BARNES & THORNBURG LLP

ARTICLES

Courts Favor Crime Coverage Of Email Hacks – For Now

March 1, 2019 | Washington, D.C.

Courts weigh in on whether crime insurance policies should cover losses due to business email compromises – and insurance companies move to adapt.

If your company were to fall victim to a business email compromise (BEC) – a scam where hackers induce fraudulent wire transfers by impersonating a corporate officer, vendor or business partner – would your insurance cover the loss? There is reason to be concerned. According to the FBI, 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 percent increase in identified global exposed losses." 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, at least where it is not specifically excluded.

Understanding How BEC Scams Work

In some versions of the scam, fraudsters send an email to a company's finance department that appears to be from a company executive, usually discussing corporate acquisitions or other financial transactions. The employee in the finance department is told that the transaction is highly confidential and that they 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, often to a foreign country. Having been tricked, the employee logs in to an online banking site and approves a wire transfer.

RELATED PEOPLE

Scott N. Godes
Partner
Washington, D.C.

P 202-408-6928
F 202-289-1330
scott.godes@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

In other versions of a BEC, hackers get access to the email account of one party, sometimes via a brute force or phishing attack. 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 – whereby the deceived employee is tricked into wiring money to the fraudster.

Using Insurance to Cover Losses

Many crime insurance policies include coverage for "computer fraud," "funds transfer fraud," or even "computer and funds transfer fraud." Computer fraud coverage typically applies to the "direct loss" of money from a fraudulent entry, change or deletion of computer data, or when a computer is used to cause money to be transferred fraudulently. Funds transfer fraud coverage typically applies to the direct loss of money caused by a message that was purportedly sent by an employee but was actually sent by someone else, fraudulently directing a financial institution to transfer money.

A reasonable policyholder, having fallen victim to a fraudulent scheme via a computer, or having transferred funds because of a fraudulent scheme, would likely expect computer fraud and/or funds transfer fraud coverage to apply to those losses. The question, however, is whether the courts agree.

What the Courts Say

Recent decisions from federal courts of appeal have resulted in coverage under crime policies for BEC losses. The first was the July 6, 2018, opinion issued in *Medidata Solutions, Inc. v. Federal Insurance Co.*, No. 17-2492 (2d Cir.). The *Medidata* trial court ruled that a crime insurance policy provides coverage for a fraudulent scheme and wire transfer. The Court of Appeals for the Second Circuit affirmed the trial court's decision.

Shortly after *Medidata* was issued, the Sixth Circuit decided on July 13, 2018, that computer fraud coverage applied to losses resulting from a BEC in *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*, 895 F.3d 455 (6th Cir. 2018). There, the policyholder (ATC) wired money to fraudsters, instead of to a vendor, after being deceived by a BEC. The Sixth Circuit ruled that the losses were "direct" and covered by crime insurance. 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. *Id*. at 462.

Holding that coverage applied, the Sixth Circuit distinguished the Eleventh Circuit's decision regarding computer fraud coverage in *Interactive Communications v. Great American*, 731 F. App'x 929, (11th Cir. 2018). 895 F.3d at 462-63. Id. at 9-10.

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

Beyond crime policies, other insurance policies might be obligated to cover these losses. If a loss arises, it's worth taking a close look at all of a company's insurance policies to determine if there is overlapping coverage that could apply.

What Policyholders Can Expect in the Future

Cynical viewers of insurance history might expect the industry to react as it has done in the past. That is, to initially cover new claims under "old" policies – then, after claims get expensive, hire coverage counsel to tell courts why the carriers actually did not mean 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, while at the same time selling new policy endorsements (often for an additional premium) that provide lower limits of coverage.

Indeed, this is what is already happening in connection with insurance for BEC losses. At least one insurance group that drafts crime insurance policies has asked for the definitions of computer fraud and funds transfer fraud to be changed – and for a new "social engineering fraud" endorsement to be approved for sale.

Insurers have rolled out these endorsements with limits on coverage that often are capped at low amounts and may also have high retentions. These endorsements are frequently available for crime policies, and sometimes for cyberinsurance policies as well.

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

- **What does the insurance policy include?** Policyholders would be well-advised to see whether the insurance program includes social engineering fraud endorsements or coverage parts.
- **What are the applicable limits?** Policyholders would be well-advised 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.
- **Are coverages available under more than one policy?** At the time of policy renewal, policyholders would be well-advised to consider asking whether social engineering fraud coverage can be added to a crime program and a cyberinsurance program.
- **Will excess coverage apply, and, if so, when?** Policyholders would be well-advised to explore whether excess policies will provide this coverage, and, if so, whether they will "drop down" to attach at the level of any sublimit, to avoid donut holes in the coverage.
- **Will other policy provisions provide coverage, beyond narrow endorsements?** If the policyholder faces a claim, policyholders would be well-advised to determine whether other insurance policies provide coverage, and whether other coverages in a crime policy might apply to the losses, notwithstanding a social engineering fraud endorsement.

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