October 2016

Fifth Circuit Rules That Fraud Involving a Computer Is Not 'Computer Fraud' Under Crime Protection Policy

The United States Court of Appeals for the Fifth Circuit held in *Apache Corp. v. Great American Ins. Co.*, No 15-20499 (5th Cir. Oct. 18, 2016), that a crime protection insurance policy does not cover loss resulting from a fraudulent email directing funds to be sent electronically to the imposter's bank account because the scheme did not constitute "computer fraud" under the policy.

Background

An employee at Apache Corporation, an oil production company based in Houston, Texas, with worldwide operations, received a telephone call from an individual identifying himself as a representative of Petrofac, a vendor of Apache. The caller instructed the Apache employee to change the bank account to which payments to Petrofac were made. The employee requested that confirmation of the change request be provided on Petrofac's letterhead.

Shortly thereafter, the fraudsters provided the Apache accounts-payable department with an email of the request on Petrofac letterhead. The letter also included a phony telephone number, which Apache personnel used to confirm the requested change. Apache then proceeded to make payment to the fraudulent account when it came time to pay Petrofac's invoices. Within one month, Apache was notified that Petrofac had not received approximately $7 million in payments that had been sent to the fraudulent account. Apache recouped a portion of the payments from its bank and attempted to recover the balance from its insurer.

Apache was insured under a crime-protection insurance policy issued by Great American Insurance Company (GAIC). Apache submitted a claim to GAIC for reimbursement of the unrecovered funds under the policy's computer-fraud coverage, which afforded coverage for loss "resulting directly from the use of any computer to fraudulently cause a transfer" of money or property to a person or place outside the company. GAIC denied coverage, claiming that the loss did not directly result from the use of a computer nor did the use of a computer cause the transfer of the funds. Apache filed suit in Texas state court and GAIC removed. The federal district court sided with Apache and held that the intervening steps of the phone call and approval of the change request by Apache's supervisors did not alter the fact that the fraudsters used a computer to perpetrate the fraud. The district court also held that GAIC's construction of the policy would effectively limit the policy to affording coverage only for computer hacking, thus rendering the policy "pointless."

Appeal

The Fifth Circuit vacated the judgment and held that the loss did not come within the scope of the computer-fraud coverage because the loss did not result directly from the use of any computer, even though the account information was changed in response to a confirming email and even though the lost funds were transferred to the fraudsters' account via electronic transfer. Rather, as the court explained, although email was part of the scheme, the use of email was merely "incidental" to the occurrence of the authorized transfer of money. Further, the court took notice of the fact that electronic communications are ubiquitous and, consequently, it is difficult to envision any fraudulent scheme that does not involve some

form of computer-facilitated communication. Thus, the court concluded that 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.

Implications

The *Apache* decision illustrates the narrow scope of coverage afforded to crime policy "computer fraud" provisions and effectively constrains the computer-fraud coverage to "hacking" type events. To trigger this coverage, the court intimated that it is not enough that a criminal utilize a computer as an instrumentality to perpetuate a scheme. Rather, the computer use necessary to trigger coverage must be the direct cause of the fraudulent transfer of money.

Although *Apache* involved a traditional crime policy, the decision has the potential to affect all technology and cyber-related coverages. For instance, in the case of cyber coverage, where the covered loss may include the release of personally identifiable information (PII) or other sensitive electronically stored information, under an *Apache*-type analysis, a policy affording coverage only where a breach results "directly from the use of any computer" may not afford coverage where the breach results from other known cyber risk events, such as skimming or the physical loss of firmware or storage media that contains the sensitive information. Likewise, where a company is induced to share PII or other information via means other than computer (as was the case in *Apache*, where the initial contact was made by phone), such a resulting breach may not be covered, even when the resulting breach occurred via computer.

Experienced coverage counsel can help policyholders evaluate their coverages, both legacy and cyber, and assist with endorsing policy language to address gaps or otherwise identify other types of policies or coverages that might apply to a particular risk.

Contacts

Walter J. Andrews
wandrews@hunton.com

Syed S. Ahmad
sahmad@hunton.com

Lawrence J. Bracken II
lbracken@hunton.com

John C. Eichman
jeichman@hunton.com

Michael S. Levine
mlevine@hunton.com

Sergio F. Oehninger
soehninger@hunton.com

Matthew T. McLellan
mclellanm@hunton.com