No. 23-55375

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

MICHAEL TERPIN,

Plaintiff-Appellant,

v.

AT&T MOBILITY, et al.,

Defendant-Appellee.

On Appeal from the United States District Court
for the Central District of California
No. 2:18-CV-06975-ODW
The Honorable Otis D. Wright II, District Court Judge

BRIEF OF CTIA – THE WIRELESS ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT–APPELLEE AND AFFIRMANCE

Joshua S. Turner
Counsel of Record
Sara M. Baxenberg
William Turner
WILEY REIN LLP
2050 M St. NW
Washington, DC 20036
Tel: (202) 719-7000
Counsel for Amicus Curiae

RULE 26.1 CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, CTIA submits the following corporate disclosure statement:

CTIA – The Wireless Association ("CTIA") states that it has no parent corporation, and no persons, associations of persons, firms, partnerships, limited liability companies, joint ventures, corporations, or any similar entities have a ten percent or greater ownership interest in CTIA.

Dated: October 2, 2023

/s/ Joshua S. Turner
Joshua S. Turner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Administrative Materials

Statutes

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

CTIA – The Wireless Association ("CTIA") is the premier trade association representing the U.S. wireless communications industry and companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. CTIA and its members are committed to reducing the risk of mobile authentication fraud, including through Subscriber Identity Module ("SIM") swap fraud and other types of mobile phone related fraud, such as port-out scams. To that end, CTIA has created working groups that include technical experts who focus on advancing measures to prevent and minimize the risk of fraud. John Marinho, *Protecting Your Account Against Mobile Authentication Fraud*, CTIA (Mar. 15, 2018), https://www.ctia.org/news/protecting-your-accounts-against-number-porting. CTIA and its members also work to empower consumers to protect their mobile accounts and data. Lorenzo Franceschi-Bicchierai, *Verizon Adds Protection Against SIM Swapping Hacks in Mobile App*, Vice Media Group (July 9, 2020), https://www.vice.com/en/article/3azv4y/verizon-sim-swapping-hack-protection-number-lock; CTIA, *Protecting Your Data*, (last visited Oct. 2, 2023) https://www.ctia.org/protecting-your-data; T-Mobile USA, Inc., *SIM Protection*, (last visited Oct. 2, 2023), https://www.t-mobile.com/support/plans-features/sim-

[1] All parties have consented to the *amicus* brief's filing. No party's counsel authored any part of this brief. No party or party's counsel, or person other than *amicus*, contributed money to the brief's preparation or submission.

protection. CTIA has also offered comments before the Federal Communications Commission ("FCC") aimed at finding a balanced approach to combat SIM swap fraud when it does occur. Protecting Consumers from SIM Swap and Port-Out Fraud, Comments of CTIA, FCC 21-102, WC Docket No. 21-341 (Nov. 15, 2021), https://www.fcc.gov/ecfs/document/111560258257/1 ("CTIA Comments").

CTIA and its members have a critical interest in the correct interpretation of Section 222 of the Communications Act, as well as providing the Court a robust understanding of the state of mobile technology security—including the risk posed by judicial mandates that could stifle innovation, jeopardize other important goals made possible through rapid, efficient SIM swaps, and create perverse incentives for consumers to take a backseat when it comes to protecting their own data. For the reasons described below, this Court should affirm the decision of the district court.

SUMMARY OF ARGUMENT

A Subscriber Identity Module, or SIM, is a mobile communications device component that allows wireless networks to properly associate a telephone number with a specific device. The SIM is an innovation that allows customers to quickly upgrade their mobile devices or switch wireless providers without lengthy delays or the inconvenience of having to get a new number. Millions of these changes are made every year, only a small fraction of which are unauthorized. And only a tiny percentage of those end up involving actual consumer financial losses, since an

unauthorized SIM change or "swap" in isolation causes no financial loss.[2] If financial loss ultimately occurs, a SIM swap is just one part of a criminal scheme that involves several other steps, service providers, and online platforms unrelated to telecommunications services.

Here, the district court confronted one of those rare cases involving financial harm. The court correctly concluded that AT&T was not responsible for the losses ultimately incurred by the Appellant when a group of criminals undertook a bribery scheme involving fraudulent access to the Appellant's mobile phone number, his Gmail account, his Microsoft account, a document stored on his Microsoft OneDrive that contained his cryptocurrency wallet credentials, and his cryptocurrency wallet.

Appellant and supporting *amici* EPIC and the National Consumers League ("EPIC *amici*") ask this court to reverse the district court's holdings not because the law requires or even allows it, but because they view unauthorized SIM swaps as a broader policy problem. They seek to turn wireless providers into omnibus insurers by imposing a duty on wireless providers to prevent all unauthorized SIM swaps and to hold consumers harmless from any and all consequences of fraudulent SIM swaps—even where, as here, those consequences resulted directly from intervening

---

[2] Closely related to SIM swaps are port-out scams. In a fraudulent SIM swap, a fraudster gets the victim's wireless carrier to move the victim's service to a phone in the fraudster's possession. In a port-out scam, a fraudster opens an account with a different carrier, posing as the victim, and has the victim's number transferred to this account.

criminal acts, including the theft of information that is neither related to a telecommunications service nor otherwise protected by federal law. In the process, they disregard entirely the existence of robust federal laws governing how wireless providers are required to handle customer requests for access to accounts and handle SIM swaps and port-out requests.

Appellant and EPIC *amici* base their arguments on a fundamentally inaccurate set of assumptions and insinuations: that fraudulent SIM swaps are rampant, that these swaps regularly lead to significant financial loss for average consumers, and that consumers simply have no choice but to use their mobile phones to secure their information and financial accounts. Each of these ideas is wrong. Unauthorized SIM swaps are extremely uncommon, in large part due to the efforts that the wireless industry has undertaken to prevent and protect against this fraud. When unauthorized SIM swaps do occur, the consumer protections afforded by entities such as banks and credit card companies help to guard against financial loss. And while cryptocurrency investment can carry more risk than more traditional bank investments, cryptocurrency platforms, too, can and do offer security protections to their customers. Those protections can be used to guard funds and cannot be circumvented by a SIM swap.

More generally, there are numerous, simple steps that consumers can and do take to safeguard their personal information. In fact, SMS was not designed for user

authentication, and while it can be a convenient option in some cases, it should come as no surprise that federal law does not impose the kind of obligations for which Appellant and EPIC *amici* advocate on a system that was never intended to be used as an authentication platform.

Appellant and EPIC *amici* offer a distorted and overly simplified view of the cybersecurity landscape. In reality, cybersecurity hygiene is an ever-evolving, multi-stakeholder pursuit that involves security measures well beyond SIM swap procedural safeguards. It requires efforts by other players in the ecosystem (i.e. financial institutions, cryptocurrency platforms, email providers, and more) particularly including consumers themselves. These stakeholders are best positioned to understand the risks and security options most appropriate for a particular consumer's use of third-party services.

Appellant and EPIC *amici* are also wrong on the application of federal law. The Communications Act of 1934, 47 U.S.C. §151 *et seq*., as amended, ("the Act" or "the Communications Act") places strict limits on the types of information that telecommunications carriers are obligated to protect. Appellant and EPIC *amici* ask this court to broaden the relevant statutory terms beyond recognition, which would allow for liability in circumstances that Congress never intended. They also ask this Court to ignore the numerous steps in the causal chain, a string of criminal acts, the theft of Appellant's personal information unrelated to his mobile phone account, and

hacking involving several other digital accounts wholly unrelated to AT&T's provision of telecommunications services—that directly caused Appellant's loss of cryptocurrency.

Rather than the judicially-created, broad, industry-wide policy changes requested by Appellant and EPIC *amici*, this Court should simply apply governing law to the facts of this case. That is precisely what the district court did when it found that no information subject to protection under federal law was shown to have been disclosed here, and that neither the SIM swap nor AT&T proximately caused Appellant's losses. As a result, this court should affirm the orders under appeal.

ARGUMENT

I. APPELLANT AND EPIC *AMICI'S* ARGUMENTS ARE PREMISED ON MISAPPREHENSIONS ABOUT WIRELESS TECHNOLOGY, CYBERSECURITY, AND THE FRAUD LANDSCAPE.

Appellant and EPIC *amici* invite this Court to grant a judicial imprimatur to their policy views on how to best protect consumers from unauthorized SIM swaps. To justify the request, they craft a misleading narrative about the stakeholders involved, applicable regulations, the solutions available, and the degree of danger (i.e., the supposed prevalence of unauthorized SIM swaps and the state of the cybersecurity ecosystem). But that narrative rests on a series of false premises. And, in any event, this Court should readily reject Appellant and EPIC *amici*'s invitation to engage in communications and cyber policymaking.

A. Consumers Depend on Seamless SIM Swaps to Stay Connected.

Cellular phones are an essential part of American life. Hundreds of millions of people—97% of American adults—own a mobile phone. Pew Research Center, *Who Owns Cellphones and Smartphones*, Mobile Fact Sheet (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/. Of that 97%, nearly 90% own a smartphone. *Id*. The ubiquity of smartphones should come as no surprise. Today's smartphones are a modern marvel. They allow fast and reliable mobile communications across the globe, all occurring over small, sleek devices that are simple for consumers to use, and require minimal troubleshooting or visits to a brick-and-mortar store.

SIMs are a critical component of this communications environment. They route telecommunication services to customers, they allow customers to upgrade devices or replace lost devices, and they help customers switch wireless providers without losing their phone number.

An easy and efficient SIM swap and port-out process is pro-competition and pro-consumer, in that it reduces the friction involved when moving from one device or one carrier to another. Without having to worry about lengthy delays in moving their telephone numbers, consumers are free to compare wireless service offerings on price, quality, and features—and to switch when a better deal comes along. The wireless industry supports this flexibility, and the FCC has recognized its benefits

for decades. *See, e.g., In the Matters of Loc. No. Portability Porting Interval & Validation Requirements Tel. No. Portability*, 24 F.C.C. Rcd. 6084, 6085 ¶ 2 (2009) (discussing wireless number portability requirements); *In the Matters of Loc. No. Portability Porting Interval & Validation Requirements Tel. No. Portability*, 11 F.C.C. Rcd. 8352, 8368 ¶ 30 (1996) ("Number portability promotes competition between telecommunications service providers by, among other things, allowing customers to respond to price and service changes without changing their telephone numbers"). Indeed, the FCC directly regulates the number portability process to ensure that these objectives are met, limiting the type of information that a carrier may require to carry out a port request. *See* 47 C.F.R. § 52.36 ("A telecommunications carrier may require only the data described in paragraphs (b) and (c) of this section to accomplish a simple port order request from an end user customer's new telecommunication's [sic] carrier.")

Beyond convenience, an efficient SIM swap and port-out process can be critical to consumer safety. That includes the ability to stay connected with family and friends, as well as law enforcement, emergency services, and protective resources when escaping domestic violence or abuse. This is why federal policy encourages making SIM swaps and port-outs easy to accomplish and discourages friction that can frustrate customers and can introduce risk, such as to customers on family or shared plans that may need to quickly and discreetly change numbers or

devices. Here, too, federal law imposes requirements on wireless providers—under the Safe Connections Act of 2022, a provider must separate from a shared mobile service contract the line of a domestic violence survivor (and the line of any individual in the survivor's care) from the abuser's line unless separation is operationally or technologically infeasible. *See* Safe Connections Act of 2022, Pub. L. No. 117-223 (2022), 47 U.S.C. § 345. Unnecessary and overly broad restrictions on SIM swaps and port-outs (whether by regulation or new duties imposed by courts) can have unintended consequences such as giving a domestic abuser more control over a victim's ability to escape or impeding consumers' access to emergency services.

Finally, the ability to perform a quick and efficient SIM swap can often help *enhance* the security of a subscriber's account and personal information. For example, in the case of a lost phone an authorized SIM swap can ensure that a bad actor cannot impersonate the subscriber if the phone falls into the wrong hands.

B. Wireless Providers Work Hard to Ensure That Unauthorized SIM Swaps Are Extremely Uncommon.

Given all of these benefits, it is no wonder that, on average, wireless providers process hundreds of thousands of SIM swaps each month. And more than 99% of those requests are legitimate—fraud affects less than 1% of these transactions. CTIA Comments at 1, 8.

The efforts that the wireless providers have undertaken to combat unauthorized SIM swaps have played a big part in that success. Of course, these efforts are complex: overly restrictive or onerous procedures can hamper the benefits laid out above by efficient SIM migration, causing consumer harm that could outstrip the fraud these procedures seek to prevent. Thus, to help reduce fraud, for many years wireless providers have embraced a nuanced approach that centers on adapting internal security procedures to ever-evolving attack methods, providing consumer education, and establishing outside partnerships with financial institutions and law enforcement.

With respect to internal procedures, wireless providers take a variety of approaches, but they have one thing in common: working to build and iterate successful programs aimed at deterring, detecting, and quickly fixing unauthorized SIM swaps. For example, providers have long taught employees about authentication, fraud prevention, and social engineering. Wireless providers have the flexibility to adopt company-specific training programs to help employees recognize and prevent fraudulent SIM swap requests. In addition, wireless providers have implemented security measures such as account and SIM card pass codes and have begun requiring multi-factor authentication and providing notice to consumers when a SIM swap is requested. Some providers have also deployed sophisticated algorithms to detect and halt unauthorized SIM swaps when they do occur.

These flexible, risk-based approaches are consistent with existing federal law and seek to balance the importance of combatting fraud with the other important objectives that are accomplished with a speedy, efficient SIM swap and port-out process. Of course, no protections are completely effective, and even the most diligent training programs cannot prevent all fraud, especially when a determined criminal already has extensive customer information from other sources and knowingly violates the carrier's policies. But the procedures and training put in place by wireless providers have helped minimize the opportunities for these SIM swaps to occur in the first instance.

Wireless providers have also helped empower consumers by providing tools that allow customers to freeze or lock accounts if an unauthorized SIM swap occurs. Wireless providers have also focused heavily on educating consumers, making sure that their subscribers are aware of SIM swap and port-out fraud, and providing tips on how to prevent these scams. For example, all three major US providers—AT&T, T-Mobile, and Verizon—suggest ways that customers can protect their phones and *See, e.g.*, AT&T, *What You Need to Know About SIM Swap Scams*, SIM Swapping, (last visited Oct. 2, 2023), https://about.att.com/pages/cyberaware/ni/blog/sim_swap; T-Mobile, *Online Safety and Cybersecurity* (last visited Oct. 2, 2023), https://www.t-mobile.com/privacy-center/education/online-safety-cybersecurity.html; Verizon, *SIM Swapping* (last

visited Oct. 2, 2023), https://www.verizon.com/about/account-security/sim-swapping. Consumer education is important, because ultimately it is the consumer who decides whether and how to use their mobile number for authentication; wireless providers simply have no way to control (or even to know) what off-network services consumers choose to use their device with.

Wireless providers also work with financial institutions and law enforcement agencies to prevent and eliminate fraud. For example, providers notify law enforcement of breaches of Consumer Proprietary Network Information ("CPNI"), a subset of data defined by federal law, in accordance with federal regulations. *See* 47 U.S.C. § 222. This allows the providers and law enforcement to work together to reduce possible damage flowing from these breaches. Wireless providers also work with law enforcement agencies to identify bad actors, mitigate the impact of fraudulent disclosures, and combat further fraud. Further, wireless providers have developed relationships with financial institutions and implemented technology that allows information sharing with these financial institutions, in order to facilitate the exchange of real-time information that allows better authentication of customers and the triage of individual cases of fraudulent SIM changes.

These and other efforts have minimized unauthorized SIM swaps such that unauthorized swaps are only a tiny portion of all SIM swaps. They are also a tiny portion of all fraud. EPIC *amici*'s own brief implicitly concedes as much. That brief

asserts that unauthorized SIM swap crimes "affect thousands every year and resulted in over $70 million in reported losses in 2022 alone." Amicus Br. at 3. However, the FTC's investigative Consumer Sentinel Network reflects a total of $8.8 billion in reported fraud losses over that same period. Lesley Fair, *FTC crunches the 2022 numbers. See where scammers continue to crunch consumers*, FTC Business Blog (Fed. 23, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/ftc-crunches-2022-numbers-see-where-scammers-continue-crunch-consumers. Thus, even assuming the numbers cited by EPIC *amici* are correct and do not overstate the losses attributable to unauthorized SIM swaps, these fraudulent transactions are involved in a fraction of one percent of fraud losses in a given year.

Even where unauthorized SIM swaps occur, those facing actual financial loss as a result of this criminal activity comprise an even smaller group, and tend to be people who have intentionally chosen assets, such as cryptocurrency, that are subject to less cybersecurity regulation or loss protection. In contrast, established financial institutions, such as banks, have taken robust measures to safeguard consumers against losses, and to insure against losses that do occur.

C. Security Measures Surrounding the SIM Swap Process Are Just One Tool in a Multi-Faceted, Multi-Stakeholder Effort to Curtail Consumer Fraud and Promote Cybersecurity.

Cybersecurity and fraud prevention are complex undertakings. Fighting fraud is necessarily a collaborative process. But Appellant and EPIC *amici* overlook that

wireless providers are only one part of this broader effort to prevent the types of financial losses perpetrated by fraudsters. Appellant and EPIC *amici* also incorrectly suggest that wireless providers have no incentive to compete based on security. As a result, their argument goes, heightened legal protection around the SIM swap process is the only solution. That premise is false. So too is the conclusion.

First, as set forth above, wireless providers already work to prevent SIM swap fraud and have developed programs that are fully compliant with federal law and policy which expect wireless providers to balance pro-competitive customer choice and mobility against security steps that may slow down SIM swaps. But no matter what steps a provider takes, it can never ensure that a device, account, or network is "100% secure." Providers must constantly shift and improve their practices to respond to evolving threats. Just as the industry identifies a security solution, hackers are already at work attempting to dismantle it.

Despite all of this, providers aggressively and *constantly* work to stay ahead of evolving cyber-attacks and fraudster tactics by deploying new authentication and fraud prevention tools as well as monitoring tactics to catch fraud before it even happens. Sometimes wireless providers work together to form and agree upon industry best practices. For example, CTIA, as the wireless industry's primary trade association, leads a cybersecurity working group that brings together all sectors of wireless communications—including service providers, manufacturers and wireless

data, internet and applications companies—to advise on security policy and best practices. Cybersecurity Working Group, CTIA https://www.ctia.org/cybersecurity-working-group (last visited Sept. 30, 2023). In other instances, contrary to the claim by Appellant and EPIC *amici*, individual providers undertake their own fraud-prevention activities. For example, in comments to the FCC, AT&T noted that it uses data analytics to "a sophisticated risk-scoring model for certain [] transactions." Protecting Consumers from SIM Swap and Port-Out Fraud, Comments of AT&T at 6, FCC 21-102, WC Docket No. 21-341 (Nov. 15, 2021). Depending on the score, heightened authentication requirements might be required before approving a SIM swap. *Id*. Allowing customers to choose biometric account authorization is another method that providers use to combat this kind of fraud. Protecting Consumers from SIM Swap and Port-Out Fraud, Comments of Verizon at 2-3 and Comments of T-Mobile USA, Inc. at 3, FCC 21-102, WC Docket No. 21-341 (Nov. 15, 2021).

In addition to these public-facing steps, others take place behind the scenes and cannot readily be discussed without providing a roadmap for bad actors to avoid their effectiveness. But all are aimed at reducing the ability of criminals to target wireless consumers with fraudulent activity while avoiding significant negative impact to the customer experience—something the providers clearly have every incentive to undertake.

Second, the wireless industry is not and cannot be the only line of defense against fraud. Criminal fraudsters and scammers are often sophisticated actors, using unauthorized SIM swaps and port-outs as part of a broader scheme to do harm. These schemes often require "socially engineering" consumers into disclosing personal information, as well as consumer engagement with other non-carrier applications or offerings. Thus, wireless providers implementing protections against unauthorized SIM swaps alone will not prevent all consumer fraud. Even if wireless providers were to employ every available protection, a criminal can still steal subscriber information if an application on the phone or user activity leaves a consumer's information vulnerable.[3] All stakeholders, including financial services companies, social media providers, and law enforcement, must be involved in the effort to protect consumers from fraud. SIM swapping scams largely target financial accounts and social media accounts. These entities are in the best position to conduct risk assessments of their services and their customer's use of them, and to advise customers on appropriate security steps for those unique use cases. Thus, it is imperative for financial institutions, cryptocurrency services, social media

[3] The marketplace has already recognized as much. Accordingly, as explained in the next section, consumers have many alternatives to SMS-based two-factor authentication. These solutions may provide enhanced security for particularly sensitive data such as cryptowallets.

companies, and others whose technology platforms are frequent targets of hackers and scammers to adopt aggressive, risk-based measures to protect consumers.

The precise appropriate measures will need to be considered on a case-by-case basis, but a risk-based approach confirms that in some circumstances SIM-based two-factor authentication will *not* be the most secure approach. Indeed, SIMs were not designed and were never intended for off-network identity verification. As a result, while SIM-based authentication has evolved into a widely used and convenient tool, it may not be appropriate for higher-risk transactions, including those involving financial institutions and cryptocurrency assets. As the FTC has explained in the context of its Safeguards Rules:

> "[i]n some cases, use of SMS text messages as a factor may be the best solution because of its low cost and easy use, if its risks do not outweigh those benefits under the circumstances. In other instances, however, the use of SMS text messages may not be a reasonable solution, such as when extremely sensitive information can be obtained through the access method being controlled, or when a more secure method can be used for a comparable price. A financial institution will need to evaluate the balance of risks for its situation."

Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272 (Dec. 9, 2021) (to be codified at 16 CFR pt. 314), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information. For sensitive transactions, financial institutions and others involved in the retention and storage of sensitive data are best positioned to determine what level of security is most appropriate. And as risks and

the need for security increases, so do the costs and complexity of providing that service. A judicial decree transforming mobile providers into third-party security authentication services—and forcing them to bear the costs and risks of securing even the most sophisticated types of transactions—would increase costs for all, without increasing security.

In addition to creating back-end security solutions, all stakeholders must do their part to educate consumers about how to protect against fraud, and how to take steps that are important for their service or offering. Crucially, customers must act in accordance with this advice and work collectively with industry practices to protect their assets.

D. Customers Can and Do Take Steps to Protect Themselves from Fraud and Financial Loss.

Appellant and EPIC *amici* suggest that individuals are powerless to prevent against cybercrimes like the one perpetrated against Appellant. In fact, consumers have numerous tools at their disposal to protect themselves. They are a critical part of the cybersecurity ecosystem, and often are the best-positioned to take preventative action where risks are particularly high.

There is no single, one-size-fits-all solution. A risk-based approach to security means balancing convenience and ease of access with the need to protect sensitive data or other information. After reviewing the educational materials provided by wireless providers, financial services and social media companies,

regulators, consumer advocacy organizations, and others, consumers have the power to exercise the types of good cyber hygiene advised in those sources of guidance. Consumers can choose the security methods that are best for them, and that provide the best protection for their assets.

As noted above, while SMS-based two-factor authentication may be suitable because of its ubiquity and convenience, it is not the most secure form of authentication for all types of transactions. Financial institutions can and should limit the use of SMS authentication, but customers must also take responsibility for employing a risk-based approach. In high stakes financial transactions, for example, consumers may well wish to look beyond SMS and employ additional, layered security approaches. This is widely understood by stakeholders operating in these areas. For example, Coinbase, a cryptocurrency exchange platform encourages users to find alternatives to SMS, calling it the "Least Secure" form of two-step authentication. Coinbase, *What Is 2-Step Verification*, (last visited Oct. 2, 2023), https://help.coinbase.com/en/coinbase/getting-started/getting-started-with-coinbase/2-factor-authentication-2fa-faq..

EPIC *amici*'s claim that there are no readily available alternatives to SMS authentication is also simply not correct. Far from being an "obscure exception" that is "likely unknown to most consumers," using an app for two-factor authentication is both straightforward and readily available to all consumers.

Indeed, the iPhone comes with a built-in app that performs this function, *see e.g.* https://support.apple.com/guide/iphone/automatically-fill-in-verification-codes-ipha6173c19f/ios, and Google offers an Authenticator app that can be used on Android devices, *see e.g.,* https://support.google.com/accounts/answer/1066447?hl=en&co=GENIE.Platform%3DAndroid. These are just two examples that are readily available; there are many others just a few clicks away in the respective app stores, available on any wireless smartphone.

And where customers engage in particularly risky behavior involving sensitive data, such as investments in untraceable assets in less regulated cryptocurrency markets, the need to take all available precautions is especially pronounced. There are many potential ways for a consumer with cryptocurrency assets to help keep them safe, including not linking crypto accounts to widely available information like phone numbers, following crypto wallet instructions (which often include cautions about not placing credentials online), using a non-SMS authenticator, or even by keeping credentials in an air-gapped, cold-storage wallet.[4] In keeping with the need for a risk-based approach to security, consumers in these kinds of transactions undoubtedly have both the sophistication *and the*

[4] An air-gapped cold storage wallet is a device that does not have any Internet connectivity, and therefore cannot be remotely accessed or hacked.

incentive to seek out additional security tools that may be more appropriate than SMS.

Thus, consumers are empowered to protect themselves against fraudsters through these various tools and cyber hygiene best practices. They can do so using different tools depending on the different levels of risk they may face depending on their specific type of activity. Those tools are not only readily available, they are well-understood and widely recommended.

II. APPELLANT AND EPIC *AMICI'S* EXPANSIVE READING OF SECTION 222 IS ERRONEOUS, BUT EVEN IF IT WERE CORRECT, THERE IS NO BASIS ON THIS RECORD TO HOLD AT&T LIABLE FOR DAMAGES.

Appellant and EPIC *amici* both focus heavily on their vision of unauthorized SIM swaps as a societal problem, rather than the legal questions at issue in this case. Indeed, the EPIC *amici* are quite blunt in this regard, asking the Court to overturn the decision below because they claim that providers "need the incentive" to stop unauthorized SIM swaps. EPIC Br. at 6. But the Appellants also rely heavily on an appeal to broader policy concerns. *See* Appellant Br. at 11 (asserting that "[t]his case is . . . of wider importance because it relates to the ubiquitous practice of . . . two-factor authentication," and that the Court should reverse the lower court because "[w]hen a telecommunications behemoth like AT&T fails to protect that gateway . . . customers, like Terpin, will predictably suffer disastrous consequences").

As laid out in Section I, *supra*, wireless providers are already taking aggressive actions to combat fraud, and there is no basis for claiming that providers "need [an] incentive" to employ cybersecurity measures or to meet their statutory obligations under Section 222 of the Communications Act. But in any event, questions about incentivization of regulated entities—and the meaning of technical telecommunications terms and concepts, the obligations imposed on telecommunications carriers, and the provision of private causes of action—are better left for Congress and the FCC as the agency charged with implementing the Communications Act.[5]

Ultimately, none of Appellant and EPIC *amici*'s claims about the prevalence of unauthorized SIM swaps or who is best positioned to prevent this type of fraud speak to the questions before this Court, which ask whether Plaintiffs can show on this record that AT&T violated Section 222 of the Communications Act, whether Appellant's losses are sufficiently causally connected to any such violations, and whether Appellant's other claims were appropriately dismissed or denied. Focusing,

[5] Indeed, the FCC currently has a pending proceeding on potential actions the agency could take to combat unauthorized SIM swaps. *See Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, FCC 21-102, WC Docket No. 21-341 (2021). *Amicus* EPIC filed comments in that proceeding, arguing for many of the same policy outcomes that it seeks in this Court. Comments of the National Consumer Law Center and EPIC, WC Docket No. 21-341, *available at* https://www.fcc.gov/ecfs/document/111608400758/1 (filed Nov. 15, 2021). Thus, to the extent that any of the policy issues raised by Appellant or EPIC *amici* do need to be addressed, the FCC has the vehicle in place to do so.

as the Court must, on the legal questions at issue in this appeal, the district court's rulings should be readily upheld.

Appellant asks this Court to take an unprecedented view of both Sections 222 and 206 of the Communications Act. In so doing, Appellant incorrectly states that the district court "left Terpin (and other victims of unauthorized SIM swaps) without any recourse against telecommunication carriers violating customers' statutory rights." App. Br. At 10. In fact, parties impacted by unauthorized SIM swaps have a recourse if those swaps involve violations of Section 222, but only (a) where those statutory violations have actually occurred; and (b) insofar as the party impacted by the SIM swap has sustained damages that are a consequence of the carrier's violation. As AT&T correctly explains in its brief, neither circumstance is present here.

A. No Information Protected By Section 222 Was Disclosed In The Unauthorized SIM Swap.

The district court properly determined that there was no evidence demonstrating that the unauthorized SIM swap resulted in the disclosure of information protected by Section 222. 1 ER-15. As AT&T explains, Appellant and EPIC *amici* offer a shifting conception of what information was disclosed and whether that information falls under subsections (a) or (c) of the statute. AT&T Br. at 19-26; see also *Amici* Br. at 19-24. Further, they base their theory of liability in part on an expansive reading of Section 222(a) that would swallow and render

superfluous carriers' clearly defined and carefully tailored obligation in Section 222(c). AT&T Br. at 22-24; see also EPIC Br. at 21-22.

AT&T is correct, however, that this Court need not reach questions regarding the interaction between Sections 222(a) and 222(c) or the type of information covered by each subsection, because there is no proof in the record that any information covered by *any* part of Section 222 was disclosed, no matter how broadly the statute is interpreted. As AT&T explains, the only information that was "disclosed" as a result of the SIM swap was the content of post-swap text messages sent in response to the criminals' requests initiated through edge services. These messages were never intended for Appellant, and thus are neither customer proprietary network information ("CPNI"), 47 U.S.C. § 222(c), nor proprietary information ("PI"), *id.* § 222(a). AT&T Br. at 19-20.

Indeed, the content of post-swap text messages could not be covered by Section 222. SMS services are an "information service" and not a "telecommunications service" under federal law. *Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, Declaratory Ruling, FCC 18-178, 33 FCC Rcd 12075, ¶ 2 (2018). Both Sections 222(a) and 222(c) apply exclusively to "telecommunications carriers," 47 U.S.C. § 222(a), (c), also referred to under the Communications Act as "common carriers," *id.* § 153(11), (51). The definition of CPNI, similarly, is expressly limited to certain specific information

related to customers' use of telecommunications services. *Id.* § 222(h)(1).[6] Common carrier services under the Communications Act stand in contrast to "information services," *id.* § 153(24), which are subject to less regulation than common carrier services and are not subject to Section 222. Because the FCC has clarified that mobile messaging services, including SMS and Multimedia Messaging Service ("MMS") are information services, these services simply are not covered by Section 222.

Further, it does not matter that AT&T is a telecommunications carrier or that it has other obligations under Section 222. The Ninth Circuit has emphasized that whether an entity is a "common carrier" is an activity-based classification, not a status-based classification. *FTC v. AT&T Mobility*, 883 F.3d 848 (9th Cir. 2018). AT&T acts as an information service provider, not a common carrier, with respect to its provision of SMS service—even where a customer receives common carrier services from AT&T at the same phone number. *See, e.g.*, *id*. at 860; *Telesaurus VPC, LLC v. Power*, 623 F.3d 998, 1005 (9th Cir. 2010) ("Whether an entity in a

[6] As set forth in Section 222(h)(1), CPNI is limited to "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information."

given case is to be considered a common carrier or a private carrier turns on the particular practice under surveillance.") (quoting *S.W. Bell Tel. Co. v. FCC*, 19 F.3d 1475, 1481 (D.C. Cir. 1994). Accordingly, even if text messages intended for a criminal who stole a subscriber's phone number could be considered the type of "information" contemplated by Section 222, a wireless provider's "disclosure" of such messages still falls outside the statute.

As AT&T addresses in its brief, AT&T Br. at 24-25, Appellant offers a 'half-hearted' argument," correctly rejected by the district court for lack of any evidence, that the criminals accessed other information such as Appellant's SIM number or the IMEI number of his phone—information that, as AT&T correctly explains, is not CPNI in any event. AT&T Br. at 25-26 (quoting district court decision at 1-ER-20).

EPIC *amici* go even further, suggesting that any unauthorized SIM swap *must* result in a Section 222 violation because the SIM swap process should involve user authentication questions which necessarily will involve proprietary information. EPIC Br. at 21-22. That supposition—which is based on conjecture, and which may or may not be true in the ordinary course of SIM swaps, where carriers take care to mask sensitive information—would impose a strict liability standard that results in a violation of Section 222 anytime there is some unauthorized account activity, whether or not it includes actual access to the information defined as CPNI. This is inconsistent with FCC precedent, which requires only that carriers act reasonably in

protecting information covered by Section 222. *See In Re Verizon Communications*, Notice of Apparent Liability for Forfeiture and Admonishment, FCC 20-25, ¶¶ 7, 83 (Feb. 28, 2020). Indeed, even the EPIC brief concedes that the standard for protecting CPNI is "every *reasonable* precaution," and not strict liability. EPIC Br. at 22 (emphasis added). But the conjecture about the disclosure of information that may be involved in the authentication process is irrelevant here, where there is no evidence that any such information was accessed.

Finally, nothing in Section 222, which carefully prescribes certain information that carriers have a duty to protect, comes close to supporting EPIC *amici's* theory that any unauthorized SIM swap must, as a matter of law, involve a per se violation of the statute.[7] Indeed, in their comments to the FCC, NCLC and EPIC concede that Section 222 "does not explicitly authorize the Commission to hold carriers responsible for customer losses as we suggest." Comments of NCLC and EPIC at 5.

[7] Because of the strictly defined nature of CPNI, which encompasses things like which numbers were called and how long those calls lasted, CPNI is actually *not* generally used in the identity verification process (contrary to the claim by EPIC *amici*). Instead, these processes typically rely on other information, such as PIN codes and one-time-passwords, that do not fall within the statutory definition of CPNI.

B. Even If Information Protected By Section 222 Was Disclosed, AT&T Cannot Be Liable For Damages Under Section 206.

As AT&T correctly explains, the Appellant's various theories of liability all must fail because even if there were a disclosure of information protected by Section 222 in the course of the unauthorized SIM swap, that disclosure is not the proximate cause of Appellant's loss. AT&T Br. at 43-51.

Appellant and EPIC *amici* seek to impose a duty that is not only unlimited in terms of what information it protects, but also unfettered in terms of what damages can be sought. Appellant's loss resulted from a chain of actions involving one criminal bribing another, unauthorized access to Gmail, unauthorized access to Microsoft's servers, and the fortuitous discovery of a discarded file in the electronic trash.

AT&T is correct in establishing that common law causation principles apply to federal statutory claims, and in explaining why none of Appellant's theories can lead to this result. AT&T Br. at 43-51. The disclosure of allegedly protected information was not what caused Appellant's losses. The actual cause of loss here was far more complex, involving multiple different events that had to occur, including the Appellants ill-advised practice of putting his cryptocurrency credentials online, which rendered them vulnerable to theft after hackers penetrated his electronic accounts.

CTIA writes separately to emphasize a key issue involving Section 206—the source of a litigant's cause of action for alleged violations of Section 222—that the district court below had no reason to address: Whether this section applies at all.

Because the district court found that there was no disclosure of protected information here, the court did not need to grapple with the limits of Section 206 and whether Appellant had established an available cause of action under the Communications Act. Had the district court confronted this question, Plaintiffs' theory of liability would have faced an insuperable problem: like Section 222, Section 206 applies only to actions taken by common carriers, and the relevant activity at issue in this case—the transmission of SMS messages—is not a common carrier service.

CONCLUSION

In light of the foregoing, and for the reasons set forth in AT&T's brief, the Court should affirm the orders under appeal.

Dated: October 2, 2023

Respectfully submitted,

CTIA – THE WIRELESS ASSOCIATION
By Counsel

/s/ Joshua S. Turner

Joshua S. Turner
Counsel of Record
Sara M. Baxenberg
William Turner
WILEY REIN LLP
2050 M St. NW
Washington, DC 20036
Tel: (202) 719-7000
jturner@wiley.law
sbaxenberg@wiley.law
wturner@wiley.law

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing Brief of CTIA – The Wireless Association as *Amicus Curiae* in support of Defendant-Appellee complies with the typeface requirements of Fed. R. App. P. 32(a)(5)(A) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface in 14-point Times New Roman font.

I further certify that the foregoing brief does not exceed the length limitations specified in Fed. R. App. P. 29(a)(5) and Circuit Rule 32-1(a), because the brief contains 6,589 words according to the count of Microsoft Word, excluding the portions of the brief exempted by Fed. R. App. P. 32(f).

Dated: October 2, 2023

/s/ Joshua S. Turner
Joshua S. Turner

CERTIFICATE OF SERVICE

I hereby certify that on October 2, 2023, I filed the foregoing Brief of CTIA – The Wireless Association as *Amicus Curiae* in support of Defendant-Appellee with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit using the appellate CM/ECF system. All participants in this case who are registered CM/ECF users will be served a true and correct copy of this Motion through that system.

Dated: October 2, 2023

/s/ Joshua S. Turner
Joshua S. Turner