

Federal Communications Commission 45 L Street NE Washington, DC 20554

News Media Information 202-418-0500 Internet: <u>www.fcc.gov</u> TTY: 888-835-5322

DA 23-1148 Enforcement Advisory No. 2023-03 Released: December 11, 2023

# FCC ENFORCEMENT ADVISORY

## TELECOMMUNICATIONS CARRIERS MUST PROTECT CONSUMERS' PRIVACY AND SENSITIVE DATA BY TAKING REASONABLE STEPS TO PREVENT SIM FRAUD SCHEMES

# Threat Actors Increasingly Target Telecommunications Carriers and Consumers Through Fraudulent SIM Swapping

American consumers rely upon their mobile phones and the networks on which they operate in order to live, work, and play. These technologies are uniquely critical because of the ways in which they facilitate consumers' access to additional opportunities and services. Consumers frequently use their mobile phones, and rely on carriers, to authenticate their identities in order to access third-party accounts and platforms via multi-factor authentication—i.e., by requesting one-time passcodes ("OTPs") through Short Message Service ("SMS") and voice calls.<sup>1</sup> Unfortunately, threat actors are increasingly targeting this convenience by finding ways to intercept authentication texts and calls through fraudulent subscriber identity module ("SIM") swapping schemes. The Department of Homeland Security's Cyber Safety Review Board ("CSRB") issued a report outlining how threat actors compromised access to telecommunications providers' infrastructure to intercept these authentication passcodes to carry out data breaches in furtherance of ransom and extortion schemes.<sup>2</sup> Telecommunications service providers should familiarize themselves with the threats and vulnerabilities described in the CSRB report so as to fulfill their duties to protect their customers' sensitive information.

Section 222 of the Communications Act of 1934, as amended (the "Act"), confers upon "[e]very telecommunications carrier" a "duty to protect the confidentiality of proprietary information" of "customers." In particular, it limits the circumstances under which a carrier may "use, disclose, or permit access to" certain types of customer proprietary information, referred to as "customer

<sup>&</sup>lt;sup>1</sup> U.S. Dep't of Homeland Security, Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus\$ and Related Threat Groups*, 5 (July 24, 2023), <u>https://www.cisa.gov/sites/default/files/2023-</u>08/CSRB Lapsus%24 508c.pdf (*Cyber Safety Review Board Report*).

 $<sup>^{2}</sup>$  *Id.* at 5, 12-16 (describing how threat actors stole customer information, source code, and other sensitive information through SIM swap fraud and other attacks).

proprietary network information" ("CPNI").<sup>3</sup> The Federal Communications Commission, the agency tasked with implementing and enforcing section 222, does so as informed by its mission of "promoting safety of life and property."<sup>4</sup> To advance that mission, the Commission recently adopted updates to its rules to further protect consumers from threats of SIM fraud schemes.<sup>5</sup>

The FCC's Enforcement Bureau ("Bureau"), in coordination with the Privacy and Data Protection Task Force,<sup>6</sup> issues this Enforcement Advisory to advise consumers and telecommunications service providers of the increased threat of fraudulent SIM swapping. We also remind telecommunications carriers of their duties and obligations to protect customer information generally, and specifically in order to combat fraudulent SIM swapping schemes that harm consumers and the broader public safety.

A telecommunications carrier's failure to reasonably protect customer information, including through allowing fraudulent SIM swap schemes, can independently violate the Act and Commission rules.<sup>7</sup> These failures may result in monetary forfeiture, additional reporting obligations, and/or other administrative remedies.

### **Risks Associated with SIM Fraud**

Threat actors are increasingly engaging in SIM swap and port-out fraud (collectively, "SIM Fraud") schemes to gain control of consumers' mobile phone accounts and wreak havoc on people's financial and digital lives without ever needing to gain physical control of a device. This fraudulent activity primarily occurs through two means. In the first type of scheme, a threat actor convinces a victim's wireless provider to transfer the victim's mobile service and telephone number from the victim's cell phone to a cell phone in the threat actor's possession. This type of fraud is also known as "SIM swapping" because it involves an account being fraudulently transferred (or swapped) from a device associated with one SIM to a device associated with a different SIM.

In the second type of scheme, the threat actor, posing as the victim, opens an account with a wireless provider other than the victim's current provider. The threat actor then arranges for the

<sup>&</sup>lt;sup>3</sup> 47 U.S.C. § 222(a), (c). *See also id.* § 222(h)(1) (defining CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information."). CPNI includes, but is not limited to, the phone numbers called by a consumer; the frequency, duration, and timing of such calls; any services purchased by the consumer, such as call waiting; and location information related to the telecommunications service. In addition, for purposes of the CPNI rules (47 CFR § 64.2001, *et seq.*), the term "carrier" is defined to include interconnected VoIP providers. *See* 47 CFR § 64.2003(o).

<sup>&</sup>lt;sup>4</sup> 47 U.S.C. § 151.

<sup>&</sup>lt;sup>5</sup> See Protecting Consumers from SIM Swap and Port-Out Fraud, WC Docket No. 21-341, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-95 (WCB Nov. 16, 2023) (SIM Fraud Report and Order and FNPRM).

<sup>&</sup>lt;sup>6</sup> See Press Release, Fed. Commc'ns Comm'n, Chairwoman Rosenworcel Launches New 'Privacy and Data Protection Task Force,' (June 14, 2023), <u>https://docs.fcc.gov/public/attachments/DOC-394384A1.pdf</u>.

<sup>&</sup>lt;sup>7</sup> See 47 U.S.C. §§ 201(b), 222(a), (c), (h)(1); 47 CFR § 64.2010.

victim's phone number to be transferred (or "ported out") to the account with the new wireless provider controlled by the threat actor.

The CSRB report described above found that threat actors used various techniques, including emergency disclosure requests from telecommunications carriers, to obtain access to victims' CPNI and other personal information to facilitate these fraudulent schemes.<sup>8</sup>

Consumers use cell phone numbers to authenticate their identities across a variety of accounts, including with wireless providers, financial institutions, healthcare providers, and retail websites. SIM Fraud threatens consumers' privacy across these platforms by enabling threat actors to intercept authentication calls and texts. Once intercepted, the threat actors can take control of these accounts, which could result in illicit access to private health information, theft from financial accounts, or the sale or ransoming of information housed in social media accounts.<sup>9</sup> This fraudulent activity threatens public safety as well. These schemes may impact a consumer's ability to access important services, including emergency services, that are keyed to a consumer's mobile account or ability to make a call.<sup>10</sup>

SIM Fraud can have national security consequences as well. In at least one instance, threat actors targeted telecommunications service providers of U.S. government employees in an unsuccessful attempt to compromise mobile phone accounts associated with Federal Bureau of Investigation and Department of Defense personnel.<sup>11</sup> Illicit access to accounts held by U.S. government or military personnel may provide threat actors with sensitive personal information that could be used to target U.S. national security interests.<sup>12</sup>

## Telecommunications Carriers' Obligations to Protect Customer Privacy Helps Combat SIM Fraud Schemes

Telecommunications carriers have an obligation to protect the privacy and security of information about their customers to which they have access as a result of their unique position

<sup>&</sup>lt;sup>8</sup> Cyber Safety Review Board Report, supra note 1, at 7.

<sup>&</sup>lt;sup>9</sup> See, e.g., Press Release, U.S. Dep't of Justice, San Antonio Pair Plead Guilty to SIM Swap Scheme (Oct. 12, 2022), <u>https://www.justice.gov/usao-wdtx/pr/san-antonio-pair-plead-guilty-sim-swap-scheme</u>; Press Release, U.S. Dep't of Justice, California Resident Pleads Guilty for His Role in Sim Swap Scam Targeting at Least 40 People, Including New Orleans Resident (May 18, 2022), <u>https://www.justice.gov/usao-edla/pr/california-resident-pleads-guilty-his-role-sim-swap-scam-targeting-least-40-people</u>; Alina Machado, *Woman Loses Life Savings in SIM Swap Scam*, NBC MIAMI (Aug. 26, 2022), <u>https://www.nbcmiami.com/responds/woman-loses-life-savings-in-sim-swap-scam/2845044/;</u> Press Release, U.S. Dep't of Justice, Two Men Facing Federal Indictment in Maryland for Scheme to Steal Digital Currency and Social Media Accounts Through Phishing and "Sim-Swapping" (Oct. 28, 2020), <u>https://www.justice.gov/usao-md/pr/two-men-facing-federal-indictment-maryland-scheme-steal-digital-currency-and-social-media</u>; Press Release, U.S. Dep't of Justice, Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges, (May 9, 2019), <u>https://www.justice.gov/usao-edmi/pr/nine-individuals-connected-hacking-group-charged-online-identity-theft-and-other; Lorenzo Franceschi-Bicchierai, *Hacker Who Stole \$5 Million By SIM Swapping Gets 10 Years in Prison*, VICE (Feb. 1, 2019), <a href="https://www.vice.com/en/article/gyaqub/hacker-joel-ortiz-sim-swapping-10-years-in-prison">https://www.vice.com/en/article/gyaqub/hacker-joel-ortiz-sim-swapping-10-years-in-prison</a>.</u>

<sup>&</sup>lt;sup>10</sup> See e.g., SIM Fraud Report and Order and FNPRM, supra note 5, at para. 7.

<sup>&</sup>lt;sup>11</sup> Cyber Safety Review Board Report, supra note 1, at 8.

<sup>&</sup>lt;sup>12</sup> See id., e.g., at 8.

as network operators and as the gatekeeper to their customers' access to the network.<sup>13</sup> The Act specifically limits the manner and circumstances under which a carrier may disclose CPNI that it has received or obtained by virtue of its provision of a telecommunications service.<sup>14</sup> Together, these obligations require telecommunications carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, as well as properly authenticating customers prior to disclosing CPNI when a customer contacts a carrier via phone, online, or in a store.<sup>15</sup>

In order to protect customers from unauthorized account changes, carriers must notify customers immediately of certain account changes.<sup>16</sup> Notifications are required whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed.<sup>17</sup> These specific notification requirements are critical, but they are only part of the general obligation to protect customers' information, which must take into consideration the nature of the vulnerabilities and what is known about threat actors.<sup>18</sup>

Where a carrier fails to meet these legal obligations, the FCC Enforcement Bureau is charged with investigating and enforcing all violations of the Act, including violations of sections 201 and 222 of the Act, or the Commission's regulations adopted under the Act.

#### What's Next for Carriers and Consumers

To strengthen protections against SIM Fraud, the Commission adopted a *Report and Order and Further Notice of Proposed Rulemaking* that revises the Commission's CPNI and Local Number Portability (LNP) rules to protect against SIM swap and port-out fraud.<sup>19</sup> These new rules will require wireless providers to:

<sup>15</sup> See 47 CFR § 64.2010(a).

<sup>16</sup> See id. § 64.2010(f)

<sup>17</sup> Id.

<sup>19</sup> SIM Fraud Report and Order and FNPRM, supra note 5. The SIM Fraud Report and Order and FNPRM follows from a Notice of Proposed Rulemaking adopted by the Commission in September 2021. See Protecting Consumers (continued....)

<sup>&</sup>lt;sup>13</sup> 47 U.S.C. § 222(a). See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (2007 CPNI Order); Declaratory Ruling, 28 FCC Rcd 9609 (2013) (2013 Declaratory Ruling).

<sup>&</sup>lt;sup>14</sup> 47 U.S.C. § 222(c)(1). Subsequent to the adoption of section 222(c)(1), Congress added section 222(f). Section 222(f) provides that for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. *Id.* § 222(f). Section 222(d) delineates certain exceptions to the general principle of confidentiality, including permitting a carrier to use, disclose, or permit access to CPNI obtained from its customers to protect telecommunications services users "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

<sup>&</sup>lt;sup>18</sup> See 2007 CPNI Order, 22 FCC Rcd at 6959-6960, paras. 63-65; 2013 Declaratory Ruling, 28 FCC Rcd at 6910-11, 9619-6921, paras. 5-7, 29-34; see also, e.g., AT&T Inc., Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1763-64, para. 60 (2020) (stating that AT&T was on notice that its safeguards were inadequate after disclosure of a breach and finding it was unreasonable for AT&T to continue to rely on faulty safeguards after discovery of the incident).

- adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider;
- adopt processes for responding to failed authentication attempts;
- institute employee training for handling SIM swap and port-out fraud; and
- establish safeguards to prevent employees who receive inbound customer communications from accessing CPNI in the course of that interaction until after the customer has been authenticated.

The *Report and Order* also adopts rules that will enable customers to act to prevent and address fraudulent SIM changes and number ports, including requiring wireless providers to:

- notify customers regarding SIM change and port-out requests;
- offer customers the option to lock their accounts to block processing of SIM changes and number ports; and
- give advanced notice of available account protection mechanisms.

The *Report and Order* also establishes requirements to minimize the harms of SIM swap and port-out fraud when it occurs, including requiring wireless providers to:

- o maintain a clear process for customers to report fraud;
- o promptly investigate and remediate fraud; and
- promptly provide customers with documentation of fraud involving their accounts.

Finally, to ensure wireless providers track the effectiveness of authentication measures used for SIM change requests, the *Report and Order* requires that providers keep records of SIM change requests and the authentication measures they use.<sup>20</sup>

In addition to consumer benefits, strengthening SIM Fraud safeguards provides national security benefits and helps protect survivors of domestic violence. Such safeguards strengthen national security by ensuring that threat actors cannot fraudulently access government mobile accounts to use them for nefarious purposes. Further, improvements to the CPNI Rules related to SIM swapping can act as a shield for domestic violence survivors by preventing bad actors, such as abusers, from taking control of a survivor's phone or phone number. The proceeding to protect consumers from SIM swap and port-out fraud is part of the Commission's continuing commitment to protecting consumers, improving carrier privacy and data protections, and making sure those carriers meet their obligations – thus defending consumers and the nation.

### **Recent Enforcement Action Involving CPNI**

The Commission is aggressively investigating potential violations of section 222 of the Act and the CPNI rules. Service providers should track threat actor behavior in the market, as well as the Commission's enforcement actions for guidance that may be relevant to addressing SIM Fraud.

*from SIM Swap and Port-Out Fraud*, WC Docket No. 21-341, Notice of Proposed Rulemaking, 36 FCC Rcd 14120 (2021) (*SIM Fraud NPRM* or *NPRM*).

<sup>&</sup>lt;sup>20</sup> While the rule changes adopted in the *Report and Order* are not yet in effect, carriers should continue to meet their obligations under the existing requirements of the Act and the CPNI rules.

*Q Link and Hello Mobile*. In July 2023, the Commission proposed a \$20 million fine against Q Link Wireless LLC ("Q Link") and Hello Mobile Telecom LLC ("Hello Mobile" and with Q Link, the "Companies") for apparently failing to protect the privacy and security of subscribers' CPNI. The investigation revealed apparent violations of section 222 of the Act and three provisions of section 64.2010 of the Commission's rules. The Companies relied on readily available biographical information and account information to control online access to CPNI, which apparently violated the CPNI rules and placed customers' sensitive personal data at risk. The investigation also found that the companies apparently violated the Commission's rules by failing to employ reasonable data security standards, placing customers at increased risk for privacy violations and threat actors' potential misuse of their sensitive personal data. In addition, Q Link apparently violated the FCC rule that prohibits the use of readily available biographical information for back-up authentication and password reset purposes.

#### About the Task Force

The FCC's Privacy and Data Protection Task Force is an FCC staff working group created by Chairwoman Rosenworcel. The Task Force is led by the Chief of the Enforcement Bureau, Loyaan A. Egal, and coordinates across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors, including data breaches (such as those involving telecommunications providers) and vulnerabilities involving third-party vendors that service regulated communications providers.

Media inquiries should be directed to 202-418-0500 or MediaRelations@fcc.gov.

Issued by: Chief, Enforcement Bureau