Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM-Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

COMMENTS ON REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC)

Submitted January 16, 2024

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Rose Blackwell
Winter Clerk
Electronic Privacy Information Center
University of Virginia School of Law

Summary

In these comments, the Electronic Privacy Information Center (EPIC) applauds the Commission's Report and Order for setting forth rules that will strengthen protections for consumers against SIM swap and port-out fraud. EPIC also responds to the Commission's Further Notice of Proposed Rulemaking, urging the Commission to continue to develop regulations that will incentivize carriers to effectively reduce security vulnerabilities. We propose that the Commission:

1. Harmonize CPNI and CPI rules with SIM swap and port-out fraud authentication requirements;
2. Establish additional authentication requirements;
3. Require carriers to report incidents of fraud;
4. Articulate its enforcement power under Section 201(b) and Section 222 of the Communications Act of 1934 to eliminate loopholes which allow carriers to evade liability in litigation and to facilitate coordination with other enforcement efforts; and
5. Not delay the effective date of its order.

Table of Contents

Comments

I. Introduction

The **Electronic Privacy Information Center (EPIC)** files these comments to applaud the Federal Communications Commission ("Commission" or "FCC") for its response to vulnerabilities leading to SIM swap and port-out fraud, to support the agency's new rules and proposals,[1] and to urge additional measures. EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has long defended the rights of consumers and has played a leading role in developing the Commission's authority to address emerging privacy and cybersecurity issues.[3] EPIC routinely advocates for greater protections for consumers from exploitative or negligent data practices before the Commission,[4] before other regulators,[5] and as amicus curiae before the courts.[6]

---

[1] *In re* Protecting Consumers from SIM Swap and Port-Out Fraud, WC Dkt. No. 21-341 (Rel. Nov. 16, 2023), https://www.fcc.gov/document/fcc-adopts-rules-protect-consumers-cell-phone-accounts-0 [hereinafter "Report and Order"]. The Final Rule was published in the Federal Register at 88 Fed. Reg. 85,794 (Dec. 8, 2023) and is available at https://www.federalregister.gov/documents/2023/12/08/2023-26338/protecting-consumers-from-sim-swap-and-port-out-fraud. The Further Notice of Proposed Rulemaking was published at 88 Fed. Reg. 86,614 (Dec. 14, 2023) and is available at https://www.federalregister.gov/documents/2023/12/14/2023-26701/protecting-consumers-from-sim-swap-and-port-out-fraud.

[2] Electronic Privacy Information Center, https://epic.org/.

[3] *See In re* Implementation of the Telecommunications Act of 1996: Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, EPIC Petition, CC Docket No. 96-115 (Oct. 25, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513325075.

[4] *See, e.g.*, *In re* Empowering Consumers Through Broadband Transparency, Comments of CDT, EPIC, and Ranking Digital Rights, CG Docket No. 22-2 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/102161424008021; *In re* Location-Based Routing for Wireless 911 Calls, Comments of EPIC, PS Docket No. 18-64 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009; *In re* Rates for Interstate Inmate Calling Services, Letter Comment of EPIC, WC Docket No. 12-375 (Dec. 15, 2022) https://www.fcc.gov/ecfs/search/search-filings/filing/121545964412.

[5] *See, e.g.*, Comments of EPIC, *In re Global Tel*Link Corporation*, FTC File No. 212-3012 (Dec. 21, 2023), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-global-tellink/.

[6] *See, e.g.*, Br. of Amici Curiae Electronic Privacy Information Center and National Consumers League, No. 23-55375 (9th Cir. Aug. 2, 2023), https://epic.org/documents/michael-terpin-v-att-mobility-llc/; Br. of Amici Curiae Electronic Frontier Foundation and Electronic Privacy Information Center, No. 22-1744(L) (4th Cir. Nov. 22, 2022), https://epic.org/documents/peter-maldini-v-marriott-international-inc/.

We support the Commission's proposal to harmonize CPNI rules with authentication and data access requirements put forth in the Rule and Order and urge the Commission to expand these requirements to all customer proprietary information. We also urge the Commission to (1) mandate stronger authentication measures, (2) regulate carrier responses to SIM swap and port-out fraud, (3) articulate explicitly that successful SIM swap fraud indicates a carrier's violation of Sections 201(b) and 222 of the Communications Act of 1934, and (4) facilitate various litigation and enforcement efforts to more effectively incentivize carriers to shore up deficient cybersecurity and employee oversight practices.

II. Additional Regulation is Necessary to Effectively Prevent Fraud.

The Commission is implementing significant changes to protect consumers from SIM swapping fraud.[7] Nevertheless, SIM swap fraud is likely to continue: the Federal Bureau of Investigation reported a total of more than $72 million in losses from SIM swapping fraud in 2022,[8] up from just $12 million across a three-year period between 2018 and 2020.[9]

In the past year, the Department of Justice brought multiple criminal actions against major fraudsters such as Amir Golshan, who caused $740,000 in losses through multiple SIM swap schemes from 2019 to 2023.[10] Four Florida men were convicted of conspiracy to commit wire fraud in 2023 after stealing over $509,475 in cryptocurrency by SIM swapping victims'

[7] Report and Order at Appendix A.
[8] *See* FBI, Internet Crime Report 2022 at 24, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. By comparison, this is less than half the losses reported by the FBI due to ransomware over that same time period. *See id.*
[9] 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), https://www.ic3.gov/Media/Y2022/PSA220208. By 2021, the FBI was receiving 1,611 SIM swapping complaints in a single year, totaling more than $68 million in losses. *See id*.
[10] *See* Press Release, United States Dep't of Justice, 'SIM Swapper' Sentenced to Eight Years in Prison for Campaign of Fraud and Deception, Including Hacking into Instagram Accounts (Nov. 27, 2023), *available at* https://www.justice.gov/usao-cdca/pr/sim-swapper-sentenced-eight-years-prison-campaign-fraud-and-deception-including.

phone numbers.[11] Additionally, an Arizona man was found guilty of stealing nearly $1 million in cryptocurrency after gaining access to the victim's cryptocurrency accounts through a SIM swap attack.[12]

Victims of SIM swap fraud regularly lose their life savings from otherwise safe and insured bank accounts. Cryptocurrency investors like those described above make up a smaller proportion of victims than average customers with several hundred dollars in their bank accounts, making this an urgent issue for all consumers. A Colorado man lost $24,500 when money was transferred out of his Wells Fargo bank account through a SIM swap attack, which the local police department said was likely initiated by an international criminal.[13] A Florida woman lost her life savings of over $68,000 when it was transferred out of her Citibank account during a SIM swap attack.[14] California's Regional Enforcement Allied Computer Team (REACT) emphasized that most victims are "people who are having their life's savings or their child's college savings stolen," rather than the cryptocurrency investors that more frequently make the news.[15] After-the-fact criminal prosecutions are not enough. Just as car thefts enabled by security vulnerabilities are better cured through patching the vulnerability than through one-

[11] *See* Press Release, United States Dep't of Justice, Four Men Sentenced to Federal Prison for SIM-Swapping Scheme Based In Orlando (Dec. 13, 2023), *available at* https://www.justice.gov/usao-mdfl/pr/four-men-sentenced-federal-prison-sim-swapping-scheme-based-orlando.
[12] *See* Press Release, United States Dep't of Justice, Hacker Sentenced to 30 Months for SIM Swapping Conspiracy Resulting in Theft of Nearly $1 Million in Cryptocurrency (Oct. 27, 2023), *available at* https://www.justice.gov/usao-az/pr/hacker-sentenced-30-months-sim-swapping-conspiracy-resulting-theft-nearly-1-million.
[13] *See* Jeremy Jojola, Hacker Steals Man's $24,500 in savings using 'SIM swapper' attack (Mar. 2, 2023), https://www.9news.com/article/news/crime/hacker-sim-card-swap-scam/73-c7f0d7a1-5c90-46f6-b316-7eb2814fe485.
[14] *See* Alina Machado, Woman Loses Life Savings in SIM Swap Scam (Aug. 26, 2022), https://www.nbcmiami.com/responds/woman-loses-life-savings-in-sim-swap-scam/2845044/.
[15] *See* Busting SIM Swapper and SIM Swap Myths, KrebsonSecurity (Nov. 7, 2018) [hereinafter "Busting SIM Swapper"].

off criminal enforcement,[16] so too is SIM swapping better prevented by tightening carrier security measures rather than relying on individual criminal cases to act as a deterrent.

SIM swap fraud is an especially concerning crime because, in addition to its impact across financial demographics, there are few mitigation tactics consumers can undertake on their own. Even where consumers have alternatives to SMS-based authentication,[17] they may be unaware of these options.[18] SIM swapping is so pernicious in part because it subverts what is intended to be a security mechanism, turning it into an attack vector. Additionally, SIM swaps are typically facilitated by a complicit employee or an employee duped by a criminal actor impersonating a customer.[19] Attackers can also discover information used to facilitate SIM Swap fraud through data breaches, which have affected most major carriers including T-Mobile, Verizon, and AT&T.[20] Hundreds of customer complaints to the FCC and the Federal Trade Commission (FTC) each year show that despite victims' best efforts, SIM swaps are generally successful because provider employees do not know how to address SIM swap fraud, providers refuse to provide documentation of attacks, and provider employees are often involved in the fraud themselves.[21]

---

[16] *See, e.g.*, Press Release, Attorney General Tong Announces Investigation into Hyundai and Kia Over Theft-Prone Vehicles (June 20, 2023), *available at* https://portal.ct.gov/AG/Press-Releases/2023-Press-Releases/AG-Tong-Announces-Investigation-into-Hyundai-and-Kia-Over-Theft-Prone-Vehicles.

[17] However, SMS-based 2FA may be the only option. *See, e.g.*, "Zeddie-", 2FA SMS – PSA, r/Visible, posted "9 mo. ago", https://www.reddit.com/r/Visible/comments/133r9ex/2fa_sms_psa/ (last visited Jan. 16, 2024).

[18] *See, e.g.*, Consumer Reports, 2023 Consumer Cyber Readiness Report 5 (Sept. 2023), https://innovation.consumerreports.org/wp-content/uploads/2023/09/2023-Consumer-Cyber-Readiness-Report.pdf (82% of consumers use SMS-based 2FA, as compared with 50% who use an MFA app); National Cybersecurity Alliance, STUDY: More than One-Third of Tech Users Fell Victim to Phishing Despite Access to Training Geared Towards Identifying Attacks (Sept. 29, 2022), https://staysafeonline.org/news-press/press-release/press-release-oh-behave-2022 (43% of respondents said they had never heard of MFA).

[19] *See* Busting SIM Swapper.

[20] *See, e.g.*, *In re* Data Breach Reporting Requirements, Report and Order, WC Docket No. 22-21 (Rel. Dec. 21, 2023) at ¶ 3 n. 5, *available at* https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf [hereinafter "Data Breach Report and Order"].

[21] Report and Order at ¶ 8.

Measures taken by carriers to prevent SIM swapping fraud are demonstrably inadequate. Fraud persists and grows year after year, while carriers continuously fail to detect obviously fraudulent behavior. For example, AT&T failed to detect more than two dozen unauthorized swaps in one month by a single employee and failed to detect one dozen unauthorized swaps in one month by a different employee.[22] It also failed to detect the difference in location between the hacker attempting to swap service and the phone from which service would be transferred away,[23] and additionally failed to act when the hacker attempted to move 40 different wireless accounts to the same IMEI number.[24] In two separate cases, AT&T failed to take action to prevent SIM swapping fraud even after receiving personal contact from the targeted subscriber.[25]

The Commission must take action to protect consumers and compel carriers to take measures to stop SIM swap and port-out fraud.

III. The Commission Should Harmonize CPNI and CPI Rules with SIM Swap Rules.

The Report and Order increased authentication requirements for SIM changes and port-outs as well as for CPNI disclosure in the limited context of inbound customer communications.[26] We support the Commission's order limiting employee access[27] and its proposal to require notification of failed authentication attempts.[28] However, we urge that limits to employee access should be supplemented by strict liability for providers when a breach is facilitated by an employee even in the absence of inbound customer communication. SIM swap fraud is often perpetrated by carrier employees or fraudsters using compromised employee

[22] *See* Fifth Am. Compl. at ¶ 162, *Seth Shapiro v. AT&T Mobility, LLC*, No. 2:19-08972-CBM-RAO (C.D. Cal. Jan. 20, 2023).
[23] *See id.* at ¶ 175(a).
[24] *See id.* at ¶ 199.
[25] *See id.* at ¶ 108; *See* Second Am. Compl. at ¶ 88-89, *Michael Terpin v. AT&T Inc et al.*, No. 2:18-06975-ODW-KS (C.D. Cal. Mar. 16, 2020).
[26] *See* Report and Order at ¶ 50.
[27] *See id.*
[28] *See id.* at ¶ 105.

accounts to access CPNI and then conduct a SIM swap.[29] Additionally, the prevalence of SIM swapping itself indicates a need for stronger authentication standards for CPNI. Once a SIM swapper takes control of a victim's phone number, the victim's CPNI is vulnerable because customers can be authenticated for CPNI access through calls to the account holder's number.[30]

Prompt notification to impacted consumers of their increased risk of cyber-attack or identity theft must be a cornerstone of 21st century consumer protection practices.[31] As we explained in our comments in the Data Breach Reporting Rules docket:

> While it is unfair to place the burden on consumers when providers fail in their charge as custodians of consumer data, the current [dismal] data security reality is such that the best interim solution is to equip consumers to protect themselves from the downstream impacts of data breaches such as identity theft and account compromise.[32]

Even with effective SIM swap preventative measures, strong privacy and data protection rules will still be necessary to protect consumers. The Commission recognizes that criminal actors may continue to conduct SIM swap and port-out fraud even with effective regulation.[33] Though safeguards to prevent SIM swap fraud are important tools to mitigate consumer harm, criminal actors' ability to adapt means that consumer data may still be left vulnerable. Therefore, the

[29] *See, e.g.*, *Ross v. AT&T Mobility, LLC*, No. 19-CV-06669-JST, 2020 WL 9848766 (N.D. Cal. May 14, 2020) (where an employee accessed the victim's CPNI and then conducted a SIM swap using the accessed information); Cyber Safety Review Board, Review of the Attacks Associated with Lapsus$ and Related Threat Groups 7 (July 24, 2023), https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf [hereinafter CSRB Report].
[30] Fed. Commc'ns Comm'n, Report and Order and Further Notice of Proposed Rulemaking, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Information, FCC 07-22 ¶ 18 (Apr. 2, 2007), https://docs.fcc.gov/public/attachments/FCC-07-22A1.pdf [hereinafter "2007 CPNI Order"].
[31] Report and Order at ¶¶ 105, 107.
[32] Reply Comments of Electronic Privacy Information Center, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, *In re* Data Breach Reporting Requirements, WC 22-21 at 19 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814 [hereinafter "EPIC et al. Data Breach Reply Comments"]; *id.* at 24 n.83 (citing to PwC, Are we ready for the Fourth Industrial Revolution?, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/fourth-industrial-revolution.html (last visited Jan. 16, 2024) (64% of consumers want assurance of immediate notification if personal data is compromised)).
[33] Report and Order at ¶¶ 21, 26, 27.

Commission should incentivize carriers to strengthen privacy and data protections for consumer information as a means of mitigating harm from successful SIM swapping attempts as well.

The Commission should expand its authentication requirements and increased protections to customer proprietary information (CPI) such as social security numbers and financial records.[34] Though these types of information do not reveal a customer's use of communication services, they are still "derived from a customer's relationship with a provider," making them protected CPI under Section 222.[35] Additionally, pursuant to Section 201(b) of the Communications Act, the Commission should find that any unauthorized exposure of personally identifying information is unjust or unreasonable.[36] The FCC has found these types of information protectable in several enforcement actions,[37] as well as in its recent update to its data breach notification rules.[38] Expanding new authentication requirements and consumer protections to non-CPNI will protect consumers from fraudulent activity connected to exploitable customer information by making it harder for criminal actors to obtain non-CPNI and use it for further financial and identity crime. As the proposed regulations represent measures to improve cybersecurity for telecom carriers, for the same reasons articulated in the Data Breach

[34] Report and Order at ¶ 102 ("Should the Commission apply any harmonized rules to all customer proprietary information?").
[35] 2007 CPNI Order at ¶ 1 n.2; *see also* Data Breach Report and Order at ¶¶ 16, 118-126 (citing to Section 201(b) and Section 222 as authorizing the Commission to adopt breach notification rules designed to safeguard sensitive personal information a carrier has received from the customer or relating to the customer, in connection with its customer relationship, for example social security number).
[36] 47 U.S.C. § 201(b). As the Commission notes this would be consistent with the FTC's corresponding enforcement authority for inadequate data security measures under section 5 of the FTC Act. *See* Report and Order at ¶ 126. *See also* EPIC et al. Data Breach Reply Comments at 9-11.
[37] *See In re* Cox Communications, Inc. 30 FCC Rcd. 12302, 12307 ¶ 4 (Nov. 5, 2015) (defining "proprietary information" as any information "that should not be exposed widely to the public, whether that information is sensitive for economic or personal privacy reasons"); *In re* Terracom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.EB-TCD-13-00009175 (Oct. 2014) (proposing a fine for companies holding customer's financial information, public benefit statements, and identifying information on insecure servers); *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) (fining companies for making customer's identifying information available without a password).
[38] Data Breach Report and Order at ¶¶ 16, 118-126.

Reporting Requirements docket, we agree with the Commission that the Congressional Review Act would not apply here.[39]

The Commission's proposal to harmonize requirements for CPI and SIM changes will reduce gaps in CPNI security and better secure customer information. Additionally, the FCC has already deemed it an effective fraud mitigation technique to only allow employee access to CPNI for SIM changes after customer authentication.[40] Establishing the same standards for access to CPNI and CPI more broadly will be effective in limiting multiple types of fraud.

We also respond to CTIA's ex parte that addresses location information and proprietary information.[41] CTIA takes issue with the Commission citing to NALs as a source of authority for "location information" being considered CPNI;[42] regardless of what merits if any this argument may have, the inclusion of location information was established by Congress in the Wireless Communications and Public Safety Act of 1999, not by the Commission itself.[43] Regarding proprietary information,[44] the Commission's questions about harmonization in this docket are consistent with its recent rule in docket 22-21[45] and should be met with gratitude by industry representatives, who so often clamor for regulatory harmonization rather than disparate rules.[46]

[39] Report and Order at ¶ 103; *see also* Data Breach Report and Order at ¶ 140 (citing to EPIC et al. Data Breach Reply Comments at 12).
[40] Report and Order at ¶ 50.
[41] Ex Parte, CTIA (Nov. 8, 2023), available at https://www.fcc.gov/ecfs/search/search-filings/filing/1109425224347 [hereinafter "CTIA Ex Parte"].
[42] *See id.* at 13.
[43] Originally Section 222(h)(1) was labelled as Section 222(f)(1). *See* Telecommunications Act of 1996, PL 104-104 (Feb. 8, 1996). Section 222(f)(1) was re-assigned to Section 222(h)(1) and "location" was added to the list of CPNI in 1999. *See* Wireless Communications and Public Safety Act of 1999, PL 106-81 (Oct. 26, 1999).
[44] CTIA Ex Parte at 11-12.
[45] Data Breach Report and Order at ¶ 5.
[46] *See, e.g.*, Comments of T-Mobile, *In re* Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, IB Dkt. No. 23-119 at 23 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831234137677; Comments of Verizon at 22 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108312266504640; Comments of CTIA at 49 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108311863500689; Reply Comments of CTIA at 6 (Oct. 2, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10022428126256.

IV. The Commission Should Establish Additional Authentication Requirements for SIM Changes.

The Commission made significant changes to the authentication requirements for SIM swaps and port-outs, limiting information carriers can use to authenticate customers and restricting employee access to CPNI.[47] These rules will limit many methods of initiating SIM swap fraud. To substantially eliminate instances of SIM swap fraud, however, the Commission should eliminate password and SMS-based authentication, require a flexible 24-hour waiting period for SIM changes, and continuously update authentication requirements based on carrier reports. The Commission states that its regulations represent "baseline rules, rather than prescriptive requirements" and require providers to consistently monitor and improve authentication policies but do not mandate specific authentication methods.[48] This is consistent with a 2020 letter from then-Chair Pai addressing the Commission's 2007 rules, describing them as requiring affirmative measures beyond the explicit terms of the Commission's regulations.[49] Despite the FCC's past efforts, incidents of SIM swapping continue to grow without stronger required authentication practices.[50]

---

[47] Report and Order at Appendix A.

[48] *Id.* at ¶¶ 20, 52.

[49] 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", Report and Order at ¶ 52 n. 208; Letter from FCC Chair Pai to Sen. Markey et al. at 2 (Feb. 14, 2020), *available at* https://docs.fcc.gov/public/attachments/DOC-362599A2.pdf, 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; *In re* Protecting Consumers from SIM Swap and Port-Out Fraud, Notice of Proposed Rulemaking, WC Docket No. 21-341 at ¶ 22 n. 66 (Rel. Sept. 30, 2021), *available at* https://docs.fcc.gov/public/attachments/FCC-21-102A1.pdf (citing to 47 U.S.C. §§ 222(a), 201(b); *TerraCom, Inc., and YourTel America, Inc*., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014)).

[50] Blockchain infrastructure provider Skip Protocol published a detailed summary of a December 17, 2023 SIM swap attack targeting the company's cofounder. *See* Skip Protocol, *Skip Incident Report: Sim Swap—December 17, 2023* (Dec. 26, 2023), https://medium.com/@skip_protocol/skip-incident-report-sim-swap-december-17-2023-f5686ba49efe. A December 21, 2023 SIM swap attack targeted the founder of Rug Radio, a media platform and NFT distributor, and a December 22 SIM swap attack targeted Jae Chung, founding partner of Manifold Trading. *See* Tom Mitchelhill, *SIM Swappers Hit Manifold trading, Rug Radio Founders Ahead of Holidays* (Dec. 22, 2023), https://cointelegraph.com/news/sim-swap-hack-manifold-trading-rug-radio-founders-crypto-exploits.

The lack of adequate authentication protections coupled with the increase in data breaches is a recipe for a continued increase in SIM swaps, despite criminal enforcement against the fraudsters themselves. Stolen credentials are an increasingly popular method of attack used by threat actors, as noted in Verizon's 2023 Data Breach Investigations Report.[51] The Cyber Safety Review Board (CSRB) has outlined how traditional methods of authentication, absent heightened protections, can be vulnerable to social engineering.[52] As a result, large numbers of customers are exposed to increased risk of SIM swapping in the aftermath of a data breach.[53] We additionally note that if adoption of credit freezes is any indicator, providing even a no-cost method for freezing SIM swap and port-out requests is unlikely to reach most consumers. In a December 2021 survey, fewer than one-third of respondents had frozen their credit at one time for any reason and only three percent of consumers froze their credit after receiving a data breach notice. [54]

Carrier policies permitting rapid SIM changes are a major factor enabling SIM swap fraud because attackers are able to gain access to information and accounts within minutes of an attack, and when a carrier can resolve the issue, the victim has already suffered substantial losses.[55] The Commission declined to mandate a 24-hour waiting period for SIM changes after a

[51] Use of stolen credential is more prevalent than any other threat actor method, including ransomware. *See* Verizon, Data Breach Investigations Report at fig. 14 (2023), https://www.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/. Notably, the same report notes that the percentage of social engineering attacks facilitated by pretexting have increased almost every year since 2016. *See id.* at fig. 5, *available at* https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/.
[52] *See* CSRB Report at 6-7.
[53] *See, e.g.*, *Fraser v. Mint Mobile, LLC*, No. C 22-00138 WHA, 2022 WL 1240864 (N.D. Cal. Apr. 27, 2022) (finding that a SIM swapper stole $466,000 worth of cryptocurrency after a customer's information was exposed in a data breach and used to conduct a SIM swap).
[54] *See* Identity Theft Resource Center, New Identity Theft Resource Center Research Shows Consumers Know About Credit Freezes, But Rarely Use Them (Dec. 15, 2021), *available at* https://www.idtheftcenter.org/post/new-identity-theft-resource-center-research-shows-consumers-know-about-credit-freezes-but-rarely-use-them/.
[55] Report and Order at ¶ 70 n. 266.

SIM change request[56]—contrary to the CSRB's recommendation[57]—because the FCC found such a delay to be overly burdensome and opted instead for instant SIM swap procedures in favor of expediency for legitimate customers. However, this incentivizes illegitimate SIM swaps as attackers are often able to cause instantaneous damage once they have access.[58] To limit the speed of attacks, the Commission should enforce a 24-hour waiting period within which a customer is notified through email of an attempted SIM change and given the opportunity to approve or reject the change. Offering customers an opportunity to approve a SIM swap may mean that the swap can happen immediately upon approval, easing the process for legitimate customers while barring attackers from conducting fraudulent SIM swaps without the victim's knowledge. The Commission should update authentication requirements for SIM changes to eliminate PIN and password-based authentication[59] (especially where there has been a data breach) and eliminate SMS-based authentication.[60]

In addition to strengthening authentication regulation, the Commission should compare carrier reports to customer report records to ensure that carriers are submitting accurate information about SIM swap attacks and other breaches and should bring timely, meaningful enforcement actions against carriers who are not meeting reporting requirements.[61] As outlined in the sections below, and as the CSRB recommends, the Commission should do more than merely establish a reporting and oversight mechanism: it should use enforcement actions for

[56] Report and Order at ¶ 34.
[57] *See* CSRB Report at 35.
[58] Report and Order at ¶ 34.
[59] *See, e.g.*, CSRB Report at 8.
[60] *See* CSRB Report at 48 ("NIST, CISA, and Okta are among those organizations that consider SMS/voice MFA the weakest form of MFA").
[61] Current reporting measures seem woefully inadequate. *See, e.g.*, Cynthia Brumfield, The FCC's data breach reporting requirements are broken, Metacurity (June 9, 2023), *available at* https://metacurity.substack.com/p/the-fccs-data-breach-reporting-requirements.

failures to prevent SIM swap fraud to incentivize providers to improve their security practices.[62] However, a reporting mechanism will also be an important tool in updating regulations to respond to threats, as updates will be informed by comprehensive data about the nature of SIM swap attacks over time.

V. Providers Should be Required to Take Additional Explicit Steps to Mitigate and Respond to SIM Swap Fraud.

Through its Report and Order, the Commission established carrier response mechanisms to combat SIM swapping. Carriers are now required to maintain information regarding SIM change requests and port-out requests, which must be retained for a minimum of 3 years.[63] Additionally, carriers must provide customers notice of account protection measures and develop processes for customers to report SIM swap and port-out fraud, which carriers must then investigate promptly and take steps to remedy.[64] The Commission explains that these are comprehensive solutions because customers will be able to quickly notify their carrier of fraud and receive documentation, which will be helpful in contacting financial institutions and credit reporting agencies.[65]

Recent cases, however, exemplify how carrier responses to SIM swap attacks may not be sufficient unless strictly regulated. In *Shapiro v. AT&T Mobility, LLC*, a customer alleged that his phone number was SIM swapped four separate times and that despite AT&T having SIM swap mechanisms in place, he suffered financial losses or had personal accounts breached each

[62] CSRB recommends that the Commission and FTC not merely require regular reporting and document and enforce best practices, but also "incentivize better security at telecommunications providers by enacting penalties for fraudulent SIM swaps or lax controls." CRSB Report at 36-37. We note that the fine for the most egregious violation of CPNI revealed to date is still yet to be collected, nearly four years later. *See* FCC Proposes Over $200M in Fines for Wireless Location Data Violations (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.
[63] Report and Order at ¶ 46.
[64] *Id*. at ¶ 18, 72.
[65] *Id*. at ¶ 75.

time.[66] In *Terpin v. AT&T Mobility, LLC*, a customer's phone number was SIM swapped after his provider changed his account's security level from "standard" to "extra" and added instructions that representatives should not validate the account without a new passcode.[67] These cases indicate that requiring providers to act without specific instructions or oversight will likely lead to continued SIM swap and port-out fraud, as providers' measures may not be sufficiently secure to stop subsequent fraud.

The White House's National Cybersecurity Strategy suggests the policy principle that the burden should shift to the most capable avoider of harm, explicitly calling for policies that: "[e]nsur[e] that the biggest, most capable, and best-positioned entities – in the public and private sectors – assume a greater share of the burden for mitigating cyber risk."[68] In the case of SIM swapping, this is clearly the carriers themselves. The carriers are also the least cost avoiders—and implementing reasonable security measures is both effective and inexpensive. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable.[69] The FTC has often noted that reasonable security measures are relatively low cost.[70] Carrier prioritization of usability over security[71] is part of what has allowed the problem

[66] No. 2:19-CV-8972-CBM-FFM, 2020 WL 4341778 (C.D. Cal. May 18, 2020).
[67] 399 F. Supp. 3d 1035 (C.D. Cal. 2019).
[68] Fact Sheet, The White House, Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan (July 13, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/.
[69] *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).
[70] *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).
[71] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, & Arvind Narayanan, Princeton Univ., An Empirical Study of Wireless Carrier Authentication for SIM Swaps, Proceedings of the Sixteenth Symposium on Usable Privacy and Security at 61 (Aug. 10-11, 2020), *available at* https://www.usenix.org/system/files/soups2020-lee.pdf [hereinafter Princeton Study].

to continue to worsen in recent years. REACT officials have agreed that a "fire needs to be lit" under carriers to address this problem.[72]

To ensure telecommunications providers are responding appropriately to fraud and customer concerns, the Commission must take further action to ensure that providers' measures are effective. The FCC requires providers to track and maintain data regarding SIM change and port-out requests.[73] It should also require providers to submit sets of aggregate data to the Commission specifically regarding fraudulent SIM swaps and port-out requests, how fraudulent requests were perpetrated, and how the provider responded to fraudulent activity. This would allow the Commission to monitor carrier policies in responding to fraud and analyze if responses are targeting the most significant issues at hand. This approach would also still allow for affirmative measures beyond the explicit terms of the Commission's regulations.

VI. The Commission Should Enforce Section 201(b) and Section 222 Against Carriers that Allow SIM Swap Fraud to Occur and Facilitate Other Accountability Measures.

The Commission should articulate that carriers who facilitate SIM swap fraud are in violation of Section 201(b) and Section 222 and use its enforcement power accordingly. Throughout the Report and Order, the FCC emphasizes that service providers are already legally obligated to protect consumers' confidential information under Section 222. The Commission explains that where the Report and Order offers "baseline requirements," carriers will likely need to go further at times to fulfill their Section 222 duty to protect CPNI.[74] But merely stating that there is a duty to protect CPNI on its own does not appear to sufficient to compel carriers to take all possible and necessary steps.

[72] *See* Busting SIM Swapper.
[73] Report and Order at ¶ 46.
[74] *Id*. at ¶ 13.

a. The Commission should facilitate private litigation as an incentive to carriers to correct deficient cybersecurity practices.

Despite increased private litigation between SIM swap fraud victims and common carriers, victims have largely been unable to recover damages for losses suffered as a result of carrier vulnerabilities leading to SIM swap fraud. In litigation, carriers argue that the data exposed in a SIM swap attack is not CPNI and therefore is not subject to the additional protections offered by Section 222.[75] For example, in *Bayani v. T-Mobile USA, Inc.*, T-Mobile argued that a SIM swap conducted through its network was not a violation of Section 222 because a criminal using a victim's phone line does not involve carrier disclosure of CPNI.[76]

Carriers have already argued, and at least one district court has agreed, that language in a carrier's Terms of Service such as "no security measures are perfect" and the carrier "cannot guarantee that your Personal Information will never be disclosed in a manner inconsistent with this Policy" absolves carriers of liability for deficient cybersecurity practices that enable SIM swap attacks.[77] The Commission should be explicit that such contract language carries no weight in cases of SIM swapping fraud. To give them weight would be contrary to public policy as well as be inconsistent with other agency authorities. Boilerplate disclaimer provisions cannot rob people of their rights to reasonable cybersecurity measures; to hold they do in SIM swapping cases would eradicate Congressionally mandated protections under Sections 222 and 201(b). Notably, FTC enforcement actions also charge that disclaimers do not excuse unreasonable security practices. As an example: expressly stating that cybersecurity is not 100% guaranteed to

[75] *See, e.g.*, Br. of Appellee AT&T Mobility LLC, *Michael Terpin v. AT&T Mobility LLC et al*, No. 23-55375 at 19-20 (9th Cir. Sept. 25, 2023); Answer to Am. Compl., *Seth Shapiro v. AT&T Mobility, LLC*, No. 2:19-08972-CBM-RAO, Doc. 161, at 49 (Feb. 13, 2023).
[76] No. 2:23-CV-00271-JHC, 2023 WL 6959287, 5 (W.D. Wash. Oct. 20, 2023).
[77] Order Granting Def.'s Mot. for Summ.J. and Den. Ex Parte Appl., *Michael Terpin v. AT&T Mobility, LLC et al.*, No: 2:18-06975-ODW-KS, Doc. 243, at 11 (Mar. 28, 2023).

prevent unauthorized access to personal information does not discharge a company's duties to take reasonable measures to safeguard consumer information.[78]

Additionally, carriers argue that they are not responsible for harms because of contractual terms or limited knowledge of fraud. In *Ross v. AT&T Mobility, LLC*, for example, AT&T argued that it was not liable for a SIM swap attack because the victim did not contract with AT&T in reliance on the company's misrepresentations or omissions and that the misrepresentations occurred after her decision to contract.[79] Carriers also argue they are not liable because they did not have the requisite level of knowledge to be responsible under the Computer Fraud and Abuse Act or Stored Communications Act.[80]

Carriers will be most effective in reducing this type of fraud when they are facing high financial incentives, which will push them to react to advancements in fraud and strengthen investigatory and compensation procedures. The Commission has a broad mandate under Section 222 to protect consumer privacy through regulating common carriers, and it has previously enforced privacy protections for broad-reaching harms beyond traditional CPNI breaches.[81] It has also found deficient cybersecurity practices to be unjust or unreasonable practices in violation of Section 201(b).[82] By articulating that SIM swap fraud implicates a carrier's violation

[78] *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.
[79] No. 19-CV-06669-JST, 2020 WL 9848766, 16 (N.D. Cal. May 14, 2020).
[80] *See, e.g.*, *Cheng v. T-Mobile USA, Inc.*, No. 22-CV-3996 (PKC), 2023 WL 6385989 (S.D.N.Y. Sept. 29, 2023) (holding that T-Mobile was not liable under the Computer Fraud and Abuse Act because it did not "knowingly" commit a violation by executing a fraudulent SIM swap); *Bayani v. T-Mobile USA, Inc.*, No. 2:23-CV-00271-JHC, 2023 WL 6959287 (W.D. Wash. Oct. 20, 2023) (holding that T-Mobile did not "knowingly divulge" the victim's information and therefore was not liable under the Stored Communications Act).
[81] *See In Re* Cox Commc'ns, Inc., *supra* note 37.
[82] For example, the Commission drew on its 201(b) authority in two 2015 privacy-related enforcement actions. *See in re* AT&T Services, Inc., 30 F.C.C. Rcd. 2808 at ¶ 2 (F.C.C. 2015) ("The failure to reasonably secure customers' personal information violates a carrier's duty under Section 222 of the Communications Act, and also constitutes an unjust and unreasonable practice in violation of Section 201 of the Act."); *id.* at ¶ 3 ("The Notice of Apparent Liability in *TerraCom* states that Section 201(b) applies to carriers' practices for protecting customers' PII and CPNI."); *In Re* Cox Commc'ns., Inc., 30 F.C.C. Rcd. 12302 (F.C.C. 2015) ("Privacy Laws" means Sections 47

of Sections 222 and 201(b), the Commission will compel carriers to take all possible actions to protect consumers to avoid enforcement action.

Articulating this mandate with respect to SIM swap fraud will also be an effective tool for victims seeking compensation through litigation, as it will empower them to bring suit for breach of carriers' obligations. The Commission should mandate that privacy policies and contracts unambiguously state (1) carriers' obligation to protect the privacy of all customer data beyond traditional CPNI and (2) carriers' knowledge of the harms that may result from improper data disclosures. This will prevent carriers from using contractual language and statements of limited knowledge to disclaim liability in suits.

The Commission could mitigate harm to consumers by mandating that cases cannot be arbitrated. As we noted in our comments in the initial NPRM in this docket,[83] arbitration clauses prevent individuals from seeking relief in the courts, instead requiring consumers to engage in secret, often expensive, and often unfair tribunals that do not comply with the rules of evidence or civil procedure established in the American judicial system. Results of arbitration proceedings are non-transparent, and non-appealable.[84] Unfortunately, many SIM swapping fraud cases have

---

U.S.C. §§ 201(b), 222, and 551, and 47 C.F.R §§ 64.2001-2011, insofar as they relate to the security, confidentiality, and integrity of PI and/or CPNI.)"). The Commission also invoked 201(b) in its 2014 NAL against TerraCom and YourTel. *See in re* TerraCom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1_Rcd.pdf.

[83] *See* Comments of National Consumer Law Center and Electronic Privacy Information Center at 7 n. 26 (Nov. 15, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/111608400758 (citing to Consumer Fin. Prot. Bureau, Arbitration Study, Report to Congress Pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act § 1028(a), at § 1.4.1 (Mar. 2015), *available at* http://files.consumerfinance.gov. The Consumer Financial Protection Bureau (CFPB)'s 2015 report on arbitration in consumer financial products provides some important data on the prevalence of arbitration clauses in certain industries. *See also* Elizabeth G. Thornburg, *Contracting with Tortfeasors: Mandatory Arbitration Clauses and Personal Injury Claims*, 67 Law & Contemp. Probs. 253, 271 (2004) ("[A]rbitration clauses that provide slanted processes or limited remedies undermine the efficiency goal of personal injury law. A powerful contracting party can impose inadequate arbitration systems on countless potential plaintiffs. By doing so, it can reduce the anticipated cost of its accidents significantly and thereby decrease the deterrent effect of tort law."). Arbitrators in most arbitration cases are not required to give a reasoned explanation of the result. *See* Paul D. Carrington & Paul H. Haagen, *Contract and Jurisdiction*, 1996 Sup. Ct. Rev. 331, 347–348. Arbitrators need not follow rules of evidence. *See* Davis v. Prudential Sec., 59 F.3d 1186, 1190 (11th Cir. 1995)).

[84] *See id.*

been relegated to arbitration.[85] Frequent, visible litigation could serve as an important tool to the Commission, allowing it to identify common vulnerabilities and methods of fraud through the facts of litigation. While the FCC has its own reporting system, discovery and other tools of private litigation could shine a light on important issues in SIM swapping as criminals develop their methods. In addition to data collection and reporting, open cases will lead to greater transparency into carriers' role in combatting SIM swap fraud.

b. The Commission should hold carriers strictly liable for SIM swap fraud conducted through their devices and networks.

Should the Commission decide to allow vulnerable authentication measures or limit employee authentication procedures to circumstances of direct interactions with customers, it should institute additional measures to safeguard against SIM swap fraud conducted through carrier devices and networks.[86] Holding the carrier strictly liable for such breaches is one method to incentivize better internal security practices, especially where an employee has been bribed to turn over protected consumer information. The Commission could also incentivize carriers to implement security measures to ensure that if carrier devices fall into the wrong hands, criminal actors are unable to access CPNI and other protected information.[87] Alternatively, similar to its recent data breach notification rule, the Commission could apply a rebuttable presumption of liability on the carrier's part where a SIM swap fraud was successful.[88]

[85] *See, e.g.*, Weiss v AT&T (MDFL 23-cv-00120); Saadeh v T-Mobile (D. N.J. 21-cv-12871); Armen Mard v T-Mobile (C.D. Cal. 21-cv-06904); Middleton v T-Mobile (EDNY 20-cv-03276).
[86] The Commission has received several ex parte requests to constrain customer authentication prior to employee access to CPNI to customer interactions. *See, e.g.*, CTIA, Notice of Ex Parte, WC Docket No. 21-341 (Rel. Nov. 9, 2023); Voice on the Net Coalition, Notice of Ex Parte, WC Docket No. 21-341 (Rel. Nov. 7, 2023).
[87] As some carriers may have already done. *See, e.g.*, Joseph Cox, How SIM Swapper Straight-Up T-Mobile Stores, 404 Media (Nov. 10, 2023 9:00 AM), https://www.404media.co/how-hackers-straight-up-steal-t-mobile-tablets-to-sim-swap/.
[88] *See* Data Breach Report and Order at ¶ 53.

c. The Commission should facilitate cooperation with other enforcement agencies.

The Commission could also coordinate with other government efforts to protect against SIM swap and port-out fraud. If the Commission is unable to enforce fraud prevention measures under Section 201(b) and Section 222, it could coordinate with the FTC to bring action against telecommunications companies as information service providers. The FTC litigates against common carriers when operating outside of their telecommunications service offerings.[89] By coordinating responses with the FTC, the Commission could pursue enforcement from all angles and ensure that common carriers are not able to avoid their responsibilities in court.[90]

Additionally, the Commission could coordinate with state cybersecurity efforts by working with state attorneys general on broad litigation targeting deceptive telecommunications practices. State attorneys general have authority to sue telecommunications providers for data breaches.[91] State attorneys general may be compelled to act in response to growing SIM swap fraud, especially considering that pre-paid telecommunications plans—more often used by low-income customers—may be more vulnerable to SIM swap attacks.[92] The Commission could provide resources and backing to encourage state attorneys general to bring suit.

---

[89] AT&T Mobility, LLC paid a $60 million settlement in litigation with the FTC regarding deceptive marketing practices. *See* FTC, AT&T to Pay &60 Million to Resolve FTC Allegations It Misled Consumers with 'Unlimited Data' Promises, *available at* https://www.ftc.gov/news-events/news/press-releases/2019/11/att-pay-60-million-resolve-ftc-allegations-it-misled-consumers-unlimited-data-promises.

[90] *See, e.g.*, Br. of Amicus Curiae CTIA, *Michael Terpin v. AT&T Mobility, LLC, et al.*, No. 23-55375 at 24-26 (9th Cir. Oct. 2, 2023) (arguing that because SMS services are an information service, they fall outside the scope of the protections of Section 222 of the Communications Act such that carriers cannot be held liable for post-swap text messages because they are not acting in their capacity as a common carrier when providing SMS service).

[91] A coalition of state Attorneys General reached a $2.43 million settlement with T-Mobile in response to a 2015 data breach. *See* Connecticut Joins Combined $16 Million Multistate Settlements Over 2012 and 2015 Experian Data Breaches, *available at* https://portal.ct.gov/AG/Press-Releases/2022-Press-Releases/Connecticut-Joins-Combined-$16-Million-Multistate-Settlements-Over-Experian-Data-Breaches. The New York Attorney General sued Avid Telecom in 2023 for illegal robocalls. *See* Attorney General James Sues Telecommunications Company Over Illegal Robocalls, *available at* https://ag.ny.gov/press-release/2023/attorney-general-james-sues-telecommunications-company-over-illegal-robocalls.

[92] Princeton Study at 68.

VII. The Commission Should Not Delay Implementation of the Report and Order.

The Commission received multiple requests for delayed implementation of the new standards put forth in the Report and Order.[93] EPIC urges the Commission to maintain its six-month implementation requirement. The FCC repeatedly acknowledges that many carriers claim to already have effective measures in place.[94] As SIM swap fraud continues to harm helpless consumers, it is vital that the Commission require carriers to prioritize taking action to protect their customers.

VIII. Conclusion

While the Report and Order made significant headway in securing customer data and preventing SIM swap and port-out fraud, the Commission must enhance its regulations and enforcement mechanisms to stop this form of fraud. The Commission should prioritize oversight and enforcement to ensure that common carriers are taking action to prevent their customers from falling victim to SIM swap and port-out fraud.

Respectfully submitted, this the 16th day of January 2024, by:

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Rose Blackwell
Winter Clerk
Electronic Privacy Information Center
University of Virginia School of Law

[93] *See, e.g.*, CTIA, Petition for Partial Reconsideration, WC Docket No. 21-341 (Rel. Jan. 9, 2024); Competitive Carriers Association, Ex Parte, WC Docket No. 21-341 (Rel. Nov. 13, 2023).
[94] *See* Report and Order ¶¶ 22, 52.