Cyber Scams are Not Computer Fraud under Commercial Crime Insurance

Main Contact(s)

Amanda T. DiMatteo

Robert A. McCall

Related Practices

Insurance Coverage and Bad Faith Litigation

By Amanda T. DiMatteo, Robert A. McCall on July 6, 2017

The endless stream of email scams has forced courts to confront an important coverage issue under commercial crime policies – whether these types of scams fall within coverage for Computer Fraud. Courts have increasingly reached the conclusion that loss arising from an occurrence of cyber deception or social engineering will generally not be covered under the computer fraud insuring agreement of a commercial crime policy. The two best examples have come out of federal courts in California and Texas.

The language of the computer fraud insuring agreement in the ISO Standard Form Crime Protection Policy focuses coverage to hacking incidents. Insuring Agreement 5 provides coverage for "loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of **money, securities** or **other property** from your **premises** or **banking premises** to a person, entity, place or account outside of your control." Crime Protection Policy, ISO SP 00 01 04 12 (Rev. 2012), Insuring Agreement 5 (terms in **bold** are defined by the ISO form). Thus, the insuring agreement covers direct loss caused by the use of any computer to fraudulently transfer covered property, but will not respond to loss incurred as the result of a social engineering scheme whereby an insured knowingly and voluntarily transfers covered property.

In July 2016, the Ninth Circuit Court of Appeals held that the Computer Crime insuring agreement of a Travelers policy did not provide coverage for an automated transfer of funds from the insured to a third party pursuant to authorization from the insured. See Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332 (9th Cir. 2016). Pestmaster, a company specializing in pest control, hired a payroll company to administer payroll and submit payroll taxes. Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., No. CV 13-5039-JFW MRWX, 2014 WL 3844627, at *1 (C.D. Cal. July 17, 2014). Pestmaster authorized the payroll company to obtain payment of approved invoices by initiating computer transfers of funds from Pestmaster's bank account to the payroll company's bank account to meet payroll and tax obligations. Id. Pestmaster alleged that the payroll company had fraudulently failed to remit payroll taxes to the IRS. Id. Pestmaster further alleged that the payroll company wrongly used the funds to pay its own obligations rather than Pestmaster's federal payroll tax obligations. Id. at *8.

The Travelers policy provided coverage for "direct loss of, or your direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud." Id. at *5. The policy defined Computer Fraud as:

The use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises:

1. to a person (other than a Messenger) outside the Premises or Banking Premises; or
2. to a place outside the Premises or Banking Premises.

Id. at *4-*5. The Ninth Circuit interpreted the phrase "fraudulently cause a transfer" to require "an unauthorized transfer of funds." Pestmaster Servs., Inc., 656 F. App'x at 333. Critically, the Ninth Circuit advised that "[b]ecause 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." Id.

Last October, the Fifth Circuit Court of Appeals similarly adopted a narrow interpretation of the Computer Fraud insuring agreement in the context of a social engineering scheme. See Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 253 (5th Cir. 2016). An employee of Apache Corporation, an international oil-production company, received a telephone call from a person purporting to be a representative of a vendor for Apache. Id. at 253. The caller instructed Apache to change the bank account information for the vendor payments. Id. The Apache employee replied that a change in bank account information could not be processed without a formal request on the vendor's letterhead. Id. A week later, Apache's accounts payable department received an email from an address spoofing the vendor's proper email domain. Id. An Apache employee called the telephone number provided on the attached letter to verify the request. Id. A different Apache employee approved and implemented the change. Id. Within one month, Apache received notification from the vendor that it had not received approximately $7 million that Apache had transferred to the fraudulent account. Id.

The Fifth Circuit determined that the insured's loss was not a covered occurrence. Id. at 259. The "computer use" at issue in Apache was "an email with instructions to change a vendor's payment information and make 'all future payments' to it." Id. at 258. The Apache Court reasoned that "[t]he email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money." Id. The Court continued: "viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache elected to pay legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers." Id. at 259.

The Pestmaster and Apache decisions suggest that a uniform interpretation of this language is developing among appellate courts, which clarifies the scope of coverage under a crime policy's computer fraud insuring agreement. There is, however, other commercial crime insurance coverage available in the market to cover these types of scams. Insurers have offered specific cyber deception and social engineering endorsements to address these risks.

