2018 WL 2149769
Only the Westlaw citation is currently available.
This case was not selected for
publication in West's Federal Reporter.
See Fed. Rule of Appellate Procedure 32.1
generally governing citation of judicial
decisions issued on or after Jan. 1, 2007.
See also U.S. Ct. of App. 11th Cir. Rule 36-2.
United States Court of Appeals, Eleventh Circuit.

INTERACTIVE COMMUNICATIONS INTERNATIONAL, INC. et al., Plaintiff-Appellants,
v.
GREAT AMERICAN INSURANCE CO., Defendant-Appellee.

No. 17-11712
|
(May 10, 2018)

Appeal from the United States District Court for the Northern District of Georgia, D.C. Docket No. 1:15-cv-02671-WSD

Attorneys and Law Firms

Kristen Kabat Bromberek, Daniel F. Diffley, Tejas S. Patel, Alston & Bird, LLP, Atlanta, GA, for Plaintiff-Appellant

Michael A. Graziano, F. Joseph Nealon, Eckert Seamans Cherin & Mellott, LLC, Washington, DC, H. Michael Bagley, Drew Eckl & Farnham, LLP, Atlanta, GA, for Defendant-Appellee

Before MARCUS and NEWSOM, Circuit Judges, and BUCKLEW,* District Judge.

* Honorable Susan C. Bucklew, United States District Judge for the Middle District of Florida, sitting by designation.

Opinion

PER CURIAM:

***1** This insurance-coverage case arises out of a "Computer Fraud" policy issued by Great American Insurance Company to Interactive Communications International, Inc. and HI Technology Corp. (together, "InComm"). InComm sells "chits"—each of which has a specific monetary value—to consumers, who can then "redeem" them by loading their value onto a debit card. InComm lost a lot of money—$11.4 million—when fraudsters manipulated a glitch in InComm's computerized interactive-telephone system that enabled them to redeem chits multiple times, with each duplicative redemption of an already-redeemed chit defrauding InComm of the chit's value. We hold, though, that InComm's insurance policy does not cover its loss. Although the fraudsters did "use [a] computer" within the meaning of the policy, we conclude that InComm's loss did not "result[ ] directly" from the computer fraud, as required by the policy's plain language.

I

InComm operates a network that allows consumers to put money onto general-purpose reloadable debit cards issued by banks. In particular, InComm sells "chits" to consumers, which they can then use to transfer funds to their cards. After purchasing a chit at a retailer like CVS or Walgreens, a consumer can simply call InComm to redeem the chit and have its value moved over to his card.

When a consumer dials InComm's 1-800 number to redeem a chit, he is connected to InComm's interactive voice response ("IVR") computer system. The IVR system uses eight computers that process voice requests or telephone touch-tone codes. To redeem a chit through InComm's IVR, a consumer enters his debit card number and the PIN located on the back of the chit. The IVR then credits the value of the chit to the card, and the funds become immediately available to the cardholder.

After making the funds available for use, InComm is contractually obligated to transfer money, equivalent to the value of the redeemed chit(s), to the bank that issued the debit card. By contract, InComm is obligated to transfer the funds within 15 days, although as a matter of standard practice, InComm typically does so within 24 hours. The funds are maintained in the card-issuing bank, for the cardholder's benefit, until he uses the card to conduct a transaction. Because InComm's computer system immediately credits the value of a redeemed chit to a debit card, a cardholder could make purchases using a debit card before or after funds sufficient to cover the

value of the redeemed chit are transferred from InComm to the card-issuing bank.

Between November 2013 and May 2014, fraudsters exploited a vulnerability in InComm's IVR system that enabled multiple redemptions of a single chit. Specifically, the fraudsters figured out that they could redeem a single chit multiple times by making two or more concurrent calls to the IVR system and simultaneously requesting the redemption of a particular chit. One call would transfer the funds from the chit to the debit card account, while the other would return the chit to an "unredeemed" state, allowing it to be redeemed again. Over seven months, InComm's system processed 25,553 fraudulent redemptions associated with 1,988 individual chits.

***2** The fraudulent redemptions cost InComm $11.4 million. The vast majority of that loss—$10.7 million—was redeemed on debit cards issued by Bancorp bank. It is that $10.7 million sum that is at issue in this case. Pursuant to InComm's contract with Bancorp, InComm sold chits to consumers and provided the IVR computer system that allowed the users to transfer the chit's value to their Bancorp-issued debit cards. Once InComm's IVR system was used to redeem a chit, the chit's value was made available for use on the Bancorp card. Bancorp was obligated to transfer funds to merchants to cover purchases made using their debit cards, and InComm, in turn, was obligated to transfer funds equivalent to the value of the redeemed chit(s) to a Bancorp account through which Bancorp pays for those purchases.

The fraudsters' simultaneous calls to InComm's IVR system resulted in duplicate funds being made immediately available on Bancorp customers' debit cards. Because InComm believed the transactions to be legitimate, it wired funds to Bancorp to cover the purchasing power made available on the cards.

II

The insurance policy at issue protects InComm against "Computer Fraud." In particular—and the language is important—the policy provides coverage 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."

InComm seeks coverage for the $10.7 million lost to Bancorp debit card holders who fraudulently manipulated InComm's IVR system to effectuate duplicate redemptions of InComm chits.

The district court granted Great American's motion for summary judgment. It held that the computer-fraud policy did not cover InComm's claimed loss for two reasons. First, the court concluded that the fraud was not accomplished through "the use of a[ ] computer" within the meaning of InComm's policy; and second, it held that, in any event, InComm's loss did not "result[ ] directly" from the use (computer or otherwise) of the IVR system. Although we disagree with the district court's determination that the fraudsters' simultaneous phone calls to the IVR system did not constitute "use of a[ ] computer," we agree with the court's conclusion that InComm's loss did not "result[ ] directly" from the computer fraud. Accordingly, we affirm the district court's judgment that InComm's loss is not covered.

III

Great American contends, and the district court concluded, that the policy does not cover InComm's claimed loss because the scam was not perpetrated through "the use of a[ ] computer." We disagree.

All parties agree that the IVR system comprises eight computers that process transaction requests from cardholders. Thus, the dispute over the "use of a[ ] computer" provision reduces to the question whether phone calls made to a computer system constitute "use" of that computer system.

The district court started with the dictionary definitions of the terms "computer" and "telephone." Based on those definitions, it concluded that "[a] 'telephone' is not a 'computer' " but, rather, "a completely different device." Thus, the court held, the phones with which fraudsters had dialed the IVR system were not computers within the meaning of InComm's policy.

But because the fraud here involved both telephones and computers, we cannot stop there. The question is whether

the fraudsters "use[d]" both phones and computers to perpetrate their scheme—namely, *using* the phones to manipulate—and thereby *use*—the IVR computers. In rejecting InComm's argument, the district court seems to have imposed additional conditions not required by the policy's plain language—for instance, that the computer "use" be knowing. *See, e.g.*, Dist. Ct. Op. at ——("There is no record evidence that cardholders even realized their telephone calls resulted in interaction with a computer.").

***3** But the plain meaning of the word "use"—indeed, as evidenced in the very definitions cited by the district court—comfortably supports an understanding that encompasses the callers' access and manipulation of InComm's IVR system. The district court, for instance, cited both the Oxford Dictionaries' online definition of the term "use" to mean "take, hold, or deploy (something) as a means of accomplishing or achieving something; employ," and *Webster's Encyclopedic Unabridged Dictionary*'s definition to mean "to employ for some purpose; put into service; make use of." *Oxford Dictionaries*, https://en.oxforddictionaries.com/definition/use; *Webster's Encyclopedic Unabridged Dictionary of the English Language* 2097 (2001). Those definitions, it seems to us, fit like a glove. Here, the callers clearly "deploy[ed]"—or "employ[ed]"—the IVR computer system "as a means of accomplishing or achieving" fraudulent duplicate redemptions of InComm chits. *See Oxford Dictionaries,* https://en.oxforddictionaries.com/definition/use. So too, under the district court's Webster's-based definition, the callers "used" the IVR system, "employ[ing]" it "for some purpose; put[ting it] into service; mak[ing] use of" it. *See Webster's Encyclopedic Unabridged Dictionary of the English Language* (2001).

Other dictionaries confirm what the district court's own indicate. *Webster's Second New International Dictionary*, for instance, defines "use" as "to convert to one's service; to avail oneself of; to employ." *Webster's New International Dictionary* at 2806 (2d ed. 1939). There simply can be no doubt that the fraudsters "convert[ed]" InComm's IVR computer system to their service and "avail[ed]" themselves of it by submitting fraudulent reload requests to the computer system in a way that yielded duplicate chit redemptions. To be clear, it is not the case, as the district court suggested, that the IVR system was just "somehow involved" in the fraudsters' scheme, or that the system was merely "engaged at any point in the causal chain." Rather, the fraudsters interfaced directly with the IVR computer system to effectuate their duplicate redemptions. Thus, we conclude that the fraud against InComm *was* perpetrated through the "use of a[ ] computer" within the terms of its insurance policy.

IV

But that is not the end. The question remains whether the "loss of ... money" that InComm suffered here "result[ed] directly" from the use of the IVR. Like the district court, we conclude that it did not. [1] In explaining why, we must explore two sub-issues. First, as a matter of law, what exactly does the phrase "result[ ] directly" mean? And second, as a matter of fact, when did InComm's loss occur?

[1] We assume for the purposes of this opinion—without deciding—that the use of the IVR "fraudulently cause[d] a transfer of ... property from inside the ... banking premises ... to a person [or] place outside those premises" within the meaning of InComm's policy.

A

Not surprisingly, the parties have different views about what it means for a loss to "result[ ] directly" from a computer fraud. For its part, InComm contends—not without some support—that the policy's "resulting directly" language entails only a showing of proximate cause. *See, e.g.*, *Scirex Corp. v. Fed. Ins. Co.*, 313 F.3d 841, 850 (3d Cir. 2002) (applying Pennsylvania law that equates "direct cause" with "proximate cause"); *see also Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821, 831-32 (6th Cir. 2012) (holding that under Ohio law, a "proximate cause" standard should be used "to determine whether plaintiffs sustained loss 'resulting directly from' the 'theft of Insured property by Computer Fraud' "). With its own cases in tow, Great American urges us instead to adopt a reading of "resulting directly" that requires immediacy between conduct and result. *See, e.g.*, *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed.Appx. 252, 258 (5th Cir. 2016) (declining to extend coverage where a loss caused by a fraudulent transfer was "the result of other events and not directly [caused] by the computer use"). [2]

2 The delta between the parties' competing readings may be smaller than it appears. As Justice Cardozo taught us years ago, proximate cause serves to limit liability, not expand it. *See Palsgraf v. Long Island R. Co.*, 248 N.Y. 339, 162 N.E. 99, 101 (1928). To that end, *Black's* defines "Proximate Cause," in relevant part, as "[a] cause that *directly* produces an event and without which the event would not have occurred.—Also termed (in both senses) *direct* cause; *direct* and proximate cause...." *Black's Law Dictionary* at 265 (10th ed. 2014) (emphasis added). *Webster's Second* provides a similar definition: "[A] cause which *directly* or with no mediate agency produces an effect; specifically in law, that which in ordinary natural sequence produces a specific result, no independent disturbing agencies intervening." *Webster's New International Dictionary* at 1995 (2d ed. 1939).

***4** Rather than following the thread of close-but-not-quite-on-point cases from other jurisdictions, however, we look to the plain language of InComm's policy. It is a fundamental principle of Georgia law—and law more generally—that words in contracts "generally bear their usual and common signification[.]" Ga. Code Ann. § 13-2-2(2); *accord, e.g.*, A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* at 69 (2012) ("The ordinary meaning rule is the most fundamental semantic rule of interpretation. It governs constitutions, statutes, rules, and private instruments."). Accordingly, if the phrase "resulting directly" has a "common signification"—*i.e.*, an ordinary meaning—then we have to find and enforce it.

The dispute here, of course, is not about the term "resulting," but rather the word "directly": What does it mean for a result to follow a cause "directly"? Common-language and legal dictionaries provide a clear (and essentially the same) answer. *Webster's Second*, for instance, defines "direct" to mean "(1) straight; proceeding from one point to another in time or space without deviation or interruption; not crooked or oblique ...; (2) Straightforward; going straight to the point ...; (3) Immediate; marked by the absence of an intervening agency or influence; making contact or effected without an intermediary[.]" *Webster's New International Dictionary* at 738 (2d ed. 1939). In the same way, *Black's* defines "direct" to mean "(1) straight, undeviating; (2) straightforward; (3) free from extraneous influence, immediate; (4) of, relating to, or involving passing in a straight line of descent, as distinguished from a collateral line." *Black's Law Dictionary* at 265 (10th ed. 2014).

The theme is unmistakable. In accordance with the term's ordinary meaning, we hold that, for purposes of InComm's policy, one thing results "directly" from another if it follows straightaway, immediately, and without any intervention or interruption.

B

Which leads to the factual question: When, exactly, did InComm's loss occur? And based on the answer to that question, did InComm's loss "result[ ] directly" (as we have interpreted that phrase) from the fraudsters' misuse of InComm's IVR computer system?

We conclude that although the fraudsters' manipulation of InComm's computers set into motion the chain of events that ultimately led to InComm's loss, their use of the computers did not "directly"—which is to say immediately and without intervention or interruption—cause that loss. To the contrary, several steps typically intervened between the fraudulent manipulation of the IVR system to enable duplicate chit redemptions, on the front end, and InComm's ultimate loss, on the back. Here is a timeline of sorts:

- **Step 1**: The fraudsters manipulate InComm's IVR system to enable a duplicate chit redemption. For each fraudulently redeemed chit, a fraudster's debit card is immediately credited with purchasing power, but InComm's funds are neither transferred, nor disturbed, nor altered in any way.

- **Step 2**: Shortly after processing a redemption call through the IVR system, InComm transfers money (equal to the amount of the redeemed chits) to an account at Bancorp for the purpose of paying debts incurred by debit card holders. Bancorp maintains the account "for the benefit of" InComm as "holder[ ] of the Cardholder Balances for the benefit of [Debit] Cardholders." Although InComm is contractually obligated to transfer funds to the Bancorp account within 15 days of making the corresponding purchasing power available on debit cards, as a matter of regular business practice it transfers the money to Bancorp within 24 hours. The

funds remain in the Bancorp account until needed to cover purchases made on a consumer's debit card.

***5** • **Step 3**: A debit card user makes a purchase from a merchant, incurring debt to be paid from the InComm-earmarked Bancorp account.

• **Step 4**: Bancorp transfers money from the account to the merchant to cover the purchase made by the cardholder. [3]

[3] In the ordinary course, the fraud and transfer of funds would proceed as sequenced here. It is at least possible, however, that the expenditure of the fraudulently obtained funds could occur almost immediately after the commission of the fraud. Therefore, even though InComm transfers funds to Bancorp within 24 hours of a chit redemption, it is possible that a cardholder might spend fraudulently obtained funds before InComm makes the corresponding transfer to Bancorp. Despite this potential variation in the sequencing of steps leading to InComm's loss, InComm has always maintained that its loss occurred at the moment it transferred funds to Bancorp, not at the moment that fraudulently obtained purchasing power was used by cardholders. *See, e.g.*, Br. of Appellant 21 ("InComm's loss ... occurred when the money was transferred to Bancorp."). Thus, the potential for variation in the timing of cardholder purchases in the fraud-loss sequence does not change the outcome of this case. We are not obliged to consider arguments not raised by the parties. *See United States v. Campa*, 529 F.3d 980, 989 (11th Cir. 2008) (arguments not made in a party's initial brief are abandoned).

InComm insists that its loss occurred at Step 2—and is thus "directly" the result of the Step-1 fraud. In particular, InComm says that upon transfer of funds to the account held by Bancorp, it lost both ownership and control of those funds. But the facts of the case demonstrate otherwise—that, in fact, InComm retained at least some control over the funds held by Bancorp even after the Step-2 transfer, and could prevent their loss by intervening to halt the disbursement of money from the Bancorp account to merchants at Step 4. On one particular occasion, after identifying fraud associated with $1.9 million in duplicate redemptions by some debit card holders, InComm stepped in to prevent the cards from engaging in further transactions. InComm did so unilaterally, and indeed did not even inform Bancorp that it had done so for nearly a month. That $1.9 million was not "los[t]"; rather, it remains to this day in the InComm-earmarked account held by Bancorp.

Accordingly, InComm's loss did not occur with the Step-2 transfer of funds to the account held by Bancorp. Rather, the loss did not occur until—at Step 4—Bancorp actually disbursed money from the InComm-earmarked account to pay merchants for purchases made by cardholders. That was the point at which InComm could not recover its money. That was the point of no return.

That being the case, it seems clear to us that InComm's loss did not "result[ ] directly" from the initial computer fraud. Far from being immediate, the loss was temporally remote: days or weeks—even months or years—could pass between the fraudulent chit redemption and the ultimate disbursement of the fraud-tainted funds from InComm's Bancorp account. And it is not just that the loss was remote in time; the chain of causation involved intervening acts and actors between the Step-1 fraud and the Step-4 loss. Even after a chit was fraudulently redeemed, each of the following had to occur: (1) InComm had to transfer money to the Bancorp account; (2) the cardholder had to make a purchase using fraudulently obtained funds; and (3) Bancorp had to disburse money from InComm's account to cover the purchase and pay the merchant. It was only at that point that InComm's loss truly materialized. The lack of immediacy—and the presence of intermediate steps, acts, and actors—makes clear that the loss did not "result[ ] directly" from the initial fraud.

V

***6** Because InComm's loss did not "result[ ] directly" from the fraudulent use of its IVR computer system, the loss is not covered by its insurance policy. We therefore affirm the district court's grant of summary judgment in favor of Great American.

AFFIRMED.

All Citations

--- Fed.Appx. ----, 2018 WL 2149769

End of Document