The Tug-of-war Of BEC Scheme Insurance Coverage

CYBERSECURITY AND PRIVACY | NOVEMBER 9, 2016

John C. Pitblado

The financial services industry has long been on the forefront of technological advances in commerce. In the 1950s, Bank of America commissioned a consortium of Stanford scientists to develop one of the first commercial applications of the then-newly emerging field of “electronic brains” (aka “computers”). This effort resulted in Electronic Recording Machine, Accounting, (ERMA), an automated system used for counting checks. Among other notable advances, this led to numerical bank account numbers (the old alphabetical by-name lists to which new customers were added had to be reshuffled with every new name), and magnetic ink character recognition, the readily recognizable ‘computeristic’ font used for the numbering found on checks.These first commercial computers were impressive:

> The final ERM [prototype] contained more than a million feet (304,800 meters) of wiring, 8,000 vacuum tubes, 34,000 diodes, 5 input consoles with MICR readers, 2 magnetic memory drums, the check sorter, a high-speed printer, a power control panel, a maintenance board, 24 racks holding 1,500 electrical packages and 500 relay packages, and 12 magnetic tape drives for 2,400-foot (731-meter) tape reels. ERM weighed about 25 tons, used more than 80 kW of power and required cooling by an air conditioning system.

Financial institutions were also at the forefront of computerizing sales transactions. In the late 1960s and 1970s, Bank of America’s National BankAmericard (later, Visa) and a consortium of competing banks called the Interbank Card Association (later, MasterCard) began competing over the nascent “credit card” sales industry. That competition quickly led to the development of real-time credit account checks through phone lines, the development of automated teller machines, and eventually, electronic point-of-sale technology.

So, it should not be surprising that banks and other financial institutions were also at the forefront of computer fraud and hacking. And their insurers were close behind.

Financial institution bonds or “fidelity” bonds were developed long ago to protect banks and other financial institutions from theft and fraud, particularly by employees, as “theft by one’s own personnel invariably cost financial institutions more each year than any external cause.”

These policies, sometimes also called commercial crime policies (for nonbanking entities), have not changed much from their original form, but insurers have responded to new risks by adding riders. One such rider is the “computer systems” rider, which has been in use since at least the mid-1990s. See e.g. Hudson United Bank v. Progressive Cas. Insurance Co., 152 F. Supp. 2d 751, 754 (E.D. Pa. 2001) (addressing coverage for 1997 auto insurance financing fraud scheme under provision covering “fraudulent ... change of Electronic Data or Computer program with any Computer System operated by the Insured.”).

Typically, the “computer systems” rider is worded to require “fraudulent ... change” to the insured’s computer network or data. Courts have generally interpreted this language to require that the “change” be unauthorized in some fashion, generally meaning perpetrated by an unauthorized user. To wit, last year, New York’s high court found no coverage under a computer systems fraud rider for a Medicare fraud scheme perpetrated by a healthcare provider using an electronic payment system submitted through his company’s computer network. The court noted that the rider was not meant to cover any fraud committed by an authorized user of a computer, but rather was meant to cover “losses resulting from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be ‘hacking’ of the computer system.” Universal Am. Corp. v. Nat'l Union Fire Insurance Co. of Pittsburgh, Pa., 25 N.Y.3d 675, 681, 37 N.E.3d 78, 81 (2015) (emphasis added).

Consistent with this analysis, the Eighth Circuit recently held, in State Bank of Bellingham v. BancInsure Inc., 823 F.3d 456 (8th Cir. 2016), that a direct hack of an insured bank's computer network by an unauthorized (and unknown) user that resulted in the wiring of funds to a foreign account set up by the hacker was covered under a similar provision.

Recently, this delineation of coverage as depending on whether the computer use was authorized, and thus merely incidental to the fraud scheme, was thrown into some disarray by a federal district court in Texas, which held that losses from a "business email compromise" (BEC) (also known as "social engineering") scheme were covered under a commercial crime policy's computer fraud provision.

In Apache Corp. v. Great Am. Insurance Co., No. 4:14-CV-237 (S.D. Tex. Aug. 7, 2015), the court addressed a now-familiar scheme. An employee of the insured corporation was duped by an phone call purporting to be from a vendor, requesting that the vendor's wiring instructions be changed to a new bank account. The employee asked that the requested change be sent in writing on the vendor's letterhead. The fraudster then created letterhead by cutting and pasting the vendor's logo off its website, and sent a scanned copy of the signed letter via an email that appeared to be from the vendor's domain, but was not. Another employee, upon being forwarded the written 'verification,' then called the number on the letterhead (which was fraudulent), and upon receiving confirmation of the change, rerouted the vendor's payments to a fraudulent account. The insured suffered $2.4 million in losses before the scheme was detected. The court held that this was covered, because the fraudster's scheme was perpetrated, in part, through the insured's computer network, insofar as it involved email.

The decision was later cited favorably in a similar case in Georgia, where an insured suffered a $1.7 million loss from a similar BEC scheme, and the court held it was covered under a computer systems fraud rider. See Principle Solutions Group LLC v. Ironshore Indem. Inc., No. 1:15-CV-4130-RWS, (N.D. Ga. Aug. 30, 2016).

Likewise, a policyholder in coverage litigation in Manhattan federal court cited the Apache decision in its summary judgment briefing, regarding coverage for an alleged $4.7 million BEC scheme. See Medidata Solutions Inc. v. Federal Insurance Co., No. 15-CV-00907 (S.D.N.Y.).

But just as soon as it looked like the Apache decision was gaining traction, the circuit courts have stepped in and restored order. First, the Ninth Circuit, in a short opinion, found no coverage for losses from a BEC scheme under a computer systems fraud rider. That court, in vacating a California federal court decision finding coverage, held that:

> The Policy defines Computer Fraud as "[t]he use of any computer to fraudulently cause a transfer ... ." We interpret the phrase "fraudulently cause a transfer" to require an unauthorized transfer of funds. When Priority 1 transferred funds pursuant to authorization from Pestmaster, the transfer was not fraudulently caused. Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a "General Fraud" Policy. While Travelers could have drafted this language more narrowly, we believe protection against all fraud is not what was intended by this provision, and not what Pestmaster could reasonably have expected this provision to cover.

Pestmaster Servs. Inc. v. Travelers Cas. & Sur. Co. of Am., No. 14-56294 (9th Cir. July 29, 2016)

And citing the Pestmaster decision, the Fifth Circuit reversed the lower court ruling in Apache, finding no coverage. Following on the reasoning of the Pestmaster decision, the Fifth Circuit stated:

> We take judicial notice that, when the policy was issued in 2012, electronic communications were, as they are now, ubiquitous, and even the line between "computer" and "telephone" was already blurred. In short, few — if any — fraudulent schemes would not involve some form of computer-facilitated communication.

Apache Corp. v. Great Am. Insurance Co., No. 15-20499 (5th Cir. Oct. 18, 2016).

Unsurprisingly, the Fifth Circuit's Apache decision was cited by the insurer in a pending motion for reconsideration in the Principle Solutions case, and was cited by the insurer in a supplemental summary judgment brief in the Medidata case. Decisions in both are likely to come in the next few weeks or months. Depending on how they come out, we may see the issue teed up again in either the Eleventh or Second Circuit courts.

One thing is clear: It will no longer suffice to simply hope that your company is sufficiently sophisticated not to fall prey to such a scheme. According to recent FBI data, since Jan. 1, 2015, BEC losses in the U.S. have grown an astonishing 1,300 percent, reaching 22,143 cases with losses totaling over $1.3 billion.

So what does this mean for policyholders and insurers? One clue is referenced in the initial Principle Solutions decision, which held inadmissible evidence that the insurer submitted showing that it offered for sale an entirely separate rider which was designed to address schemes like those at issue, called “Cyber Deception” coverage, and which differed in material ways from the “computer systems” fraud coverage. Given that there is now a developing consensus at the circuit court level that BEC/social engineering scheme losses are not covered by a standard “computer systems” rider, policyholders should ensure that they address the issue with their insurer or broker when shopping for fidelity bonds. Insurers writing fidelity coverage should take note as well, as the market for new coverage addressing BEC losses will likely expand dramatically, and underwriting a new coverage may be difficult, given the dramatic growth in these types of losses.

Republished with permission by Law360 (subscription required). Originally published by PropertyCasualtyFocus.