**No. 23-55375**

**IN THE UNITED STATES COURT OF APPEALS**
**FOR THE NINTH CIRCUIT**

---

MICHAEL TERPIN,
*Plaintiff-Appellant*,

v.

AT&T MOBILITY, LLC, ET AL.,
*Defendant-Appellee.*

---

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

---

# BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AND NATIONAL CONSUMERS LEAGUE AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

---

Megan Iorio
Christopher Frascella
Tom McBrien
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

*Attorneys for* Amici Curiae

August 2, 2023

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amici curiae* the Electronic Privacy Information Center and National Consumers League state that they have no parent corporation and that no publicly held corporation owns 10% or more of its stock.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### Cases



### Statutes



### Other Authorities

**Regulations**

## INTEREST OF THE *AMICI CURIAE*

EPIC is a public interest research center in Washington, D.C. that focuses on emerging privacy and technology issues.[1] EPIC has expertise in cybersecurity, FCC authorities protecting privacy, and SIM swapping. EPIC filed the petition that gave rise to the FCC's 2007 CPNI Order, *see, in re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information,* CC Docket No. 96-115; Report & Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 ¶11 (rel. Apr. 2, 2007), and recently urged the agency to do more to protect consumers from SIM swapping through their Section 222 and CPNI Rules authorities, *see, in re Protecting Consumers from SIM Swapping and Port-Out Fraud,* Comments of EPIC and NCLC, WC Docket No. 21-341 (Nov. 15, 2021). EPIC regularly participates as *amicus* and in rulemakings to protect consumers from deficient data security practices. *See, e.g.,* Brief for EPIC et al. as *Amicus Curiae* Supporting Plaintiffs-Appellants, *In Re: Marriott International, Inc. Consumer Data Security Breach Litigation*, No. 22-1744(L) (4th Cir. filed Nov. 22, 2022); *Disrupting Data*

---

[1] In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. Both parties consent to the filing of this *amicus* brief.

*Abuse*, EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security (Nov. 21, 2022); EPIC, *Data Security*.[2]

Founded in 1899, the National Consumers League (NCL) is America's pioneering consumer and worker advocacy organization. As one of America's leading anti-fraud organizations, evidenced by programs like its flagship Fraud.org campaign, NCL's interest in this case is to protect the ability of consumers to secure redress when, through no fault of their own, their sensitive personal information is compromised by companies they do business with. Given the importance of SMS and device-based authentication methods in multi-factor authentication systems, it is critical that telecommunications carriers be held accountable when their information security lapses lead to such authentication systems being compromised.

[2] https://epic.org/issues/cybersecurity/data-security/.

## SUMMARY OF THE ARGUMENT

This panel will be the first in the country to decide whether wireless carriers can be held liable for SIM swap attacks. These attacks affect thousands every year and resulted in over $70 million in reported losses in 2022 alone. If upheld, the District Court's decision would eliminate any incentive for carriers to prevent SIM swapping or to mitigate the damage from an attack. That result would leave most of us vulnerable to have our finances wiped out and our personal information exposed.

SIM swapping occurs when a wireless carrier employee transfers a phone subscriber's cell phone service to a device that the employee or another bad actor controls, typically with the intent to steal money from the subscriber. SIM swap attacks are a fast-growing type of fraud that threaten cell phone users with potentially devastating financial losses. As carrier technology and employees are necessary to effectuate a SIM swap, carriers are in the best position to stop these attacks. But without the threat of legal liability, carriers have little incentive to prevent SIM swapping. Carriers do not suffer losses from the scams—only consumers do. And because all carriers have similar disclaimers about their obligations, consumers do not have a meaningful marketplace choice to switch to a carrier who will provide better protections against these losses. Carriers must be

incentivized to prevent SIM swapping attacks, and the only way to do that is through imposing legal liability when they fail.

There are requirements in place that impose responsibilities on carriers to safeguard customer data and prevent security breaches. The District Court failed to recognize that Congress and the FCC have imposed duties on carriers to safeguard the very data that is compromised in a SIM swap attack. Letting carriers off the hook, as the District Court did, because they insert boilerplate "no guarantees" of cybersecurity clauses in their contracts undermines existing statutory and regulatory duties on carriers and ensures that SIM swapping will continue.

## ARGUMENT

### I. SIM SWAPPING IS A GROWING NATIONWIDE PROBLEM THAT ONLY CARRIERS CAN STOP.

A SIM swap attack occurs when a fraudster successfully obtains access to the phone call and text message services of another consumer; from there, the fraudster can impersonate their victim to access various accounts and perpetrate further crimes, such as stealing the money in the victim's bank account. *See, e.g.*, *In re Protecting Consumers from SIM Swap and Port-Out Fraud,* Notice of Proposed Rulemaking, WC Docket No. 21-341 ¶ 1 (Rel. Sept. 30, 2021) [hereinafter "FCC SIM Swap NPRM"]. SIM swapping is a growing threat that consumers are largely unaware of and are ill-equipped to protect themselves

against. Telecom carriers on the other hand are the very lever by which the fraudster takes control of the consumer's account. A fraudster needs to trick (or, as in the instant case, bribe) an employee or agent of the subscriber's telecom carrier into assigning the victim's number to a SIM card in the bad actor's control, which transfers the intended victim's phone service over to the fraudster. See FCC SIM Swap NPRM at ¶ 2. Customers occasionally have a legitimate need to transfer service to a different SIM card, but carriers are obligated to employ reasonable measures to ensure requests are not fraudulent, for example by requiring the purported subscriber to answer authentication questions before permitting the employee to view account information and effectuate the swap. *See, e.g.*, *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information,* CC Docket No. 96-115; Report & Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 ¶ 13-16, 20-21, 23, 33-36 (rel. April 2., 2007) [hereinafter "2007 CPNI Order"].

Carriers are in control of the entire process to effectuate a SIM swap, from the technical and procedural infrastructure that enables SIM swaps, to the hiring, training, and oversight of the employees or agents who are needed to perpetrate the fraud. The carriers know that these attacks are frequently occurring and they have the necessary expertise and control to stop them. *See* Kevin Lee, et al. Center for

Information Technology Policy, Princeton University, An Empirical Study of Wireless Carrier Authentication for SIM Swaps at 67, 71, Sixteenth Symposium on Usable Privacy and Security (August 2020) [hereinafter "CITP Study"]. But they need the incentive to do so. Because carriers do not themselves suffer losses from SIM swapping, the only incentive carriers have to prevent SIM swapping comes from the legal consequences imposed on them from failing to prevent the fraud.

**A. SIM swapping is a rising threat.**

SIM swapping is a pervasive and growing issue. And the targets are not just millionaires in cryptocurrency—ordinary Americans are having their life savings wiped out through SIM swap attacks.

In just a few years, SIM swapping has become one of the most menacing cybersecurity threats to consumers in the United States. In the three-year period from January 2018 to December 2020, the FBI's Internet Crime Complaint Center (IC3) received 320 complaints related to SIM swapping, totaling $12 million in losses. *See* FBI, Public Service Announcement, Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public, I-020822-PSA (Feb. 8, 2022). By 2021, the FBI was receiving 1,611 SIM swapping complaints in a single year, totaling more than $68 million in losses. *See id.* In 2022, complaints were up to 2,026, totaling $72.6 million in losses. *See* FBI Internet Crime Report 2022 at 24. By comparison, in 2022 the FBI reported 2,385 complaints related to

ransomware, *see id.* at 23, totaling $34 million in losses, *see id.* at 24, less than half the losses reported for SIM swaps.

Even these staggering numbers may be an underreporting of the problem. As Sen. Ron Wyden observed in a letter expressing concern about SIM swapping, "consumer complaints usually only reflect a small fraction of the number of incidents." Letter from Sen. Ron Wyden et al. to FCC Chair Ajit Pai (Jan. 9, 2020) [hereinafter "Wyden et al. Letter"]. SIM swapping is so prevalent that a law enforcement official with the California cybercrime task force REACT said that it is "probably REACT's highest priority at the moment, given that SIM swapping is actively happening to someone probably even as we speak right now." Busting SIM Swapper and SIM Swap Myths, KrebsonSecurity (Nov. 7, 2018) [hereinafter "Busting SIM Swapper"].

SIM swapping victims come from a variety of backgrounds and suffer "significant distress, inconvenience, and financial harm as a result of SIM swapping." FCC SIM Swap NPRM at ¶ 3. As law enforcement officials with REACT have emphasized:

> [SIM swapping] is not just stealing millions from millionaires…. Most of the victims are not in that category. Most are people who are having their life's savings or their child's college savings stolen. They're victims who have families and 9–5 jobs, and who got into the crypto space because they were investing and trying to make ends meet. We only tend to hear or read about these attacks when they result in millions of dollars in losses. But the reality is there's a lot of

> other thefts involving much more diminished amounts that are really negatively impacting peoples' lives.

*See* Busting SIM Swapper. There have been numerous news stories highlighting consumers losing most of their life savings of $50,000-$90,000 to SIM swap attacks. *See, e.g.*, Alina Machado, Woman Loses Life Savings in SIM Swap Scam, NBC6 South Florida (Aug. 26, 2022); Michael Finney and Randall Yip, *7 Bay Area Citibank Customers Say $600k Combined Drained from Accounts by Online Scammers*, ABC7 (Aug. 31, 2022).[3] Even the FTC's then-Chief Technologist at one point was targeted. *See* Dan Goodin, *FTC's Chief Technologist Gets Her Mobile Phone Number Hijacked by ID Thief*, Ars Technica (June 7, 2016).

The threat of SIM swapping continues to rise, and successive breaches of telecom carrier data will exacerbate this issue. Data breaches expose consumer information that make it easier to pull off SIM swap attacks. *See* FCC SIM Swap NPRM at ¶ 3. Telecom carriers have allowed perennial data breaches of subscriber data, with increasing frequency. *See id.* at ¶ 22 n 66 (noting current safeguards are not sufficient); *In re Data Breach Reporting Requirements*, Notice of Proposed Rulemaking, WC Docket No. 22-21 at ¶ 1 (Jan. 6, 2023) (noting increasing number

---

[3] https://www.nbcmiami.com/responds/woman-loses-life-savings-in-sim-swap-scam/2845044/; https://abc7news.com/citibank-fraud-login-bank-account-hack-unauthorized-transfers/12178298/.

of telecom data breaches). Equipped with breached subscriber information, fraudsters can more effectively impersonate consumers and bypass authentication measures, thereby facilitating a SIM swap attack which enables access to further sensitive consumer information.

### B. SIM swapping is largely unavoidable by consumers due to the carrier's role in the scam and due to widespread use of SMS-based two-factor authentication.

Not only is SIM swapping a rising threat, but it is difficult for consumers to avoid due to the role of the telecom carrier in effectuating the scam and the prevalence of SMS-based authentication. Congress, regulators, and federal and local law enforcement agree on these points.

Multi-factor authentication (MFA) is a cybersecurity protocol that requires more than just a username and password to log in. *See* More than a Password, CISA[4]; Wyden et al. Letter at 1. A common form of MFA is text-message (or SMS-based) authentication in which a person trying to sign into their account receives a numerical code by text that they must input to access their account. This extra authentication step is meant to protect against the possibility that the user's username and password were breached and a fraudster is attempting to log in to the

[4] https://www.cisa.gov/MFA.

account. Unless the fraudster also has access to the rightful user's phone, the fraudster will not be able to satisfy this second factor and will not be able to access the user's account.

Part of what makes SIM swapping so dangerous to consumers and effective for fraudsters is that it subverts this otherwise protective authentication protocol, making it easier, instead of harder, for wrongful users to obtain access to sensitive information and accounts. The SMS message that was supposed to go to the rightful account holder to authenticate their identity instead goes directly to the fraudster who is now able to successfully satisfy the MFA requirements. *See* Busting SIM Swapper.

There is very little consumers can do to prevent SIM swapping, as the people and technology needed to effectuate a SIM swap are entirely within the carrier's control. *See* FCC SIM swap NPRM at ¶¶ 5, 7; CITP Study at 61-62 (reporting insecure authentication mechanisms of five major carriers that allow fraudsters to effectuate a SIM swap without any authentication, or to access subscriber account information before providing the carrier's employee with authentication of their identity). As a matter of practical reality, the carrier is generally the only one who can prevent a SIM swap from occurring, with a few obscure exceptions likely unknown to most consumers such as utilizing a second app for authentication or setting up a separate PIN for account changes—most

consumer advice pertains to mitigating damage or avoiding being targeted rather than blocking the attack. *See, e.g.*, FBI, Public Service Announcement, Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public, I-020822-PSA (Feb. 8, 2022); Alvaro Puig, SIM Swap Scams: How to Protect Yourself, FTC Consumer Alert (Oct. 23, 2019); Nathanael Andrews, "*Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers for Sim-Swap Attacks and Wireless Provider Liability*, 16 Nw. J. Tech. & Intell. Prop. 79, 90–91 (2018) (citing to Jeremy Feigelson & Camille Calman, *Liability for the Costs of Phishing and Information Theft*, 13 J. Internet L. 1, 19-20 (2010)).

Subscribers do not have the option of moving to a meaningfully more protective provider, as evidenced by the fact that SIM swap cases have been brought against each of the major carriers, *see, e.g.*, *Ayeni v. Bank of America N.A. et al.*, No. 2023-cv-00618 (removed to D. Nm. on July 24, 2023) (suing Verizon for failing to prevent SIM swap attack); *Bayani v. T-Mobile*, No. 2023-cv-0027 (W.D. Wa. filed Feb. 27, 2023). The prolonged nature of phone service contracts also makes switching carriers difficult.

SIM swapping is a pervasive and growing threat, which consumers cannot reasonably avoid because the technique succeeds or fails based on the carrier's conduct not, the consumer's, and subverts the industry-standard SMS-based account authentication.

### C. Telecom carriers are both the least cost avoiders and the most competent avoiders in preventing SIM swap attacks.

Carriers are in the best position to prevent SIM swapping. Carriers are in control of the people and technology needed to perform a SIM swap, which makes them the most competent avoiders. Reasonable data security measures are also effective and inexpensive, which makes carriers the least cost avoiders.

Telecom carriers are the most capable and best-positioned avoider of cybersecurity risk, especially in the context of SIM swapping. Without the wireless providers' assistance, SIM-swap victims are largely powerless to avoid the harm of SIM-swap attacks. *See, e.g.*, Andrews at 105. The White House's National Cybersecurity Strategy recommends shifting the burden for cybersecurity away from individuals and onto "organizations most capable and best-positioned to reduce risks for all of us." Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023). Telecom carriers are best-equipped to understand the vulnerabilities of their own networks and to control the actions of their employees, and are able to be the most responsive. *See, e.g.*, Andrews at 93. SIM swapping cannot happen without the carrier's complicity (e.g. through compromised employees). REACT officials agree that a "fire needs to be lit" under carriers to address this problem. *See* Busting SIM Swapper. Because it is practically impossible for consumers to protect themselves from SIM swapping but

it is entirely within the carrier's power to prevent SIM swapping attempts, the onus must be on the carrier to prevent SIM swap attacks.

In addition to being the only party with the capability to avoid these attacks, the telecom carrier is also in the best position to carry the expense and obligation to prevent the harm of SIM swapping, *see, e.g.*, *Avila v. Collins*, 820CV00295DOCADS, 2021 WL 3053312, at *4 (C.D. Cal. July 19, 2021) (citing *Nat'l Union Fire Ins. of Pittsburgh v. Riggs Nat'l. Bank of Washington D.C.*, 5 F.3d 554, 557 (D.C. Cir. 1993) (Silberman, J., concurring)). Although telecom carriers have an interest in spending less money on employee training and oversight and in maintaining a convenient process for transferring a subscriber's account to a new SIM card, implementing reasonable security measures is both effective and inexpensive. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable. *See* 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016); Kamala D. Harris, Attorney General, *California Data Breach Report* at 32 (2016); Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* at 3 (July 9, 2019) (estimating 95% of breaches could have been prevented). The FTC has often noted that reasonable security measures are a relatively low cost. *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23,

2022) [hereinafter "*CafePress*"]; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018). Independent studies have also found that carriers have improperly prioritized usability over security. CITP Study at 61. Costs of harm should be internalized to the least cost avoider. Requiring the carriers to bear the costs of the losses incurred because of their failures to implement available and affordable protections would incentivize carriers to invest in adequately preventative cybersecurity measures so as to avoid incurring the more expensive costs of their own cybersecurity failures.

In addition to being the most competent avoider and the least cost avoider, AT&T in particularly has had abundant notice that its subscribers have been vulnerable to SIM swap fraud. In 2015, the FCC issued a Consent Decree against AT&T about employees being bribed to expose CPNI and other sensitive customer information. *See In re AT&T Services, Inc.*, EB-TCD-14-0016243 at ¶ 1 (Apr. 8, 2015) [hereinafter "Consent Decree"]. The Consent Decree's obligations included protecting CPNI and personal information from unauthorized access, use, or disclosure by employees. Despite that Consent Decree, AT&T did nothing to prevent an employee known to have engaged in SIM swapping from continuing to do so. *See, e.g.*, Pl.'s Statement of Genuine Disputes of Material Facts (and Conclusions of Law), 4- ER-582 ¶ 86; *id.* at 4-ER-591 ¶ 93.

## II. TELECOM CARRIERS CANNOT CONTRACT AWAY THEIR CYBERSECURITY DUTIES.

The law does not allow telecoms to effectively disclaim all liability for any cybersecurity deficiencies. The Federal Communications Act (FCA), along with the FCC's implementing rules, impose duties on carriers to protect the very data compromised in SIM swap attacks. Allowing carriers to disclaim liability through broad, boilerplate contract provisions would deny consumers statutory and regulatory protections granted by Congress and would contradict relevant agency authorities and public policy.

### A. AT&T violated its statutory duties under 47 U.S.C. §§ 222 and 201(b) to protect consumers from SIM swapping.

Under the Federal Communications Act, telecom carriers have a "fundamental duty" to "to take every reasonable precaution" to protect multiple types of consumer information. *See, e.g.*, FCC SIM Swap NPRM at ¶ 15; 2007 CPNI Order at ¶ 64. 47 U.S.C. § 222 governs each carrier's duty to protect the confidentiality of customer proprietary network information (CPNI) and of customers' "proprietary information," a broader category of consumer data than CPNI. 47 U.S.C. § 201(b) prohibits carriers from employing unjust and unreasonable practices; this includes deficient data security practices. When a carrier's employee or agent effectuates a SIM swap, the carrier violates these duties. AT&T has repeatedly violated the duties Congress and the FCC imposed on

all carriers in failing to prevent SIM swap attacks alleged in the case of Michael Terpin and others. *See, e.g.*, *Shapiro v. AT&T Mobility, LLC*, No. 2019-cv-08972 (C.D. Cal. filed Oct. 17, 2019); *Weiss v. AT&T Mobility, LLC*, No. 2023-cv-00120 (M.D. Fl. filed Jan. 23, 2023).

**1. Carriers are required by Section 222 and FCC rules to protect information that relates to service information, as well as proprietary information, certain personally-identifiable information, and certain login information.**

Section 222 has three provisions that address the confidentiality of subscriber information relevant to the information breached during a SIM swap. Section 222(h) defines what CPNI is; Section 222(c) charges carriers with protecting CPNI from unauthorized access, disclosure, or use; and Section 222(a) charges carriers with protecting the confidentiality of proprietary information more generally.

Section 222(h) describes CPNI as any information that "relates to the quantity, technical configuration, type, destination and amount of use" of the relevant telecommunications service—not merely the actual quantity, technical configuration, etc., data itself. 47 U.S.C. § 222(h)(1)(A). The FCC has emphasized that CPNI includes but is not limited to personally identifiable information (PII) about phone subscribers derived from their relationship with their telecom carrier. *See* 2007 CPNI Order at ¶1 n.2. Because consumers have to provide CPNI to

telecom carriers for their phones to function, carriers are charged with protecting the data from unauthorized access, disclosure, or use. See 47 U.S.C. § 222(c)(1).

Section 222(a) protects the broader category of "proprietary information," which is not statutorily defined. 47 U.S.C. § 222(a). However, the FCC has construed "proprietary information" as any subscriber information that "should not be exposed widely to the public, whether that information is sensitive for economic or personal privacy reasons." *See In re Cox Communications, Inc.*, 30 FCC Rcd. 12302, 12307 ¶ 4 (Nov. 5, 2015) [hereinafter "2015 Cox Order"]. The obligation to protect this information is also established through other enforcement actions. *See, e.g., In re TerraCom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175 (Oct. 24, 2014) [hereinafter "2014 NALs"]; *In re Quadrant Holdings LLC, Q Link Wireless LLC, and Hello Mobile LLC*, 202232170008, 2022 WL 3339390, at *7 n 25 (F.C.C. Aug. 5, 2022). The Commission has also specifically construed section 222(a) as protecting types of information that could permit access to a subscriber's financial account or other online account, such as combinations of account usernames and passwords. *See*

2015 Cox Order at 12306-07.[5] This is the type of information that AT&T failed to protect in this case when its deficient cybersecurity practices resulted in the fraudster getting access to subscriber accounts.

**2. Section 201(b) requires carriers to implement reasonable cybersecurity measures.**

Section 201(b) prohibits carriers from employing unjust or unreasonable practices, which includes deficient data security practices. The FCC has stated that: "carriers are now on notice that in the future we fully intend to assess forfeitures for [Section 201(b) data security and consumer notification] violations." 2014 NALs at ¶ 53. The FCC has also investigated whether a carrier engaged in unjust and unreasonable practices by failing to employ reasonable data security practices to protect proprietary information and CPNI, *see* 2015 Cox Order at 12309 ¶ 11, signaling that deficient cybersecurity in safeguarding either data type is a violation of Section 201(b).

Additionally, the FCC's Section 201(b) authority is parallel to the FTC's authority under Section 5 of the FTC Act, which authorizes the FTC to bring enforcement actions against companies that perform unfair or deceptive acts or

---

[5] Section I ¶ 2(s) (defining "Personal Information")). NB "personal information" is likely a clerical error, as 47 U.S.C. § 222(a) refers to "proprietary information", as does the rest of the FCC's 2015 Cox Order.

practices (UDAP). *See, e.g.*, *FCC-FTC Consumer Protection Memorandum of Understanding* 1-2 (Nov. 16, 2015).[6] The FTC can use its UDAP authority to police deficient data security practices in companies under its jurisdiction. *See, e.g.*, *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). The FCC's authority under Section 201(b) likewise applies to deficient telecom carrier data security practices to the extent they are unjust or unreasonable.

In sum, the FCC has established that carriers have a duty under sections 222(h) and 222(c) to protect certain types of information relating to phone service; a duty under Section 222(a) to protect personal information derived as a result of the carrier-customer relationship, certain types of information that permit access to other accounts, and sensitive subscriber information; and a duty under Section 201(b) to employ sufficient cybersecurity practices.

### 3. A successful SIM swap indicates a carrier has violated Sections 222 and 201(b).

When a carrier employs negligent cybersecurity practices that enable a fraudulent SIM swap, it violates its duties under Section 222 and Section 201(b). On the most fundamental level, because a SIM swap gives someone who is not authorized by the subscriber control over their account, it presumptively entails a

---

[6] https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf.

violation of the FCC's CPNI Rules, Section 222, and Section 201(b). On a technical level, the process of changing a SIM card requires access to and/or use of CPNI. More generally, manifestly deficient cybersecurity practices are violations of Section 222 as well as unjust and unreasonable practices under Section 201(b).

A carrier who fails to institute effective measures to prevent a SIM swap attack has violated the FCC's CPNI rules as well as Section 222. *See* 2007 CPNI Order at ¶ 35 (citing to § 222(c); 47 C.F.R. § 64.2009). The District Court found that the only CPNI that Terpin proved AT&T disclosed was his phone number, *see* Order Granting Def.'s Mot. for Summ.J. and Den. Ex Parte Appl., 1-ER-19-20, however other CPNI is inherently disclosed, accessed, or used during or as a direct result of a SIM swap attack. When the carrier transfers service from the subscriber's device to the fraudster's, any calls or SMS-based communications including alerts, authentication messages, and personal text messages then go to the fraudster rather than to the subscriber. The mere existence of these personal communications to the subscriber (let alone their contents) are CPNI as they reveal information that "relates to the quantity, technical configuration, type, destination and amount of use" of the defrauded subscriber's telecommunications service. See § 222(h). However, the lack of any messages or calls also constitutes information relating to the quantity, type, and amount of use of a subscriber's telecommunications service. This means that even if no personal messages or calls

go to the fraudster, CPNI has still been accessed, disclosed, or used in violation of Section 222(h).

Additionally, the process of transferring service to another SIM card requires accessing the technical configuration information of both SIM cards, and may involve accessing, disclosing, or using information about both devices in which those cards are installed. This would reveal information related to the technical configuration of the defrauded subscriber's telecommunications service, thus exposing CPNI without authorization. See § 222(h).

To the extent that other sensitive subscriber information is compromised in a SIM swap attack, this is also a violation of Section 222(a)'s protections for non-CPNI proprietary information. The SIM swap process should involve user authentication questions and answers. *See, e.g.*, 2007 CPNI Order at ¶¶ 14, 21, 23, 35. If it does, a successful SIM swap necessitates unauthorized access, disclosure, or use of information protected by Section 222(a)'s confidentiality provisions and is therefore a Section 222 violation. Moreover, the FCC's 2015 Cox order emphasizes that Section 222(a) protects "any combination" [of name, account number, access code, password, etc.] that would permit access to a financial account, or specific authentication information that would permit access to an online account. *See* 2015 Cox Order at 12306-07. However, if the carrier's process does not involve authentication questions, the failure to implement such basic

cybersecurity safeguards is itself a violation of the carrier's duties under Sections 222 and 201(b).

Carriers are obligated to take "every reasonable precaution" to protect their customers' data in the specific context of SIM swapping and port-out fraud attacks, *see, e.g.*, 2007 CPNI Order at ¶ 64. This is a "fundamental duty", FCC SIM Swap NPRM at ¶ 15; Letter from FCC Chair Pai to Sen. Markey et al. (Feb. 14, 2020) at 2, which requires carriers to take affirmative measures beyond the explicit terms of the Commission's regulations. *See, e.g.*, 2007 CPNI Order at 6946, ¶ 35; FCC SIM swap NPRM at ¶ 66 (citing to 47 U.S.C. §§ 222(a), 201(b); 2014 NALs). The record shows that AT&T did not take "every reasonable precaution" to prevent the SIM swaps that defrauded Terpin and other subscribers. *See, e.g.*, Decl. of Michael Terpin in Supp. of Pl.'s Opp'n. to AT&T's Mot. for Summ.J., 4-ER-685 at ¶4.

The FCC has established that unauthorized CPNI disclosures are indicia of presumptively unreasonable data security practices. As a result, unauthorized access, disclosure, or use of CPNI means that the carrier presumptively did not take every reasonable precaution. *See, e.g.*, *In re AT&T Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, File No.: EB-TCD-18-00027704 (Feb.

28, 2020),[7] at ¶ 8 (citing to 2007 CPNI Order at 6959, ¶ 63); *id.* at ¶ 52 (treating unauthorized disclosure of CPNI as "prima facia evidence that a carrier has failed to protect the information") (citing to 2007 CPNI Order at 6959–60, ¶ 65).

On top of the above obligations, which apply to all carriers, AT&T was also subject to a Consent Decree for failing to prevent bribed employees from violating the confidentiality of subscriber data, indicating adequate knowledge of the risks as well as clear duties to prevent the risks. In 2015, the FCC subjected AT&T to a $25 million consent decree for failure to prevent unauthorized access to CPNI effectuated by bribed employees. *See* Consent Decree at ¶ 7-8 (Apr. 8, 2015). The Consent Decree/Order stipulated that AT&T would maintain an information security program "reasonably designed to protect CPNI and Personal Information from unauthorized access, use, or disclosure by Covered Employees and Covered Vendor Employees", *id.* at ¶ 18(b), and that AT&T "shall monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the Act, the CPNI Rules, and this Consent Decree."

[7] N.B. this NAL was not unique to AT&T, all (then-four, now three) major carriers received NALs for their failure to safeguard consumer information in this manner.

*Id.* at ¶ 18(c). The unauthorized access, use, or disclosure of CPNI such as Terpin's is a clear indication of an unreasonable data security practice and therefore a violation of AT&T's Consent Decree as well.

The District Court erred in defining CPNI so narrowly and in failing to hold that carriers presumptively violate their duties under Sections 222 and 201(b) when their employees effectuate a SIM swap attack. We infer that the District Court found that the fraudster obtained information about Terpin's Microsoft account independently of the SIM swap process, and that the District Court would hold that one-time password information used for SMS-based two-factor authentication in order to access email and/or financial accounts does not constitute CPNI (including PII) nor proprietary information. This cannot be so. AT&T gave the fraudsters the tools needed to commit their crimes; but for the carrier's unreasonable security protocols the fraudster would never have had access to the consumer's authentication information.

If these facts don't lead to liability, it is unclear under what circumstances a plaintiff could ever hold a carrier liable for violations of its statutory duties in the context of SIM swapping.

### B. Telecom carriers cannot evade their responsibilities through disclaimers in their contracts.

According to the District Court, contractual language like "no security measures are perfect" and a carrier "cannot guarantee that your Personal Information will never be disclosed in a manner inconsistent with this Policy," Order Granting Def.'s Mot. for Summ.J. and Den. Ex Parte Appl., 1-ER-16, absolve carriers of any liability for deficient cybersecurity practices that enable SIM swap attacks. This is contrary to public policy and inconsistent with other agency and judicial authorities. Boilerplate disclaimer provisions cannot rob people of their rights to reasonable cybersecurity measures, as this would eradicate Congressionally-mandated protections under Sections 222 and 201(b).

It is contrary to public policy to enforce contracts that equate to a waiver of a statutory right, see *Brooklyn Sav. Bank v. O'Neil*, 324 U.S. 697, 704–06 (1945) (holding that private right granted in public interest to effectuate legislative policy cannot be waived unless Congress intended waiver). Holding that consumers can waive the protections that carriers are statutorily required to provide would encourage violations of the statutes in question, see *Brooklyn Sav. Bank* at 709–10, which here would include 47 U.S.C. Sections 222 and 201, see subsection II.A *infra*. It would also be contrary to public policy to permit boilerplate contract

provisions to shift the burden for adequate security protocols from the least cost avoider to each individual consumer, see subsection I.C *supra*.

Because of the context in which telecom carriers like AT&T provide service to consumers, including their use of boilerplate contracts terms and their controlling role in setting and enforcing security protocols, AT&T's disclaimer aligns with characteristics that California courts have found render exculpatory contract provisions invalid. *See Tunkl v. Regents of U. of Cal.*, 383 P.2d 441, 444–46 (Cal. 1963) (internal citations omitted) (listing characteristics). Mobile service is a matter of practical necessity for many members of the public. *See Riley v. California*, 573 U.S. 373, 385 (2014) ("modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."). AT&T (a "seller" under *Tunkl*) offers no provision in its WCA by which its subscribers ("purchasers" under *Tunkl*) may pay additional reasonable fees and obtain protection against carrier negligence; it simply disclaims cybersecurity liability wholesale. Additionally, SIM swapping cannot occur but for the carelessness (or complicity) of a carrier's agents, placing the person or property of the subscriber under the control of the carrier, subject to the risk of carelessness by their agents.

At least one District Court within the Ninth Circuit has held that a User Agreement disclaimer saying no security measure is "100%" effective cannot de

facto relieve the provider of its responsibility to provide "reasonable" security. *See In re Adobe Sys., Inc. Priv. Litig.,* 66 F. Supp. 3d 1197, 1221 (N.D. Cal. 2014) (internal citations omitted) (finding dispute adequately alleged despite Adobe invoking cybersecurity disclaimer terms). Adobe represented in its agreement that it would provide "reasonable" security, then attempted to argue that there could be no actionable dispute about adequacy of security because its Agreement expressly provided that no security measure is 100% effective. *See id.* AT&T has stated that its customers must trust that AT&T will protect their information, "will follow not only the letter but the spirit of the law", and "always take responsibility," Terpin's Second Am. Compl., 6-ER-1103, beyond its own representations AT&T is subject to statutory and regulatory duties to protect subscriber information, see subsection II.A *infra*. But now, like Adobe, AT&T seeks to argue that it cannot be held liable for cybersecurity deficiencies because it has disclaimed them via contract. The Northern District of California denied this dubious escape hatch to Adobe; the Ninth Circuit should similarly not permit AT&T to evade its cybersecurity duties.

FTC enforcement actions also charge that disclaimers do not excuse unreasonable security practices. Expressly stating that cybersecurity is not 100% guaranteed to prevent unauthorized access to personal information does not discharge a company's duties to take reasonable measures to safeguard consumer

information. *See, e.g.*, Complaint, *In re Wyndham Worldwide Corp., et al.,* FTC File No. 12-1365-PHC-PGR at ¶ 21 (Aug. 9, 2012); *CafePress* at ¶ 8.

If the court gives exculpatory provisions for cyber incidents full effect in telecom carrier contracts, it will incentivize each carrier to disregard its obligations to protect its subscribers from cyber incidents except to the extent that those obligations directly and significantly impact the company's own bottom line. A consumer cannot simply take their business elsewhere, as evidenced by cases brought against each of the major carriers. *See, S*ection I.B *supra*. The court should not take away the only effective incentive for consumers to compel carriers to prevent this harm.

The Ninth Circuit should prohibit data security-related liability exemptions like those in AT&T's WCA from applying in the SIM swapping context.

## CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to reverse the District Court's grant of summary judgment for AT&T.

**Date:** August 2, 2023

/s/ Megan Iorio
Megan Iorio
Christopher Frascella
Tom McBrien
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

*Attorneys for Amici Curiae*
*Electronic Privacy Information Center*
*& National Consumers League*

## CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

**This brief contains 6,072 words,** excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:

[ ] it is a joint brief submitted by separately represented parties;
[ ] a party or parties are filing a single brief in response to multiple briefs; or
[ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

**Signature:** */s/ Megan Iorio* **Date:** August 2, 2023

## CERTIFICATE OF SERVICE

I certify that on August 2, 2023, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

**Date:** August 2, 2023

/s/ Megan Iorio
Megan Iorio
Christopher Frascella
Tom McBrien
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

*Attorneys for Amici Curiae*
*Electronic Privacy Information Center*
*& National Consumers League*