Will Your Company’s Insurance Cover Losses Due to Phishing and Social Engineering Fraud?
Scott Godes

If your company fell victim to a business email compromise – a scam that frequently involves hackers fraudulently impersonating a corporate officer, vendor, business partner, or others, getting companies to wire money to the hackers – would your insurance cover? There is reason to be concerned about this sort of attack, as the FBI has explained that the “scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses” in actual and attempted losses in US dollars. The good news for policyholders is that courts across the country have been ruling that crime insurance policies should provide coverage for this sort of loss.

How do business email compromises work?

In early versions of business email compromises, the hackers send emails that appear to be from company executives, discussing corporate acquisitions or other financial transactions, and are received by company employees in the finance department. See, e.g., Medidata Sol., Inc. v. Federal Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y. 2017), aff’d, 729 F. App’x 117 (2d Cir. 2018), request for reh’g en banc denied (Aug. 23, 2018). The employee is told that the transaction is highly confidential, and that the employee should work closely with an attorney or other financial advisor to help close the deal. The employee then is told to wire money to cover the costs of the transaction, very often to a foreign country. Having been defrauded, the employee logs in to an online banking site, and approves a wire transfer.

In other versions of a business email compromise, hackers get access to email accounts of one party, sometimes via a brute force attack where an attacker breaks into a system by guessing a password, or via a phishing attack where a user is fooled into typing a username and password into a fraudulent site. Then, the hacker sends out emails from the compromised account, pretending to be a vendor, and asking for payment to be sent to a different bank account. See, e.g., Am. Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of Am., 835 F.3d 455 (6th Cir. 2018), request for reh’g en banc denied (Aug. 28, 2018). Again, having been defrauded, the employee has money wired to the fraudster, instead of to the vendor.

Will insurance cover losses due to business email compromises?

* Scott Godes is a partner at Barnes & Thornburg LLP. He represents corporate policyholders and insureds in insurance coverage matters, and focused his practice on insurance coverage for cybersecurity and data privacy matters in 2008.

3 Josh Fruhlinger, What is phishing? How this cyber attack works and how to prevent it, CSO Online (Aug. 9, 2018), https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
The answer to whether insurance carriers will cover these losses – without court intervention – is “it depends.” Recent decisions have ordered insurance carriers to provide coverage. And the insurance industry has been scrambling to write new endorsements for their insurance policies that the insurance companies say provide coverage for business email compromises.

A common place for seeking coverage for these losses is under crime insurance policies. Many crime insurance policies include coverage for “computer fraud,” “funds transfer fraud,” or even “computer and funds transfer fraud.” Exemplar “computer fraud” coverage applies to “direct loss” of money resulting from the fraudulent entry, change, or deletion of computer data, or when a computer is used to cause money to be transferred fraudulently. Exemplar “funds transfer fraud” coverage applies to direct loss of money caused by a message that initially received by the policyholder, which purports to have been sent by an employee, but was sent fraudulently by someone else, that directs a financial institution to transfer money. A reasonable policyholder, which fell victim to a fraudulent scheme via a computer, or transferred funds because of a fraudulent scheme, likely would think that computer and funds transfer fraud coverages would apply to the losses.

**What have courts said?**

Two recent decisions from federal courts of appeal, and one decision from a state court, have resulted in coverage under crime policies for business email compromise losses.

The first is the July 6, 2018, opinion issued in Medidata Solutions, Inc. v. Federal Insurance Co., 729 F. App’x 117 (2d Cir. 2018). The Medidata trial court ruled that a crime insurance policy provides coverage for a fraudulent scheme and wire transfer. 268 F. Supp. 3d 471 (S.D.N.Y. 2017). The Court of Appeals for the Second Circuit affirmed the trial court’s decision. In Medidata, the policyholder’s employees received emails that purported and appeared to be from high-level company personnel but were, in fact, sent by fraudsters. Based on those emails, and messages from purported outside counsel, Medidata wired nearly $5 million to the fraudsters. It sought coverage under a crime policy that it bought from Chubb that had computer fraud, funds transfer fraud, and other coverages. The trial court ruled that computer fraud and funds transfer fraud coverages both applied. It rejected the arguments that the loss was not “direct” because there were steps in between the original fraudulent message and the wiring of funds.

On appeal, the Second Circuit ruled that Medidata’s loss was “direct” under the insurance policy language. “Federal Insurance further argue[d],” as carriers have done in many business email compromise cases, “that Medidata did not sustain a ‘direct loss’ as a result of the spoofing attack, within the meaning of the policy.” 729 F. App’x at 119. The Court of Appeals held that because “[t]he spoofed emails directed Medidata employees to transfer funds in accordance with an acquisition, and the employees made the transfer that same day,” the loss was direct. *Id.* The court rejected the insurance carrier’s argument that the loss was not direct because “the Medidata employees themselves had to take action to effectuate the transfer”; the employees’ actions were not “sufficient to sever the causal relationship between the spoofing attack and the losses incurred.” *Id.* The Court of Appeals did not address the trial court’s ruling that funds transfer
fraud coverage applied, “[h]aving concluded the Medidata’s losses were covered under the computer fraud provision.” *Id.*

Shortly after *Medidata* was issued, the Sixth Circuit decided on July 13, 2018, that computer fraud coverage applies to losses resulting from a business email compromises in *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*, 835 F.3d 455 (6th Cir. 2018). There, the policyholder wired money to fraudsters, instead of a vendor, because of a business email compromise. The Sixth Circuit reversed the district court, ruling that the losses are “direct,” covered by crime insurance.

In a published opinion, the Court of Appeals held there was “‘direct loss’ [that] was ‘directly caused by the computer fraud[,]’ even though the policyholder had engaged in “multiple internal actions” and “signed into the banking portal and manually entered the fraudulent banking information emailed by the impersonator” after receiving the initial fraudulent emails. 835 F.3d at 462.

Holding that coverage applied, the Sixth Circuit distinguished the Eleventh Circuit’s unpublished decision regarding computer fraud coverage in *Interactive Communications v. Great American*, 731 F. App’x 929 (11th Cir. 2018). *See id.* After the policyholder in *American Tooling* had “received the fraudulent email at step one,” it “conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two.” *Id.* at 463. The loss occurred at step two; as such, “the computer fraud ‘directly caused’ [the policyholder’s] ‘direct loss.’” *Id.* By contrast, the Sixth Circuit explained, the policyholder in *Interactive Communications* only suffered losses at step four in a significantly more complicated chain of events. *See id.* at 462-63.

The third is the July 30, 2018, opinion issued in *Ubiquiti Networks, Inc. v. National Union Fire Insurance Co.*, No. 18CV322879, slip op. (Cal. Super. Ct. July 30, 2018). In *Ubiquiti*, the parties dispute whether funds transfer fraud and computer fraud coverage within a commercial crime policy provides coverage for fraudulent wire transfers. Over $46 million was wired to foreign bank accounts, because of emails and telephone calls that impersonated the CEO and outside counsel and instructed an employee to wire funds. The insurer demurred, asserting that the loss was not covered.

The *Ubiquiti* policy’s “‘Funds Transfer Fraud’ [covers loss] . . . ‘resulting directly from a ‘fraudulent instruction’ directing a financial institution to transfer, pay or deliver “funds” from your “transfer account[.]’” Slip op. at 5. One of the three definitions for “fraudulent instruction” in the *Ubiquiti* policy is “‘[a]n electronic, telegraphic, cable, teletype, teletacsimile, telephone or written instruction initially received by you which purports to have been transmitted by an “employee” but which was in fact fraudulently transmitted by someone else without your or the “employee’s” knowledge or consent.’”

The insurer asserted that the messages between the impersonator and the policyholder, then the policyholder and the bank, were not fraudulent instructions. *See* slip op. at 6. The insurer argued that the fraudulent instruction did not go to the bank first, that messages from the attorney do not qualify, and that the message from the employee to the bank was not fraudulent. *See id.* The *Ubiquiti* rejected those arguments.
The *Ubiquiti* court also discussed the application of “Computer Fraud” coverage. *See id.* That coverage applies to “loss . . . ‘resulting directly from the use of any computer to fraudulently cause a transfer of [] property from inside the “premises” or “banking premises” to “a person other than a ‘messenger’) outside those ‘premises’” or a “place outside those ‘premises.’”’” Slip op. at 6-7. The court rejected the insurance carrier’s assertion that such coverage applies only to situations in which “a ‘scheming third-party hacker [breaks] into the computer to directly cause the transfer via the computer.’” Slip op. at 7. The court refused to interpret the Computer Fraud section of the crime policy “as covering hacking only.” Slip op. at 7.

These decisions are great news for policyholders pursuing coverage under crime policies for losses resulting from business email compromises. And a best practice, in light of this new authority, is to examine denial letters carefully, giving due consideration to whether these decisions could be used to argue in favor of coverage.

**What options are available to policyholders going forward?**

Cynical viewers of insurance history might view the state of coverage as similar to what the industry has done in the past. That is, initially, cover new claims under “old” policies. Then, after claims get expensive, hire coverage counsel to tell courts why the carriers must not have meant to cover these new claims (whether the drafting history reflects such an intent or not). Next, get insurance regulators to approve exclusions purportedly tailored explicitly to the risk, and, at the same time, sell new policy endorsements (often for additional premium) that provide lower limits of coverage for the risk.

That’s what is happening in connection with insurance for business email compromises. At least one insurance group that drafts crime insurance policies has asked for a definition of computer and funds transfer fraud to be changed, and a new social engineering fraud endorsement to be approved for sale.4 Insurers have rolled out these endorsements with limits of coverage that often are capped at low amounts,5 and might also have high retentions. These endorsements frequently are available for crime policies and, sometimes, are available for cyberinsurance policies as well.

So what are some best practices for policyholders trying to structure an insurance program for these risks? These questions should provide helpful tips:

1. **What does the insurance policy include?** A best practice is to look to see whether the insurance program includes social engineering fraud endorsements or coverage parts.

2. **What are the applicable limits?** A best practice is to check the policy limits that would apply to those coverages. Binder letters might not disclose a sublimit, and the policyholder might not realize the limit of coverage is lower than the full policy limit until it is too late.

---


5 Chubb, *Social Engineering Fraud Coverage* (Aug. 28, 2018), [https://www2.chubb.com/us-en/business-insurance/social-engineering-fraud-coverage-for-crime-insurance.aspx](https://www2.chubb.com/us-en/business-insurance/social-engineering-fraud-coverage-for-crime-insurance.aspx) (stating that “[c]overage is available up to $250,000 per occurrence, with no annual aggregate, though higher limits can be considered with additional underwriting.”).
3. **Are coverages available under more than one policy?** At the time of policy renewal, a best practice is to consider asking whether social engineering fraud coverage can be added to a crime program and a cyberinsurance program.

4. **Will excess coverage apply, and, if so, when?** A best practice is to explore whether excess policies will provide this coverage, and, if so, will “drop down” to attach at the level of any sublimit, to avoid donut holes in the coverage.

5. **Will other policy provisions provide coverage, beyond narrow endorsements?** If the policyholder faces a claim, a best practice is to determine whether other coverages might apply to the losses, notwithstanding a social engineering fraud endorsement.

6. **What happens if the insurance carrier says, “no,” or that sublimits apply?** If the insurance carrier denies coverage, or tries to apply a sublimit, a final best practice is for policyholders to be mindful of the interpretation that two Courts of Appeals have used for computer fraud coverage in similar contexts.

This article should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult your own lawyer on any specific legal questions you may have concerning your situation.