Dickie McCamey
ATTORNEYS AT LAW

2/21/2017 | Articles

Cybercrime Insurance Outlook 2017: Man vs. Machine

As 2017 unfolds, it remains to be seen whether an emerging trend of stricter readings of cybercrime insurance policies to limit or exclude the reach of computer fraud crimes protection coverage will continue. One case decided late last year illustrates the trend, and the view that whether or not computer fraud coverage applies will be based in large part on the degree of human involvement in bringing about the criminal losses.

In *Apache Corp. v. Great American Ins. Co.*, No. 15-20499, 2016 WL 6090901 (5th Cir. Oct. 18, 2016), the Fifth Circuit Court of Appeals ruled that a policy covering losses arising out of computer fraud did not apply to a fraudulent financial transfer "that was the result of other events and not directly by the computer use."

Of interest to the appeals court in *Apache* was that the crime started with a telephone call from the thief, posing as a vendor to the insured, requesting a change of bank wiring instructions through which the insured paid the vendor. Pursuant to Apache's request for the change of wiring instructions in writing, the thief provided the instructions via email, although the email address did not match the vendor's email domain on file. After a telephone call made by Apache following up the email, however, Apache instructed its bank to change the wiring instructions.

Apache discovered that the wiring change was ultimately fraudulent, resulting in net losses of $2.4 million. Apache filed a claim with Great American under its crime protection insurance policy which included computer fraud coverage. The insuring agreement in the Great American policy provided for payment of losses "resulting directly from the use of any computer to fraudulently cause a transfer of [such money] from inside the premises or banking premises . . . to a place outside those premises."

Great American denied the claim on the grounds that the losses did not result directly from the use of a computer, but rather human error. Apache sued Great American for coverage in Texas state court, and the case was removed to the U.S. District Court for the Southern District of Texas, after which both parties cross-moved for summary judgment. The federal district court granted the insured's motion for summary judgment in favor of coverage, and denied the insurer's motion for summary judgment, but refused to impose statutory penalties on the insurer.

Following appeal by both parties to the U.S. Court of Appeals for the Fifth Circuit, the appeals court reversed judgment for Apache, relieving Great American of its indemnity obligations. A three-judge panel held that that numerous intervening non-computer actions were taken between the digital actions of the posing vendor's email and the computer bank transfer of funds. Such non-computer acts, the court noted, included telephone calls, approval of the change in wiring instructions by Apache's management, the receipt and processing of invoices by Apache, and Apache's approval of invoices for payment. The court finally found that Apache's instructions to the bank to effectuate the wiring change were verbal as well.

The Court held:

> The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would . . . convert the computer-fraud provision to one for general fraud . . . . 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.

This is reflected in the evidence at hand. Arguably, Apache invited the computer-use at issue, through which it now seeks shelter under its policy, even though the computer-use was but one step in Apache's multi-step, but flawed, process that ended in its making required and authorized, very large invoice-payments, but to a fraudulent bank account.

For the *Apache* court, then, a critical area of focus in the analysis of coverage of cybercrime insurance is the nexus between the crime and the degree of computer versus human involvement. *Apache*, and decisions like it, impose rather strict limits on the scope of cyber insurance coverage, setting a bright line between fraud which is primarily the result of flawed human systems and fraud which is primarily digital and computer-driven.

Cybercrime and related technology insurance coverage is still very much an emerging insurance market. Policy language, therefore, remains varied, and such variance imposes obligations on both insurers and insureds to be precise in their understanding of what kinds of protections the policy terms, conditions, and endorsements provide.

Charles E. Haddick, Jr.
717-731-4800
chaddick@dmclaw.com
@cjhinsurancelaw
blog: badfaithadvisor.com