THOMSON REUTERS

Westlaw®

Chit happens: Cyberfraud coverage decisions based on use and causation

By Lawrence A. Levy, Esq., *Rivkin Radler LLP*

JUNE 29, 2018

Cyber-related fraud, theft and other cybercrimes have become ubiquitous in the business and financial news. Hackers and other actors with nefarious intent look to exploit vulnerabilities in computer systems.

These new types of losses have led to the development of new insurance products to address them, which in turn have created unique insurance coverage issues. Hacking and computer fraud are examples of new losses creating these new coverage issues.

Two questions generally arise in any coverage dispute involving policies issued to cover computer fraud: whether the perpetrators of the alleged fraud were authorized to use the computer through which the fraud was committed, and whether the fraudulent computer activity caused the loss.

The first question arises because cyberliability insurance policies limit coverage to the actions of users who are not authorized to use the computers.[1] Courts distinguish computer "hacking" from the authorized use of a computer. Everyone uses computers, but not all users are hackers.

Hacking is an unauthorized use of a computer and is generally covered, provided that the other terms and conditions of the policy are satisfied. Losses resulting from the authorized use of a computer, however, generally are not covered.

The causation question arises because policy language often restricts coverage to damage "directly caused by" or "resulting directly from" computer activity.[2] As in tort law, the resolution of this issue is often dependent on how long of a causal chain will be recognized.

In other words, at what point is an act too distant from the injury for it to be deemed the cause?

Causation case law is inconsistent and often depends on how courts frame the issue. Some jurisdictions will find causation exists even in cases involving a long chain of events, while other courts reject shorter causal chains.

Courts that have accepted causation from a long chain of events have applied a proximate cause standard that "does not unambiguously limit coverage to loss resulting 'solely' or 'immediately' from the [act] itself."[3]

In contrast, courts that have rejected larger causal chains that they deem are too tenuous base their holdings on the plain and unambiguous word, "direct," which means without any intervening or incidental causes.[4]

The causation issue and the authorized-use issue often arise in the same dispute. Rarely do these disputes present the issue of what constitutes the mere "use of a computer" because, in most instances, the use of a computer is self-evident.

Recently, however, a federal appellate court addressed the issue of what constitutes the use of a computer in the context of computer fraud, as well as the causation issue.

> The 11th Circuit noted that whether the claim involved the "use of a computer" depended on whether phone calls made to a computer system constitute "use" of that computer system.

In *Interactive Communications International Inc. v. Great American Insurance Co.*,[5] the policyholder operated a network that allowed consumers to deposit money onto general-purpose, reloadable debit cards issued by various banks.

Specifically, the policyholder, Interactive Communications, sold "chits" through retailers such as Walgreens and CVS to consumers, who would then call the policyholder via a toll-free number to redeem the chits and have their value moved to consumers' debit cards.

The toll-free number connected consumers to the policyholder's interactive voice response computer system, which used eight computers to process voice requests or telephone touch-tone codes. Once a consumer entered the number and PIN associated with the debit card, the IVR credited the value of the chit to the card, making the funds immediately available to the cardholder.

Over a six-month period, fraudsters exploited a vulnerability in the IVR system that enabled them to make multiple redemptions of a single chit. The fraudsters deduced that they could redeem a single chit multiple times by making simultaneous calls to the IVR system requesting the redemption of the same chit.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

the answer company™
THOMSON REUTERS®

The fraudulent redemptions cost the policyholder $11.4 million, the great majority — $10.7 million — of which was redeemed on debit cards issued by Bancorp Bank. Because the policyholder believed the transactions were legitimate, it wired funds to Bancorp to cover the value of the cards.

The policyholder, which was insured by Great American Insurance Co., sought coverage for the $10.7 million lost to Bancorp debit cardholders who fraudulently manipulated the IVR system to obtain duplicate redemptions of the chits.

The multi-risk policy provided the following coverage:

> Computer Fraud
>
> [Great American] will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or
>
> b. to a place outside those premises.

The insurer disclaimed and in the resulting coverage litigation, the U.S. District Court for the Northern District of Georgia granted the insurer's motion for summary judgment, holding that the fraud was not accomplished through the use of a computer and the loss did not "result directly" from the use of the IVR system.

The 11th U.S. Circuit Court of Appeals disagreed with the District Court's conclusion that the phone calls did not involve the use of a computer, but it affirmed the District Court's judgment because the loss did not directly result from the computer fraud.

The 11th Circuit noted that whether the claim involved the "use of a computer" depended on whether phone calls made to a computer system constitute "use" of that computer system.

The District Court had limited its analysis of the issue to the unremarkable conclusion that a telephone is not a computer and that the phones used to dial into the IVR system were not computers within the meaning of the policy.

However, the 11th Circuit recognized that the fraudsters used phones to manipulate — and thereby use — the IVR computers.

The appeals court held that "the plain meaning of the word 'use' ... comfortably supports an understanding that encompasses the callers' access and manipulation of [the policyholder's] IVR system."[6]

The court next addressed the causation issue, which required it to decide the meaning of the phrase "result directly" and when the policyholder's loss occurred.

As to the first question, Great American argued that the "resulting directly" language required immediacy between the fraudulent act and the result. Interactive Communications contended that "resulting directly" required only a showing of proximate cause.

The 11th Circuit resolved this issue based on the ordinary meaning of "directly" and held that "one thing results 'directly' from another if it follows straightaway, immediately, and without any intervention or interruption."[7]

The court then turned to the second, factual question: When did the loss occur, and did it "result directly" — immediately without intervention or interruption — from the fraudsters' use of the computer system?

The decision demonstrates how the framing of the causation issue is critical.

The 11th Circuit concluded that the fraudsters' use of the policyholders' computers did not directly cause the loss. It found four steps between the fraudulent manipulation of the computer system and the policyholder's loss.

The first step was the manipulation of the IVR system to enable duplicate chit redemption.

The second step involved the transfer of money by the policyholder to an account at Bancorp maintained for the purpose of paying charges incurred by the debit card holders.

The third occurred when the debit cardholder used the card to make a purchase, thereby incurring a debt to be paid from the designated Bancorp account.

Finally, Bancorp transferred money from the account to the merchant to cover the purchase.

The policyholder argued that the loss occurred at step two, when it transferred money to the account at Bancorp.

However, because the policyholder maintained some control over the funds held by Bancorp even after that transfer, the court held that the loss did not occur until the fourth step, when Bancorp disbursed the money from the account to pay the merchants. At that point, the policyholder could no longer recover its money.

In other words, the duplicitous redemption phone calls to the IVR system may have set the process in motion, and the transfer of funds by Interactive Communications to the dedicated Bancorp account may have furthered the process, but the loss occurred only when Bancorp transferred funds to cover a purchase.

Accordingly, the 11th Circuit concluded that the loss did not follow immediately, without any intervention or interruption, from the computer fraud.

© 2018 Thomson Reuters

Rather, the loss was temporally remote (weeks or months could pass between the initial chit redemption and the disbursement of funds), and the chain of causation involved intervening acts and actors between the first and fourth steps. For this reason, the court said the loss was not covered.

The decision demonstrates how the framing of the causation issue is critical. Here, the court declined to impose a proximate cause requirement that effectively writes the term "directly" out of the policy.

Instead, the 11th Circuit applied the plain and unambiguous meaning of the policy language and examined two factors to resolve the issue: the temporal relationship between the fraud and the resultant loss as well as how remote or direct in the chain of causation the loss is to the fraudulent act. Courts will ideally consider both factors in construing this provision.

Moreover, the 11th Circuit's holding regarding whether the fraudulent activity involved the "use" of a computer establishes that courts must look beyond the means of the fraudulent activity — in this instance, phone calls — and focus on what is being manipulated by the fraudulent activity.

Here, because the fraudsters used the phones to manipulate the IVR computer system, the 11th Circuit held that the fraudulent activity involved the use of computers.

NOTES

[1] *See, e.g.*, *Universal Am. Corp. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, 25 N.Y.3d 675, 37 N.E.3d 78, 16 N.Y.S.3d 21 (2015) (holding that the policy language, "fraudulent entry" of data, referred to unauthorized access into the policyholder's computer system and thus did not apply to fraudulent content submitted by authorized users).

[2] *See, e.g.*, *Am. Tooling Ctr. Inc. v. Travelers Cas. & Sur. Co.*, No. 16-cv-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017) (under Michigan law, intervening events between the use of a computer and the loss preclude a finding of a "direct loss" that was "directly caused" by the use of a computer).

[3] *Retail Ventures Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821 (6th Cir. 2012); *see also State Bank of Bellingham v. BancInsure Inc.*, No. 13-cv-900, 2014 WL 4829184 (D. Minn. Sept. 29, 2014). Other courts have held that the policy language "result directly" is ambiguous because it is susceptible to more than one reasonable interpretation and have construed such language against the insurer. *See, e.g.*, *Principle Solutions Group LLC v. Ironshore Indem. Inc.*, No. 15-cv-4130, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).

[4] *See Pestmaster Servs. v. Travelers Cas. & Sur. Co.*, No. 13-cv-5039, 2014 WL 3844627 (C.D. Cal. July 17, 2014), *aff'd*, 656 F. App'x 332 (9th Cir. 2016); *Am. Tooling*, 2017 WL 3263356; *Pinnacle Processing Grp. Inc. v. Hartford Cas. Ins. Co.*, No. 10-cv-1126, 2011 WL 5299557 (W.D. Wash. Nov. 4, 2011).

[5] No. 17-11712, 2018 WL 2149769 (11th Cir. May 10, 2018).

[6] Courts construing computer fraud policies generally have not addressed what constitutes the use of a computer. Rather, the decisions that discuss the term "use" focus on whether such use was authorized. *See, e.g.*, *Pestmaster*, 656 F. App'x 332 (the provision, "fraudulently cause a transfer" requires the unauthorized transfer of funds); *Universal Am.*, 25 N.Y.3d 675 (policy insuring against fraudulent entry of electronic data covers losses incurred from unauthorized access to the computer system); *Am. Tooling,* 2017 WL 3263356 (computer fraud requires an unauthorized infiltration or "hacking" of policyholder's computer system). Neither the 11th Circuit nor the District Court addressed whether the use of the IVR computer system was authorized.

[7] *Interactive Commc'ns*, 2018 WL 2149769 at *4.

This article first appeared in the June 29, 2018, edition of Westlaw Journal Insurance Coverage.

ABOUT THE AUTHOR

Lawrence A. Levy is senior counsel in **Rivkin Radler LLP**'s insurance coverage practice group in Uniondale, New York, where he represents large insurance companies in complex coverage disputes including toxic tort, asbestos, environmental, directors and officers, and errors and omissions claims.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.

© 2018 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.