and "data" as including any "representation of information." Those definitions proved pivotal in the court's decision. Medidata's email system—from which some of the fraudulent emails were sent—was hosted by Google (a system "utilized by" the insured) and the fraud was perpetrated by manipulating information in hidden system fields. The nature of the changes make the email appear to be sent from a legitimate email address and to display the correct employee profile, all while directing reply messages to the imposter's account. Had Medidata's crime policy defined the terms more narrowly—for example, to cover only systems "owned and operated by" the company, as many policies do—Medidata would have been out of luck. Thus, the case should serve as a reminder that policy definitions matter and must be tailored to each policyholder's unique risks, as well as its unique IT infrastructure, systems and vendor relationships. Policyholders should evaluate key terms with personnel who understand the inner workings of the company's technology and the role of vendors in supporting or enhancing that technology.

Lesson Three: Exclusions matter. Insurers commonly argue that fraudulently-induced losses are not covered because the purported "loss" was "authorized," either because the policy excludes coverage for "authorized" transfers or only covers "unauthorized" transfers. For example, in Apache, the court noted that the fraudulent transfer was authorized by an employee, albeit to a fraudulent bank account, and that such authorization was one of the reasons the loss was not covered. Medidata found the opposite—that actions by an "authorized" employee did not transform the cybercrime into an authorized act. This split among courts means that policyholders must pay close attention to exclusions and coverage caveats (which act like exclusions) to ensure that crime policies envision the use of employees as pawns in criminal schemes.

Lesson Four: Venue matters. In the event of a coverage dispute, the location of your business may determine whether the court finds that your crime policy covers the loss as coverage construction and application can vary widely by state. In American Tooling Center, a Michigan federal court held that precedent required strict interpretation of the term "direct," whereas cases involving similar policy

language did not in other jurisdictions. The strict interpretation meant that the court required causation without any intervening events, including human action. In other words, according to the court, the email had to effect the fraudulent transfer, not the employee's authorization based on the email.

In contrast, in Principal Solutions, a federal court in Georgia refused to apply the narrow interpretation of "direct" endorsed by the insurer, finding the term ambiguous. Because of this ambiguity, the court interpreted the policy in favor of coverage, concluding that the policyholder reasonably expected the policy would cover fraudulent money transfers even despite intervening events between the initial email and ultimate transfer.

Understanding which state's law will apply and how that law may affect policy interpretation can help you negotiate better coverage terms or gauge and prepare for potential exposure.

Lesson Five: Business protocol matters. Medidata required multi-level approval and still lost its money—in part because no one picked up the phone to confirm the president's purported written request. Just as we now use multi-factor authentication for accessing secure servers and sensitive data repositories, a similar approach should be considered for corporate finance transactions. Multi-step authentication should be multi-manner as well, meaning that old-fashioned face-to-face and verbal communication can be a helpful check on technology. Indeed, the court in Apache blamed the company's "multi-step, but flawed, process" as causing the loss, not the criminal's emails and telephone calls.

Michael S. Levine is a partner at Hunton & Williams LLP in the Washington, DC office. He has more than 20 years of experience managing, negotiating and litigating insurance disputes and advising clients on insurance coverage matters. Michael can be reached at (202) 955–1857 or mlevine@hunton.com. Jennifer White is an associate in the Washington, DC office. Her practice focuses insurance coverage counseling and litigation, with an emphasis on cyber insurance matters. Jennifer can be reached at (202) 955–1866 or jewhite@hunton.com.