

**MAY 17, 2018**

For more information,
contact:

Tony Tatum
+1 404 352 3714
ttatum@kslaw.com

Shelby Guilbert
+1 404 840 1156
sguilbert@kslaw.com

Ken Fowler
+1 212 556 2227
kfowler@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

New York
1185 Avenue of the Americas
New York, New York 10036-
4003
Tel: +1 212 556 2100

Eleventh Circuit Delivers Partial Victory for Policyholders in Important Computer Fraud Insurance Coverage Ruling

The United States Court of Appeals for the Eleventh Circuit issued an important computer fraud insurance decision on Thursday, May 10, delivering a significant partial victory for policyholders that operate public-facing interactive voice response (“IVR”) computer systems. The Eleventh Circuit’s decision in *Interactive Communications International, Inc. v. Great American Insurance Co.*,¹ (“*InComm*”) may benefit policyholders considerably because it holds that a third party’s use of a telephone to manipulate an IVR system constitutes the “use” of a “computer”—which is an element required to trigger coverage under many computer fraud policies.²

At the same time, however, the court in *InComm* held that coverage was unavailable because, under the specific facts of this case, the policyholder’s loss did not result “directly” from the use of the computer, as required by the policy.³

Although *InComm* is an unpublished opinion applying Georgia law, the decision likely will carry persuasive force in many jurisdictions because it interprets policy provisions using a plain-language approach, and because it is one of the first appellate-court cases to interpret the relevant provisions in the context of a computer fraud or cyber policy.

BACKGROUND

InComm provides services to customers who have purchased general-purpose, reloadable debit cards issued by banks.⁴ After the customers purchase the debit cards—typically at a retailer like CVS or Walgreens—they can purchase “chits” sold by *InComm* that allow the customer to load additional funds onto their debit cards.⁵ After purchasing a chit, the customers call *InComm*’s toll-free number to load the new funds onto the debit card.⁶ During the call, customers are connected to *InComm*’s IVR computer system and then enter—orally or using the phone’s numbered



keys—the debit card number and the chit number.⁷ The IVR computer system then credits the value of the chit to the customer's card, and the funds become immediately available to the cardholder. Pursuant to InComm's contracts with the banks that issued the debit cards ("issuing banks"), InComm must transfer money equaling the value of the chit to the issuing bank within 15 days.⁸ The issuing bank maintains the funds until the customer uses the debit card to make a purchase from a merchant, at which point the issuing bank transfers the money to the merchant's bank.⁹

From November 2013 to May 2014, fraudsters exploited a vulnerability in InComm's IVR computer system that enabled them to redeem a single chit multiple times by making two or more concurrent calls to the IVR system while requesting the redemption of the same chit.¹⁰ The fraudsters made 25,553 fraudulent redemptions, causing InComm a loss of \$11.4 million.¹¹ Of that loss, \$10.7 million was redeemed on debit cards issued by Bancorp bank.¹²

After discovering the fraud and paying Bancorp for the fraudulent transactions, pursuant to its contract, InComm sought coverage for the \$10.7 million under its Computer Fraud policy ("Policy") issued by Great American Insurance Co. ("Great American").¹³ The Policy provided, in relevant part, that 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 ... to a person (other than a messenger) outside those premises; or ... to a place outside those premises."¹⁴ InComm sought insurance coverage under the Policy, but Great American denied InComm's claim, contending (1) that InComm's loss did not result from "the use of any computer to access the IVR system, which is designed to be accessed by telephone," and (2) that "[n]o funds or property were automatically transferred as a result of the chit cards being reloaded."¹⁵

THE DISTRICT COURT PROCEEDINGS AND RULING

InComm initiated a coverage action in the United States District Court for the Northern District of Georgia. The district court granted summary judgment in favor of Great American, holding that coverage was barred for two reasons. First, the district court held that InComm's loss did not arise out of the "use of any computer." The district court concluded that telephones were not computers and that the cardholders did not "use" the IVR system, as there was "no record evidence that cardholders even realized their telephone calls resulted in interaction with a computer."¹⁶ The district court reasoned that the fact that "a computer was somehow involved in a loss does not establish that the wrongdoer 'used' a computer to cause the loss."¹⁷

Second, the district court held that, even if a computer was used to cause InComm's loss, the loss did not "result[] directly" from the computer use.¹⁸

THE ELEVENTH CIRCUIT'S OPINION

On appeal, the Eleventh Circuit held that the district court erred in holding that InComm's loss did not result from the "use of a[] computer," but affirmed the district court judgment because it agreed that the loss did not result "directly" from the computer use.¹⁹

First, relying on dictionary definitions, the Eleventh Circuit explained that the fraudsters "used" a computer because they "deployed"—or "employed"—the IVR computer system "as a means of accomplishing or achieving" fraudulent duplicate redemptions of InComm chits.²⁰ The Eleventh Circuit concluded that 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,"²¹ and it rejected the district court's characterization that the "the IVR system was just 'somehow involved' in the fraudsters' scheme."²²

Second, however, the Eleventh Circuit held that InComm's losses did not result *directly* from the use of the IVR computer system.²³ In reaching this holding, the court declined InComm's invitation to treat the "directly result from" requirement as language that "entails only a showing of proximate cause," and it also rejected Great American's suggestion that the



same language “requires immediacy between conduct and result.”²⁴ Instead, after reviewing dictionary definitions of the word “direct,” the court found that “for purposes of InComm’s policy, one thing results ‘directly’ from another if it follows straightaway, immediately, and without any intervention or interruption.”²⁵ The court then concluded that “several steps typically intervened between the fraudulent manipulation of the IVR system,”²⁶ including “(1) InComm had to transfer money to the [issuing bank] account; (2) the cardholder had to make a purchase using fraudulently obtained funds; and (3) [the card-issuing bank] had to disburse money from InComm’s account to cover the purchase and pay the merchant.”²⁷ The Eleventh Circuit stressed that InComm “retained at least some control over the funds held” by the issuing banks even after it transferred those funds, noting that after identifying the fraud, InComm intervened and prevented the disbursement of \$1.9 million.²⁸ Accordingly, the Eleventh Circuit affirmed the grant of summary judgment in favor of Great American.²⁹

KEY TAKEAWAYS

InComm is a positive development for policyholders insofar as it provides new, appellate-court authority for the proposition that a computer fraud policy requiring the “use” of a “computer” may cover losses for actions taken by third parties that use other devices to manipulate the policyholder’s computers. This is an important development for the many policyholders that deploy public-facing IVR computer systems, especially those in the financial services and payment-processing industries.

However, the Eleventh Circuit’s opinion upheld the finding of no coverage based on the Policy’s use of causal language requiring a “direct” connection between the covered wrongful act and the loss. The latter finding was highly fact-intensive and tied to the specific language in InComm’s policy, and thus may not be a harbinger for other computer fraud claims. At the same time, the court’s construction of the “directly results from” requirement in InComm’s policy illustrates the importance of carefully reviewing causation triggers in insurance policies. If InComm’s Policy had contained the words “or indirectly” between the words “directly” and “results from,” the Eleventh Circuit might not have affirmed Great American’s denial of \$10.7 million in insurance coverage.

Policyholders should carefully review their computer fraud, crime, and cyber policies when negotiating coverage, and consult with attorneys to ensure that, where appropriate, their policies cover losses arising out of fraudulent financial transactions and the nefarious manipulation of electronic payment processing systems.

We work closely with our clients and their risk managers to collect from their insurers for losses arising from computer fraud, fraudulent transactions, data privacy breaches, property damage, business interruption, and other losses caused by criminal actors, and have obtained billions of dollars in insurance recoveries for our policyholder clients.



ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,000 lawyers in 20 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.”

ABU DHABI	CHICAGO	HOUSTON	NEW YORK	SILICON VALLEY
ATLANTA	DUBAI	LONDON	PARIS	SINGAPORE
AUSTIN	FRANKFURT	LOS ANGELES	RIYADH	TOKYO
CHARLOTTE	GENEVA	MOSCOW	SAN FRANCISCO	WASHINGTON, D.C.

¹ No. 17-11712, 2018 WL 2149769 (11th Cir. May 10, 2018).

² *Id.* at *2–3.

³ *Id.* at *3–5.

⁴ *Id.* at *1.

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.* at *1–2.

¹² *Id.* at *2.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *InComm Holdings, Inc. v. Great American Ins. Co.*, No. 1:15-cv-02671-WSD, slip op., at 11 (N.D. Ga. March 16, 2017).

¹⁶ *Id.* at 26.

¹⁷ *Id.* at 25.

¹⁸ *Id.* at 27–36.

¹⁹ *InComm*, No. 17-11712, 2018 WL 2149769, at *1.

²⁰ *Id.* at *3 (alterations adopted).



²¹ *Id.* at *2.

²² *Id.* at *3.

²³ *Id.* at *3–5.

²⁴ *Id.* at *9.

²⁵ *Id.* at *10–11.

²⁶ *Id.* at *4.

²⁷ *Id.* at *5.

²⁸ *Id.*

²⁹ *Id.*