Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

No Coverage For Fraudulent Withdrawal Of Electronic Funds

Law360, New York (December 04, 2013, 11:39 PM ET) -- On Nov. 21, 2013, District Court Judge Orinda Evans ruled that an all-risk insurance policy did not provide coverage to a real estate brokerage company for online fraudulent withdrawals from the company's bank account. Metro Brokers Inc. v. Transportation Insurance Co., No. 1:12-CV-3010-ODE (N.D. Ga. Nov. 21, 2013).[1] The evidence suggested that a hacker obtained Metro's online banking log-in credentials through a key logger "Zeus" virus that was found on several of Metro's computers. The court gave effect to two exclusions concerning cyber risks and recognized that specialty coverage is available to policyholders. The court's decision is an important one for insurers who exclude or provide first-party or liability cyber coverage and for policyholders who may make a claim for cyber losses.

Cyber Risks

The decision in Metro Brokers is part of a growing body of case law on cyber risk insurance issues. Typically, cyber risks involve misappropriation of intellectual property or proprietary information, corruption of data and systems, disruption of operations or the fraudulent transfer of electronic funds. But all cyber risks have one thing in common: unauthorized access to a computer or a computer system.

The average cost of a data breach to a U.S. company in 2012 has been estimated at $5.4 million.[2] The decision in Metro Brokers is timely given the recent number of cyber attacks in the U.S., most notably the attack on Adobe Systems Inc. in October. Hackers stole the source code to some of Adobe's most popular software as well as, reportedly, the personal data of 38 million of its customers, including names, credit card information, user IDs and passwords.[3] According to the Federal Bureau of Investigation, identity theft is the fastest growing white collar crime in the U.S. There is a robust market for the illegal trading and selling of personal information.

Another type of cyber risk known as denial of service ("DOS") attacks is also becoming more common. DOS attacks involve the deliberate overloading of a network or server with emails or communication requests that causes the system to crash. DOS attacks can have far-reaching effects. In 2012 and 2013, Wells Fargo was hit with DOS attacks that severely disrupted its online banking operations and reportedly affected 21 million online customers and 8.5 million mobile banking users.[4]

As cyber hackers become more sophisticated insurers can expect cyber risk claims to continue to increase. Cyber risks costs that may be insured by an all risk or specialty policy include costs to repair and/or restore the data, forensic costs, preventive costs, business interruption loss, replacement of stolen property (e.g., funds) and costs to cover extortion payments to would-be hackers.

A discussion of the court's recent decision in Metro Brokers follows.

Fraudulent Withdrawals From Metro's Bank Account

Metro, a real estate brokerage company, maintained bank accounts at Fidelity Bank and used the bank's automated clearing house ("ACH") system to make payments, such as its payroll. A Metro employee would log onto the bank's online banking system with a username and password and would then receive a randomly generated security code for each transaction.

In December 2011, a thief (or thieves) logged onto the bank's online system using the electronic credentials of a Metro employee and made at least two withdrawals from a Metro client escrow account. The hacker(s) directed the funds to other bank accounts throughout the U.S. The parties agreed that the evidence suggested that the hacker(s) learned Metro's login credentials through the "Zeus" virus that was found on several of Metro's computers.

Metro submitted a claim to its insurer, TIC, which denied based on the policy's "malicious code" and "system penetration" exclusions. TIC also took the position that the policy's "forgery and alteration" coverage endorsement did not provide coverage for Metro's losses.

Forgery Coverage and the Electronic Data Exclusions in the TIC Policy

The TIC policy contained a forgery and alteration endorsement as part of the policy's additional coverages. The endorsement provided coverage as follows:

We will pay for loss resulting directly from 'forgery' or alteration of, on or in any check, draft, promissory note, bill of exchange or similar written promise, order or direction to pay a sum certain money, made or drawn by or drawn upon you, or made or drawn by one acting as an agent or claiming to have been so made or drawn. … We will consider signatures that are produced or reproduced electronically, mechanically, or by facsimile the same as handwritten signatures.

The policy defined "forgery" as "the signing of the name of another person or organization with intent to deceive; it does not mean a signature which consists in whole or in part of one's own name signed with or without authority, in any capacity for any purpose."

The policy also contained exclusions for losses caused by "malicious code" and "system penetration." These exclusions included broad anti-concurrent cause language:

We will not pay for loss or damage caused directly or indirectly by any of the following. Such loss or damage is excluded regardless of any other cause or event that contributes concurrently or in any sequence to the loss.

j. Malicious Code
Any “malicious code”
k. System penetration
Any “system penetration”

The policy broadly defined “malicious code” and “system penetration” as, essentially, access that results in “electronic data peril” (defined as “corruption, unauthorized use, distortion, deletion, damage, destruction of any other harm to or misappropriation or copying of, “electronic data” or information”). This would include “electronic data peril” caused by computer viruses.

The Court’s Analysis

In granting summary judgment to TIC, the court noted that “TIC obviously intends to eliminate coverage for any and all losses resulting from an internal or external breach to the insured’s electronic systems and/or data” and that the policy used “extraordinarily broad exclusionary language” which permitted TIC to deny Metro’s claim.

Metro’s position was that no malicious code or system penetration caused the fraudulent withdrawals. Metro argued that the hacker’s use of the electronic withdrawals constituted a forgery of Metro’s electronic signature on the electronic transfer process. TIC’s position was that there was no forgery of a “check, draft, promissory note, bill of exchange, or similar written promise” required for coverage under the forgery endorsement. TIC also argued that the endorsement is subject to the malicious code and system penetration exclusions which applied to Metro’s claim.

The court first addressed the forgery endorsement and found that it did not apply because Metro’s loss was not caused by “forgery” of a negotiable instrument insured under the endorsement (i.e., forgery or alteration of “a check, … or similar written promise, order or direction to pay a sum certain money").

The court noted it was clear that the transfers did not involve a check, draft, promissory note, or bill of exchange. Instead, the court focused its analysis on the “similar written promise, order or direction” clause and concluded that based on the list of items in the endorsement, the endorsement only provided coverage for forgeries to a negotiable instrument.

Negotiable instruments have intrinsic value; a document lacking the words “order” or “bearer” cannot be considered a negotiable instrument. The court also looked at the federal Electronic Funds Act (15 U.S.C. §1693a(6)) and its Georgia counterpart (O.C.G.A. § 11-4A-102) which distinguish between electronic fund transfers and negotiable instruments. The court also found it persuasive that the ACH transfers were not “written” but were triggered by the click of a button. The court observed that it makes sense for insurance policies to differentiate between traditional and electronic transfers because the later are more prone to fraudulent activity as the “signatures” cannot be scrutinized in the same way that paper signatures can.

The court also held that the broad malicious code and system penetration exclusions barred Metro’s claim. The court disagreed with Metro’s argument that the cause of the loss was the person who used the hacked information to make the transfers as opposed to the computer virus itself.

The court acknowledged that a person undoubtedly caused the loss and that "it is exceedingly unlikely that a computer virus could or would transfer funds … without a considerable level of human involvement and culpability." Nonetheless, the court found that the loss was caused directly or indirectly by malicious code or system penetration and that the virus was not too remote of a cause. The court noted that specialty coverages are available for computer fraud and gave effect to the exclusions' anti-concurrent cause language which excluded loss or damage "regardless of any other cause or event that contributes concurrently or in any sequence to the loss."

When dealing with cyber risk claims, as with other types of claims, insurers and insureds will want to review the specific language of the policy at issue. The decision in Metro Brokers offers guidance as to how a court may treat a policyholder's claim under a traditional all risk policy and the effect of broad computer fraud exclusions.

—By James A. Kitces, Robins Kaplan Miller & Ciresi LLP

James Kitces is an associate Robins Kaplan Miller & Ciresi's Atlanta office.

Robins Kaplan Miller & Ciresi LLP represented the defendant in Metro Brokers Inc. v. Transportation Insurance Co.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Robins, Kaplan, Miller & Ciresi L.L.P. represented the defendant in the case, Transportation Insurance Company.

[2] Ponemon Institute, 2013 Cost of Data Breach Study, May 2013.

[3] Wall Street Journal, Nov. 11, 2013, Hacker Attack on Adobe Sends Ripples Across Web, Yadron, Danny.

[4] Los Angeles Times, Sept. 25, 2012, Wells Fargo is latest victim in cyber attack spree, Reckard, E. Scott; Los Angeles Times, March 26, 2013, Another cyber attack targets Wells Fargo website, Reckard, E. Scott.