Ninth Circuit Allows $24 Million AT&T Sim Swap Case to Proceed to Trial

NEW YORK, NY, UNITED STATES, October 2, 2024 /EINPresswire.com/ -- On September 30, 2024, the United States Court of Appeals for the Ninth Circuit held that a $24 million SIM swap fraud case against AT&T Wireless can proceed to trial.


SIM Swap Lawyer Marc D. Fitapelli

The Ninth Circuit's September 30, 2024 decision reversed a March 28, 2023 decision by the Central District of California.

The practical result of the September 30, 2024 Ninth Circuit decision is that the Plaintiff's case will likely proceed to trial before the Central District of California.

The case is Terpin v. AT&T Mobility LLC and the case number is 2:18-CV-06975.

The decision will be used as a precedent by countless other victims of SIM swapping fraud. It is good news for AT&T Sim swap fraud victims, but bad news for AT&T. The Ninth Circuit's decision comes after AT&T admitted on July 24, 2024 that customer data was illegally downloaded by hackers.

Factual Background

Sim Swap fraud occurs when a hacker is provided with access to a victim's mobile phone number. With this access, a hacker can intercept two factor authentication, or 2FA, codes sent by financial institutions. In Terpin v. AT&T, a teenage hacker was able to bribe an employee of AT&T to bypass AT&T's typical security measures. The hacker convinced AT&T to transfer control of the plaintiff's cell phone to a cell phone controlled by the hacker.

After the sim swap occurred, the hacker requested various password resets to the plaintiff's phone number, including a password reset from a Microsoft OneDrive Account. Unfortunately, the hacker was able to access a document in the Plaintiff's trash folder, which gave the hacker credentials for plaintiff's cryptocurrency wallets. Armed with this information, the hacker was

> Call us at 800-767-8040 if you were a victim of SIM swapping. If you had money or cryptocurrency stolen, we may be able to help you recover your losses."
>
> *Marc D. Fitapelli, Esq.*

able to steal $24 million from the plaintiff, Michael Terpin, a well-known cryptocurrency investor.

Procedural History

Mr. Terpin sued AT&T in District Court asserting several causes of action, including violation of the Federal Communications Act. On March 28, 2023, the District Court dismissed Terpin's entire lawsuit on summary judgment. Mr. Terpin appealed to the Ninth Circuit. On September 30, 2024, the Ninth Circuit reversed, in part, the district court's decision. Most significantly, the Ninth Circuit reversed the District Court's dismissal of Mr. Terpin's claims under the Federal Communications Act. Those claims, the Ninth Circuit held, should proceed to trial before the district court.

Federal Communications Act Claims

In Terpin v. AT&T, the Ninth Circuit found that AT&T may have violated the Federal Communications Act in two discrete ways. First, the Ninth Circuit held that the SIM swap gave the hacker "access" to "information that relates to . . . the technical configuration" of Terpin's telecommunications service. 47 U.S.C. § 222(h)(1)(A). The technical "configuration" of a customer's telecommunications service, included the "devices associated with that service."

Second, the SIM swap gave the hacker access to information "that relates to" the "type, destination, location, and amount of use of a telecommunications service" by allowing the hacker to receive all incoming communications sent to plaintiff's phone number. 47 U.S.C. § 222(h)(1)(a). According to the Ninth Circuit, "the password reset messages themselves are communications sent to Terpin's phone number and thus qualify as CPNI. See 47 U.S.C. § 222(h)(1).

The Ninth Circuit also argued that AT&T's view of the Federal Communications Act would lead to "absurd results." Here is the Court's argument: "If [the hacker] had walked into the AT&T affiliate store, asked [an AT&T employee] to print Terpin's recent call log, and looked at the call log, AT&T would not dispute that [the hacker] had access to CPNI. Yet under AT&T's view, [the hacker] had no access to CPNI when he walked into the store, updated Terpin's account to change the SIM associated with Terpin's phone number, gained control over all incoming communications with Terpin's phone number, and received confidential password reset messages sent to Terpin's phone number. Our decision avoids this paradox."

The Court also argued that its decision was consistent with the FCC's views. In a report addressing new proposed CPNI rules, the FCC recognized that SIM swap fraud "allows the bad actor to gain access to information associated with the customer's account, including CPNI."

ATTORNEY ADVERTISING

About MDF Law

MDF Law did not represent any of the parties to this matter. MDF law is a national law firm with offices in New York and California. The firm exclusively represents consumers and victims of serious financial crime. MDF Law currently represents other victims of SIM swap fraud in cases against AT&T wireless and other mobile providers. If you or someone you know lost money as a result of a SIM Swap, call the lawyers at MDF Law at 800-767-8040.

California Office: 1902 Wright Place, Suite 200, Carlsbad, CA 92008
New York Office: 28 Liberty Street, 30th Floor, New York, NY 10005

Marc Fitapelli
MDF Law
+1 212-203-9300
email us here
Visit us on social media:
X
