October 25, 2023

FCC FACT SHEET*

Protecting Consumers from SIM Swap and Port-out Fraud

Report and Order and Further Notice of Proposed Rulemaking – WC Docket No. 21-341

Background: This *Report and Order*, if adopted, would address two fraudulent practices bad actors use to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone. In the first type of scam, known as "SIM swapping" a bad actor convinces a victim's wireless provider to transfer the victim's mobile service and number from the victim's cell phone to a cell phone in the bad actor's possession. This scam involves an account being fraudulently transferred (or swapped) from a device associated with one subscriber identity module (SIM) to a device associated with a different SIM. In the second type of scam, referred to as port-out fraud, the bad actor, posing as the victim, opens an account with a wireless provider other than the victim's current provider. The bad actor then arranges for the victim's phone number to be transferred (or "ported out") to the account with the new wireless provider controlled by the bad actor.

What the *Report and Order* Would Do:

- Set baseline requirements that establish a uniform framework across the mobile wireless industry, giving wireless providers the flexibility to deliver the most advanced and appropriate fraud protection measures available while not impinging on customers' ability to upgrade and replace their devices or choose their preferred wireless provider.
- Revise the Commission's Customer Proprietary Network Information (CPNI) and Local Number Portability (LNP) rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider, and require that providers keep records of SIM change requests and the authentication measures they use.
- Adopt additional rules that reinforce that requirement, including requiring wireless providers to 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 interact with customers from accessing CPNI until after customers have been authenticated.
- Adopt 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.
- Establish requirements to minimize the harms of fraud when it occurs, including requiring wireless providers to maintain a clear process for customers to report fraud, promptly investigate and remediate fraud, and promptly provide customers with documentation of fraud involving their accounts.

What the *Further Notice* Would Do:

- Seek comment on whether to harmonize the Commission's existing requirements governing customer access to CPNI with the SIM change authentication and protection measures in the *Report and Order*, and on what steps the Commission can take to harmonize government efforts to address SIM swap and port-out fraud.

---

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in WC Docket No. 21-341, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs/). Before filing, participants should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 *et seq.*

Before the
Federal Communications Commission
Washington, D.C. 20554

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

REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING*

Adopted: [] **Released: []**

Comment Date: (30 days after Federal Register Publication)
Reply Comment Date: (60 days after Federal Register Publication)

By the Commission:

TABLE OF CONTENTS

* This document has been circulated for tentative consideration by the Commission at its November open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's ex parte rules apply and presentations are subject to "permit-but-disclose" ex parte rules. *See, e.g.*, 47 C.F.R. §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. See 47 CFR §§ 1.1200(a), 1.1203.

I. INTRODUCTION

1. Today, we adopt measures designed to address two fraudulent practices bad actors use to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone. In the first type of scam, a bad actor convinces a victim's wireless provider[1] to transfer the victim's mobile service and number from the victim's cell phone to a cell phone in the bad actor's possession. This scam is also known as "SIM swapping" because it involves an account being fraudulently transferred (or swapped) from a device associated with one subscriber identity module (SIM) to a device associated with a different SIM. In the second type of scam, the bad actor, posing as the victim, opens an account with a wireless provider other than the victim's current provider. The bad actor then arranges for the victim's phone number to be transferred (or "ported out") to the account with the new wireless provider controlled by the bad actor.

2. In this *Report and Order*, we take aim at these scams, with the goal of foreclosing the opportunistic ways in which bad actors take over customers' cell phone accounts. In doing so, we balance the important objectives of protecting consumers from harmful fraudulent conduct while at the same time not impinging on customers' ability to upgrade and replace their devices or choose their preferred wireless provider. Specifically, we revise our Customer Proprietary Network Information (CPNI) and Local Number Portability (LNP) rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider. We also require wireless providers to immediately notify customers whenever a SIM change or port-out request is made on customers' accounts, and take additional steps to protect customers from SIM swap and port-out fraud. Our approach sets baseline requirements that establish a uniform framework across the mobile wireless industry while giving wireless providers the flexibility to deliver the most advanced and appropriate fraud protection measures available.

3. In the accompanying *Further Notice of Proposed Rulemaking* (*Further Notice*), we seek comment on whether to harmonize the existing requirements governing customer access to CPNI[2] with the SIM change authentication and protection measures we adopt today. We also seek comment on what steps the Commission can take to harmonize government efforts to address SIM swap and port-out fraud.

II. BACKGROUND

4. *SIM Swap and Port-Out Fraud.* Cell phone numbers are frequently used as a means of authenticating the identity of users for various types of accounts, including accounts with wireless providers, e-mail and social media providers, financial institutions, healthcare providers, and retail websites.[3] Because so many consumers have their cell phones with them at all times, authentication using text messages and phone calls can be incredibly convenient, but these authentication methods also have

[1] In this item, when we use the term "wireless provider" we intend to encompass providers of commercial mobile radio service (CMRS) as defined in section 20.3 of the Commission's rules. 47 CFR § 20.3 (defining commercial mobile radio service as a mobile service that is "(1) provided for profit, *i.e.*, with the intent of receiving compensation or monetary gain; (2) An interconnected service; and (3) Available to the public, or to such classes of eligible users as to be effectively available to a substantial portion of the public," or the "functional equivalent of such a mobile service").

[2] *See id.* § 64.2010.

[3] For example, a consumer logging in to a bank account might be asked not only to provide the correct username and password, but also to input a one-time passcode sent via text message to the consumer's cell phone. Similarly, a consumer who has forgotten the password for a social media account may be prompted to enter a one-time passcode sent via text message to the consumer's cell phone before being allowed to reset the password.

incentivized bad actors to find ways to intercept authentication texts and calls. Two techniques they use to accomplish this involve misuse of mechanisms that enhance competition in the telecommunications marketplace and ensure that customers can access telecommunications services using the devices and providers of their choosing: SIM changes and number porting.

5. SIM changes allow customers to keep their wireless services and phone numbers when they upgrade their cell phone or replace a cell phone that is lost or broken. A SIM facilitates the proper routing of texts and calls to a customer's cell phone so long as the SIM associated with the customer's phone number is assigned to that customer's phone.[4] While SIM changes historically occurred by removing a physical SIM card from an old phone and placing it in a new phone, now wireless providers virtually reassign embedded, electronic SIMs in modern phones from an old phone to a new one.[5] Bad actors have successfully taken advantage of this legitimate practice by impersonating a customer of a wireless provider and convincing the provider to reassign the virtual SIM card from the real customer's device to a device controlled by the bad actor, a practice known as "SIM swap fraud."[6] This allows the bad actor to gain access to information associated with the customer's account, including CPNI, and gives the bad actor control of the customer's phone number so that the bad actor receives the text messages and phone calls intended for the victim.[7]

6. Number porting allows customers to retain their phone numbers when they switch from one service provider to another, which enables customers to choose a service provider that best suits their needs.[8] To initiate a port between two wireless providers, a customer must provide certain identifying information (i.e., telephone number, current account number, five-digit ZIP code, and any customer-assigned passcode) to the new wireless provider. The new wireless provider then sends a request to port the customer's number with this identifying information through the numbering administrator to the current wireless provider.[9] Once the current wireless provider verifies this information (thus "validating the port"), the two wireless providers coordinate through the numbering administrator to port the customer's number to the new wireless provider.[10] As with SIM swap fraud, bad actors have successfully taken advantage of this legitimate practice by impersonating a customer of a wireless provider and convincing the provider to port the real customer's telephone number to a new wireless provider and a

[4] Each mobile device has its own unique SIM. A SIM can be a physical card or a digital, virtual card embedded into the phone itself (eSIM card). FCC, *eSIM Cards FAQ*, https://www.fcc.gov/consumers/guides/esim-cards-faq. In either form, the SIM "contains unique information that identifies it to a specific mobile network" and "allows subscribers to use their mobile devices to receive calls, send SMS messages, or connect to mobile internet services." Russell Ware, *What is a SIM Card?*, Lifewire, https://www.lifewire.com/what-are-sim-cards-577532 (updated May 21, 2021).

[5] *See* FCC, *eSIM Cards FAQ*, https://www.fcc.gov/consumers/guides/esim-cards-faq (last updated July 10, 2023).

[6] CTIA, *Protecting Your Wireless Account Against SIM Swap Fraud*, https://www.ctia.org/protecting-against-sim-swap-fraud (last visited Oct. 18, 2023).

[7] *See Protecting Consumers from SIM Swap and Port-Out Fraud*, WC Docket No. 21-341, Notice of Proposed Rulemaking, 36 FCC Rcd 14120, 14122, para. 5 (2021) (*SIM Swap and Port-Out Fraud Notice*).

[8] *See generally* 47 U.S.C. § 153(37) (defining "number portability"); *Local Number Portability Porting Interval and Validation Requirements; Telephone Number Portability*, WC Docket No. 07-244, CC Docket No. 95-116, Report and Order and Further Notice of Proposed Rulemaking, 24 FCC Rcd 6084, 6087, para. 6 (2009) (*Porting Interval Order and FNPRM)*.

[9] *See Telephone Number Requirements for IP-Enabled Services Providers; Local Number Portability Porting Interval and Validation Requirements; IP-Enabled Services; Telephone Number Portability; Numbering Resource Optimization*, WC Docket No. 07-243 et al., Report and Order, Declaratory Ruling, Order on Remand, and Notice of Proposed Rulemaking, 22 FCC Rcd 19531, 19555, para. 44 (2007) (*2007 VoIP LNP Order* or *2007 LNP Four Fields Declaratory Ruling*).

[10] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14122, para. 6.

device that the bad actor controls.[11] This "port-out fraud" likewise gives the bad actor control over the customer's phone number, thereby allowing the bad actor to receive text messages and phone calls intended for the victim.

7. Once a fraudulent SIM swap or port-out request has been completed, the bad actor has acquired the means to take control of many more of the victim's accounts, which can result in substantial harm to the customer. For instance, because the bad actor can now intercept text messages and phone calls used to authenticate a customer's financial, social media, and other accounts, the bad actor may have the means to gain access to these accounts and then change login credentials, obtain sensitive information, drain bank accounts, and sell or try to ransom social media accounts.[12] Victims can also be harmed by the loss of service on their devices—the phone going dark or only allowing 911 calls—which is typically the first sign that SIM swap or port-out fraud has occurred.

8. The Commission and the Federal Trade Commission (FTC) have received hundreds of customer complaints about SIM swap and port-out fraud.[13] Some of the complaints describe wireless provider customer service representatives and store employees who do not know how to address instances of fraudulent SIM swaps or port-outs, resulting in customers spending many hours on the phone and at retail stores trying to get resolution. Other customers complain that their wireless providers have refused to provide them with documentation related to a fraudulent SIM change, making it difficult for them to pursue claims with their financial institutions or law enforcement. Several customer complaints filed with the Commission allege that a wireless provider's store employees are involved in the fraud or that

[11] FCC, *Port-Out Fraud Targets Your Private Accounts*, https://www.fcc.gov/port-out-fraud-targets-your-private-accounts (last updated July 10, 2023).

[12] *See, e.g.*, Department of Justice, U.S. Attorney's Office, Western District of Texas, *San Antonio Pair Plead Guilty to SIM Swap Scheme* (Oct. 12, 2022), https://www.justice.gov/usao-wdtx/pr/san-antonio-pair-plead-guilty-sim-swap-scheme; Department of Justice, U.S. Attorney's Office, Eastern District of Louisiana, *California Resident Pleads Guilty for His Role in Sim Swap Scam Targeting at Least 40 People, Including New Orleans Resident* (May 18, 2022), https://www.justice.gov/usao-edla/pr/california-resident-pleads-guilty-his-role-sim-swap-scam-targeting-least-40-people; 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/; U.S. Department of Justice, Office of the U.S. Attorneys, District of Maryland, *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), https://www.justice.gov/usao-md/pr/two-men-facing-federal-indictment-maryland-scheme-steal-digital-currency-and-social-media; U.S. Department of Justice, Office of the U.S. Attorneys, Eastern District of Michigan, *Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges* (May 9, 2019), https://www.justice.gov/usao-edmi/pr/nine-individuals-connected-hacking-group-charged-online-identity-theft-and-other (reporting the indictment of nine individuals alleged to have participated in thefts of victims' identities to steal cryptocurrency via "SIM Hijacking"); Lorenzo Franceschi-Bicchierai, *Hacker Who Stole $5 Million By SIM Swapping Gets 10 Years in Prison* (Feb. 1, 2019), https://www.vice.com/en/article/gyaqnb/hacker-joel-ortiz-sim-swapping-10-years-in-prison (reporting that a 20-year old student who stole more than $5 million in cryptocurrency by hijacking the phone numbers of around 40 victims pleaded guilty and accepted a plea deal of 10 years in prison, believed to be the first person convicted of a crime for SIM swapping); Gertrude Chavez-Dreyfuss, *U.S. Investor Sues AT&T for $224 million over loss of cryptocurrency* (Aug. 15, 2018), https://www.reuters.com/article/us-cryptocurrency-at-t-lawsuit/u-s-investor-sues-att-for-224-million-over-loss-of-cryptocurrency-idUSKBN1L01AA.

[13] According to staff review of informal complaints submitted through the Commission's Consumer Complaint Center, https://consumercomplaints.fcc.gov/hc/en-us, the Commission received approximately 300 complaints in 2020 concerning SIM swap or port-out-fraud, 400 in 2021, and 500 in 2022. The FTC identified 966 consumer reports of "Phone Carrier Switching" in 2020, 157 in 2021, and 188 in 2022. *See* Federal Trade Commission, Consumer Sentinel Network Data Book 2022 (Feb. 2023), at Appx. B, p. 88, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf. The FTC published a consumer alert regarding SIM swap scams in 2019. Alvaro Puig, FTC, *SIM Swap Scams: How to Protect Yourself* (Oct. 23, 2019), https://consumer.ftc.gov/consumer-alerts/2019/10/sim-swap-scams-how-protect-yourself.

providers completed SIM changes despite the customer having previously set a PIN or password on the account.

9. A study published in 2020 by a group of Princeton University researchers found that some wireless providers are using insecure mechanisms to authenticate the identities of individuals making SIM change requests.[14] The researchers opened ten pre-paid accounts each with five major wireless providers— AT&T Mobility, LLC (AT&T), T-Mobile US, Inc. (T-Mobile), Tracfone, US Mobile, and Verizon Wireless (Verizon)—and called to request a SIM change on each account. The researchers found that all five wireless providers "used insecure authentication challenges that could easily be subverted by attackers."[15] Specifically, the research team identified six types of information used by the wireless providers to authenticate their customers that were or could be vulnerable to abuse.[16] For example, authentication based on recent payment information was exploitable because some wireless providers do not have systems that prevent a bad actor from purchasing a refill card and submitting it on a victim's account, then requesting a SIM change using the known refill as authentication.[17] Call history information was exploitable because a bad actor could bait a victim into placing calls to specific phone numbers and provide those phone numbers as authentication, and in some cases it appeared that customer service representatives had the discretion to allow authentication with incoming call information.[18] The researchers also found that certain authentication information, such as device information, was vulnerable because it is readily available to bad actors.[19] Additionally, they noted that recent research has shown that preset answers to "security" questions are an insecure means of authentication, because answers that are memorable are also frequently guessable by an attacker.[20] The research team also found that "in general, callers only needed to successfully respond to one challenge in order to authenticate, even if they had failed numerous prior challenges in the call."[21] And in some instances, wireless providers disclosed personal customer information without any authentication at all, including information that could be used to authenticate a customer.[22]

10. The researchers also examined the potential downstream consequences of fraudulent SIM swaps. They "evaluated the authentication policies of over 140 online services that offer phone-based authentication to determine how they stand up to an attacker who has compromised a user's phone number via a SIM swap."[23] The researchers found that 17 websites across different industries have

[14] *See* Kevin Lee, Ben Kaiser, Jonathan Mayer, Arvind Narayanan, Center for Information Technology Policy, Princeton University, *An Empirical Study of Wireless Carrier Authentication for SIM Swaps*, August 2020, at Appx., available at https://www.usenix.org/system/files/soups2020-lee.pdf.

[15] Lee et al. at 1.

[16] These types of information were: (1) Personal Information: including street address, e-mail address, date of birth; (2) Account Information: last 4 digits of payment card number, activation date, last payment date and amount; (3) Device Information: IMEI (device serial number), ICCID (SIM serial number); (4) Usage Information: recent phone numbers called; (5) Knowledge: PIN or password, answers to security questions; and (6) Possession: one-time passcode sent via text message or e-mail. *Id.* at 2.

[17] *Id*. at 2-3.

[18] *Id.*

[19] *Id.* at 3.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.* at 1.

implemented authentication policies with logic flaws that would allow an attacker to fully compromise an account with just a SIM swap.[24]

11. *Privacy of Telecommunications Customer Information.* Section 222 of the Communications Act of 1934, as amended (the Act) obligates telecommunications carriers to protect the privacy and security of information about their customers to which they have access as a result of their unique position as network operators.[25] Section 222(a) requires carriers to protect the confidentiality of proprietary information of and relating to their customers, among others.[26] Section 222(c)(1) provides that a carrier may only use, disclose, or permit access to individually identifiable CPNI that it has received or obtained by virtue of its provision of a telecommunications service: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived or its provision of services necessary to, or used in, the provision of such telecommunications service.[27] CPNI is defined 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."[28] The Commission has not provided an exhaustive list of what constitutes CPNI, but it has explained that 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.[29]

12. The Commission first promulgated rules implementing the express statutory obligations of section 222 in 1998.[30] In addition to imposing restrictions on the use and disclosure of CPNI, the Commission adopted a set of rules designed to ensure that telecommunications carriers establish effective

[24] *Id.*

[25] 47 U.S.C. § 222. *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket Nos. 96-115, et al., Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14419-20, paras. 12-14 (1999) (*CPNI Reconsideration Order*) (denying petitions for reconsideration and forbearance seeking different treatment for wireless providers under the Commission's CPNI rules, concluding that "there is nothing in the statute or its legislative history to indicate that Congress intended the CPNI requirements in section 222 should not apply to wireless carriers").

[26] 47 U.S.C. § 222(a).

[27] 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.

[28] 47 U.S.C. § 222(h)(1).

[29] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927, 6931, para. 5 (2007) (*2007 CPNI Order*); *see also AT&T, Inc.*, File No.: EB-TCD-18-00027704, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1757, paras. 33-35 (2020) (finding that customer location information is CPNI under the Act).

[30] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket Nos. 96-115, et al., Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (*CPNI Order*).

safeguards to protect against unauthorized use or disclosure of CPNI.[31] Among other things, the Commission required telecommunications carriers to train their personnel as to when they are and are not authorized to use CPNI and required carriers to have an express disciplinary process in place for when personnel improperly use CPNI.[32] In addition, the Commission required each carrier to annually certify its compliance with the CPNI requirements and to make this certification publicly available.[33]

13. In 2007, the Commission amended its CPNI rules to address "pretexting," a scheme in which a bad actor pretends to be a particular customer or other authorized person to obtain access to that customer's call detail or other private communications records.[34] The Commission concluded that "pretexters have been successful at gaining unauthorized access to CPNI"[35] and that "carriers' record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI."[36] The new amendments to the rules restricted the release of call detail information[37] based on customer-initiated telephone contact, imposed password requirements for customer account access, and required carriers to appropriately authenticate both new and existing customers seeking access to CPNI online.[38] The Commission also required carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI[39] and to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed.[40] To protect customers from malicious account changes, these carrier notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change.[41] In addition, the Commission modified its CPNI rules to require carriers to notify law enforcement and customers of security breaches involving CPNI.[42] The Commission has made clear that carriers are free to implement more rigorous security measures to meet their section 222 obligations to protect the privacy of CPNI and that carriers have a fundamental duty to remain vigilant in their protection of CPNI.[43] Finally, the Commission also extended the application of its CPNI rules to providers of interconnected Voice over Internet Protocol (VoIP) service, finding that it is

---

[31] *See id.* at 8195, paras. 193-202; 47 CFR §§ 64.2001-2009 (1998).

[32] *See* 47 CFR § 64.2009(b) (1998); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198.

[33] 47 CFR § 64.2009(e) (1998); *see also CPNI Order*, 13 FCC Rcd at 8199, para. 201; *CPNI Reconsideration Order*, 14 FCC Rcd at 14468-69, n.331 (clarifying that carriers must "make these certifications available for public inspection, copying and/or printing at any time during regular business hours at a centrally located business office of the carrier").

[34] *2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1 & n.1.

[35] *Id.* at 6934, para. 12.

[36] *Id.* at 6933.

[37] The Commission defined "call detail" information to include "any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call." *2007 CPNI Order*, 22 FCC Rcd at 6936, n.45.

[38] *See id.* at 6936-41, 6945-46, paras. 13-22, 33-36; 47 CFR § 64.2010(b)-(e).

[39] *See 2007 CPNI Order*, 22 FCC Rcd at 6945-46, paras. 33-36; 47 CFR § 64.2010(a).

[40] *See 2007 CPNI Order*, 22 FCC Rcd at 6942, para. 24; 47 CFR § 64.2010(f).

[41] 47 CFR § 64.2010(f).

[42] *2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32; 47 CFR § 64.2011.

[43] *See 2007 CPNI Order*, 22 FCC Rcd at 6945-46, paras. 33-35. In addition, the Commission required affirmative customer consent ("opt-in consent") before a carrier could disclose a customer's CPNI to a carrier's joint venture partners or independent contractors for the purposes of marketing communications-related services to that customer. *See id.* at 6947-53, paras. 37-50.

"reasonable for American consumers to expect that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VoIP provider, given that these services, from the perspective of a customer making an ordinary telephone call, are virtually indistinguishable."[44] Additionally, in 2007 Congress adopted criminal prohibitions both on obtaining CPNI from a telecommunications carrier and on the sale, transfer, purchase, or receipt of fraudulently obtained CPNI.[45]

14. *Local Number Portability.* Section 251(b)(2) of the Act requires local exchange carriers (LECs) to "provide, to the extent technically feasible, number portability in accordance with requirements prescribed by the Commission."[46] The Act and the Commission's rules define number portability as "the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another."[47] Section 251(e)(1) of the Act gives the Commission exclusive jurisdiction over the North American Numbering Plan and related telephone numbering matters in the United States.[48] Although the Act excludes Commercial Mobile Radio Service (CMRS) providers from the statutory definition of "local exchange carrier,"[49] the Commission extended the LNP obligations to CMRS providers pursuant to its independent authority in sections 1, 2, 4(i) and 332 of the Act.[50] Wireless providers have been required to provide wireless number portability since 2003.[51]

---

[44] *Id.* at 6956, para. 56; *see also id*. at 6954-57, paras. 54-59. We note that, in 2008, Congress ratified the Commission's decision to apply section 222's requirements to interconnected VoIP by adding language to section 222 that expressly covers "IP-enabled voice service," defined by reference to the Commission's definition of "interconnected VoIP service." *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283 (2008); 47 U.S.C. § 222(d)(4), (f)(1), (g) (applying provisions of section 222 to "IP-enabled voice service"); *id.* § 615b(8) (defining "IP-enabled voice service" as having "the meaning given the term 'interconnected VoIP service' by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)").

[45] Telephone Records and Privacy Protection Act of 2006, Pub. L. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039).

[46] 47 U.S.C. § 251(b)(2).

[47] 47 U.S.C. § 153(37); 47 CFR § 52.21(m). The Commission has interpreted this language to mean that consumers must be able to change providers while keeping their telephone number as easily as they may change providers without taking their telephone number with them. *See Telephone Number Portability; Carrier Requests for Clarification of Wireless-Wireless Porting Issues*, CC Docket No. 95-116, Memorandum Opinion and Order, 18 FCC Rcd 20971, 20975, para. 11 (2003) (*Wireless Number Portability Order*), *aff'd*, *Central Tex. Tel. Coop., Inc. v. FCC*, 402 F.3d 205 (D.C. Cir. 2005).

[48] 47 U.S.C. § 251(e)(1).

[49] 47 U.S.C. § 153(32).

[50] *See Telephone Number Portability*, CC Docket No. 95-116, First Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 8352, 8431, para. 153 (1996) (*First Number Portability Order*); *Telephone Number Portability*, CC Docket No. 95-116, First Memorandum Opinion and Order on Reconsideration, 12 FCC Rcd 7236, 7315-17, paras. 140-42 (1997) (*First Number Portability Order on Reconsideration*) (affirming the Commission's decision to impose number portability obligations on CMRS providers).

[51] *See* 47 CFR § 52.31(a); *see also First Number Portability Order*, 11 FCC Rcd at 8439-41, paras. 164-68 (discussing implementation schedule for CMRS providers); *see also Cellular Telecommunications Industry Association's Petition for Forbearance from Commercial Mobile Radio Services Number Portability Obligations; Telephone Number Portability*, WT Docket No. 98-229, CC Docket No. 95-116, Memorandum Opinion and Order, 14 FCC Rcd 3092, 3111-12, paras. 37-39 (1999) (extending the implementation deadline for CMRS providers in the top 100 Metropolitan Statistical Areas where another carrier has made a specific request for the provision of LNP until November 24, 2002); *Verizon Wireless's Petition for Partial Forbearance from Commercial Mobile Radio Services Number Portability Obligations; Telephone Number Portability*, WT Docket No. 01-184, CC Docket No. 95-116, Memorandum Opinion and Order, 17 FCC Rcd 14972, 14981-86, paras. 23-31 (2002) (extending the implementation deadline for CMRS providers in the top 100 MSAs until November 24, 2003).

15. In 2003, the Commission clarified that for wireless ports, absent an agreement setting additional terms, wireless providers need only share basic contact and technical information with each other sufficient to validate and execute the port.[52] In 2007, the Commission clarified that a porting-out provider may not require more than a "minimal but reasonable" amount of information from the porting-in provider to validate a port request and accomplish the port.[53] The Commission concluded that for simple[54] wireline-to-wireline, wireless-to-wireless, and intermodal ports, LNP validation should be based on no more than four fields: (1) 10-digit telephone number; (2) customer account number; (3) five-digit ZIP code; and (4) passcode (if applicable).[55] This information is provided by the customer to the new carrier, who then provides it to the old carrier in order to validate the request.[56] In 2010, the Commission expanded and standardized the information exchanged between carriers when they execute a simple wireline or intermodal port, which it concluded was necessary to ensure carriers could accomplish ports within a one-business day porting interval the Commission established in 2009.[57] The Commission mandated that telecommunications carriers use 14 "Required Standard Data Fields"—and may require only those fields to accomplish such ports.[58] The Commission maintained the three customer-provided information fields from the *2007 LNP Four Fields Declaratory Ruling*—ported telephone number,

---

[52] *See Wireless Number Portability Order*, 18 FCC Rcd at 20978, para. 24.

[53] *See 2007 LNP Four Fields Declaratory Ruling*, 22 FCC Rcd at 19553, para. 42.

[54] A simple port is a port that (1) does not involve unbundled network elements; (2) involves an account only for a single line; (3) does not include complex switch translations (e.g., Centrex, ISDN, AIN services, remote call forwarding, or multiple services on the loop); and (4) does not include a reseller. *See, e.g.*, *id*. at 19556, n.153.

[55] *See id.* at 19557, para. 48; *see also id*. at 19558, para. 49 ("We are persuaded that the approach we adopt here reasonably balances consumer concerns about slamming with competitors' interest in ensuring that LNP may not be used in an anticompetitive manner to inhibit consumer choice.").

[56] *See, e.g.*, FCC, *Porting: Keeping Your Phone Number When You Change Providers*, https://www.fcc.gov/consumers/guides/porting-keeping-your-phone-number-when-you-change-providers.

[57] *See Local Number Portability Porting Interval and Validation Requirements; Telephone Number Portability*, Report and Order, 25 FCC Rcd 6953, 6959-62, paras. 9-17 (2010) (*LNP Standard Fields Order*); *id*. at 6954, para. 1 ("This Order completes the task of facilitating prompt transfers by standardizing the data to be exchanged when transferring a customer's telephone number between two wireline providers; a wireline and wireless provider; or an interconnected Voice over Internet Protocol (VoIP) provider and any other service provider."); 47 CFR § 52.36(a) ("A telecommunications carrier may require only the data described in paragraphs (b) and (c) of this section to accomplish a simple port order request from an end user customer's new telecommunications carrier."); *id*. § 52.36(d) ("For purposes of this section, the term 'telecommunications carrier' includes an interconnected VoIP provider as that term is defined in § 52.21(h).").

[58] The Commission required that service providers use the following 14 fields to accomplish a wireline or intermodal simple port: (1) "Ported Telephone Number" – the customer's telephone number; (2) "Account Number" – the customer's account number with the current service provider; (3) "Zip Code" – the zip code for the customer's address associated with the account; (4) "Company Code" – the operating company number, or OCN, of the new service provider; (5) "New Network Service Provider" – the name of the new service provider; (6) "Desired Due Date" – the date by which the customer wants the port completed; (7) "Purchase Order Number" – the customer's unique purchase order or requisition number that authorizes issuance of the port request; (8) "Version" – the version number of the order submitted by the new service provider; (9) "Number Portability Direction Indicator" – information to let the new service provider direct the correct administration of E-911 records; (10) "Customer Carrier Name Abbreviation" – the three-letter code for the name of the new service provider; (11) "Requisition Type and Status" – the type of order to be processed, such as number portability, loop with number portability, retail/bundled, resale, directory listings, etc.; (12) "Activity" – the activity involved in the service request, such as porting, new account installation, disconnection, suspension, restoration, etc.; (13) "Telephone Number of Initiator" – the telephone number for the new service provider initiating the port request; and (14) "Agency Authority Status" – which indicates that the new service provider initiating the port request has an authorization to initiate a port on file. 47 CFR § 52.36(b); *see also LNP Standard Fields Order*, 25 FCC Rcd at 6959-62, paras. 9-17. We note that when requesting a port, some of the information described above is supplied by the customer to the new or gaining carrier and some of the information is provided by the new carrier to the current carrier.

customer account number, and customer ZIP code.[59] The rules also permit customers to request that a user-created passcode be put on their account, which the customer must then provide before a port can be accomplished.[60] The Commission at the time found that the exchange of these fields struck the appropriate balance between streamlining the porting process and ensuring accurate ports, and also reasonably balanced customer concerns about unauthorized ports with competitors' interest in ensuring that porting obligations may not be used in an anticompetitive manner to inhibit customer choice.[61]

16. The members of the non-governmental, multi-stakeholder Number Portability Industry Forum (NPIF) have created "Best Practices" for porting between and within telephony carriers.[62] These Best Practices are voluntary and not mandated by the Commission, but reflect the consensus of the NPIF or its predecessor organization regarding the preferred processes for porting.[63] Best Practice 73 (Unauthorized Port Flow) specifically addresses unauthorized ports, including fraudulent ports.[64] Among other things, it encourages carriers to review "incident and/or police report details if provided" and places priority on resolving unauthorized ports that have a heightened severity of impact.[65]

17. *Notice of Proposed Rulemaking.* In September 2021, the Commission adopted the *SIM Swap and Port-Out Fraud Notice*, in which it proposed to amend the Commission's CPNI and LNP rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider.[66] The *SIM Swap and Port-Out Fraud Notice* also proposed to require wireless providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts and sought comment on other ways to protect customers from SIM swap and port-out fraud.[67]

III. DISCUSSION

18. Today we revise our CPNI and LNP rules to provide greater protection to customers from SIM swap and port-out fraud. The cornerstone of our action is a requirement that wireless providers use secure methods of authenticating customers prior to performing SIM changes and number ports. Other rules we adopt reinforce that requirement, including that wireless providers 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 interact with customers from accessing

[59] *See* 47 CFR § 52.36(b)(1)-(3).

[60] *See id.* § 52.36(c).

[61] *See generally LNP Standard Fields Order*, 25 FCC Rcd at 6956-62, paras. 6-10.

[62] NPAC, Number Portability Best Practices, https://workinggroup.numberportability.com/number-portability-best-practices (last visited Oct. 18, 2023).

[63] *See id.*

[64] Best Practice 73 addresses three types of unauthorized ports: disputed ports (usually a result of two or more parties each claiming to be the authorized end user, including business partner disputes, personal relationship disputes, dissolution of franchises); inadvertent ports (which occur as a result of an error, including incorrect number provided by End User and typographical errors in local service requests); and fraudulent ports (which occur as a result of an intentional act of fraud, theft, and/or misrepresentation). *See* Best Practice 73, NPAC, *Number Portability Best Practices*, at 1-2, https://workinggroup.numberportability.com/number-portability-best-practices (last visited Oct. 18, 2023).

[65] These include ports involving an "FCC/PUC/Attorney General complaint; court order; military institution; medical facility; business lines (i.e. national organization, main published line); emergency services; medical support services; or otherwise documented as properly reported to law enforcement." *See* Best Practice 73, NPAC, *Number Portability Best Practices*, at 4, https://workinggroup.numberportability.com/number-portability-best-practices (last visited Oct. 18, 2023).

[66] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14121, para. 3.

[67] *Id.*

CPNI until after customers have been authenticated. We also adopt rules that will enable customers to act to prevent and address fraudulent SIM changes and number ports, including requiring that wireless providers 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. We further establish requirements to minimize the harms of SIM swap and port-out fraud when it occurs, including requiring wireless providers to maintain a clear process for customers to report fraud, 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, we require that they keep records of SIM change requests and the authentication measures they use.

19. In adopting these rules, we balance the need to protect customers from the harms of SIM swap and port-out fraud with the goal of preserving the relative ease with which customers can obtain legitimate SIM changes and number ports. The record reflects that the vast majority of SIM change and port-out requests are legitimate.[68] It also shows that the efficient and effective processing of SIM changes and port-out requests promotes customer choice and competition[69] and prevents interruptions in access to wireless services that are vital to customers' everyday lives.[70] Service interruptions can be particularly problematic when they hamper the ability of customers to access emergency services.[71] We agree with the Competitive Carriers Association (CCA) that "enhanced requirements for SIM swap and port-out requests can implicate the customer experience and can intentionally or unintentionally serve as impediments to legitimate requests to change devices or change providers."[72] We are wary of setting rigid requirements that would impose significant burdens on customers without substantially protecting against SIM swap and port-out fraud.[73] We also recognize that prescribing particular security methods

[68] *See, e.g.*, T-Mobile Comments at 2 (asserting that "the vast majority of subscriber SIM swap and port-out requests are legitimate"); CTIA Reply at 1 ("[T]he overwhelming majority—well over 99%—of SIM swap and port-out requests are legitimate."); AT&T Comments at 7-8 ("By AT&T's calculation, more than 99 percent of the total SIM changes and port-outs it processes are legitimate.").

[69] *See, e.g.*, CTIA Reply at 3 ("Given the importance of [SIM changes and number porting] for enabling provision of service, competition, and consumer choice, it is critical for customers seeking to replace or upgrade their device or to change their provider to be able to do so *both* securely and without undue friction in the customer experience.") (emphasis in original); CTIA Comments at 10 ("It is critical that the LNP rules continue to protect against anti-competitive behaviors, and that any updates to address port-out fraud should be clearly tied to consumer fraud protection."); T-Mobile Comments at 2-3 ("[T]he Commission should ensure that any rule changes do not limit consumer choice between wireless providers or stifle competition by introducing undue delay or complexity to fulfilling port-out and SIM swap requests."); AT&T Comments at 1-2 ("SIM swaps and port-outs are, in short, integral features of the competitive wireless marketplace."); Verizon Comments at 1 (explaining that SIM changes and number porting "benefits competition and customer choice by enabling consumers to efficiently switch providers and take advantage of new devices and service plans").

[70] *See, e.g.*, T-Mobile Comments at 7 ("Wireless services are vital to most Americans and, therefore they must have the ability to make account changes."); *id.* at 6-7 ("T-Mobile's wireless services are a lifeline for its over 100 million postpaid and prepaid subscribers across America, who rely on wireless services for connections to family, work, public safety, and school as well as key apps and services."); AT&T Comments at 17-18 (noting that cell phones "have become an essential part of everyday life").

[71] *See, e.g.*, CTIA Comments at 9 (asserting that "[s]ervice disruptions due to strict authentication requirements could be particularly impactful for customers who are in emergency situations").

[72] CCA Comments at 7; *see also* NCTA Comments at 7 (arguing that certain prescriptive requirements "would create unnecessary obstacles for consumers that desire to switch providers").

[73] *See, e.g.*, AT&T Comments at 2-3 ("Across-the-board prescriptive rules would increase consumer frustration in nearly all SIM- or port-related transactions without a concomitant reduction in the risk."); *id.* at 12-13 (explaining that specific mandates could "restrict[] consumer choice and impos[e] delays and other burdens upon the overwhelming majority (more than 99 percent) of transactions that are perfectly legitimate"); CTIA Reply at 5 ("An (continued….)

can place greater burdens on some customers because of their technical and financial means, digital literacy, accessibility needs, and other particularized circumstances.[74] We anticipate that the approach we take today will provide meaningful protection to customers while preserving the competition and customer choice that SIM changes and number porting are meant to facilitate and avoiding undue burdens that hinder access to wireless services.

20. To that end, we set baseline rules, rather than prescriptive requirements, that establish a uniform framework across the mobile wireless industry for the types of policies and procedures providers must employ to combat SIM swap and port-out fraud. The record indicates that several wireless providers already rely, at least partly, on some of these policies and procedures.[75] We are concerned, however, that a lack of consistency in how wireless providers apply these measures and a lack of uniformity in the use of these measures industry-wide leaves some customers vulnerable to SIM swap and port-out fraud. The rules we adopt ensure that all wireless providers are taking consistent and comprehensive steps to address this fraud. For wireless providers that already employ the measures we require, in many cases our rules simply raise the bar by requiring them to adapt, refine, or consistently apply those existing practices. For wireless providers that do not, our new rules require them to implement new practices to meet the baseline standards. We anticipate that our approach will ensure that customers receive effective protection from SIM swap and port-out fraud regardless of the wireless telecommunications services they purchase or the wireless provider from whom they purchase them.

21. In setting baseline requirements, rather than prescriptive rules, our approach also gives wireless providers the flexibility to establish the specific fraud protection measures they use so that they can deliver the most advanced protections available. The record provides substantial evidence that to best combat SIM swap and port-out fraud, wireless providers need flexibility.[76] In particular, we are persuaded that wireless providers need such flexibility so that they can adapt their security methods to keep pace with the evolving threat landscape. Verizon notes that "fraudsters are sophisticated and

approach that is unnecessarily rigid will adversely affect legitimate customers' ability to swap SIM cards and port numbers, which are both critical to ensuring provision of service, customer choice, and competition.").

[74] *See, e.g.*, CCA Comments at 7 (noting that when security measures cause frustration, "customers, especially those who are older or less familiar with technology, may be deterred from selecting a provider who may offer a better service" and therefore that the Commission "should be attentive to ensuring that heightened authentication procedures are customer friendly"); T-Mobile Comments at 6-7 (asserting that the Commission should strive for SIM swap and port-out fraud rules that "promote diversity, inclusion, and accessibility of wireless services"); Verizon Comments at 6 ("As the NPRM notes, in-store customers in need of a SIM change may not be tech savvy, so flexibility to allow some form of physical documentation will be needed.").

[75] *See, e.g.*, CTIA Comments at 3-4 (highlighting "the variety of tactics used to combat SIM swapping and port-out fraud"); CTIA Reply at 5-9 (further detailing the tactics providers use); NCTA Comments at 4-5 (explaining that wireless providers already use many of the practices proposed in the *SIM Swap and Port-Out Fraud Notice* to prevent SIM swap and port-out fraud today); CCA Comments at 6 (noting that many CCA members already have implemented the measures proposed in the *SIM Swap and Port-Out Fraud Notice* to combat SIM swap and port-out fraud); AT&T Comments at 13 ("Carriers are already authenticating customers using one or more of the methods identified in the Commission's existing and/or proposed rules."); T-Mobile Comments at 1 ("T-Mobile has robust protections in place to help prevent fraudulent SIM swapping and port-outs from occurring.").

[76] *See, e.g.*, AT&T Comments at 11 ("Effective mitigation requires an agile approach to managing these risks that can only be achieved within a flexible framework."); NCTA Comments at 2 ("[I]f the Commission moves forward with new rules to address fraud, the best approach would be to establish a flexible standard requiring heightened authentication measures for SIM swap requests. The Commission should adopt a similarly flexible requirement to take reasonable measures to prevent port-out fraud."); CTIA Comments at 16 ("[T]echnical, rigid, and narrow requirements will not move the needle for consumer protection in the same way that a smart, flexible, future-proof, and risk-based framework will."); CCA Comments at 6 ("The Commission should resist, however, from requiring a defined set of measures that all carriers should uniformly adopt."); Verizon Comments at 5 ("[P]roviders must have flexibility both to develop and implement new methods beyond those enumerated in the draft rule.").

constantly look to circumvent any protections, no matter how robust."[77] We also recognize that "[r]apid technological changes introduce new vulnerabilities that existing rules may be unequipped to address."[78] We are therefore concerned by record evidence that a static set of prescriptive requirements may incentivize some wireless providers to rely exclusively on those security methods and discourage them from innovating and adopting new and improved practices to address evolving fraud techniques used by bad actors.[79] We also share concerns that setting specific requirements could either provide a roadmap for bad actors seeking to commit fraud[80] or lock in measures that quickly prove to be ineffective or obsolete.[81] The aim of our action today is to better protect telecommunications customers from fraudulent schemes; in doing so, it is important that our rules, while functioning as baseline safeguards, do not serve as obstacles to adoption of better security practices. Indeed, the record asserts that establishing rules that provide flexibility will incentivize wireless providers to develop and adopt new and improved methods to protect against SIM swap and port-out fraud[82] and enable them to quickly adapt their security measures to

[77] Verizon Comments at 1; *see also* AT&T Comments at 11 ("Bad actors perpetually look for creative ways to gain access to consumers' financial or social media accounts."); CCA Comments at 4-5 ("[S]ophisticated hackers and other bad actors are resourceful and often find ways to skirt safeguards to sensitive information.").

[78] CCA Comments at 4-5.

[79] *See, e.g.*, AT&T Comments at 14 ("[L]ocking in a particular list of authentication methods would play into bad actors' hands by discouraging carriers from adopting new methods not expressly blessed by the Commission's rule, while inhibiting the ability of carriers and other stakeholders to innovate, as necessary and appropriate, to address evolving threats."); Better Identity Coalition at 6 (asserting that if the Commission enshrined guidelines or standards into regulation, "it might inadvertently preclude carriers from deploying new innovations that emerge after [those guidelines and standards were developed] that might address new threats or more efficiently identify or authenticate consumers."); FIDO Alliance Comments at 3 (arguing that reliance on the four specified authentication methods may disincentive providers from adopting stronger authentication measures); CCA Comments at 4-5 (cautioning against adopting rules that "might inhibit a provider's ability to respond to new threats as they emerge" and noting that if "a future technology, proves to be more effective or secure than today's technologies, the Commission should ensure that its rules do not end up serving as an obstacle to adoption of better practices"); CTIA Reply at 14 ("The Commission should thus ensure that its regulatory approach does not impede providers' ability to protect their customers.").

[80] *See, e.g.*, AT&T Comments at 12-13 ("[S]pecific mandates in this context could provide a roadmap for bad actors who would quickly tailor their tactics to circumvent them."); Verizon Comments at 5 (arguing that enumerating particular methods to prevent unauthorized SIM changes "will give bad actors a roadmap and that may prove less effective over time"); CTIA Comments at 10-11 ("[R]igid and prescriptive requirements hurt security more than they may help. . . . [I]f every provider authenticates requests in the same way, fraudsters and scammers will find a way around such uniform 'safeguards.'"); Better Identity Coalition at 2-3 (suggesting that if the Commission prescribes specific authentication requirements, "attackers would simply adapt their attack methods to target these new authenticators, with the net effect being no significant slowdown in the pace of SIM Swap attacks").

[81] *See, e.g.*, CCA Comments at 5 (asserting that specific methods "could become obsolete quickly"); CTIA Comments at 11 ("[A]voiding rigid rules that are tied to specific technologies or tools will also help to future-proof FCC guidance when it comes to authentication."); T-Mobile Comments at 2 ("[W]hat constitutes a 'secure method of authentication' is likely to change over time."); Better Identity Coalition at 4 ("One constant in cybersecurity is that threats are constantly evolving, as are the tools used to stop threats. But regulations are permanent, or in a best-case scenario, infrequently updated. Any regulatory approach that seeks to tie MNOs to using specific authentication technologies is certain to fail to keep up as threat and security both evolve.").

[82] *See, e.g.*, CTIA Reply at 15 (arguing that "a more flexible approach that allows for innovation and iteration is best"); CCA Comments at 4 (asserting that any rules the Commission adopts should be "sufficiently flexible to account for evolving technologies"); Princeton Comments at 4 ("Authentication methods and security practices continue to evolve, and carriers should be welcome—and encouraged—to adopt innovative safeguards."); T-Mobile Comments at 12-13 ("Flexibility will promote innovation and improved security for customers."); NCTA Comments at 7 ("An adaptable standard as discussed above will best incentivize carriers to adopt solutions that provide effective security for their customers and services while not handcuffing carriers to specific technology or processes as new solutions emerge.").

respond to evolving techniques and technologies used by bad actors.[83] Accordingly, we agree with AT&T that "[t]he best way to combat ever-evolving fraud tactics is to allow industry players the ability to adapt and respond to these changing threats in real-time,"[84] and we afford wireless providers this flexibility with the rules we adopt in this *Report and Order*.

22. Flexibility will also permit wireless providers to use the specific security practices that are effective and appropriate under the circumstances. We are persuaded that any given measure will rarely prove foolproof, necessary, or suitable in all instances,[85] and therefore that wireless providers should have the ability to tailor the security mechanisms they use. AT&T, for instance, asserts that it has had success in deploying measures strategically to reduce the incidents of SIM swap and port-out fraud,[86] and with our rules, we seek to foster such outcomes. Our flexible approach enables wireless providers to implement security measures that are designed to address a customer's particular circumstances and preferences, and also allows wireless providers to implement measures that are best suited for their business models, technologies, and the services they offer.[87] We also recognize that some wireless providers may seek to use a risk-based model, whereby they apply different mechanisms to protect customers based on the likelihood of fraud for a particular SIM change or port-out request, and we do not want to hinder these targeted efforts.[88] For these reasons, we conclude that wireless providers should

[83] *See, e.g.*, CTIA Comments at 10-11 (asserting that "[f]lexibility is a cornerstone of effective risk management, as it allows providers to develop and deploy innovative tools that can meet evolving threats and stay ahead of the fraudsters, as opposed to 'checking the box' on stagnant compliance requirements"); CTIA Reply at 15-16 (explaining that flexibility will help prevent security practices from lagging behind bad actor tactics); Verizon Comments at 5 ("[P]roviders must have flexibility both to develop and implement new methods beyond those enumerated in the draft rule to keep ahead of bad actors and to abandon measures that no longer work."); CCA Comments at 5 (asserting that "the Commission should allow for flexibility for carriers to respond quickly and nimbly to new threats and to encourage adopting innovative solutions to threats"); Somos Comments at 2 ("As with most fraud the telecom industry suffers, the bad actors are constantly evolving. Solutions should evolve, as well.").

[84] AT&T Comments at 2.

[85] *See, e.g.*, AT&T Comments at 5 & 12-13 (explaining that "no method of authentication is foolproof or effective in every instance" and that "[e]ven proposals that have merit in certain circumstances should not be foisted onto all carriers in all circumstances"); T-Mobile Comments at 12 (noting that failed authentication attempts occur with regularity for legitimate users and therefore may not necessarily signal nefarious activity that requires heightened security measures); FIDO Alliance Comments at 3-4 (explaining, for example, that one-time use passcodes sent by SMS as a method of authentication are "useless" if a customer's phone is lost or stolen).

[86] AT&T Comments at 2-3 ("Wireless carriers have developed substantial expertise in detecting and combating new forms of fraud. Significantly, AT&T has limited the incidences of fraudulent SIM swaps and port-outs by remaining flexible and varied in the tools it employs, allowing us to be at least as agile as the fraudsters.").

[87] *See, e.g.*, CTIA Comments at 3 & 18 (explaining that flexibility for notifications is needed so that providers can "account for the complexities of notifications in various contexts"); CTIA Reply at 15-16 (noting that the record illustrates "that flexibility is important to continue to allow providers to meet the diverse needs of their customers"); Princeton Comments at 11-12 (declining to take a position on how investigations of fraud should be conducted, "since the details will vary by account compromise"); AT&T Comments at 5 (explaining that the tools it uses to combat SIM swap and port-out fraud "are tailored to different customers, services, and technologies because they must be"); *id.* at 11 (explaining that because customer needs vary, the "diverse characteristics of these customers and the products and services they utilize lend themselves to different risk-management approaches"); CCA Comments at 5 (explaining that "[c]arriers often adopt policies that serve the specific needs of their consumers"); T-Mobile Comments at 9 (asserting that notification methods "should be flexible and reflect customers' preferences").

[88] *See, e.g.*, AT&T Comments at 13-14 ("AT&T employs data-driven analytics to make an initial risk assessment for specific postpaid transactions, which drives confidence in the authenticity of the transactions and allows them to be completed without delay or burden to the customer."); CTIA Reply at 11-12 ("One key step in protecting consumers and businesses against account takeovers is for organizations to deploy risk-appropriate authentication practices."); T-Mobile Comments at 2 ("Organizations should use authentication measures that correspond to the value and sensitivity of the accounts involved.").

have the flexibility to determine which specific measure will be most effective at protecting customers against SIM swap and port-out fraud in a given circumstance in accordance with our baseline rules.

23. We further anticipate that our flexible approach will enhance protections for customers without placing undue costs and burdens on wireless providers. We are cognizant that in some instances, strict prescriptive requirements to prevent SIM swap and port-out fraud could be technically and economically infeasible for wireless providers to implement, particularly for smaller providers.[89] Even in the instances when wireless providers do have the means to implement prescriptive requirements, those requirements could prove burdensome on providers if they become obsolete or ineffective and providers are compelled to maintain them alongside new and better practices they adopt to address the evolving threat landscape.[90] By setting baseline requirements and giving wireless providers flexibility on how to meet them, we allow providers to adopt the most cost-effective and least burdensome solutions to achieve the level of security needed to protect customers against SIM swap and port-out fraud in a given circumstance. Additionally, because many of our rules build on existing mechanisms that many wireless providers already use, we expect that our new rules will further minimize the costs and burdens for those providers.

A. Strengthening the Commission's CPNI Rules to Protect Consumers

24. In this section, we adopt baseline measures designed to reduce the incidence of SIM swap fraud without impinging on customers' ability to upgrade and replace their devices. As proposed in the *SIM Swap and Port-Out Fraud Notice*,[91] we require wireless providers to use secure methods to authenticate customers that are reasonably designed to confirm a customer's identity prior to effectuating SIM changes, but we depart from our proposal specifying particular methods of authentication, to allow providers the flexibility they need to implement the most modern and effective authentication methods on an ongoing basis. We also adopt rules to require wireless providers to implement procedures to address failed authentication attempts and to notify customers of SIM change requests prior to effectuating a SIM change. Additionally, we adopt rules that allow customers to lock their accounts to prevent SIM changes, require wireless providers to track the effectiveness of the authentication measures they have implemented, and safeguard against employee access to CPNI prior to authentication. In each instance, we afford wireless providers needed flexibility while enhancing protections for customers.

25. The record makes clear that because SIMs are only used to facilitate service for mobile wireless devices, SIM swap fraud is a practice that is exclusive to mobile wireless services.[92] Thus, we

[89] *See, e.g.*, CCA Comments at 6 ("The Commission should also keep in mind the constraints with which many small carriers operate against in adopting security measures. Smaller carriers may have more limited app or e-commerce platforms, and may not currently have the capability, for example, to generate a one-time port out PIN via an app on a 24/7/365 basis."); T-Mobile Comments at 12 (asserting that it would be technically difficulty to track multiple failed authentication attempts because users attempt to access their accounts across various platforms, such as over the phone, online, or in retail stores run by the carrier or a third party); CTIA Comments at 16 (same).

[90] *See, e.g.*, AT&T Comments at 13 (asserting that the methods of authentication proposed by the Commission "would introduce new and often unwanted complexities in the SIM swap process for carriers and their customers. Fundamentally, requiring the use of particular authentication methods for every SIM swap would impose tremendous burdens on carriers and customers without clear additional benefit").

[91] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14130, para. 23.

[92] *See, e.g.*, AT&T Comments at 1 (noting that "SIM swaps allow customers to replace a defective SIM or, more commonly, to upgrade or replace an outdated, lost, stolen, or damaged phone, tablet, or other mobile device, without disruption to their wireless service"); CCA Comments at 1 (explaining that SIM swap fraud is a method malicious actors use to steal mobile accounts); CTIA Comments at 1-2 (discussing SIM swap fraud exclusively in the context of wireless services); National Consumer Law Center (NCLC) and Electronic Privacy Information Center (EPIC) Comments at 2 (NCLC/EPIC Comments) (noting that "American cell phone users . . . are extremely vulnerable to having their telephone numbers hijacked by fraudsters through the process of SIM swapping and port-out fraud"); NCTA Comments at 1 (explaining that with SIM swap fraud, "the bad actor convinces the wireless provider to

(continued….)

apply these new requirements to providers of commercial mobile radio service (CMRS), as defined in section 20.3 of Title 47 of the Code of Federal Regulations,[93] including resellers of CMRS, except our new rule requiring telecommunications carriers to establish safeguards and processes so that employees are unable to access CPNI until after a customer has been properly authenticated, which we apply to all telecommunications carriers subject to our CPNI rules.[94] We apply these new requirements to all SIM changes that wireless providers perform.[95] Further, we require wireless providers to implement these rules with respect to customers of both pre-paid and post-paid services, consistent with the protections afforded by section 222. We see no reason why the protections should not apply to all customers of CMRS, including customers of resellers, particularly considering indications in the record that pre-paid customers are disproportionately impacted by fraud and that many customers impacted by such fraud are low-income customers who can ill afford such losses.[96]

1. Customer Authentication Requirements

26. We update our CPNI rules to protect customers from the risk of fraudulent SIM swaps by requiring wireless providers, prior to conducting a SIM change, to use secure methods to authenticate a customer that are reasonably designed to confirm a customer's identity,[97] except to the extent otherwise required by the Safe Connections Act or the Commission's rules implementing that statute.[98] We define

transfer the customer's service from the subscriber identity module (SIM) in the customer's phone to a new SIM in the bad actor's phone"); T-Mobile Comments at 1 (expressing support for "the Commission's efforts to make it harder for bad actors to take control of consumers' cell phone accounts through fraudulent subscriber identity module ("SIM") swapping"); Verizon Comments at 2 (explaining that "SIM changes help customers by enabling them to easily move a mobile phone number to a new SIM card"); *see also* Lee et al. at 61 (explaining that a SIM swap attack involves "unauthorized change to the victim's mobile carrier account" whereby "the attacker diverts service, including calls and messages, to a new SIM card and device that they control").

[93] 47 CFR § 20.3. Under this definition, our new rules apply to both facilities-based wireless providers as well as resellers of wireless services. Additionally, given that section 332(c)(1)(A) of the Act requires that providers of commercial mobile service be treated as common carriers, 47 U.S.C. § 332(c)(1)A), our rules cover "any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment," 47 U.S.C. § 217.

[94] *See* 47 CFR § 64.2003(o) (definition of "telecommunications carrier," which for purposes of our CPNI rules, includes "an entity that provides interconnected VoIP service").

[95] Verizon suggests that requirements we adopt may not be necessary for all SIM changes, asserting that "[t]he vast majority of SIM changes do not raise security concerns," Verizon Comments at 6, but Verizon did not explain how carriers may know that certain SIM changes are lower risk than others and its assertion did not receive support in the record, so we decline to limit the applicability of our requirements to only certain SIM changes.

[96] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14137, para. 45 (seeking comment on whether the rule should apply only to certain services or accounts); *see also, e.g.*, Princeton Comments at 13 (recommending that "any new rules apply to both prepaid and postpaid wireless carriers"); NCLC/EPIC Comments at 2 (noting that "American cell phone users, particularly those who rely on prepaid phones, are extremely vulnerable to having their telephone numbers hijacked by fraudsters" and that prepaid phone customers are "generally low-income consumers").

[97] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14130, para. 23. We encourage wireless providers to use secure authentication methods that accommodate the needs of the broad spectrum of customers they may serve. *See infra* para. 56.

[98] The Safe Connections Act of 2022, Pub. L. No. 117-223, 136 Stat. 2280 (Safe Connections Act), which is codified at 47 U.S.C. § 345, requires wireless providers to separate lines from a multi-line account upon request of a survivor of domestic violence and other related crimes and abuses. 47 U.S.C. § 345(b)(1). The Commission proposed rules implementing this requirement and sought comment both on authentication of survivors seeking line separations and how to prevent fraud related to line separation requests. *See Supporting Survivors of Domestic and Sexual Violence; Lifeline and Link Up Reform and Modernization; Affordable Connectivity Program*, WC Docket Nos. 22-238, 11-42, 21-450, Notice of Proposed Rulemaking, FCC 23-9, paras. 44-45, 103 (rel. Feb. 17, 2023) (*Safe* (continued….)

"SIM," for purposes of these rules, as "a physical or virtual card associated with a device that stores unique information that can be identified to a specific mobile network."[99] The record reflects significant support for strengthening authentication requirements for SIM change requests,[100] and we find that the requirement we adopt today most appropriately balances the need to increase protection for customers from these types of fraudulent schemes while providing wireless providers the flexibility the record shows they need to respond to new and emerging threats.[101] We are persuaded by commenters that a general security authentication standard will afford customers the highest level of protection by allowing wireless providers to implement the authentication methods raised in the record,[102] or develop new authentication

Connections Notice). In an Order adopted today implementing the Safe Connections Act, the Commission adopted rules to require covered providers to attempt to authenticate, using multiple authentication methods if necessary, that a survivor requesting a line separation is a user of a specific line or lines. *See* Public Release, *Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238, Report and Order, FCC 23-XX, para. 52 (rel. Oct. 25, 2023) (*Publicly Released Draft Safe Connections Order*). Covered providers must use methods that are reasonably designed to confirm the survivor is actually a user of the specified line(s) on the account when the survivor is not the primary account holder or a designated user, and this authentication shall be sufficient for requesting a SIM change when made in connection with a line separation request. *See id.* To the extent this requirement differs from other authentication requirements, including those in 47 CFR § 64.2010, the line separation authentication requirements the Commission adopts to implement 47 U.S.C. § 345 serve as an exception to those other requirements. *See id.*

[99] *See* Appx. A (revised 47 CFR § 64.2010(h)). We slightly revise this definition from that proposed in the *SIM Swap and Port-Out Fraud Notice* to provide greater clarity that a SIM is not necessarily a physical card. *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14130, para. 23 (proposing a similar definition but with "contained within " in place of "associated with"); NCLC/EPIC Comments at 3 (writing that they are "encouraged" by the Commission's proposal and definition of "SIM").

[100] *See, e.g.*, Bank Policy Institute/BITS (BPI/BITS) Comments at 1 ("BPI/BITS supports reasonable measures to require additional authentication factors to reduce these risks."); CCA Comments at 3 (agreeing that "some degree of heightened authentication procedure is appropriate in the context of SIM swaps or port outs to prevent the increasing risk of fraud"); Princeton Comments at 2 ("We support the Commission's proposal to require that carriers complete strong customer authentication before effectuating a SIM swap."); Somos Comments at 2 ("It should be required that trusted identity verification and validation, as qualification of a SIM swap transaction must be implemented."); ATL Comments at 1 (supporting "additional fraud prevention methods and requiring all carriers to adopt secure methods of authenticating a customer before SIM changes"); Prove Comments at 2-3 ("Prove believes that carriers should securely authenticate customers prior to effectuating any SIM swap or port-out request.").

[101] *See* AT&T Comments at 11; Verizon Comments at 5; CCA Comments at 5; CTIA Comments at 16-17; T-Mobile Comments at 12-13; NCTA Comments at 2-6; Somos Comments at 2; CTIA Reply at 15.

[102] *See, e.g.*, FIDO Alliance Comments at 4 (citing the benefits of the FIDO standards public key cryptography approach); Better Identity Coalition Comments at 3-4 (explaining that "industry and government are moving away from knowledge-based approaches to authentication (i.e. passwords) to those that are possession-based, such as authentication based on the FIDO2 standards"); OPUS Research Reply at 1 (promoting the use of "voice biometrics as part of a multi-factor approach to strong customer authentication"); Prove Comments at 2-6 (suggesting development and use of a "neutral, cross-industry, consumer-managed tool" based on the authentication factors of possession, reputation, and ownership); Princeton Comments at 5-6, 12 (supporting the use of multi-factor authentication and implementation of a system for carriers to check whether a SIM was recently swapped); NCTA Comments at 5 (asserting that "multi-factor authentication that considers biometrics, devices, app-based tokens, and other unique identifiers . . . also provide security and offer benefits to consumers, including ease of use"); Robert Ross Comments at 5-8 (recommending the Commission require authentication solutions based on the principles of layered security, non-profit solutions, a combination of customer-facing and non-customer facing methods, and a combination of technology and human solutions, with examples provided); BPI/BITS Comments at 2-3 (expressing support for "app-based push notification to a trusted mobile device, biometrics identifiers, or cryptographic keys," for certain types of data); ID.me Comments at 4 ("The FCC should require carriers to comply with NIST SP 800-63-3 IAL2, AAL2, and FAL2 before authorizing SIM Swap and Port-Out transactions."); iProov Comments at 5-7 (recommending the Commission require "at least two independent authentication factors" be used and that the list of secure methods include a strong multi-factor authentication factor, such as cloud biometrics, "that does not rely on possession of the device or number"); T-Mobile Comments at 3 (explaining that customers are permitted to set up

(continued….)

methods, in ways that both account for advances in the technology and tactics used by bad actors and that work best for their customers and the particular services they offer.[103] Additionally, we believe this flexibility alleviates record concerns about the limited information wireless providers may have to authenticate customers of pre-paid accounts.[104]

27. While the approach we take today gives wireless providers the *flexibility* to adapt to evolving threats, it also creates an *obligation* that they adapt to those threats. Specifically, our rule establishes a requirement that wireless providers regularly, but not less than annually, review and, as necessary, update their customer authentication methods to ensure those methods continue to be secure.[105] The record reflects that while many authentication measures may be effective today, evolving tactics may mean those methods will not work tomorrow or in all circumstances.[106] If wireless providers fail to evolve their authentication methods over time, we expect their methods eventually will become ineffective. Therefore, we require wireless providers to regularly, but not less than annually, review their authentication methods, and update them as necessary to ensure that the authentication methods remain effective.

28. Because we impose a general requirement for secure and reasonably designed customer authentication, both permitting and obligating wireless providers to design effective methods to authenticate customers, we decline to enumerate the four specific authentication methods the Commission specified in the *SIM Swap and Port-Out Fraud Notice* as those that would meet the standard of secure authentication methods.[107] We are convinced by the record that specifying approved authentication methods may incentivize wireless providers to rely exclusively on those methods or discourage them from adopting new methods to address evolving techniques used by bad actors.[108] Further, some commenters

multi-factor authentication "using methods including security questions, SMS, or device-based biometrics such as Face ID or fingerprint recognition on devices that support such features").

[103] *See, e.g.*, CTIA Reply at 11-12 ("One key step in protecting consumers and businesses against account takeovers is for organizations to deploy risk-appropriate authentication practices."); T-Mobile Comments at 2 ("Organizations should use authentication measures that correspond to the value and sensitivity of the accounts involved.").

[104] *See* CTIA Comments at 14-15 (noting that "fighting fraud in the pre-paid context is different than in the post-paid context" and that "providers ordinarily do not collect or have detailed identity information for pre-paid customers"); T-Mobile Comments at 8 (stating that "[p]repaid service generally does not require identity validation for account set-up"); CCA Comments at 6 (noting that pre-paid customers "often do not provide an accurate address or other identifying information, making it difficult for carriers to authenticate an account request"); CTIA Comments at 19-20 (noting that a flexible approach will better serve customers, including pre-paid customers).

[105] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14132, para. 27 (seeking comment on how we can account for changes in technology, recognizing that some methods may become hackable over time while additional secure methods of authentication will likely be developed).

[106] *See* AT&T Comments at 11 ("While passwords remain a useful and typically effective authentication tool, especially when used in combination with other security mechanisms, that may not be the case in the future. New forms of network-based authentication offer promise for preventing unauthorized access incidents in ways that may be more user-friendly as well."); Better Identity Coalition Comments at 5-6 (explaining that some forms of multi-factor authentication can be subject to phishing, but other forms are phishing resistant); iProov Comments at 5-7 (explaining that some biometrics can be vulnerable to social engineering and that device-based biometrics are not as secure as cloud-based biometrics).

[107] Those four methods were: (i) the use of a pre-established password; (ii) a one-time passcode sent via text message to the account phone number or a pre-registered backup number; (iii) a one-time passcode sent via e-mail to the e-mail address associated with the account; or (iv) a passcode sent using a voice call to the account phone number or a preregistered back-up telephone number. *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14130, para. 23. No commenters supported our imposing these as the exclusive forms of authentication.

[108] *See* AT&T Comments at 14 ("The practical effect of the list is that carriers will feel constrained in using non-listed methods for fear that anything else would be unauthorized."); Better Identity Coalition at 4 ("[W]e have some concerns that if the four authentication methodologies are the only ones listed in the regulation, that it may

(continued….)

assert that requiring specific authentication methods would be burdensome for wireless providers.[109] Additionally, the record reflects that setting specific authentication methods could provide a roadmap for bad actors seeking to commit fraud.[110] The record also highlights potential vulnerabilities of the four authentication methods we proposed,[111] which counsels against us codifying these as secure methods of authentication in perpetuity. For these reasons, we conclude it is most appropriate to allow wireless providers to analyze and implement the most effective and secure methods of authenticating customers requesting a SIM change.[112]

29. We nevertheless place boundaries on the use of certain information for customer authentication for SIM change requests in light of evidence in the record of their particular vulnerability. Namely, we conclude, consistent with our proposal, that methods of authentication that use readily available biographical information, account information, recent payment information, and call detail information do not constitute secure methods of authentication.[113]

30. We decline to restrict the use of SMS-based customer authentication for SIM change requests, but we strongly encourage wireless providers to use this mechanism only when paired with other secure methods of authentication, i.e., as part of multi-factor authentication (MFA). In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on the potential security vulnerabilities of SMS-based authentication.[114] The record clearly expresses concern about the security risks of SMS-based authentication when used by third parties, such as financial institutions, largely because this

discourage the use of stronger, more innovative approaches to authentication."); FIDO Alliance Comments at 3 (arguing that reliance on the four specified authentication methods may disincentive carriers to adopt stronger authentication measures).

[109] *See* AT&T Comments at 13 (explaining that "requiring the use of particular authentication methods for every SIM swap would impose tremendous burdens on carriers and customers without clear additional benefit"); Prove Comments at 2 ("The authentication protocols proposed in the NPRM are, however, overly prescriptive, out-of-date (or soon will be), ineffective, easy to compromise, and overly burdensome for both carriers and consumers.").

[110] AT&T Comments at 14-15 ("[F]ixed authentication methods for SIM changes and port-outs will provide a roadmap to bad actors"); CTIA Comments at 10-11 ("[I]f every provider authenticates requests in the same way, fraudsters and scammers will find a way around such uniform 'safeguards.'").

[111] *See* Better Identity Coalition Comments at 2-3 (asserting that the four methods we proposed "are all based on authentication methods that are known to be easily compromised" and describing the weaknesses with each); FIDO Alliance Comments at 3-4 (same); Prove Comments at 2-3 (same).

[112] For similar reasons, we also decline to require carriers to comply with the National Institute of Standards and Technology (NIST) Digital Identity Guidelines or other standards proposed in the record. *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14132, para. 28. *See* CTIA Reply at 18-19 (arguing that while the NIST Digital Identity Guidelines or FIDO Standards might be useful tools, they should not be mandated); Better Identity Coalition Comments at 5 (asserting that while the NIST guidelines are a helpful reference point, they should not be the basis of the Commission's regulation because they are only updated every 5-7 years and reliance on them "could inadvertently preclude innovation that might better guard against attacks"); iProov Comments at 8; T-Mobile Comments at 13 (asserting that the NIST guidelines are a good reference point for best practices but are not a suitable compliance tool). *But see* ID.me Comments at 4 ("The FCC should require carriers to comply with NIST SP 800-63-3 IAL2, AAL2, and FAL2 before authorizing SIM Swap and Port-Out transactions.").

[113] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14132, para. 30; *see also* Princeton Comments at 11 (affirming the finding in its 2020 report that biographical information, account information, recent payment information, and call detail information have significant security shortcomings and therefore should not be used as the exclusive means of authentication, individually or in combination with each other). We seek comment in the *Further Notice* on whether we should harmonize our CPNI rules with the SIM change rules we adopt today, and we therefore take no action, at this time, to amend our existing rules to prohibit providers from relying on recent payment and call detail information to authenticate customers for online, telephone, or in-person access to CPNI. *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14132-33, para. 30.

[114] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14130-31, para. 24.

authentication method becomes vulnerable following fraudulent SIM swaps.[115] The record evidence is less clear that SMS-based authentication is an insecure mechanism in every instance it is used, such as to authenticate the identity of individuals requesting a SIM change, particularly when sent over a provider's own network, rather than the Public Switched Telephone Network (PSTN).[116] We also acknowledge that, in some instances, it may be the most practical means a provider can authenticate a customer, particularly when considering the needs of a particular customer.[117] We anticipate that the approach we take here

[115] *See, e.g.*, BPI/BITS Comments at 2-3 (explaining that a one-time passcode (OTP) sent via SMS can be vulnerable following a fraudulent SIM swap and that "for applications with higher-stakes consumer data such as financial applications, OTP factors remain a target for bad actors"); iProov Comments at 7 (noting SMS-based authentication is vulnerable in part because of SIM swaps, which allow bad actors to intercept calls and messages); CTIA Comments at 5 ("While SMS-based two-factor authentication may be perfectly suitable to some settings, it may not uniformly be appropriate for all types of transactions."); CTIA Reply at 12 ("SIM cards and the telecommunications accounts associated with them are not always an appropriate method of authentication for third-party apps and services, including organizations like financial and crypto service providers, to rely on to authenticate their end users."); T-Mobile Comments at 14 ("Entities with sensitive consumer information or assets (e.g., financial services, cryptocurrency wallets, healthcare, insurance, etc.) should be encouraged to use appropriate authentication methods that correspond to the sensitivity of accounts or transactions. SMS as the second factor should not necessarily be the sole authentication method."); Yubico Comments at 1 ("[A]uthentication based on a person's phone number that can be SIM Swapped is not a sustainable model due to the fact that the phone number is not fully controlled by the end user."); FIDO Alliance Comments at 2 (explaining how fraudulent SIM swaps allow criminals and foreign adversaries "to undermine some weaker forms of multi-factor authentication (MFA) such as one-time passcodes (OTPs) transmitted via SMS"); Better Identity Coalition Comments at 2 (noting that attackers trick customers into handing over OTPs sent via SMS when used in other sectors). Several commenters assert that the use of SMS-based authentication by third parties creates significant incentive for bad actors to carry out SIM swap fraud. *See, e.g.*, Better Identity Coalition Comments at 2 (asserting that the fact that SMS "is widely used as an authentication method [by many companies and organizations] has created incentives for criminals to launch SIM Swap attacks"); FIDO Alliance Comments at 3 ("To truly eliminate SIM Swap attacks, the best way to do so is to get companies and organizations to shift from SMS-based authentication to more secure forms of MFA."); T-Mobile Comments at 14 ("[T]he reliance of financial and cryptocurrency firms on SMS for authentication is driving fraudsters to constantly pursue new avenues of SIM and porting fraud.").

[116] *See, e.g.*, Verizon Comments at 5 & n.12 (noting that in some cases, SMS "can be an effective authenticator" and that the FTC has found that "in some cases 'use of SMS text messages as a factor may be the best solution because of its low cost and easy use'" (quoting the FTC's Safeguards Rule)); AT&T Comments at 6 (noting that "[a]t a higher risk threshold, AT&T uses SMS confirmations – two-way, no charge communications sent to postpaid customers asking them to approve or reject a pending SIM swap or port-out transaction"); Princeton Comments at 3 ("We support allowing SMS and voice call authentication methods when the carrier can deliver the passcode exclusively over its own network and to a specific known device (e.g., smartphone) or point of service (e.g., landline phone) connected to the network and controlled by the customer."); CTIA Comments at 5 ("SMS text messaging may be an appropriate authentication factor, depending on the nature and the sensitivity of the information being accessed and whether the consumer maintains control over the device and the number associated with it."); CTIA Reply at 16 (acknowledging that a OTP sent via SMS may not be useful in the case of a lost or stolen phone, but that it "may be perfectly appropriate [for SIM change authentications] when the customer is in possession of the device"). In the *SIM Swap and Port-Out Fraud Notice*, we highlighted an investigation which found that SMS-based text messages could be easily intercepted and re-routed using a low-cost, online marketing service, but we also explained that wireless providers had reportedly mitigated that vulnerability and no commenters raised this as a concern in the record. *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14130-31, para. 24.

[117] *See, e.g.*, CCA Comments at 6 ("[C]ustomers often do not update their carrier with their most recent email addresses or do not regularly check email, whereas a phone number is current and texts are easily accessible. Other carriers have noted that for customers with prepaid accounts, customers often do not provide an accurate address or other identifying information, making it difficult for carriers to authenticate an account request with this kind of information."); CTIA Reply at 16 ("[T]he record makes clear that customer needs vary, for example as between consumer and business customers, and that those variable customer needs inform authentication practices."). We recognize that SMS-based authentication also is a common authentication method used by wireless providers. *See, e.g.*, AT&T Comments at 6 ("AT&T routinely uses a one-time PIN delivered via SMS message or an outbound

(continued….)

strikes the right balance between protecting customers against SIM swap fraud while preserving the relative ease with which customers can obtain legitimate SIM changes. We emphasize, however, that our rules create an ongoing obligation that wireless providers ensure the authentication methods they use are secure. Accordingly, permitting wireless providers to use SMS-based authentication does not create a safe harbor for use of this authentication method. We will continue to monitor the use of SMS-based authentication and may later revisit our decision to permit its continued use.[118]

2. Response to Failed Authentication Attempts

31. We require wireless providers to immediately notify customers in the event of failed authentication attempts in connection with SIM change requests,[119] except to the extent otherwise required by the Safe Connections Act of 2022 (47 U.S.C. § 345) or the Commission's rules implementing that statute.[120] We conclude that such notifications will empower customers to take action to prevent unauthorized access to their account when failed authentication attempts are fraudulent. We specify that such notifications must be reasonably designed to reach the customer associated with the account but otherwise permit wireless providers to determine the method of providing these notifications, taking into consideration the needs of survivors pursuant to the Safe Connections Act and our implementing rules. We also require that such notifications use "clear and concise language" but do not prescribe particular content or wording for the notifications.

32. We decline to require that wireless providers delay SIM changes for 24 hours in the event of failed authentication attempts while notifying customers via text message and/or email regarding the failed authentication attempts.[121] The record reflects that strict requirements involving 24-hour delays or account locks could be overly burdensome for customers that are engaged in legitimate SIM changes.[122] We also anticipate that the notification requirement for failed authentication attempts, coupled with the

voice call to a postpaid customer's device for enhanced customer validation, including with SIM swaps."); CCA Comments at 3 (noting that two-factor authentication with a OTP sent to a phone number is "among the procedures that already are gaining prevalence" by wireless providers and noting that several of CCA's members prefer text messages for authentication purposes); CTIA Comments at 3-4 (noting that some wireless providers combat SIM swap and port-out fraud by "[e]mploying multi-factor authentication when account changes are requested, including one-time passcodes sent via text message").

[118] Princeton Comments at 3 ("Commission staff should periodically revisit the security of these authentication methods and reevaluate whether to retain them.").

[119] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14133, para. 33 (seeking comment on what processes providers can implement to prevent bad actors from attempting multiple authentication methods, including potentially notifying customers).

[120] *See Publicly Released Draft Safe Connections Order*, para. 52 and 47 CFR § 64.6402(b) (requiring that covered providers attempt to authenticate, *using multiple authentication methods if necessary*, that a survivor requesting a line separation is a user of a specific line or lines) (emphasis added); *id.* at para. 100 and 47 CFR § 64.2010(f)(2) (clarifying that the rule requiring carriers to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed does not apply when such changes are made in connection with a line separation request made pursuant to the Safe Connections Act); *id.* at para. 77 and 47 CFR § 64.6402(i) (prohibiting a covered provider from notifying a primary account holder of a survivor's request for a SIM change when made in connection with a line separation request pursuant to 47 U.S.C. § 345 and the implementing rules); *id.* at para. 101 (making clear that compliance with the Safe Connections Act and rules implementing it supersede an preempt any conflicting obligations under state law, Commission's rules, or state rules).

[121] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14133, para. 33 (seeking comment on potential delay and notification requirements in the case of multiple failed authentication attempts).

[122] *See* NCTA Comments at 6 ("[F]orcing providers to lock a customer out of their own account for a certain amount of time can arbitrarily punish customers who are less adept at navigating the authentication process and proving their identity in a secure way."); AT&T Comments at 2-3; CTIA Comments at 16; T-Mobile Comments at 7.

requirement we adopt below that wireless providers immediately notify customers upon receiving a SIM change request, will be sufficient to empower customers to quickly address unauthorized SIM change attempts.

33. We also require wireless providers to develop, maintain, and implement procedures for responding to failed authentication attempts in connection with a SIM change request that are reasonably designed to prevent unauthorized access to a customer's account, which, among other things, take into consideration the needs of survivors pursuant to the Safe Connections Act and our implementing rules.[123] We are bolstered by the Princeton University researchers who found evidence that wireless providers' procedures to respond to suspicious authentication attempts may be inadequate or nonexistent.[124] Specifically, they determined that some wireless providers only required callers to successfully respond to one authentication challenge to obtain a SIM change even if the caller had failed numerous previous authentication attempts.[125] While the *SIM Swap and Port-Out Fraud Notice* raised these issues, no commenters offered evidence to counter the researchers' findings. Without procedures in place to respond to failed authentication attempts, bad actors can seek to circumvent wireless provider authentication mechanisms to fraudulently obtain a SIM change. We anticipate that requiring wireless providers to establish procedures to respond to failed authentication attempts that are reasonably designed to prevent unauthorized access to a customer's account will impede these fraud attempts. In requiring providers to establish procedures to address failed authentication attempts, we recognize that tracking such attempts across platforms is not without its challenges,[126] but we are not persuaded that doing so is technically infeasible.[127] As such, we conclude that whatever burdens may be associated with this requirement are outweighed by the Commission's interest in protecting customers against fraudulent activity.

34. At the same time, we are persuaded by T-Mobile's argument that wireless providers need flexibility with respect to failed authentication attempts because it is common for customers to lose or forget their authentication data, leading to multiple failed attempts.[128] As such, we decline at this time to adopt prescriptive requirements for how wireless providers must respond to failed authentication attempts in connection with a SIM change request outside of the immediate notification described above. We find that anchoring this rule in a reasonableness standard will give wireless providers flexibility to design procedures to handle failed authentication attempts that protect against fraudulent activity while

[123] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14133, para. 33; Princeton Comments at 7. *See also* 47 U.S.C. § 345; 47 CFR § 64.6402(b) (a covered provider shall attempt to authenticate, using multiple methods if necessary, that a survivor requesting a line separation is the user of a specific line); 47 CFR § 64.6402(i) (a covered provider shall not notify a primary account holder of a survivor's request for a SIM change when made in connection with a line separation request pursuant to 47 U.S.C. § 345 and this subpart).

[124] *See* Princeton Comments at 7 ("We saw no evident response from carriers to our suspicious customer authentication attempts.").

[125] Lee et al. at 62; *see also* Princeton Comments at 6 ("[W]e found that carriers did not implement adequate safeguards for preventing an attacker from repeatedly calling customer service and attempting a SIM swap.").

[126] *See* T-Mobile Comments at 12 (asserting that it would be technically difficult to track multiple failed authentication attempts because users attempt to access their accounts across various platforms, such as over the phone, online, or in retail stores run by the carrier or a third party); CTIA Comments at 16 ("[D]eveloping procedures to track multiple failed authentication attempts as contemplated in the NPRM would be challenging for providers, as authentication attempts may occur across different settings (e.g., in person, online, or over the phone) and they may occur at disparate times.").

[127] For example, CTIA's proposal that carriers should only be required to develop and implement procedures for responding to multiple failed authentication attempts "where a carrier has reason to believe such attempts are fraudulent" implies that wireless carriers can and do track multiple authentication attempts, or, at a minimum, are technically capable of doing so.

[128] T-Mobile Comments at 7.

preventing unnecessary burdens on legitimate customer activity.[129] We decline, however, to adopt CTIA's suggestion to require the development and implementation of such procedures only where a wireless provider has reason to believe multiple authentication attempts are fraudulent; CTIA does not address how such determinations would be made absent the very procedures we require.

3. Customer Notification of SIM Change Requests

35. To provide customers with an early warning that their account may be subject to fraudulent activity, we adopt our proposal to require wireless providers to immediately notify customers of any requests for a SIM change associated with the customer's account[130] and specify that the notification must be delivered before a wireless provider effectuates a SIM change, except to the extent otherwise required by the Safe Connections Act of 2022 (47 U.S.C. § 345) the Commission's rules implementing that statute.[131] The record evinces firm support for this requirement[132] and provides good reason—time is often of the essence with SIM swap fraud, and notifying customers of a SIM change request before effectuating the request will enable customers to act promptly to mitigate damages and inconvenience resulting from fraudulent or inadvertent SIM changes.[133] We also expect that requiring notification before the request is processed will prevent the notification from being delivered to the bad actor after a SIM swap has occurred. For these reasons, we agree with Princeton University that "[t]here is an unambiguous and material security upside," to immediate customer notification of SIM change requests, and "the only downside is a very infrequent notification that the customer can easily discard" for legitimate requests.[134]

36. We therefore disagree with AT&T's contention that notification of all SIM change requests is unnecessary because "AT&T employs various tools to assess the risk level of a particular postpaid SIM change or port-out request and very often can determine at the outset that a request is legitimate."[135] The notification requirement we adopt today will provide a uniform safety measure for all

[129] *See* CTIA Reply at 23 (calling for any adopted rules related to failed authentication attempts to be "based on a reasonableness standard, as it would promote robust authentication practices through a flexible, risk-based lens"); Princeton Comments at 6-7 (recommending that the Commission "require that the procedures be reasonably designed to prevent unauthorized access to a customer's account").

[130] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14133, para. 34.

[131] *See Publicly Released Draft Safe Connections Order* at para. 77 and 47 CFR § 64.6402(i) (prohibiting a covered provider from notifying a primary account holder of a survivor's request for a SIM change when made in connection with a line separation request pursuant to 47 U.S.C. § 345 and the implementing rules).

[132] *See, e.g.*, Princeton Comments at 7 ("We support the Commission's proposal requiring customer notification for SIM swap attempts."); T-Mobile Comments at 2 ("The Commission should adopt its proposal to require reasonable efforts to notify users of port-out requests and SIM changes."); DC Stone Comments (Express) ("At the consumers['] option, no SIM porting should be permitted without first sending a notifying email (or SMS message) to a prearranged contact email address (or phone number)."); *see also* Verizon Comments at 6 ("[N]otifying the customer of attempted and/or executed SIM changes, can be useful tools in some cases.").

[133] *See* Princeton Comments at 7 (asserting that notice of a SIM swap attempt is "essential, so that a customer can take prompt action to protect their telecommunications account (e.g., updating a compromised password), their other accounts (e.g., stopping a fraudulent payment), and their devices (e.g., removing malware from a compromised device)"); Prove Comments at 2, 6 (asserting that "consumers should receive timely notice of high risk events such as SIM swaps and port-out requests, and be afforded the opportunity to prevent account takeovers before they are completed"); Andreas Carlos Freund Comments (Express) ("Strengthening these rules will . . . ensure customers are apprised of an attempted attack, so that they can take additional measures to protect their privacy."); *see also 2007 CPNI Order*, 22 FCC Rcd at 6942, para. 24 (explaining that, with respect to other types of account changes, the Commission has found that notification is an important tool for customers to monitor their account's security and enables them to take appropriate action in the event of fraudulent activity).

[134] Princeton Comments at 7.

[135] AT&T Comments at 15.

requests across the mobile wireless industry, which we anticipate will reduce the instances and mitigate the harms of SIM swap fraud. We also disagree with AT&T's assertion that customers will become so inundated with SIM change notifications that they will "eventually become numb or immune to them or tire of and consciously choose to ignore them, thus undermining all value they might otherwise have when the threat of fraud is real."[136] Nothing in the record, or our understanding of the SIM change process, supports the notion that customers request SIM changes at such a rate that, upon the adoption of this rule, wireless providers will be forced to inundate their customers with the required notifications.[137]

37. Also contrary to AT&T's assertions,[138] we do not anticipate that the notification requirement we adopt today will be overly burdensome for wireless providers to implement. As an initial matter, wireless providers should already have processes in place to immediately notify customers of certain account changes involving CPNI in accordance with our existing rules,[139] so they should be able to build on these processes to provide immediate notification regarding SIM change requests. The record also demonstrates that some wireless providers already notify customers of SIM change requests in most instances and therefore will only need to update their processes to notify customers in all cases.[140] Additionally, as discussed below, we give wireless providers flexibility on how to deliver the required notifications, which we expect further minimizes any potential burdens associated with our new rule. In any event, we find that the benefits of our notification requirement outweigh the potential burdens.

38. We permit wireless providers to determine the method of providing notifications regarding SIM change requests involving a customer's account, but specify that the notifications must be reasonably designed to reach the customer associated with the account,[141] and delivered in accordance with customer preferences, if indicated.[142] Although some commenters suggest that we should specify the means by which a wireless provider should deliver SIM change request notifications,[143] we agree with industry commenters that providers need flexibility to determine the most appropriate method to notify

[136] AT&T Comments at 15; *see also* CTIA Comments at 18 (asserting that notifications can be appropriate in "many instances" but that notifications "must be weighed against other goals, and in general, avoid unnecessary friction in the user experience or other unintended consequences, such as notice fatigue").

[137] *See* Princeton Comments at 7.

[138] *See* AT&T Comments at 15 (asserting that a notice requirement would impose burdens on wireless providers).

[139] 47 CFR § 64.2010(f); *2007 CPNI Order*, 22 FCC Rcd at 6942, para. 24 (requiring carriers to "notify customer immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed").

[140] *See* AT&T Comments at 6 (explaining that for transactions meeting a certain threshold of AT&T's "risk model," it will send one-way SMS notifications of a SIM change request, and for transactions meeting a higher risk threshold, it will require customers confirm the SIM change request via an SMS notification); T-Mobile Comments at 4 (noting that as part of its efforts to "help customers secure their accounts, T-Mobile notifies customers of account changes and requests"); Verizon Comments at 6 ("Verizon already employs (or is on track to employ) many of the methods identified in the NPRM, such as notifying customers of high-risk SIM change authentication attempts, failed or otherwise, and of other account changes."); CTIA Comments at 18 (explaining that "there are many instances where notifications to consumers are appropriate and providers can and do make reasonable efforts to provide them").

[141] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14134, para. 36. Our rule does not impose a duty on carriers to confirm that the notification has been received and read by the actual customer and therefore it does not impose strict liability on carriers if the notification fails to reach the customer or require carriers to wait to complete a SIM change after delivering a notification. *See* AT&T Comments at 16.

[142] For example, this would include delivering a notification in the language of the customer's choosing, if the wireless provider permits communications preferences in other languages and the customer has previously indicated such choice.

[143] *See, e.g.*, Princeton Comments at 7; Prove Comments at 6; DC Stone Comments (Express).

their customers of a pending SIM change request,[144] so that providers can account for "the complexities of notifications in various contexts,"[145] as well as the technical capabilities, accessibility needs, or broadband access of individual customers. For example, when a customer is requesting a SIM change because the customer's phone is lost or stolen, our flexible approach enables wireless providers to use methods of notification that are most likely to reach the customer under those circumstances, such as an email or a text or call to a pre-determined back-up phone number.[146] We also aim to enable wireless providers to deliver notifications in accordance with customer preferences, needs, and established expectations.[147] As such, we permit wireless providers to use existing methods of notification that are reasonably designed to reach the customer associated with the account,[148] and we encourage them to adopt new notification methods as they are developed to stay responsive to evolving fraud schemes. We acknowledge that our new rule differs from our existing rule that providers deliver notification of other account changes involving CPNI, which specifies that those notifications may be delivered through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record.[149] We find that departing from the existing rule's approach is appropriate given the depth of harm that can occur from SIM swap fraud, the need for wireless providers to be able to choose the most effective method of quickly alerting customers so that customers can take action to mitigate harm, and the importance of providers adopting new forms of notification.

39. We also decline to prescribe particular content or wording of SIM change notifications, recognizing that wireless providers are in the best position to determine what will most effectively notify customers of SIM change requests and potential fraud and will need to tailor notifications to customers' service plans and circumstances.[150] Nevertheless, consistent with the record and our CPNI rules, we specify that such notifications must use clear and concise language that provides sufficient information to effectively inform a customer that a SIM change request involving the customer's SIM was made.[151] We observe that our rule does not prohibit wireless providers from using different content and wording for

[144] *See, e.g.*, AT&T Comments at 16; T-Mobile Comments at 2; CTIA Reply at 23.

[145] CTIA Comments at 18. *See also* AT&T Comments at 16 ("[C]arriers should be permitted to communicate with their customers via the means they deem to be most effective in a particular context."). Our rule also gives carriers the flexibility to design a notification process that accommodates scenarios beyond individual customers, such as a business customer seeking bulk SIM changes to upgrade their equipment.

[146] *See* CTIA Comments at 18 (noting that "where a phone is lost or stolen, certain notifications will not reach consumers").

[147] *See* T-Mobile Comments at 6-7 (encouraging the Commission to consider rule changes that meet "legitimate customer needs" and "promote diversity, inclusion, and accessibility of wireless services"); *id.* at 9 (asserting that the method of customer notification "should be flexible and reflect customers' preferences"); AT&T Comments at 11 (noting that "[c]ustomer needs also vary. AT&T provides customers a range of products and services to meet different wireless communications needs. The diverse characteristics of these customers and the products and services they utilize lend themselves to different risk-management approaches.").

[148] Such methods include, but are not limited to, live or automated telephone calls, text messages, emails, or push notification through wireless provider software applications. *See, e.g.*, Verizon Comments at 6 ("Providers also should have discretion to use a push notification together with supplemental verification methods to stop a high risk transaction.").

[149] 47 CFR § 64.2010(f). We seek comment in the *Further Notice* on whether we should harmonize our CPNI rules with the SIM change rules we adopt today, including for notifications.

[150] T-Mobile Comments at 10 (asserting that the "the exact language should be customizable by the carrier to account for the type of request, brand, product, and other factors"); *see also* Verizon Comments at 6 ("Prescriptive rules for the content . . . of the notification are unnecessary.").

[151] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14133, para. 34 (seeking comment on a notification requirement); Appx. A (47 CFR § 64.2010(h)(3)). *Cf.* 47 CFR § 64.2008(c) (stating the CPNI notices must be comprehensible); T-Mobile Comments at 10 (asserting that notifications should be "clear and specific").

notifications depending on a provider's risk assessment of a given SIM change request, so long as the notification uses clear and concise language and is reasonably designed to reach the actual customer.[152]

40. We further decline to require a delay for customer verification or acknowledgement in connection with notifications prior to completing a SIM change request. In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on whether we should require a 24-hour delay (or other period of time) before a wireless provider effectuates a SIM change while notifying the customer via text message, email, the provider's app, or push notification, and requesting verification of the request.[153] This approach received minimal support in the record,[154] and we are convinced by other record evidence that the burdens of delay and verification requirements outweigh the benefits, particularly given how regularly customers seek legitimate SIM changes. For instance, CTIA explains that a blanket delay would "make it exceedingly difficult for a consumer to obtain a new phone and continued service when a device breaks or is lost, representing a full day where that consumer could not rely on their wireless service for . . . 'keeping in touch with friends through voice calls and text messages' [and] placing life-saving public safety calls."[155] AT&T and T-Mobile echoed these concerns.[156] We also anticipate that the authentication, notification, and remediation requirements we adopt today will sufficiently mitigate fraudulent SIM change requests without the need for a burdensome delay and verification process. While we do not require wireless providers to implement a delay and verification process, we permit them to do so in instances when they determine these measures are necessary to protect against fraud,[157] but stress that this process should not be used to delay legitimate SIM change requests.

4. Account Locks for SIM Changes

41. We require wireless providers to offer all customers, at no cost, the option to lock or freeze their account to stop SIM changes.[158] We anticipate that this requirement will provide customers

---

[152] *See* AT&T Comments at 15 (describing AT&T's existing risk-based approach for providing SIM change notifications).

[153] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14134, para. 37.

[154] *See, e.g.*, Robert Ross Comments at 1; DC Stone Comments (Express); *see also* Prove Comments at 6-7 (suggesting that a short delay may be appropriate to allow customers to terminate a SIM change request but arguing against a long delay because it would "impose unnecessary inconveniences and costs on consumers"); T-Mobile Comments at 10 (explaining that notifications of SIM change requests could seek verification from customers but also arguing that carriers should be permitted to process requests if it does not receive a response within a certain amount of time).

[155] CTIA Comments at 9 (cleaned up).

[156] AT&T Comments at 17-18 ("[F]orcing a customer with a lost, stolen, or damaged phone to wait 24 hours (or just a few hours for that matter) before obtaining an active replacement would at best frustrate the consumer . . ., and, at worst, threaten the customer's safety and impair her ability to engage in commerce, work, and education."); T-Mobile Comments at 9 ("A 24-hour delay could cause hardship for customers with legitimate reasons to request the swap, such as a lost, stolen, or damaged phone.").

[157] CTIA Comments at 9 (asserting that a delay "may be appropriate in some situations and could help to prevent fraud while balancing important service goals" and that "the Commission should clarify that providers have flexibility to implement such delays as appropriate to address the unique circumstances of any given request or consumer"); T-Mobile Comments at 9 (explaining that verification "would help provide increased security for customers" in some circumstances).

[158] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14135, para. 39. We adopt our proposal that account locks must be offered to all customers at no cost because we find that a customer's financial means should not dictate their access to this enhanced security measure, particularly since customers with lesser financial means may suffer the greatest consequences of SIM swap fraud. This requirement is consistent with other Commission rules governing preferred carrier freezes for Local Exchange Carriers, *see* 47 CFR § 64.1190, as well as the requirements adopted for port-out locks, *infra* section III.B.3. To simplify the ability for customers to take advantage of account

(continued….)

with more consistent and meaningful protection against SIM swap fraud, and this expectation is supported by the record, which reflects that account locks can be powerful tools against SIM swap fraud, particularly for customers that are at high-risk of being a target of the practice.[159]

42. Like the other rules we adopt today, we give wireless providers flexibility on how to comply with this measure. In particular, the record does not evince a need for us to prescribe a method or methods for customers to unlock their accounts or impose a waiting period before an unlocked account can be transferred, and as such, we decline to do so at this time. We do require, however, that the process to activate and deactivate an account lock must not be unduly burdensome for customers such that it effectively inhibits them from implementing their choice.[160] Additionally, we stress that when activated, wireless providers must not fulfill SIM change requests until the customer deactivates the lock,[161] except to the extent otherwise required by the Safe Connections Act or the Commission's rules implementing that statute.[162] We find that the account lock requirement is technically feasible, particularly given evidence that some wireless providers already offer this feature to customers.[163] Additionally, we are unpersuaded by AT&T's claim that "building a system that is capable of widespread adoption of [account locks] would entail significant carrier costs and time for questionable gain."[164] We anticipate that because

locks for SIM changes and number ports, we encourage wireless carriers to offer customers the ability to activate both locks in one step.

[159] *See* BPI/BITS Comments at 3-4 (supporting "the FCC's suggestion to place control of the ability to manage SIM changes requested by telephone and/or online access in the hands of the consumer, likely on their very device" and arguing that "this consumer-managed protection is an additional layer of security"); DC Stone Comments (Express) at 1 (arguing that the Commission should "[r]equire that account freezes be made available for any consumer phone account" as "an effective tool for concerned or savvy consumers to prevent unauthorized account activity and especially fraud, just as with credit reporting agencies"); NCLC/EPIC Comments at 11 (explaining that the ability to lock one's own account "may provide meaningful protections" and "is an excellent way for an individual consumer to guard against fraud"); *but see* AT&T Comments at 17 (stating that "[a]ccount locks can be an effective tool to increase the security of customer accounts on occasion," but opposing that carriers be required to offer them in all instances).

[160] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14135, para. 39.

[161] *Id.*

[162] *See* 47 U.S.C. § 345(b)(2) (prohibiting carriers from making valid line separation requests from survivors of domestic violence contingent on any requirement or limitation); *Publicly Released Draft Safe Connections Order* at para. 76 and 47 CFR § 64.6402(l) (requiring a covered provider to effectuate a legitimate line separation request, and any associated number port and SIM change requests, regardless of whether an account lock is activated on the account); 47 CFR § 64.6402(k) (requiring that as soon as feasible after receiving a legitimate line separation request from a survivor, a covered provider shall lock the account affected by the line separation request to prevent all SIM changes, number ports, and line cancellations other than those requested as part of the line separation request pursuant to 47 U.S.C. § 345 and the Commission's rules until the request is processed or denied).

[163] *See* T-Mobile Comments at 4 ("[F]or most types of customers, T-Mobile can institute a 'SIM change block' that helps protect the customer's SIM from being used in other devices."); NCTA Comments at 4-5 ("Wireless providers already engage in many [measures to prevent to prevent SIM swap and port-out fraud] today, including . . . providing the ability to lock or freeze wireless accounts."); CTIA Reply at 26-27 ("The record demonstrates that absent a requirement, many providers already offer account freeze options to their customers."); CCA Comments at 3-4 (describing T-Mobile's free service called "Account Takeover Protection" which "blocks unauthorized users from porting numbers and allows only the billing responsible party to turn the feature off"); *see also* Verizon, *Additional Support Information*, https://www.verizon.com/support/port-out-faqs/#setup-freeze (last visited Oct. 18, 2023) (offering a "Number Lock" service that is a customer-managed porting freeze option accessible by dialing 611 or through the MyVerizon app); T-Mobile, *Account Takeover Protection by T-Mobile*, https://www.t-mobile.com/support/plans-features/account-takeover-protection (last visited Oct. 18, 2023) (providing information on account its Account Takeover Protection feature, which "adds additional security to your account by blocking unauthorized users from transferring your lines to another wireless carrier").

[164] AT&T Comments at 17.

of these existing account lock offerings and the flexible approach we take, the rule will not be unduly costly for wireless providers to implement, and that to the extent there are costs associated with the requirement, they are outweighed by the associated benefits of preventing fraudulent activity.

43. Consistent with this flexible approach, we permit wireless providers to proactively initiate a SIM swap lock on a customer's account when a provider believes the customer may be at high risk of fraud. We are persuaded by T-Mobile's assertion that such capability is valuable because wireless providers are sometimes positioned to know when a customer is at high risk of SIM swap fraud and that this tool allows them to help customers secure their accounts.[165] However, we require that wireless providers promptly provide clear notification to the customer that the lock has been activated with instructions on how the customer can deactivate the account lock if the customer chooses, and to promptly comply with the customer's legitimate request to deactivate the account lock.[166] We also caution wireless providers that any proactive initiation of a SIM change lock must be limited in duration and extend only so long as the high risk of fraud is evident to the provider. In establishing this limitation, we intend to prohibit wireless provider abuse of SIM change locks to avoid, among other outcomes, preventing the customer from terminating service with the provider or moving to another competing provider.

44. Given the protection that account locks can provide to customers, we conclude that it should be offered to customers of both pre-paid and post-paid services.[167] We are unpersuaded by AT&T's assertion that pre-paid service is not amenable to account locks because "[s]ome prepaid customers provide little personal information when they activate their account," which could make it difficult to authenticate a customer to unlock an account.[168] Because the account lock is an optional security measure for customers, wireless providers can, if necessary, require customers to provide information to use for authentication purposes to activate the account lock.

45. We also disagree with AT&T that an account lock option "should remain a tool that carriers can choose, but are not required, to offer."[169] AT&T acknowledges that "[a]ccount locks can be an effective tool to increase the security of customer accounts on occasion," but it suggests that because "they are not needed to manage the risk of fraud in every case and for every customer," wireless providers should not be required to offer them to all customers.[170] While AT&T's approach would leave the choice of whether an account lock is necessary exclusively in the hands of wireless providers, we conclude this choice should be placed principally in the hands of the customer,[171] the party that is potentially at risk for

[165] *See* T-Mobile Comments at 2, 4.

[166] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14135, para. 39.

[167] DC Stone Comments (Express) at 1 (arguing that account locks must be available for any customer account, including pre-paid accounts); *cf.* Verizon Comments at 4 ("A service provider will have limited information about the prepaid customer, and in many cases, about the customer's device. Even so, Verizon only allows authentication using reliable, available methods, and has begun integrating systems used for postpaid customers to further align and improve our methods to prevent . . . fraudulent activity.").

[168] AT&T Comments at 17; *see also* CTIA Comments at 15 (asserting that account locks "may negatively impact pre-paid customers whose devices are lost or stolen, as the pre-paid market offers consumers the option to purchase service with less identifiable information than post-paid, and thus information that may be necessary to deactivate a freeze may not have been provided when an account is initialized. Thus this may limit a consumer's ability to remove a freeze and validate an account where the consumer does not have a working device.").

[169] AT&T Comments at 17; *see also* CTIA Reply at 26-27 (arguing that "the Commission should allow wireless providers the flexibility to facilitate choice and competition for all customers when it comes to account freezes" and not require providers to offer account locks).

[170] AT&T Comments at 17.

[171] *See* BPI/BITS Comments at 3-4 (expressing support for requiring carriers to offer account locks because it "place[s] control of the ability to manage SIM changes requested by telephone and/or online access in the hands of the consumer").

SIM swap fraud, and therefore we require providers to offer the option to all customers. Likewise, AT&T's concern that "an account lock can be a source of friction" even for a postpaid customer when the "customer forgets having placed the freeze on the account or dislikes the efforts needed to unfreeze the account"[172] is not, we conclude, a valid basis for declining to require that wireless providers offer SIM change locks. The benefits of this account security measure outweigh any potential friction, and we expect that wireless providers can take steps to mitigate any such friction if they choose, such as by providing customers with periodic reminders that they have activated the account lock and on how they can deactivate the lock.[173] We are also unconvinced by comments claiming that SIM change locks may be of limited value to customers.[174] This requirement empowers high-risk and security-minded customers to enable additional protections beyond the enhanced authentication requirements and other security measures we adopt today, and it need not be activated by a large percentage of customers for it to be valuable.

5. Tracking Effectiveness of SIM Change Protection Measures

46. We require wireless providers to track and maintain information regarding SIM change requests and their authentication measures, and to retain that information for a minimum of three years.[175] We agree with the Princeton University researchers that a tracking requirement will equip wireless providers "to measure the effectiveness of their customer authentication and account protection measures,"[176] and find that they would not otherwise be able to do so effectively without collecting such information. Consistent with recommendations in the record by the Princeton University researchers, we specifically require wireless providers to collect and maintain the following information regarding SIM change requests and authentication measures: the total number of SIM change requests, the number of successful SIM changes requests, the number of failed SIM change requests, the number of successful fraudulent SIM change requests, the average time to remediate a fraudulent SIM change, the total number of complaints received regarding fraudulent SIM changes, the authentication measures the wireless provider has implemented, and when those authentication measures change.[177] We also strongly encourage them to collect and retain any additional information that will help them measure the effectiveness of their customer authentication and account protection measures. We find that the three-year retention period is appropriate because it allows providers to track the effectiveness of their measures over time and ensures the information is available for a sufficient time should the Commission request it for review.

[172] AT&T Comments at 17.

[173] Because of the authentication challenges for pre-paid customers and the potential friction for customers who may not want SIM changes to be more difficult, we decline to require account locks be activated by default, on an opt-out basis, as BPI/BITS suggests. BPI/BITS Comments at 3-4.

[174] NCLC/EPIC Comments at 11-12 ("Disclosures and the ability to freeze one's account are valuable only to those consumers who are savvy enough to a) understand the dynamics involved in freezing, b) understand that the benefits of freezing outweigh the extra burdens imposed (such as requiring that the consumer go through a series of steps to unfreeze the account, and c) actually follow through and freeze one's account."); Verizon Comments at 5 ("[A]n account freeze or lock may be superfluous or of limited interest to consumers given the corresponding need for rigorous authentication to remove the freeze or lock.").

[175] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14136, para. 43 (seeking comment on whether to require carriers to track data regarding SIM swap complaints).

[176] *See* Princeton Comments at 12.

[177] *See id.*

47. We disagree with CTIA's assertions that a recordkeeping requirement will divert resources from combating incidences of SIM swap fraud.[178] Instead we find that this data tracking requirement is critical to wireless providers' efforts to keep ahead of evolving fraud techniques. And the record reflects that some wireless providers already track and analyze information regarding SIM swap fraud and their account protection measures to improve those measures,[179] indicating that this is a practical and cost-effective practice. Thus, while we recognize that this recordkeeping requirement may not be without cost, particularly for wireless providers who do not already collect such information, we find that the benefits of this requirement far exceed any potential costs.

48. We agree with CTIA that the data tracking and retention requirements should only be prospective in nature,[180] and as such, we make clear that our rule does not obligate wireless providers to research and collect historic data. We conclude that including historic data in the data tracking requirements we adopt would be burdensome, or even impossible, for small wireless providers and those who do not already track this information.[181]

49. We decline to adopt reporting and audit requirements in conjunction with our data tracking requirement,[182] but we do require wireless providers to make the information they collect available to the Commission upon request.[183] Although regular reporting and audit requirements can improve wireless provider incentives and accountability, we do not find that such measures are necessary at this time in light of the other measures we adopt today and providers' ongoing commitment to be vigilant in combating fraud.[184] We maintain the ability to obtain collected information from wireless providers as needed, not only as a potential tool to evaluate whether providers are implementing sufficient measures to address SIM swap fraud, but also to evaluate whether the specific requirements we adopt today continue to be effective or in need of updates to address the evolution of fraud techniques.

---

[178] CTIA Reply at 24-25 ("Others call for overly onerous reporting and recordkeeping requirements. These types of rules would require wireless providers to divert resources from protecting customers to looking in the rearview mirror.").

[179] *See* AT&T Comments at 2 & 7-8 (indicating that it has tracked the total instances of SIM swap fraud and that it "continually assesses the effectiveness of its countermeasures and refines them over time as needed"); T-Mobile Comments at 6 ("T-Mobile engages in ongoing, proactive threat evaluation, and information collection on threats and fraud for internal purposes."); CTIA Reply at 1 (stating that its members report tracking the number of legitimate SIM swaps).

[180] *Compare* CTIA Reply at 24-25 (explaining that if the Commission adopts recordkeeping requirements, it should be prospective) *with* Princeton Comments at 12 ("We encourage the Commission to also consider collecting a limited amount of historical data on SIM swaps and port-outs, to understand how trends in customer use and fraudulent activity are affected by changes in authentication requirements.").

[181] *See, e.g.*, CTIA Reply at 25.

[182] *See* Princeton Comments at 12 (suggesting that carriers should be required to track and report information on SIM swap and port-out fraud to the Commission); NCLC/EPIC Comments at 6 (arguing that carriers should include information regarding SIM swap and port-out fraud in annual reports to the Commission); Robert Ross Comments at 8 (arguing that that "[c]arriers must be required to report all SIM swaps and Port-outs on a monthly basis to the FCC" and undergo annual independent audits).

[183] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14136, para. 43. Because the information we require wireless providers to collect does not include personally identifiable information (PII) or CPNI, wireless providers will not be required to provide PII or CPNI in response to Commission requests for this information, but the Enforcement Bureau may request PII or CPNI in the course of a specific investigation.

[184] AT&T Comments at 1 ("AT&T is committed to protecting its customers and deterring bad actors intent on misusing processes designed for consumer benefit to inflict harm."); T-Mobile Comments at 8 ("T-Mobile remains vigilant in its efforts to evolve its safeguards to prevent fraud."); CTIA Comments at 3 ("The wireless industry and the Commission share the goal of protecting consumers from fraud—full stop.").

Consequently, we find that there are insufficient benefits of a regular reporting requirement to outweigh the potential costs.

6. Safeguards on Employee Access to CPNI

50. We require all telecommunications carriers to establish safeguards and processes so that employees who interact directly with customers are unable to access CPNI until after a customer has been properly authenticated.[185] We find, based on the record before us, that requiring telecommunications carriers to limit employee access to CPNI until after a customer has been properly authenticated will help to minimize the incidences of SIM swap fraud by preventing customer service representatives from inadvertently or intentionally assisting bad actors in fraudulent schemes.[186] We are persuaded that, even with the customer service representative training requirements we adopt today,[187] allowing employees who interact directly with customers to access CPNI prior to proper authentication of a customer is unnecessary and possibly "invites adversaries to exploit sympathetic, inattentive, or malicious customer service representatives for account access."[188] While we anticipate that employees will comply with training requirements in good faith, "[t]here should be no opportunity for a representative to give a hint or a free pass" that will help bad actors commit fraud.[189] We therefore conclude that requiring telecommunications carriers to establish safeguards and processes so that employees who interact directly with customers are unable to access CPNI until after a customer has been properly authenticated—"a straightforward fix"[190] and standard data security best practice[191]—will provide meaningful protection in helping to combat SIM swap fraud. We find that the benefits of this requirement outweigh any potential costs, and that any such costs will be mitigated by allowing telecommunications carriers flexibility to determine the particular safeguards and processes that will prevent employees from accessing CPNI until after a customer has been properly authenticated.

51. We decline to adopt other suggested employee safeguards that are overly prescriptive and for which the costs outweigh the benefits. In the *SIM Swap and Port-Out Fraud Notice* we sought comment on other ways to avoid employee malfeasance, such as requiring two employees to sign off on every SIM change.[192] Although we anticipate that two-employee sign off could be an effective account protection mechanism and encourage wireless providers to use this procedure when appropriate,[193] we are persuaded by AT&T's argument that requiring this procedure for every SIM change would be a significant burden on legitimate SIM change requests given the uncertainty regarding whether it would

[185] *See* Appx. A (revised 47 CFR § 64.2010(a)); *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14134, para. 38.

[186] *See, e.g.*, Princeton Comments at 8; NCLC/EPIC Comments at 8-9.

[187] *See infra* section III.C(establishing requirements that carriers develop and implement training for customer service representatives to specifically address fraudulent SIM change and port-out attempts, complaints, and remediation).

[188] Princeton Comments at 9.

[189] *Id.*

[190] *Id.*

[191] *See, e.g.*, NCLC/EPIC Comments at 8-9 (explaining that minimizing access to and retention of customer data is a security best practice); Princeton Comments at 7-8 (explaining that access to CPNI prior to authorization "is an unnecessary exposure of customer data and a violation of the information security principle of minimizing system permissions"); *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last updated October 2016) ("Scale down access to data. Follow the 'principle of least privilege.' That means each employee should have access only to those resources needed to do their particular job.").

[192] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14134, para. 38.

[193] Verizon Comments at 3 ("Two-employee sign-off can be appropriate in circumstances when other authentication methods are unavailable, and Verizon trains select employees to assist customers this way.").

prevent SIM swap fraud in most instances,[194] and therefore decline to adopt it. We also reject several other requirements proposed in the record concerning customer service representatives who perform SIM changes. Specifically, a mandate that employees who perform SIM swaps be subject to enhanced background checks[195] may be financially and practically infeasible for large and small wireless providers alike, and could create an incentive for providers to reduce the number of employees capable of performing SIM changes, which would slow the processing of legitimate changes. Requiring employees to swipe a company badge when entering secure facilities is a good practice that we encourage wireless providers to adopt,[196] but the record does not address how this requirement would serve to prevent SIM swap fraud. The proposal to require employees to sign a restrictive confidentiality agreement is faulty for the same reason.[197] Moreover, a proposed restriction on use of performance incentives[198] is overly broad, could stifle competition, and might prevent customers from accessing special offers. Finally, we decline to adopt a proposal that wireless providers "be required to have heightened SIM swap customer care during [weekends and evenings]."[199] We find that providers are best positioned to implement procedures tailored to the level of risk at any given time and should have the flexibility to adjust their practices to address the evolving nature of fraudulent activity.

7. Telecommunications Carriers' Duty to Protect CPNI

52. While the record shows that some wireless providers have implemented CPNI security practices beyond those required by current rules,[200] SIM swap fraud persists. We are also concerned that some wireless providers may view the protection measures we adopt today as sufficient, rather than baseline, protections against SIM swap fraud. To ensure that wireless providers adapt their security practices on an ongoing basis to address evolving techniques used by bad actors to commit SIM swap fraud,[201] we take this opportunity to remind all telecommunications carriers of their statutory duty to "protect the confidentiality of proprietary information of, and relating to . . . customers,"[202] and their continuing preexisting legal obligation to "take reasonable measures to discover and protect against

[194] AT&T Comments at 18 ("Such a step would be time-intensive, increasing the length of the SIM swap process, and would remain susceptible to social engineering and collusion. Also, it is unclear how the second employee would evaluate the transaction separately from the first employee, or what would happen if, as can occur, a second employee is not available. Last, the frequency (and thus sheer number) of legitimate SIM changes makes this suggestion infeasible in practice.").

[195] Robert Ross Comments at 7.

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *Id.* at 8 ("SIM swappers come out on weekends and evenings when they know that customer service at mobile carriers, banks and cryptocurrency exchanges are closed. Carriers must be required to have heightened SIM swap customer care during these times.").

[200] *See, e.g.*, AT&T Comments at 4-7 (explaining that "AT&T employs a diverse set of measures to help thwart these bad actors – above and beyond existing regulatory requirements and those proposed in the NPRM," including scanning an in-store customer's ID with technology to verify its authenticity, utilizing data analytics to assess a customer's risk for fraud, and conducting customer education); Better Identity Coalition at 4 ("Notably, two major mobile network operators (MNOs) already support FIDO authentication for their customers, meaning that it is widely used in customer-facing accounts today."); T-Mobile Comments at 6 ("T-Mobile participates in efforts with other stakeholders to address verification issues and stay at the cutting edge of fraud risk management.").

[201] *See* Verizon Comments at 1-2, 5; AT&T Comments at 2 & 11; CCA Comments at 4-5; CTIA Comments at 10-11; CTIA Reply at 15-16; Verizon Comments at 5; Somos Comments at 2.

[202] 47 U.S.C. § 222(a).

attempts to gain unauthorized access to CPNI."[203] Consistent with the Commission's approach in the *2007 CPNI Order*,[204] we conclude that these existing legal obligations necessarily obligate telecommunications carriers to proactively and regularly review and monitor their policies and procedures to ensure that they continue to be effective at addressing evolving fraud techniques against customer accounts and services—including SIM swap and port-out fraud[205]—and to conduct analyses of fraud incidents to determine how the fraud occurred and implement measures to prevent such tactics from being successful again in the future.[206]

B. Strengthening the Commission's Number Porting Rules to Protect Consumers

53. Given the potential for consumer harm from port-out fraud, we conclude that the time is ripe to strengthen our number porting rules with baseline measures to increase the protections for customers against fraudulent port-outs. As with our new SIM change rules, the backbone of our new number porting rules is a requirement that wireless providers use secure methods to authenticate customers that are reasonably designed to confirm a customer's identity prior to effectuating number ports, and we also require wireless providers to notify customers of port-out requests and allow customers to lock their accounts to prevent port-outs.[207] To future-proof our requirements, we give wireless providers flexibility in how to implement them. We anticipate that these new rules will work together to provide meaningful protection to customers while preserving the efficient and effective processing of port-out requests that promotes customer choice and competition. As with our new SIM change rules, we apply these new requirements exclusively to providers of CMRS, as defined in section 20.3 of Title 47 of the Code of Federal Regulations,[208] including resellers of CMRS, as the record shows that port-out fraud

[203] 47 CFR § 64.2010(a); *see also* NCLC/EPIC Comments at 9 ("Providers must take affirmative measures to discover and protect against fraudulent activity beyond what is specifically dictated by the Commission's rules.").

[204] *2007 CPNI Order*, 22 FCC Rcd at 6945-46, paras. 33 & 35 (making clear that the adoption of rules designed to protect against pretexting "does not relieve carriers of their fundamental duty to remain vigilant in their protection of CPNI" and expressing the Commission's "expectation that carriers will take affirmative measures to discover and protect against activity that is indicative of pretexting beyond what is required by the Commission's current rules").

[205] *See, e.g.*, AT&T Comments at 7 ("AT&T's suite of tools is not static. AT&T continually assesses the effectiveness of its countermeasures and refines them over time as needed."); T-Mobile Comments at 6 ("T-Mobile engages in ongoing, proactive threat evaluation, and information collection on threats and fraud for internal purposes. For example, T-Mobile gathers and acts on threat intelligence about cybercriminals potentially targeting wireless carriers and customers, conducts penetration tests of our systems, and engages stakeholders to understand emerging attack patterns. Further, as bad actors pivot to new methods and the account takeover fraud landscape changes, T-Mobile implements new strategies to address both known and potential fraud techniques.").

[206] *See* AT&T Comments at 7 ("AT&T conducts routine forensic analysis of unauthorized SIM swaps and port-outs to assess the root cause and evaluate whether new or different countermeasures are appropriate to enhance security. This assessment has resulted in process changes, implementation of new security procedures, and more to guard against threats."); NCLC/EPIC Comments at 6 (arguing that upon being notified of fraud, carriers should establish "[a] detailed explanation of the fraud, along with an analysis of what measures the provider has taken to prevent a repeat of this breach").

[207] *See* Appx. A (adding 47 CFR § 52.37).

[208] *See supra* para. 25.

is focused on mobile wireless customers.[209] We likewise require wireless providers to implement these rules with respect to customers of both pre-paid and postpaid services.[210]

1. Customer Authentication Requirements

54. We revise our porting rules to require that wireless providers use secure methods to authenticate customers that are reasonably designed to confirm a customer's identity before completing a port-out request,[211] except to the extent otherwise required by the Safe Connections Act or the Commission's rules implementing that statute.[212] Consistent with our new SIM change authentication rules,[213] we require wireless providers to regularly, but not less than annually, review and, as necessary, update their customer authentication methods to ensure those methods continue to be secure.[214]

55. As in the SIM change context, we are persuaded by commenters that a general security authentication standard will best allow wireless providers the flexibility to respond to advances in the technology and tactics used by bad actors, providing the greatest protection for customers, and enabling providers to implement authentication methods in ways that work best for the particular services they offer.[215] The record reflects that the benefits of allowing wireless providers to determine the best method for authenticating customers outweigh speculative concerns that absent standardized authentication methods, nationwide providers could arbitrarily determine which authentication methods or controls are sufficient before effectuating ports.[216] We also agree with CCA that our approach will better serve small

[209] *See, e.g.*, AT&T Comments at 1 (noting that "SIM swaps and port-outs are, in short, integral features of the competitive wireless marketplace"); CCA Comments at 1 (explaining that port-out fraud is a method malicious actors use to steal mobile accounts); CTIA Comments at 1-2 (discussing port-out fraud exclusively in the context of wireless services); NCLC/EPIC Comments at 2 (noting that "American cell phone users . . . are extremely vulnerable to having their telephone numbers hijacked by fraudsters through the process of SIM swapping and port-out fraud"); NCTA Comments at 1 (explaining that with port-out fraud, a bad actor "ports the customer's mobile phone number to the account with the new carrier controlled by the bad actor").

[210] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14141, para. 55.

[211] *See id.* at 14139-41, paras. 53-56 (seeking comment on whether and how to authenticate customers for port-out requests).

[212] The Safe Connections Act prohibits wireless providers from making a line separation contingent on a prohibition or limitation on number portability, provided such portability is technically feasible. 47 U.S.C. § 345(b)(2)(D). The Commission's rules adopted today implementing the Safe Connections Act require covered providers to attempt to authenticate, using multiple authentication methods if necessary, that a survivor requesting a line separation is a user of a specific line or lines. *See Publicly Released Draft Safe Connections Order*, para. 52. Covered providers must use methods that are reasonably designed to confirm the survivor is actually a user of the specified line(s) on the account when the survivor is not the primary account holder or a designated user. *See id.* To the extent this requirement differs from other authentication requirements, including those in 47 CFR § 64.2010, the line separation authentication requirements the Commission adopts to implement 47 U.S.C. § 345 serve as an exception to those other requirements. *See id.*

[213] *See supra* para. 27.

[214] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14132, para. 27 (seeking comment on whether we should adopt a flexible standard requiring heightened authentication measures for SIM swap requests).

[215] *See supra* para. 29 (finding that in the SIM change context, readily available biographical information, account information, recent payment information, and call detail information do not constitute secure methods of authentication); 47 CFR § 64.2010(b).

[216] *Compare* T-Mobile Comments at 12-13 (stating that "flexibility to offer various secure methods of customer authentication . . . will promote innovation and improved security for customers"); CTIA Reply at 15-16 ("Flexibility is a critical attribute in any authentication standard: it will help prevent authentication practices from lagging behind bad actor tactics, it will facilitate continued improvements in authentication practices, and it will help providers be able to continue to meet customer needs."); CCA Comments at 5 (explaining that flexibility will allow carriers to adopt future authentication technologies that "prove[] to be more effective or secure than today's

(continued….)

wireless providers by permitting them to "use technologies that are reasonably available and have choice in the approach to take in authenticating their customers."[217] Additionally, as we concluded with regard to authentication for SIM changes, this flexible approach should resolve concerns about authenticating customers of pre-paid accounts.[218]

56. We are mindful of the potential effect on competition of our new customer authentication requirements, and thus, we require that the secure authentication methods wireless providers adopt accommodate the needs of the broad spectrum of customers they may serve, including those who do not have data plans or data-enabled devices, have varying degrees of technological literacy, or have disabilities or accommodation needs.[219] To illustrate, we observe that wireless providers may find requiring a one-time port-out PIN obtained through a provider app is an effective means for authenticating customers with a data-enabled smart phone, but that authentication measure may not be a feasible option for customers without data plans or smartphones, or for those customers who are unable to navigate the technology. As such, this requirement may necessitate the use of multiple authentication methods, such as in-person authentication using government-issued identification, over-the-phone authentication, or alternative methods for individuals with disabilities.[220]

---

technologies"); Princeton Comments at 4 ("We strongly agree that the Commission's customer authentication rules should not be technically prescriptive. Authentication methods and security practices continue to evolve, and carriers should be welcome—and encouraged—to adopt innovative safeguards."); Verizon Comments at 10-11 ("[P]roviders should retain the flexibility they enjoy today to nimbly adopt new authentication safeguards to stay ahead of bad actors."); *with* RWA Comments at 12-13 (raising concerns that without a "set of uniform authentication standards" nationwide carriers could "arbitrarily determine which authentication methods or controls are sufficient" thereby potentially increasing costs, creating "barriers for small and rural providers," or allowing nationwide carriers to "refuse ports from smaller providers deemed 'unsecure'"). We note also that under the Act and our existing rules, all carriers are required to complete legitimate ports, *see supra* para. 14, and that our new customer authentication requirements do not give carriers the authority to make determinations about the sufficiency of another carrier's authentication methods—that responsibility will belong to the Commission, and we will address any concerns regarding the adequacy of authentication methods, as well as inappropriate port denials, as needed.

[217] CCA Comments at 5 ("The Commission should also keep in mind the constraints with which many small carriers operate against in adopting security measures. Smaller carriers may have more limited app or e-commerce platforms, and may not currently have the capability, for example, to generate a one-time port out PIN via an app on a 24/7/365 basis."); *but see* ID.me Comments at 6-7 (describing its 530 commercial partners, many of which are "smaller businesses with smaller use cases" and asserting that "[c]omplying with NIST guidelines does not pose any difficulties for smaller providers when the integration is enabled by a turnkey, SaaS, credential service provider operating with open protocols").

[218] *See* CTIA Comments at 14-15 (noting that "fighting fraud in the pre-paid context is different than in the post-paid context" and that "providers ordinarily do not collect or have detailed identity information for pre-paid customers"); T-Mobile Comments at 8 (stating that "[p]repaid service generally does not require identity validation for account set-up"); CCA Comments at 6 (noting that pre-paid customers "often do not provide an accurate address or other identifying information, making it difficult for carriers to authenticate an account request"); CTIA Comments at 19-20 (noting that a flexible approach will better serve customers, including pre-paid customers).

[219] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14139-41, paras. 53-56 (seeking comment on customer authentication requirements); NCLC/EPIC Comments at 8 (recognizing that "online authentication is not a viable option for all consumers, especially senior consumers who may not always be technologically savvy" or "[l]ow-income households and households of color [that] are also likely to have limited bandwidth available to use on their mobile phones, making online authentication more difficult for them"); CCA Comments at 7 ("CCA members report experience with potential incoming customers who are unable to find the port PIN provided by their current provider and experience significant frustration" and "especially those who are older or less familiar with technology, may be deterred from selecting a provider who may offer a better service"); Verizon Comments at 6 (noting that in-store customers may be less tech savvy and so flexibility with authentication is necessary).

[220] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14131, 14146, paras. 25-26 & 73. *See* 47 CFR §§ 6.3(a)(1)(i) & 14.21(b)(1)(i) (requiring carriers to "[p]rovide at least one mode that does not require user vision" to

(continued….)

57. We do not anticipate that using secure methods to authenticate a customer requesting a port-out will be burdensome to wireless providers or unreasonably delay the processing of port-out requests. The record reflects that many wireless providers have already developed and implemented some form of customer authentication for port-out requests.[221] The approach we adopt today will allow wireless providers to continue using or building upon what is already working in the industry, helping to streamline implementation and costs. We expect wireless providers to design and implement customer authentication processes for port-out requests that minimize porting delays and maintain the industry agreed-upon two-and-a-half hour porting interval for wireless ports.[222]

2. Customer Notification of Port-Out Requests

58. We also revise our numbering rules to require wireless providers to immediately notify their customers whenever a port-out request is made, delivered in accordance with customer preferences, if indicated,[223] and specify that the notification must be delivered before a provider effectuates a port, except to the extent otherwise required by the Safe Connections Act of 2022 (47 U.S.C. § 345) or the Commission's rules implementing that Act.[224] We require that wireless providers notify their customers "immediately" of a porting request to not only ensure that porting requests are processed efficiently, but also help alert customers quickly to potential fraud to allow them to mitigate damages and inconvenience

operate a phone or use an account); 47 CFR §§ 6.3(a)(1)(iv) & 14.21(b)(1)(iv) (requiring carriers to "[p]rovide at least one mode that does not require user auditory perception" to operate a phone or use an account); 47 CFR §§ 6.3(a)(1)(ix) & 14.21(b)(1)(ix) (requiring carriers to "[p]rovide at least one mode that does not require user speech" to operate a phone or use an account).

[221] *See, e.g.*, AT&T Comments at 6-7 (describing its routine use of "a one-time PIN delivered via SMS message or an outbound voice call to a postpaid customer's device for enhanced customer validation," and its "Number Transfer PIN process to validate postpaid port-out transactions"); CCA Comments at 3-4 (describing U.S. Cellular's assigning of a PIN code to each customer that is used for customer authentication); Better Identity Coalition Comments at 4 (noting that "two major mobile network operators already support FIDO authentication for their customers"); NCTA Comments at 4-5 (describing authentication measures some wireless providers already use, including account PINs); T-Mobile Comments at 4 ("T-Mobile offers various customer authentication options, which may vary based on customer, account, and device characteristics. T-Mobile customers set up an individual 6-to-15 digit PIN that can be used to verify the customer's identity when calling customer service. . . . T-Mobile customers must provide their PIN when requesting a port-out associated with that account. Most customers that choose to create a T-Mobile ID for use on My.T-Mobile.com or with the My T-Mobile app have the option of setting up multi-factor authentication ('MFA') using methods including security questions, SMS, or device-based biometrics such as Face ID or fingerprint recognition on devices that support such features. T-Mobile uses MFA, consistent with the FCC's rules, for validating customer identity and verifying the legitimacy of account changes."); Verizon Comments at 8-9 (describing current authentication measures, including a transaction-specific "Number Transfer PIN" and notifying customers of port requests via text message and email).

[222] *See Wireless Number Portability Order*, 18 FCC Rcd at 20979, para. 26; North American Numbering Council Wireless Number Portability Subcommittee Report on Wireless Number Portability Technical, Operational, and Implementation Requirements Phase II, CC Docket No. 95-116 at 13 (filed Sept. 26, 2000).

[223] For example, this would include delivering a notification in the language of the customer's choosing, if the wireless provider permits communications preferences in other languages and the customer has previously indicated such choice.

[224] Appx. A (47 CFR § 52.37(c)); *see also Publicly Released Draft Safe Connections Order*, para. 97 ("To the extent that a survivor initiates a port-out request with a new service provider for a line that is the subject of an in-process line separation request, we prohibit the current service provider from notifying the account holder of the request to port-out that number until after the line separation request has been completed."); 47 CFR § 64.6402(i) (a covered provider shall not notify a primary account holder of a request by a survivor to port-out a number that is the subject of a line separation request).

resulting from fraudulent or inadvertent port-outs.[225] The notification requirement will provide a uniform safety measure for all port-out requests across the mobile wireless industry, which we anticipate will reduce the instances of port-out fraud.[226]

59. As with SIM change notifications, we decline to prescribe particular methods for providing port-out notifications or particular content and wording for these notifications, but do require that the notification methods be reasonably designed to reach the customer associated with the account and that the content and wording use clear and concise language that provides sufficient information to effectively inform a customer that a port-out request involving the customer's number was made.[227] We recognize that wireless providers are in the best position to determine which notification methods and what content and wording will be most effective at notifying customers of port-out requests and potential fraud under the particular circumstances, including the real-world security needs of the transaction, and the technical capabilities, accessibility needs, or broadband access of individual customers. As such, we encourage wireless providers to leverage existing notification methods that are reasonably designed to reach the customer associated with the account,[228] and to adopt new notification methods as they are developed to stay responsive to evolving fraud schemes.

60. On balance, we find that benefits accrued from early warning to customers of potential fraudulent account activity outweigh any potential burdens imposed on wireless providers by this notification requirement. First, we find that customer notification of port-out requests is unlikely to prevent or unreasonably delay customer porting requests, as we require "immediate" notification and do not require a delay or customer verification or acknowledgement of that notification before continuing the porting-out process. Second, because wireless providers are already familiar with notifying customers regarding changes to their accounts,[229] and in many cases likely already notify customers of port-out requests,[230] we anticipate that wireless providers will face low burdens in implementing today's customer notification requirement for port-out requests. We also expect that these existing notification systems can

[225] *See* Princeton Comments at 7 (noting that "notice is essential, so that a customer can take prompt action to protect their telecommunications account, their other accounts, and their devices"); Prove Comments at 6 (supporting timely notice for high risk events such as port-out requests so customers can "be afforded the opportunity to prevent account takeovers before they are completed").

[226] For the same reasons we raised in the SIM change context, we decline to impose a blanket yes/no verification requirement for authentication attempts. *See supra* para. 40; *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14139, para. 51.

[227] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14141-42, paras. 57 (seeking comment on port-out notification requirements).

[228] Such measures may include, but are not limited to, live or automated telephone calls, text messages, emails, or push notification through wireless provider software applications. Verizon Comments at 6 ("Providers also should have discretion to use a push notification together with supplemental verification methods to stop a high risk transaction.").

[229] *See* AT&T Comments at 6 (explaining that for transactions meeting a certain threshold of AT&T's "risk model," it will send one-way SMS notifications of a SIM change request, and for transactions meeting a higher risk threshold, it will require customers confirm the SIM change request via an SMS notification); T-Mobile Comments at 4 (noting that as part of its efforts to "help customers secure their accounts, T-Mobile notifies customers of account changes and requests"); Verizon Comments at 6 ("Verizon already employs (or is on track to employ) many of the methods identified in the NPRM, such as notifying customers of high-risk SIM change authentication attempts, failed or otherwise, and of other account changes."); CTIA Comments at 18 (explaining that "there are many instances where notifications to consumers are appropriate and providers can and do make reasonable efforts to provide them"); 47 CFR § 64.2010(f); *2007 CPNI Order*, 22 FCC Rcd at 6942, para. 24.

[230] *See, e.g.*, CCA Comments at 3-4 (describing the current procedures that T-Mobile, U.S. Cellular, and GCI use to notify customers of a change to their account or port-out request, and that other members are "similarly adopting heightened security measures"); *see also Wireless Number Portability Order*, 18 FCC Rcd at 10975-76, paras. 14-16.

be leveraged to help minimize any potential costs associated with notifying customers of port-out requests. Third, we disagree with AT&T's assertion that customer notification of port-out requests will result in notice fatigue, undermining its efficacy.[231] Nothing in the record supports the notion that customers request port-outs at such a rate that, upon the adoption of this rule, wireless providers will be forced to inundate their customers with the required notifications. As such, we conclude that the significant benefits of alerting customers to potential fraudulent account activity outweighs any speculative negative impacts on wireless providers or customers.

3. Account Locks for Port-Outs

61. For the same reasons explained above with respect to SIM change requests,[232] we require wireless providers to offer their customers, at no cost, the ability to lock or freeze their accounts to stop port-outs.[233] We anticipate that this requirement will provide customers with more consistent and meaningful protection against fraudulent port-outs. The record reflects that account locks can be powerful tools against fraudulent port-outs, particularly for customers that are at high-risk of being a target of the practice.[234] As in the SIM swap context,[235] we conclude that it should be offered to customers of both pre-paid and post-paid services,[236] and that this requirement is feasible for both categories of customers despite assertions to the contrary.[237]

62. Like the other rules we adopt today, we give wireless providers flexibility on how to comply with the measure.[238] In particular, the record does not evince a need for us to prescribe a method

[231] AT&T Comments at 15 (noting that mandating notice when it is not necessary would lead to frequent notifications that would leave customers "numb or immune to them or tire of [them] and consciously choose to ignore them, thus undermining all value they might otherwise have when the threat of fraud is real"); *see also* CTIA Comments at 18 (asserting that notifications can be appropriate in "many instances" but that notifications "must be weighed against other goals, and in general, avoid unnecessary friction in the user experience or other unintended consequences, such as notice fatigue").

[232] *See supra* section III.A.4..

[233] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14141-42, para. 57.

[234] *See, e.g.*, South Carolina Department of Consumer Affairs Comments at 2 ("Carriers should also offer customers the option to lock port requests, similar to an account freeze, in order to prohibit unauthorized requests."); DC Stone Comments (Express) at 1 (arguing that account locks are "an effective tool for concerned or savvy consumers to prevent unauthorized account activity and especially fraud, just as with credit reporting agencies"); NCLC/EPIC Comments at 11 (explaining that "the ability to freeze one's own account is an excellent way for an individual consumer to guard against fraud").

[235] *See supra* section III.A.4.

[236] *See, e.g.*, DC Stone Comments (Express) at 1 (arguing that account locks must be available for any customer account, including pre-paid accounts); *cf.* Verizon Comments at 4 ("A service provider will have limited information about the prepaid customer, and in many cases, about the customer's device. Even so, Verizon only allows authentication using reliable, available methods, and has begun integrating systems used for postpaid customers to further align and improve our methods to prevent . . . fraudulent activity.").

[237] *See, e.g.*, CTIA Comments at 14-15 (asserting that account locks "may negatively impact pre-paid customers whose devices are lost or stolen, as the pre-paid market offers consumers the option to purchase service with less identifiable information than post-paid, and thus information that may be necessary to deactivate a freeze may not have been provided when an account is initialized. Thus this may limit a consumer's ability to remove a freeze and validate an account where the consumer does not have a working device"); AT&T Comments at 17 (noting that "an account lock would likely create more of a burden than a benefit for prepaid customers and their carriers" given the discrepancy in information provided, but supporting an optional account freeze). Because the account lock is an optional security measure for customers, carriers can, if necessary, require customers to provide information to use for authentication purposes to activate and deactivate the account lock.

[238] *See* AT&T Comments at 2-3, 12 (arguing, generally, that the Commission should not "[prescribe] specific methods wireless carriers must employ to combat fraudulent SIM swaps and port-outs"); CTIA Reply at 26-27 (continued….)

or methods for customers to unlock or unfreeze their accounts or impose a waiting period before an unlocked account can be transferred, and as such, we decline to do so at this time. Although we do not prescribe the exact form of the account lock mechanism wireless providers must adopt, the process to activate and deactivate an account lock must not be unduly burdensome for customers such that it effectively inhibits them from implementing their choice.[239] We stress that when activated, wireless providers must not fulfill port-out requests until the customer deactivates the lock,[240] except to the extent otherwise required by the Safe Connections Act or the Commission's rules implementing that statute.[241]

63. Consistent with this flexible approach, and as we did with the SIM change rules, we permit wireless providers to proactively initiate a port-out lock on a customers' account when they believe a customer may be at high risk of fraud, so long as providers promptly provide clear notifications to those customers that a lock has been activated with instructions on how the customers can deactivate account locks if they choose and promptly deactivates the account lock upon receipt of the customer's legitimate request to do so.[242] We also caution wireless providers that any proactive initiation of a port-out lock must be limited in duration and extend only so long as the high risk of fraud is evident to the provider. In establishing this limitation, we intend to prohibit wireless provider abuse of port-out locks to avoid, among other outcomes, preventing the customer from terminating service with the provider or moving to another competing provider.

64. As with account locks for SIM changes,[243] given that several wireless providers already voluntarily offer account locks to all their customers,[244] and coupled with the flexible approach we adopt,

("While the Commission's rules should allow for port freeze options, the rules should also be flexibly designed to recognize that freezes are not always appropriate.").

[239] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14141-42, para. 57 (seeking comment on port-out lock requirements).

[240] *Id.*

[241] *See* 47 U.S.C. § 345(b)(2)(D) (prohibiting carriers from making valid line separation requests from survivors of domestic violence contingent on any requirement or limitation, including restrictions on number portability); *Publicly Released Draft Safe Connections Order* at para. 76 and 47 CFR § 64.6402(l) (requiring a covered provider to effectuate a legitimate line separation request, and any associated number port and SIM change requests, regardless of whether an account lock is activated on the account); 47 CFR § 64.6402(k) (requiring that as soon as feasible after receiving a legitimate line separation request from a survivor, a covered provider shall lock the account affected by the line separation request to prevent all SIM changes, number ports, and line cancellations other than those requested as part of the line separation request pursuant to 47 U.S.C. § 345 and the Commission's until the request is processed or denied); 47 CFR § 64.6404(a).

[242] *See supra* para. 43; *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14141, para. 57 (seeking comment on port-out lock requirements).

[243] *See supra* para. 42.

[244] *See, e.g.*, CCA Comments at 3-4 (describing T-Mobile's free service called "Account Takeover Protection" which "blocks unauthorized users from porting numbers and allows only the billing responsible party to turn the feature off"); CTIA Comments at 3-4 (noting that "examples of the variety of tactics used to combat SIM swapping and port-out fraud include . . . the ability to lock or freeze wireless accounts"); CTIA Reply at 26-27 ("The record demonstrates that absent a requirement, many providers already offer account freeze options to their customers."); T-Mobile Comments at 4 & 11 ("Qualifying customers may wish to enable safeguards such as setting up account takeover protection—a free feature that prohibits unauthorized users from porting the customer's phone line to another wireless carrier."); NCTA Comments at 4-5 ("Wireless providers already engage in many [measures to prevent to prevent SIM swap and port-out fraud] today, including . . . providing the ability to lock or freeze wireless accounts."); *see also* Verizon, *Additional Support Information*, https://www.verizon.com/support/port-out-faqs/#setup-freeze (last visited Oct. 18, 2022) (offering a "Number Lock" service that is a customer-managed porting freeze option accessible by dialing 611 or through the MyVerizon app); T-Mobile, *Account Takeover Protection by T-Mobile*, https://www.t-mobile.com/support/plans-features/account-takeover-protection (last visited

(continued….)

we are unpersuaded by AT&T's claim that implementing account lock offerings will be unduly costly and time-consuming for wireless providers.[245] To the extent there are costs associated with the requirement, we find that they are outweighed by the benefits.

4. Wireless Port Validation Fields

65. After review of the record, we decline to codify the wireless port validation fields.[246] We also decline to require wireless providers to implement a customer-initiated passcode field for all wireless-to-wireless number porting requests.[247] Currently, the mobile wireless industry uses four data fields of customer-provided information to validate a wireless-to-wireless porting request: telephone number, account number, five-digit ZIP code, and passcode (if applicable).[248] In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on whether we should "codify the types of information carriers must use to validate simple wireless-to-wireless port requests."[249] While some commenters did not oppose codification of some of the customer-provided wireless data fields, they preferred that the Commission continue to give wireless providers the flexibility to adjust to business and customer needs.[250] We are persuaded by the record that separate codification of the customer-provided data fields for validation of wireless-to-wireless ports is not necessary at this time, as we have been provided no evidence that wireless providers are not complying with the validation obligations imposed in the *Four Fields Declaratory Ruling*.[251] As such, we decline to separately codify the customer-provided wireless-to-wireless port validation fields at this time.

C. Additional Consumer Protection Measures

66. In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on whether we should adopt additional measures to address the problems associated with SIM swap and port-out fraud.[252] As discussed below, we require that wireless providers inform customers of any account protection mechanisms the provider offers, ensure that customer service representatives are trained to recognize bad actors' attempts at these fraudulent schemes, and deliver timely resolution of SIM swap and port-out fraud when it does occur. We decline, however, to establish a working group to further study and develop solutions to address the harms of SIM swap and port-out fraud. We also decline to adopt other proposals

Oct. 18, 2023) (providing information on account its Account Takeover Protection feature, which "adds additional security to your account by blocking unauthorized users from transferring your lines to another wireless carrier").

[245] AT&T Comments at 17.

[246] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14142, para. 58.

[247] *Id.* at 14142, para. 60.

[248] *See 2007 LNP Four Fields Declaratory Ruling*, 22 FCC Rcd at 19557, para. 48.

[249] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14142, para. 58.

[250] *Compare* Verizon Comments at 10 (supporting codification of "aspects" of the four data fields, noting that "ZIP code is of limited use for verification given its wide availability" and its use to complete porting requests "has resulted in unnecessary confusion") *with* CCA Comments at 6-7 (noting that data fields should not be mandatory as flexibility allows carriers to respond to "security needs and capabilities"); AT&T Comments at 15 & n.15 ("Proposed rule § 52.37(a) – (c), addressing data fields to validate a port-out request, should retain the flexibility to allow carriers to continue using temporary transaction-specific PINs assigned by the carrier in lieu of account-level passcodes assigned by customers, as the temporary PIN offers superior protection"); CTIA Comments at 19 (stating that the Commission should "not require the use of a passcode or foreclose the option for providers to use a porting-specific, one-time passcodes"); T-Mobile Comments at 10-11 (encouraging the Commission to not require one-time PINs for validating porting requests, as "secure methods of authentication and carrier practices may evolve over time").

[251] *2007 LNP Four Fields Declaratory Ruling*, 22 FCC Rcd at 19553-58, paras. 42-49.

[252] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14144-46, paras. 68-73.

in the record regarding wireless provider liability and dispute resolution related to SIM swap and port-out fraud.

67. *Customer Notice of Account Protection Measures.* Many of the account protection measures wireless providers offer and that we require wireless providers to adopt today are designed to empower customers to take steps to protect themselves from SIM swap and port-out fraud if they choose, but this empowerment will be stifled if customers are not effectively made aware of the measures that are available. Accordingly, we require wireless providers to provide notice, using clear and concise language, of any account protection measures the provider offers, including the measures we adopt in this *Report and Order*, and make this notice easily accessible via provider websites and applications.[253] We decline to specify the exact format or content of the required notice, as we agree with CCA that wireless providers are well-positioned to determine exactly how best to communicate information about account protection measures to their customers.[254] The record also demonstrates that some wireless providers have already developed content to educate customers about some account protection measures.[255]

68. We decline to require wireless providers to deliver an annual notice to customers regarding the availability of the account protection mechanisms they offer.[256] The record does not exhibit support for this requirement and we have no basis for concluding that it would be meaningfully more beneficial for customers than our requirement that wireless providers make notice about the availability of account protection measures easily accessible through provider websites and applications. We therefore decline to adopt an annual notice requirement.

69. *Employee Training.* We require wireless providers to develop and implement training for employees on how to identify, investigate, prevent, and remediate SIM swap and port-out fraud.[257] We find that adopting this employee training requirement will serve as a "first line of defense" against these damaging and evolving practices by preparing employees to defend against such fraud and preventing them from inadvertently or intentionally assisting bad actors in fraudulent schemes.[258]

---

[253] *See id.* at 14135, para. 39 (seeking comment on a notice requirement and expressing our belief that such notices should be brief, use easy-to-understand language, and be delivered in a manner that is least burdensome to customers). To provide greater clarity on what we require, the language we adopt slightly deviates from what we sought comment on in the *SIM Swap and Port-Out Fraud Notice*.

[254] *See* CCA Comments at 4 (arguing the Commission should allow "carriers to continue to communicate with their customers in the manner that they have found to be most effective").

[255] AT&T Comments at 7 ("AT&T's website provides information about SIM swap scams and misuse of the porting process and offers guidance about how customers can protect themselves against such fraud."); T-Mobile Comments at 5-6 ("T-Mobile publishes Safety Tips to educate subscribers on how to protect themselves online and directs customers to additional resources on identity theft and online safety from the FTC, CTIA, and others. T-Mobile's online resources also inform the customer of what to do if they believe someone has made unauthorized charges to their account.") (footnote omitted); CTIA Comments at 4 (stating that "[it] provides resources for consumers on steps that they can take to protect their wireless accounts").

[256] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14135, para. 39.

[257] *See id.* at 14134-35 & 14144-45, paras. 38 & 69 (seeking comment on training requirements).

[258] *See, e.g.*, NCLC/EPIC Comments at ii, 8-9 (asserting that the Commission should ensure that "providers prohibit their employees from . . . prompting leading questions or other mechanisms to enable fraudulent swaps"); NCLC/EPIC Comments at 6 (explaining that employees who assist victims "should be trained to provide responsive assistance in a timely manner"); Robert Ross Comments at 7-8 (arguing that any employee that a provider authorizes to perform a SIM swap should, amongst other precautions, "go through a higher level of training and repeat training in a program that is custom developed for high-risk transactions"); OPUS Research Comments at 1 (explaining that "the measures to secure SIM Swap and Port-Out employed by wireless service providers are . . . reliant on well-trained staff at retail stores and customer contact centers" and observing that "fraudsters employ 'human engineering' techniques to enlist support from sales or customer support personnel through multiple calls into a contact center or visits that too often result in successful identity theft in the form of SIM swaps or porting out of a

(continued….)

70. We agree with Verizon that "customer care and employee training programs are critical for preventing and identifying unauthorized and high-risk SIM changes for postpaid customers,"[259] and we find that all customers will benefit from employee training. The record reflects the industry's recognition of the importance of employee training; the country's three largest wireless providers—Verizon, T-Mobile, and AT&T—have already implemented some training measures for customer service representatives to identify, prevent, and remediate fraud.[260] The record also shows, however, that some wireless providers' current practices for customer service representative training may be lacking, as there are reported instances of wireless provider employees failing to identify, prevent, or quickly remediate SIM swap and port-out fraud.[261] We have previously determined that customer service training requirements play an important role in safeguarding the proper use of CPNI and have required telecommunications carriers to train their personnel on when they are and are not authorized to use CPNI.[262] We similarly conclude that the employee training requirement we adopt today is necessary to ensure customer service representatives are prepared to identify, prevent, and remediate fraudulent SIM change and port-out activity.

71. In applying this requirement, we give wireless providers flexibility on designing their training programs.[263] But we do require that all employees who may communicate with customers regarding SIM changes and number ports must be trained on how to recognize potentially fraudulent requests, how to recognize when a customer may be the victim of fraud, and how to direct potential victims and individuals making potentially fraudulent requests to employees specifically trained to handle such incidents.[264] Given that (1) some wireless providers already train employees on how to address

number"); ATL Comments at 1 (asserting that "implementing additional training for all customer service representatives initiating the port outs would provide consistency in security protocols").

[259] Verizon Comments at 2.

[260] *See* Verizon Comments at 3 ("Verizon also trains all customer care employees to identify and prevent unauthorized SIM change attempts through the use of multiple authentication protocols. . . . Customer care employees identifying potentially fraudulent SIM changes refer those reports to dedicated investigative teams."); T-Mobile Comments at 5 ("T-Mobile trains its employees on how to recognize fraud and account takeover attempts and how to respond if fraud occurs. Customer service representatives complete ongoing interactive training curricula on fraud and response. Moreover, T-Mobile provides resources on combatting fraud to employees. These resources are provided and maintained so that employees are knowledgeable about steps and guidelines for recognizing attack attempts and can properly respond to customer reports of fraud."); CTIA Comments at 3-4 ("While each provider's practices are different and many are not publicly visible so as to shield provider tactics from criminals, examples of the variety of tactics used to combat SIM swapping and port-out fraud include: . . . [t]raining employees to identify signs of a fraudulent SIM swap request and uses."); CTIA Reply at 7-8 ("AT&T reports that its customer service agents complete mandatory training, including on fraud prevention, authentication, social engineering, protection of CPNI, and account verification.").

[261] *See, e.g.*, Erik Faraldo Comments (Express) at 1 (reporting that he attempted to enable a port validation feature offered by his provider to prevent port-out fraud but eventually abandoned the effort due to difficulty reaching customer support, lack of knowledge about the feature by customer support representatives, and long wait times); Robert Ross Comments at 1 (detailing that it only took hackers minutes to complete a fraudulent SIM swap and that remediating the fraud took many months); Lee et al. at 7 (discussing how customer service representatives for some carriers processed SIM swaps without proper authentication under existing mechanisms).

[262] *See* 47 CFR § 2009(b); *CPNI Reconsideration Order*, 14 FCC Rcd at 14476-77, para. 130.

[263] *See, e.g.*, CCA Comments at 4 ("Should the Commission determine that additional rules are necessary to prevent SIM swap and port out fraud, it should ensure that such rules are sufficiently flexible to account for evolving technologies."); CTIA Reply at 27 ("[T]here is no one-size-fits-all solution to [protecting customer accounts] and that the measures necessary to protect different customers and different types of services vary greatly.").

[264] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14134-35, 14144-45, paras. 38, 69 (seeking comment on training requirements); Verizon Comments at 3 (explaining that customer care employees identifying potentially fraudulent SIM changes refer those reports to dedicated investigative teams, and observing that there is a toll-free number for customers to contact or obtain assistance from Verizon in the event of an unauthorized SIM change).

fraud,[265] (2) our new training requirement builds upon our existing CPNI training rule,[266] and (3) we are providing wireless providers with flexibility on how to design their training programs, we do not anticipate that imposing this training requirement will be overly costly for wireless providers.

72. *Requirements to Remedy SIM Swap and Port-Out Fraud.* We are concerned that in some cases, "consumers who have been the victims of SIM swaps or port-out fraud have had difficulties obtaining assistance from the carriers" when they report it.[267] Accordingly, we require wireless providers to maintain a clearly disclosed, transparent, and easy-to-use process for customers to report SIM swap and port-out fraud, promptly investigate and take reasonable steps within their control to remediate such fraud, and, upon request, promptly provide customers with documentation of SIM swap and port-out fraud involving their accounts.[268] These measures must be provided to victims of SIM swap and port out fraud at no cost. We anticipate that, in combination, these requirements will serve to minimize the harms that victims experience as a result of SIM swap and port-out fraud.

73. Our requirement that wireless providers maintain a clearly disclosed, transparent, and easy-to-use process for customers to report SIM swap and port-out fraud rests on our concern that customers currently struggle to report SIM swap and port-out fraud to their wireless providers.[269] When customers are unable to find information about how to report such fraud or use existing customer service avenues to do so, it not only frustrates these customers, it prevents initiation of steps to investigate and remediate the fraud, which increases the risk that fraudsters will be able to use a victim's SIM or phone number to accomplish further fraud. We anticipate that clear methods for reporting SIM swap and port-out fraud that are transparent to customers will "ensure that customers have easy access to information they need to report SIM swap, port-out, or other fraud."[270] We decline to specify the exact means wireless providers must put in place for customers to report SIM swap and port-out fraud, but we stress that the process must be a clearly disclosed, transparent, and easy-to-use process for customers to notify providers.

74. We require wireless providers to establish procedures to promptly investigate and take reasonable steps within their control to remediate SIM swap and port-out fraud because the record demonstrates that even when victims of SIM swap and port-out fraud are successful in reporting such fraud to their providers, they have difficulty obtaining assistance from their providers to remediate the fraud.[271] This is consequential because "[i]dentity theft, including SIM swap fraud, can cause intense anxiety for victims and must be addressed in a timely manner to prevent financial losses and exposure of personal information."[272] Thus, we conclude that "it should be easy for a customer to get access to appropriate carrier resources that can help mitigate the significant harms caused by SIM swap or port-out

[265] *See supra* n.260.

[266] 47 CFR § 64.2009(b) ("Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place."); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198.

[267] NCLC/EPIC Comments at 5.

[268] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14145, para. 69.

[269] Princeton Comments at 11-12 ("We recommend that the Commission require carriers to have a clearly disclosed process for customers to quickly and easily report account compromise."); NCLC/EPIC Comments at ii (asserting that the Commission should "[r]equire carriers to offer a redress program that . . . is fully accessible and transparent to all customers"); *see also SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14144-45, para. 69.

[270] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14145, para. 69.

[271] *See* Princeton Comments at 11-12 ("There are countless anecdotes of SIM swap and port-out victims who struggle to regain control of their telephone number."); NCLC/EPIC Comments at 5 ("[M]any consumers who have been the victims of SIM swaps or port-out fraud have had difficulties obtaining assistance from the carriers."); Erik Faraldo Comments (Express) (describing one customer's challenges with seeking remediation of SIM swap fraud).

[272] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14145, para. 69.

fraud."[273] Although we do not specify the procedures that wireless providers must adopt,[274] we agree with commenters that investigations must be instigated and resolved expeditiously.[275]

75. To ensure victims of SIM swap and port-out fraud have additional means to resolve other consequences that result from SIM swap and port-out fraud, we require wireless providers to give customers documentation regarding such fraud on their accounts, upon request.[276] In the *SIM Swap and Port-Out Fraud Notice*, we recognized that "customers sometimes need documentation of the fraud incident to provide to law enforcement, financial institutions, or others to resolve financial fraud or other harms of the incident" and acknowledged that "[a] SIM swap or port-out fraud victim may have difficulty obtaining such documentation from the carrier because the carrier may not have processes in place to produce such documentation."[277] Requiring wireless providers to give fraud victims supporting documentation will enable those victims to seek remedies from other institutions for additional fraud that bad actors achieve using a victim's SIM or phone number. We do not specify the form that such documentation must take or exactly what information it must contain, but it should be reasonably designed to permit customers to demonstrate to other entities that they were victims of SIM swap or port-out fraud and that bad actors may have used access to a victim's telecommunications services to carry out additional fraud.[278] Additionally, because of the potential harms that can flow from SIM swap and port-out fraud, we also require wireless providers to provide this documentation promptly.

76. We anticipate that the benefits of our requirements will outweigh any potential costs. Although commenters did not address the costs of the additional measures we adopt here, we note that at least one wireless provider has already adopted processes for customers to report SIM swap and port-out fraud, to investigate and remediate such fraud, and to provide documentation of such fraud to customers upon request.[279] We also anticipate that allowing wireless providers flexibility in how to abide by these new requirements will enable them to adopt cost-effective procedures that will also allow them to successfully resolve SIM swap and port-out fraud incidents when they occur.

77. To maintain the flexibility we believe will be required for wireless providers to adequately tailor and adapt their practices to address SIM swap and port-out fraud, we decline to impose

[273] *Id.* *See also* Kyle Ratcliff Comments (Express) (urging that the Commission "mandate carriers adopt an easy-to-use and standardized remediation process for those customers who are affected by this type of identity theft. Given the fact that so much of our day to day lives are currently managed by our smartphones, the last thing a consumer should have to do if they have been victimized is negotiate an increasingly Byzantine system of bureaucracy in order to get their rightful account ownership restored.").

[274] *See* Princeton Comments at 11-12 ("We do not take a position on what the nature of that investigation should be or how quickly the carrier should complete it, since the details will vary by account compromise.").

[275] *See* Princeton Comments at 11-12 ("If a carrier receives a credible report of compromise, it should expeditiously investigate without unreasonable delay and, if the report is accurate, restore access to the customer's account."); NCLC/EPIC Comments at 6 (asserting the reports of SIM swap and port-our fraud "should trigger . . . [i]mmediate assistance to the customer both to stop further losses [and an] internal investigation by the customer's provider to determine how the fraud was effectuated").

[276] *See* NCLC/EPIC Comments at ii (arguing that the Commission should "[r]equire carriers to offer a redress program that . . . includes all information necessary for the customer to cooperate with law enforcement").

[277] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14144, para. 68.

[278] Such documentation must address the customer's interest in protecting his or her account(s) or identity but may be tailored not to include other proprietary, confidential, or law-enforcement-related information regarding the SIM swap or port-out fraud or the account.

[279] *See* T-Mobile Comments at 5 ("If a customer is a victim of SIM swap or port-out fraud, T-Mobile takes rapid, responsive measures. Customers may report fraud or unauthorized activity by calling T-Mobile's Customer Care hotline, which is available 24/7. When fraud occurs, T-Mobile's Fraud Operations specialists act quickly to ensure all fraudulent changes are corrected and any wrongful T-Mobile account charges are refunded. T-Mobile also assists with phone number recovery and provides victims with documentation of the fraud upon request.").

prescriptive measures raised in the *SIM Swap and Port-Out Fraud Notice* and the record. Specifically, although we encourage wireless providers to establish a dedicated hotline for customers to report SIM swap and port-out fraud[280] and respond within 24 hours of a customer reporting suspected fraud,[281] we decline to require that wireless providers adopt these approaches. While the former requirement received support from the National Consumer Law Center (NCLC) and the Electronic Privacy Information Center (EPIC), we conclude that it may not benefit a wireless provider's customers if it is inconsistent with a provider's established customer service methods. The latter may be infeasible for certain incidents and is not necessary given our requirement that investigation and remediation be prompt. We also decline to require that wireless providers give customers an alternative number on a temporary basis after SIM swap or port-out fraud has occurred,[282] as that may promote number resource exhaust in certain areas or for certain wireless providers. However, we encourage wireless providers to offer customers a temporary alternative number when the efforts to remediate SIM swap or port-out fraud may take a significant amount of time or to assist customers who have critical needs to be accessible via phone at the time.[283] We do not find it necessary at this time to require that wireless providers, upon being notified by a customer of fraud, provide "detailed records of the fraud [to law enforcement]" or "offer to the customer to notify financial institutions and creditors, the three national credit reporting agencies, and others of the fraud, to help the customer recover control over their identity, if appropriate."[284] While we encourage wireless providers to take these steps upon the request of customers as part of their mitigation efforts, we conclude that our new requirement that providers give customers documentation concerning fraudulent SIM swaps and number ports will be sufficient to allow those customers to alert appropriate entities if needed. We note, however, that we will monitor consumer complaints and may evaluate the remediation programs implemented by wireless providers. If we find that such programs are not adequately resolving SIM swap and port-out fraud in a timely manner, we may take steps to implement more specific requirements in the future.

78. *Working Group.* While we recognize that the harmful effects of SIM swap and port-out fraud may extend beyond the control of wireless providers and that the incentives to engage in such fraud implicate the security practices of other industries,[285] we decline at this time to direct or rely on standard-setting bodies, industry organizations, or consumer groups to evaluate SIM swap and port-out fraud "to augment our understanding and present possible solutions."[286] Instead, we find it most appropriate to focus on solutions within the scope of the Commission's authority that we anticipate will mitigate the

[280] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14145, para. 69; NCLC/EPIC Comments at 5 ("As suggested, a dedicated and well-publicized hotline should be one component.") (footnote omitted).

[281] NCLC/EPIC Comments at ii (asserting that the Commission should "[r]equire carriers to offer a redress program that . . . provides timely responses within 24 hours after a complaint is made").

[282] *Id.* at 6 (asserting that carriers should "provide a safe alternative mobile telephone" during the mitigation process).

[283] We also recognize that adequate remediation may require providing victims with permanent replacement numbers or SIMs, and carriers should effectively assist customers with that transition should that be necessary.

[284] NCLC/EPIC Comments at 6.

[285] *See, e.g.*, AT&T Comments at 2 ("SIM swap or port-out [fraud] is only a small part of the scheme to harm the consumer, as these incidents implicate a range of stakeholders not controlled by carriers (e.g., financial institutions, cryptocurrency companies, text message aggregators) that all play a role in the verification of customer identity."); T-Mobile Comments at 1-2 ("[C]ombatting SIM swap and port-out fraud is a team effort that requires action by an entire ecosystem that includes carriers and subscribers as well as financial institutions, email providers, retail websites, social media companies and others who rely on various customer authentication methods."); CTIA Reply at 11 ("[T]he record makes it abundantly clear that others beyond the wireless sector need to engage to address the problem of fraudulent account takeovers.").

[286] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14146, para. 72.

harmful consequences of this fraud.[287] Additionally, to the extent that commenters advocated that we direct this issue to a working group before taking action,[288] we disagree with that approach and find that doing so would only delay solutions that we expect will benefit customers now. Although we decline to rely on a working group, we also do not foreclose wireless providers from forming or entering into cross-sector, multi-stakeholder efforts, independent of the Commission direction, to seek broader solutions to the harms that may ultimately result from SIM swap and port-out fraud.[289]

79. *Provider Liability and Dispute Resolution.* We decline to adopt proposals in the record that prescribe provider liability and dispute resolution requirements for disputes between wireless providers and customers.

80. NCLC and EPIC argue that the Commission should "[r]equire carriers to offer a redress program that . . . provides full coverage of losses to customers who have been the victims of a fraudulent SIM swap or port-out fraud," which they say would "[p]rovide strong financial incentives to providers to stop SIM swapping and port-out fraud."[290] We agree with CTIA, however, that telecommunications carriers are "but one link in the chain of consumer and business protection from account takeover fraud,"[291] and therefore that the responsibility for financial harms that a bad actor may be able to perpetuate following such fraud is borne by several parties, including, significantly, the bad actor. Imposing such liability on wireless providers would be inequitable and would reduce the incentives for e-mail and social media providers, financial institutions, healthcare providers, retail websites, and other entities that rely on cell phone-based identity authentication to improve their security practices,[292] as well as reduce the incentive for customers to act responsibly.[293] We note, however, that compliance with our rules is not a safe harbor for wireless providers; customers will still be able to pursue any existing remedies available by law.[294]

81. Similarly, we decline to specify, as NCLC and EPIC request, that wireless providers are "fully responsible for any abuse committed by its employees, whether the employees acted either

[287] AT&T Comments at 8 (acknowledging that "SIM swap and port-out scams implicate third parties outside the Commission's jurisdiction").

[288] *See, e.g.*, *id.* at 3 (asserting that the Commission should "first leverage existing resources and expertise . . . before deciding on a course of action"); Bandwidth Reply at 6 ("In order to fully explore and understand the full breadth of the issues and their potential solutions, Bandwidth agrees with those opening comments that recommend that the Commission support inclusive and consensus-driven industry efforts as its next step in this proceeding."); *cf.* T-Mobile Comments at 14-15 (suggesting that "the FCC could coordinate with other regulators, such as financial services or healthcare regulators, on strategies" to address SIM swap and port-out fraud and that "[t]he Commission also may want to coordinate with NIST on addressing authentication issues").

[289] *See, e.g.*, CTIA Reply at 11 ("[T]he Commission should convene a cross-sector, multi-stakeholder working group to study the broader questions in the NPRM that go beyond the rule changes proposed.").

[290] NCLC/EPIC Comments at ii.

[291] CTIA Reply at 13-14.

[292] *See id.* ("[H]olding providers solely or presumptively liable risks undermining the incentives other players involved in SIM swap losses, such as banks and crypto wallets, have to prevent fraud. Such an approach also would be inequitable.").

[293] For example, if customers knew that wireless providers must provide full coverage of losses resulting from SIM swap and port-out fraud, they might not be fully incentivized to place locks on their account or take appropriate action when they receive notice from their wireless providers about unauthorized SIM swap and port-out requests or failed authentication attempts.

[294] *See, e.g.*, *Al Weiss v. AT&T Inc.*, No. 6:23-cv-00120 (M.D. Fla., filed Jan. 23, 2023); *Eman Bayani v. T-Mobile USA, Inc.*, No. 2:23-cv-00271 (W.D. Wash. filed Feb. 27, 2023); *Samuel Whatley, II v. T-Mobile USA, Inc.*, No. 2:23-cv-1339-RMG-MGB (D.S.C. filed Apr. 3, 2023); *Feliks Roitman and Yekaterina Shkolnik v. T-Mobile USA, Inc.*, No. 1:23-cv-06159 (E.D.N.Y., filed Aug. 16, 2023).

intentionally or negligently,"[295] although we make clear that this statement does not absolve wireless providers of any liability for employee actions that already exists. We anticipate that the requirements we adopt today—including employee training regarding SIM swap and port-out fraud and restrictions on the ability of employees to access CPNI prior to authentication—will ensure that wireless providers implement adequate procedures to prevent employees from perpetuating SIM swap and port-out fraud.

82. Finally, we decline to adopt NCLC and EPIC's proposal that "any arbitration clauses in the providers' agreements with consumers explicitly exclude resolutions" of SIM swap and port-out fraud disputes at this time.[296] They urge this because "[o]therwise, consumers who have not been made whole, or who have difficulties obtaining relief for frauds that are perpetrated on them because of the provider's insufficiently strict authentication protocols, will have no meaningful way of enforcing the protections mandated by the Commission."[297] The Commission has full authority to enforce the protections it has mandated, and we anticipate that the rules we adopt today, coupled with this enforcement authority, will incentivize wireless providers to adopt strong practices to protect customers from SIM swap and port-out fraud. Nonetheless, we seek comment below on whether the Commission should require providers to exclude disputes about SIM swapping or porting fraud from arbitration clauses.[298] We encourage customers and public interest organizations to submit complaints and evidence of wireless providers failing to comply with these new rules in support of our enforcement efforts.

D. Implementation Timeframe

83. We require wireless providers to comply with the requirements we adopt today six months after the effective date of the *Report and Order* or, for those requirements subject to review by the Office of Management and Budget (OMB), upon completion of that review, whichever is later. We conclude that providing six months to achieve compliance with rules that are not subject to OMB review accounts for the urgency of safeguarding customers from these fraudulent schemes,[299] and will allow wireless providers to coordinate any updates needed to their systems and processes to comply with the Safe Connections Act and the rules we adopt to implement that statute.[300] We agree with some commenters that while many wireless providers can immediately implement the revisions to our CPNI and number porting rules, other providers may require this additional time.[301] Some wireless providers

[295] NCLC/EPIC Comments at 10.

[296] *Id.* at 6.

[297] *Id.*

[298] *See infra Further Notice*.

[299] *See, e.g.*, *2007 LNP Four Fields Declaratory Ruling*, 22 FCC Rcd at 19557, para. 48 (concluding that 90 days was sufficient time for carriers to comply with LNP validation requirements).

[300] *See generally Publicly Released Draft Safe Connections Order.*

[301] *See* T-Mobile Comments at 13-14 ("While some of the changes proposed by the FCC can be implemented immediately, others may require a longer implementation timeframe."); NCTA Comments at 8 ("[I]t is important to provide sufficient time for carriers to implement [new obligations] in a way that is robust, thorough, and clear so that they do not cause customer confusion").

already employ authentication[302] and notification[303] measures to process SIM change and port-out requests, offer account change locks,[304] provide notice to customers about available fraud protection measures,[305] and train employees on how to address SIM swap and port-out fraud,[306] and may simply need to refine those practices to align with our rules. Other providers, particularly smaller providers, may need the additional time to upgrade their systems, implement modifications to their policies and procedures, and conduct new customer service representative training.[307] We conclude that providing six months after the effective date of the *Report and Order* to implement these revisions to our CPNI and number porting rules strikes the right balance between time for wireless providers to implement these changes and accounting for the urgency of safeguarding customers from these fraudulent schemes.

[302] *See, e.g.*, AT&T Comments at 13 ("Carriers are already authenticating customers using one or more of the methods identified in the Commission's existing and/or proposed rules."); *id.* at 6-7 (describing its routine use of "a one-time PIN delivered via SMS message or an outbound voice call to a postpaid customer's device for enhanced customer validation," and its "Number Transfer PIN process to validate postpaid port-out transactions"); CCA Comments at 3-4 (describing U.S. Cellular's assigning of a PIN code to each customer that is used for customer authentication); Better Identity Coalition Comments at 4 (noting that "two major mobile network operators already support FIDO authentication for their customers"); NCTA Comments at 4-5 (describing authentication measures some wireless providers already use, including account PINs); T-Mobile Comments at 4 ("T-Mobile offers various customer authentication options, which may vary based on customer, account, and device characteristics."); Verizon Comments at 8-9 (describing current authentication measures, including a transaction-specific "Number Transfer PIN" and notifying customers of port requests via text message and email); CTIA Comments at 3-4 (noting that some providers already employ multi-factor authentication when account changes are requested).

[303] *See, e.g.*, AT&T Comments at 6 (explaining that for transactions meeting a certain threshold of AT&T's "risk model," it will send one-way SMS notifications of a SIM change request, and for transactions meeting a higher risk threshold, it will require customers confirm the SIM change request via an SMS notification); T-Mobile Comments at 4 (noting that "T-Mobile notifies customers of account changes and requests"); Verizon Comments at 6 ("Verizon already . . . notif[ies] customers of high-risk SIM change authentication attempts, failed or otherwise, and of other account changes."); CCA Comments at 3-4 (describing the current procedures that T-Mobile, U.S. Cellular, and GCI use to notify customers of a change to their account or port-out request, and that other members are "similarly adopting heightened security measures"); CTIA Comments at 3-4 (explaining that some providers notify customers when a SIM swap is initiated).

[304] *See, e.g.*, T-Mobile Comments at 4 ("[F]or most types of customers, T-Mobile can institute a 'SIM change block'. . ."); NCTA Comments at 4-5 ("Wireless providers already . . . provid[e] the ability to lock or freeze wireless accounts."); CTIA Reply at 26-27 ("[M]any providers already offer account freeze options to their customers."); CCA Comments at 3-4 (describing T-Mobile's "Account Takeover Protection" service, which "blocks unauthorized users from porting numbers and allows only the billing responsible party to turn the feature off").

[305] AT&T Comments at 7 ("AT&T's website provides information about SIM swap scams and misuse of the porting process and offers guidance about how customers can protect themselves against such fraud."); T-Mobile Comments at 5-6 ("T-Mobile publishes Safety Tips to educate subscribers on how to protect themselves online and directs customers to additional resources on identity theft and online safety from the FTC, CTIA, and others. T-Mobile's online resources also inform the customer of what to do if they believe someone has made unauthorized charges to their account.") (footnote omitted); CTIA Comments at 4 (stating that "[it] provides resources for consumers on steps that they can take to protect their wireless accounts").

[306] *See, e.g.*, Verizon Comments at 3 ("Verizon also trains all customer care employees to identify and prevent unauthorized SIM change attempts through the use of multiple authentication protocols. . . . Customer care employees identifying potentially fraudulent SIM changes refer those reports to dedicated investigative teams."); T-Mobile Comments at 5 ("T-Mobile trains its employees on how to recognize fraud and account takeover attempts and how to respond if fraud occurs."); CTIA Comments at 3-4 (listing employee training as an example of the tactics providers use to combat SIM swap and port-out fraud); CTIA Reply at 7-8 ("AT&T reports that its customer service agents complete mandatory training, including on fraud prevention, authentication, social engineering, protection of CPNI, and account verification.").

[307] *See, e.g.*, NCTA Comments at 8 ("Many of the potential solutions might require modifications to internal systems, as well as significant training of company personnel.").

E. Legal Authority

84. The rules we adopt today build on the Commission's existing rules to implement Congress's mandates to ensure that telecommunications carriers (which include, for purposes of our CPNI rules, providers of interconnected VoIP service) protect the confidentiality of proprietary information of, and relating to, customers and to provide number portability in accordance with requirements prescribed by the Commission. As such, the rules we adopt are well-grounded in our authority in sections 222 and 251, as well as other provisions of the Act.

85. *SIM Changes.* Congress, through section 222 of the Act, requires telecommunications carriers to protect the privacy and security of customers' proprietary information that carriers obtain by virtue of providing a telecommunications service.[308] Under section 222(a), every telecommunications carrier has a general duty to protect the confidentiality of proprietary information of, and relating to, customers.[309] Section 222(c)(1) provides that a telecommunications carrier may only use, disclose, or permit access to customers' individually identifiable CPNI that it has received or obtained by virtue of its provision of a telecommunications service in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived or its provision of services necessary to, or used in, the provision of such telecommunications service.[310]

86. The Commission has previously stated that to comply with these section 222 requirements, "telecommunications carriers [must] establish effective safeguards to protect against unauthorized use or disclosure of CPNI."[311] The Commission also has established rules pursuant to its section 222 authority to ensure such safeguards are in place. Among other things, the Commission's rules require carriers to take "reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI" and to "properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit."[312] Like these safeguards, our action today "strengthen[s] our privacy rules by adopting additional safeguards to protect customers' CPNI against unauthorized access and disclosure."[313]

87. Fraudulent SIM swaps result in unauthorized disclosure of and access to customers' accounts, including individually identifiable CPNI.[314] By successfully obtaining a fraudulent SIM swap, a bad actor can access CPNI such as incoming call information (including the date and time of the call and

---

[308] Congress extended this duty and others described herein to wireless providers. *See* 47 U.S.C. § 332(c)(1)(A) ("A person engaged in the provision of a service that is a commercial mobile service shall, insofar as such person is so engaged, be treated as a common carrier for purposes of this chapter.").

[309] 47 U.S.C. § 222(a).

[310] 47 U.S.C. § 222(c)(1).

[311] *See 2007 CPNI Order*, 22 FCC Rcd at 6932, para. 9 (citing the *CPNI Order*, 13 FCC Rcd at 8195, para. 193). We note that the Commission's CPNI rules apply not only to telecommunications carriers that are subject to Title II of the Act, but also to interconnected VoIP providers. *See id.* at 6954-57, paras. 54-59 (relying on the Commission's Title I ancillary jurisdiction to apply CPNI rules to interconnected VoIP service providers); *see also* 47 CFR § 64.2003(o) ("For the purposes of this subpart, the term 'telecommunications carrier' or 'carrier' shall include an entity that provides interconnected VoIP service, as that term is defined in section 9.3 of these rules.").

[312] 47 CFR § 64.2010(a); *see also 2007 CPNI Order*, 22 FCC Rcd at 6959-60, paras. 63-66.

[313] *2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1.

[314] The Act defines 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." 47 U.S.C. § 222(h)(1).

number from which the call is made), and gain access to a victim's account, potentially giving the bad actor access to other CPNI, like outgoing call history (including numbers called and the location, frequency, duration, and timing of such calls)[315] and the victim's bills and the services purchased by the victim. And as described above, fraudulent SIM swaps allow bad actors to perpetrate greater fraud by giving them the means to complete text and voice authentications to access the victim's other accounts.[316]

88. In light of the foregoing, we find that the rules we adopt today to address SIM swap fraud advance the protections against unauthorized disclosure of, and access to, individually identifiable CPNI and other sensitive personal information about customers, and therefore are squarely grounded in the Commission's authority under section 222. Our requirement that wireless providers use secure methods of authenticating their customers that are reasonably designed to confirm a customer's identity prior to effectuating a SIM change request will help prevent unauthorized disclosure of and access to such information. This requirement also sustains customer decisions regarding disclosure of their information—if a wireless provider completes a SIM change requested by someone other than the actual customer, then the wireless provider has not obtained the customer's approval to disclose their CPNI in accordance with section 222(c)(1).[317]

89. The other rules we adopt reinforce the protections afforded by this new rule. For instance, the requirement that wireless providers develop, maintain, and implement procedures to respond to failed authentication attempts will likewise serve to prevent unauthorized disclosure of and access to CPNI. The rule requiring that telecommunications carriers establish safeguards and processes so that employees who interact with customers are unable to access CPNI until after the customer has been properly authenticated will prevent inadvertent disclosure of CPNI to those making unauthorized requests and inhibit the ability of employees to participate in fraudulent SIM swaps. Employee training requirements will not only improve their ability to recognize and derail fraudulent SIM change requests, such requirements will better prepare customer service representatives to address customer complaints and remediate fraudulent SIM swaps when they do occur. Requiring wireless providers to maintain a clear process for customers to report fraud, investigate and remediate fraud, and provide customers with documentation of fraud involving their accounts will ensure that the harms of SIM swap and port-out fraud are mitigated when it does occur. And the requirement that wireless providers keep records of data regarding SIM change requests and the authentication measures they have in place will help ensure that wireless providers have information they need to measure the effectiveness of their customer authentication and account protection measures and make informed decisions about how they should be updated over time.

90. Our rules also further the goals of section 222 by enabling customers to take action to prevent and address fraudulent SIM changes, and therefore help wireless providers protect against unauthorized disclosure and access to CPNI. The requirement that wireless providers immediately notify customers regarding SIM change requests provides added protection by giving customers information they can use to notify their providers that a fraudulent request has occurred at the time of the request or shortly thereafter so that the provider can take timely steps to remediate the situation. Requiring wireless providers to offer customers the option to lock their accounts so that their providers are prohibited from processing SIM changes gives security-minded customers or those who are at high risk of fraud a tool to prevent a fraudulent request from being processed in the first instance. Additionally, our new rule that

[315] *See 2007 CPNI Order*, 22 FCC Rcd at 6936, para. 13 & n.45 (defining this information as call detail information and finding it to be CPNI).

[316] *See supra* section II.

[317] Section 222(f) of the Act also 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." 47 U.S.C. § 222(f).

wireless providers make notice of account protection mechanisms easily accessible via their websites and applications ensures that customers are aware of these tools. We also conclude that the requirements we establish to promptly resolve SIM swap and port-out fraud extend from our section 222 authority because they will help to mitigate the unauthorized disclosure of and access to CPNI.

91. Finally, the application of these new customer authentication requirements to both pre-paid and postpaid services is consistent with section 222(a)'s mandate that "[*e*]*very* telecommunications carrier . . . protect the confidentiality of [customer] proprietary information" and section 222's instruction that all "customers" of those carriers benefit from such protections.[318]

92. While section 222 provides firm foundation for our rules to address SIM swap fraud, we also find that section 251(e) of the Act provides additional authority for these rules.[319] In section 251(e)(1), Congress expressly assigned to the Commission exclusive jurisdiction over that portion of the North American Number Plan (NANP) that pertains to the United States and related telephone numbering issues.[320] The Commission retained its "authority to set policy with respect to all facets of numbering administration in the United States."[321] Because our new SIM change rules prevent and address misuse of NANP numbers assigned to wireless devices, we conclude that those rules are supported by our exclusive numbering authority within section 251(e).

93. *Number Porting*. We rely on our authority derived from sections 1, 2, 4(i), 251(e), and 332 of the Act to implement the changes to our number porting rules to address port-out fraud. As the Commission has consistently found since 1996, "[w]e possess independent authority under sections 1, 2, 4(i), and 332 of the Communications Act of 1934, as amended, to require CMRS providers to provide number portability as we deem appropriate."[322] We rely on this well-established authority to adopt number porting rules applicable to wireless providers that address port-out fraud.

94. We also find that the exclusive numbering authority that Congress granted this Commission under section 251(e)(1) provides ample authority to extend the LNP requirements as set out in this *Report and Order*. Specifically, in section 251(e)(1) of the Act, Congress expressly assigned to the Commission exclusive jurisdiction over that portion of the NANP that pertains to the United States and related telephone numbering issues.[323] The Commission retained its "authority to set policy with respect to all facets of numbering administration in the United States."[324] We find that the revisions to our number porting rules designed to protect the customers from port-out fraud fit comfortably within our exclusive numbering authority because the requirements we establish to prevent and promptly resolve

[318] 47 U.S.C. § 222(a) (emphasis added); 47 U.S.C. §§ 222(a), (c)(1), (h)(1) (all referring to "customers" of telecommunications carriers without distinguishing between customers who subscribe to pre-paid and postpaid service).

[319] 47 U.S.C. § 251(e).

[320] 47 U.S.C. § 251(e)(1).

[321] *Implementation of the Local Competition Provision of the Telecommunications Act of 1996* et al., CC Docket No. 96-98 et al., Second Report and Order and Memorandum Opinion and Order, 11 FCC Rcd 19392, 19512, para. 271 (1996) (*Local Competition Second Report and Order*) (explaining that by retaining exclusive jurisdiction over numbering policy the Commission preserves its ability to act flexibly and expeditiously).

[322] *First Number Portability Order*, 11 FCC Rcd at 8431, para. 153; *see also First Number Portability Order on Reconsideration*, 12 FCC Rcd at 7315, para. 141; *LNP Standard Fields Order*, 25 FCC Rcd at 6955 n.10; *Porting Interval Order and FNPRM*, 24 FCC Rcd at 6085 n.8; *2007 VoIP LNP Order*, 22 FCC Rcd at 19534 n.11.

[323] 47 U.S.C. § 251(e)(1).

[324] *Local Competition Second Report and Order*, 11 FCC Rcd at 19512, para. 271 (explaining that by retaining exclusive jurisdiction over numbering policy the Commission preserves its ability to act flexibly and expeditiously).

port-out fraud are necessary to address improper use of numbering resources and ensure that customers can recover their numbers when fraudulent ports have occurred.[325]

95. *Other Sources of Authority.* While the provisions discussed above provide sufficient authority for the entirety of the rules we adopt in this *Report and Order*, we find additional support under sections 201 and 303.[326]

96. Section 201(b) authorizes the Commission to prescribe rules to implement carriers' statutory duty not to engage in conduct that is "unjust or unreasonable."[327] We conclude that practices that allow for fraudulent SIM swaps and number ports are unjust and unreasonable because they are contrary to the reasonable expectations of customers, are not reasonably avoidable by customers, and can cause substantial customer harm. We also rely on our section 201(b) authority to find that the inability for customers to effectively seek remedies from their wireless providers when fraudulent SIM swaps and port outs have occurred is "unjust and unreasonable," and therefore warrants these rules.[328] We would also find these practices unjust and unreasonable when a wireless provider says it will implement reasonable measures to prevent fraudulent SIM swaps and number ports but fails to do so. Our findings here are similar to and consistent with how the Federal Trade Commission (FTC) addresses inadequate data security measures under section 5 of the FTC Act.[329]

97. We also rely on our broad authority under Title III, which allows us to protect the public interest through spectrum licensing. Pursuant to section 303(b)'s directive that the Commission must, consistent with the public interest, "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class,"[330] these revisions to our CPNI and number porting requirements prescribe the conditions under which licensed wireless providers must provide their services. They specifically require licensed wireless providers to provide their services in a way that protects the interests of their customers, including reasonable measures to prevent fraudulent acts against their customers.

---

[325] *See, e.g.*, *2007 VoIP LNP Order*, 22 FCC Rcd at 19543, para. 22 (explaining that to the extent service providers provide services that offer customers NANP telephone numbers, those service providers subject themselves to the Commission's plenary authority under section 251(e)(1) with respect to those numbers, and using that plenary authority to extend local number portability requirements to interconnected VoIP providers and their numbering partners).

[326] Sections 201 and 303 of the Act generally give the Commission authority for prescribing rules, but we also rely on these sources of authority as described herein. *See* 47 U.S.C. § 201(b) ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter."); *AT&T Corp. v. Iowa Utils. Bd.*, 525 U.S. 366, 378 (1999) (holding that the last sentence in section 201(b) "means what it says: The FCC has rulemaking authority to carry out the 'provisions of this Act,'" including provisions added by the Telecommunications Act of 1996); *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27 n.94 ("Section 201(b) authorizes the Commission to 'prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act,' including section 222."); 47 U.S.C. § 303 ("Except as otherwise provided in this chapter, the Commission from time to time, as public convenience, interest, or necessity requires, shall—(r) Make such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter.").

[327] 47 U.S.C. § 201(b).

[328] *Id.*

[329] *Privacy and Security Enforcement*, Federal Trade Commission, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Oct. 18, 2023) ("The FTC has brought legal actions against organizations that . . . misled [consumers] by failing to maintain security for sensitive consumer information.").

[330] 47 U.S.C. § 303(b); *Cellco P'ship v. FCC*, 700 F.3d 534, 542-43 (D.C. Cir. 2012).

IV. FURTHER NOTICE OF PROPOSED RULEMAKING

98. *Harmonizing the CPNI Safeguards Rules.* In this *Further Notice*, we first seek comment on whether to harmonize the existing requirements governing customer access to CPNI[331] with the SIM change authentication and protection measures we adopt today. This *Further Notice* expands on questions the Commission asked in the *SIM Swap and Port-Out Fraud Notice* and several comments in the record, but seeks more targeted feedback on a specific approach. In particular, in the *SIM Swap and Port-Out Fraud Notice*, the Commission asked "whether any new or revised customer authentication measures . . . would offer benefits for all purposes."[332] The Commission also asked whether there are "benefits to providing expanded authentication requirements before providing access to CPNI to someone claiming to be a carrier's customer," as well as "whether any heightened authentication measures required (or prohibited) should apply for access to all CPNI, or only in cases where SIM change requests are being made."[333] Additionally, the Commission proposed to add a prohibition on the use of recent payment and call detail information to authenticate customers for online access to CPNI.[334]

99. Several commenters suggested that we harmonize our CPNI authentication rules with the SIM change authentication rules we adopt.[335] These commenters offered several rationales that potentially support harmonization of these rules, including that: (1) the CPNI authentication requirements are outdated and therefore vulnerable to fraud;[336] (2) inconsistent rules are more burdensome on carriers;[337] (3) some carriers default to specified authentication measures and are disincentivized from

[331] *See* 47 CFR § 64.2010.

[332] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14136, para. 44.

[333] *Id.* at 14137, para. 46.

[334] *See id.* at 14132-33, para. 30.

[335] *See, e.g.*, CTIA Reply at 21-22 (advocating for "a *harmonized* approach to the Commission's authentication standards across a variety of settings with respect to CPNI access") (emphasis in original); Princeton Comments at 8 ("The Commission should modernize and harmonize baseline authentication requirements for telephone access to CPNI, online access to CPNI, SIM swaps, and number portability authentication methods."); Verizon Comments at 7-8 ("The Commission should thus align the existing authentication rules to the NPRM's flexible, non-prescriptive approach by requiring providers to use security [sic] authentication methods for CPNI access without dictating the provider's method.").

[336] *See, e.g.*, CTIA Comments at 18 (asserting that the CPNI rules "do not reflect the most up-to-date authentication best practices"); Verizon Comments at 7 (asserting that "[m]any customer authentication and security tools have surpassed the effectiveness of [the current CPNI rules for customer authentication]"); FIDO Alliance Comments at 4 ("In general, industry and government are moving away from knowledge-based approaches to authentication (i.e. passwords)."); Robert Ross Comments at 7 ("[I]n-store authentication is highly susceptible to human error by store personnel."); AT&T Comments at 5 ("But no method of authentication is foolproof or effective in every instance. Customers forget passwords and lose their IDs (often at the same time they lose their wireless device). By the same token, passwords can be socially engineered, hacked or stolen, and driver's licenses and other government-issued ID cards can be faked."); *but see* AT&T Comments at 5 ("Anti-fraud measures developed consistent with the Commission's existing authentication requirements protect consumers in most instances.").

[337] *See, e.g.*, Princeton Comments at 8 ("The Commission's proposed rules would establish five separate customer authentication standards: (1) telephone access to CPNI, (2) online access to CPNI, (3) in-store access to CPNI, (4) SIM swaps, and (5) number portability."); Princeton Comments at 10 ("[A] unified approach will be easier to implement: carriers need only adopt one compliant customer authentication system for all account access and operations.").

adopting more secure measures;[338] (4) a prescribed list provides a road map for bad actors;[339] and (5) the existing CPNI authentication requirements could undermine stronger authentication measures for SIM changes and number ports.[340] Harmonization also would be consistent with commenters' assertions that carriers need flexibility to implement more secure authentication measures.[341] We seek comment on these justifications.

100. We also seek comment on other potential justifications for harmonization. For instance, we tentatively conclude that harmonized authentication and protection requirements will be easier for wireless providers to implement and therefore will reduce costs and burdens on carriers, including small carriers. We further tentatively conclude that multiple authentication standards and protection requirements may be confusing for customers. Are these tentative conclusions correct?

101. We seek comment on any reasons why we should not harmonize our CPNI and SIM change authentication rules. For example, would it be costly and burdensome for carriers, particularly small carriers, to adjust the CPNI authentication and protection practices they have already implemented to comply with the authentication requirements we adopted today? Are there other reasons harmonized rules would increase the costs or burdens on carriers, including small carriers? Is there anything unique about CPNI or SIM changes that warrants different authentication measures? For instance, even if the existing measures for CPNI authentication may be outdated and less secure, are modifications to the rules unwarranted because the risk of harm from unauthorized access to CPNI is lower than from SIM swap fraud?

102. If we do choose to harmonize the rules addressing customer access to CPNI with our new SIM change safeguards, we seek comment on the extent to which the rules should be harmonized. We seek comment whether to remove the prescriptive authentication requirements in our current CPNI rules[342] and replace them with the single requirement that carriers use secure methods of authenticating the identity of a customer prior to disclosing CPNI. We also seek comment on whether to use the same definition of secure methods of authentication, which are those that are reasonably designed to confirm a customer's identity and excluding use of readily available biographical information, account information, recent payment information, call detail information, or any combination of these factors.[343] Additionally, we seek comment whether the procedures we require carriers to adopt for responding to failed

[338] *See, e.g.*, AT&T Comments at 14 ("Moreover, locking in a particular list of authentication methods would play into bad actors' hands by discouraging carriers from adopting new methods not expressly blessed by the Commission's rule, while inhibiting the ability of carriers and other stakeholders to innovate, as necessary and appropriate, to address evolving threats.").

[339] *See, e.g.*, AT&T Comments at 14-15 (asserting that "fixed authentication methods for SIM changes and port-outs will provide a roadmap to bad actors"); CTIA Comments at 11 ("[R]igid and prescriptive requirements hurt security more than they may help. . . . To this point, the NPRM asks whether 'requiring specific methods of authentication provides a 'roadmap' to bad actors.' The answer is a resounding yes.") (footnote omitted).

[340] *See, e.g.*, Princeton Comments at 10 (describing how "a unified approach to customer authentication avoids subtle inconsistencies between levels of authentication that could undermine multi-factor authentication" used for SIM swaps and number ports).

[341] *See, e.g.*, CCA Comments at 5 ("[T]he Commission should allow for flexibility for carriers to respond quickly and nimbly to new threats and to encourage adopting innovative solutions to threats."); Princeton Comments at 4 ("Authentication methods and security practices continue to evolve, and carriers should be welcome—and encouraged—to adopt innovative safeguards."); Somos Comments at 2 ("As with most fraud the telecom industry suffers, the bad actors are constantly evolving. Solutions should evolve, as well."); Verizon Comments at 7 ("To keep ahead of bad actors, providers need flexibility to employ other more secure alternatives to passwords and government-issued IDs."); Better Identity Coalition at 4 ("Any regulatory approach that seeks to tie MNOs to using specific authentication technologies is certain to fail to keep up as threat and security both evolve.").

[342] *See* 47 CFR § 64.2010(b)-(e).

[343] *See supra* section III.A.1.

authentication attempts in connection with SIM change requests should apply to all other CPNI authentications as well.[344] We also seek comment on whether the CPNI customer access rules should be harmonized with any of the other SIM change protections we adopt today. Should the CPNI rules only be harmonized to include some of these measures? If so, which measures should and should not be harmonized and why? Should we harmonize the customer notification rules for all account changes? Additionally, are there any other rules that would need to be modified for consistency if we harmonize the CPNI rules, such as the Commission's Telecommunications Relay Service (TRS) CPNI rules?[345] Should the Commission apply any harmonized rules to all customer proprietary information?

103. We tentatively conclude that we should rely on the same legal authority we used to originally implement the CPNI authentication rules in order to harmonize any of the CPNI rules, and seek comment on this tentative approach. In the *2007 CPNI Order*, as with the rules we adopted today, we relied primarily on section 222 to implement the CPNI authentication rules, and we tentatively conclude this provision continues to provide us with sufficient authority to harmonize those rules with the SIM change rules.[346] We seek comment on this tentative conclusion. We also seek comment on whether there are any legal implications for the harmonization approach we propose. For instance, in the *2016 Broadband Privacy Order*, the Commission harmonized the CPNI rules for voice providers with those it had adopted for broadband Internet access service providers,[347] but those rules were nullified by Congress pursuant to the Congressional Review Act,[348] which prohibits the Commission from reissuing a disapproved rule "in substantially the same form" and from issuing a new rule "that is substantially the same as such a rule."[349] We tentatively conclude that the 2017 action by Congress has no effect on the options we may consider here and seek comment on this tentative conclusion.

104. *Harmonizing Government Efforts to Address SIM Swap and Port-Out Fraud*. We seek comment on what steps the Commission can take to harmonize government efforts to address SIM swap and port-out fraud.[350] As several commenters noted, SIM swap and port-out fraud implicates the authentication practices of other industries.[351] We recognize that there may be other efforts within the

[344] *See supra* section III.A.2.

[345] *See, e.g.*, 47 CFR § 64.5110.

[346] *See 2007 CPNI Order*, 22 FCC Rcd at 6930-31, paras. 4-6; *supra* section III.E.

[347] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911, 13913, para. 3 (2016).

[348] Joint Resolution, Pub. L. No. 155-22 (2017).

[349] 5 U.S.C. § 801(b)(2).

[350] T-Mobile Comments at 14 ("[T]he FCC could coordinate with other regulators, such as financial services or healthcare regulators, on strategies. Other regulators may consider new rules on authentication and steer companies away from relying on methods that are not suitable given the nature and sensitivity of information or functions being accessed.").

[351] *See, e.g.*, Verizon Comments at 7 ("While a wireless provider's practices could prove to be reasonable, effective and thorough, the fraud prevention practices of the customer's financial institution, or the customer's email provider, may not."); AT&T Comments at 2 ("SIM swap or port-out [fraud] is only a small part of the scheme to harm the consumer, as these incidents implicate a range of stakeholders not controlled by carriers (e.g., financial institutions, cryptocurrency companies, text message aggregators) that all play a role in the verification of customer identity."); T-Mobile Comments at 1-2 ("[C]ombatting SIM swap and port-out fraud is a team effort that requires action by an entire ecosystem that includes carriers and subscribers as well as financial institutions, email providers, retail websites, social media companies and others who rely on various customer authentication methods."); CTIA Comments at 2 ("All actors across the mobile and Internet ecosystem—including financial and social media companies whose users' accounts are often targeted—must work together to thwart the bad actors that perpetrate these crimes."); CCA Comments at 1 ("[M]obile customers' phones have become the link between an individual's sensitive health records, banking and financial information, email, and social media accounts. SIM swap and port out fraud are two methods that malicious actors increasingly are using not only to steal mobile accounts, but also to (continued….)

government to tackle SIM swap and port-out fraud to address the broader implications of these harmful practices. We seek information about those other efforts and the extent to which they seek to address the practices of wireless providers. We also seek comment on how the Commission can work with other government entities to harmonize our approaches to addressing SIM swap and port-out fraud.

105. *Other Consumer Protection Measures*. We reiterate the Commission's request for comment on whether there are any additional requirements the Commission should consider that would help protect customers from SIM swap or port-out fraud or assist them with resolving problems resulting from such incidents.[352] For example, should we require wireless providers to explicitly exclude resolution of SIM change and port-out fraud disputes from arbitration clauses in providers' agreements with customers or abrogate such clauses?[353] Would this provide meaningful additional protections to customers from SIM swap and port-out fraud? What would be the costs to wireless providers, particularly small providers, from such a requirement?

106. *Digital Equity and Inclusion.* Finally, the Commission, as part of its continuing effort to advance digital equity for all,[354] including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations[355] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well as the scope of the Commission's relevant legal authority.

V. PROCEDURAL MATTERS

107. *Paperwork Reduction Act Analysis*. This *Report and Order* may contain new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. All such requirements will be submitted to OMB for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on any new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. § 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

108. In this *Report and Order*, we have assessed the effects of required customer notifications and notices, and related recordkeeping requirements, to protect customers from SIM swap and port-out fraud, and find that they do not place a significant burden on small businesses. Although no commenters specifically addressed whether such requirements may place burdens on small wireless providers, we note

engage in broader identity theft."); Princeton Comments at 12 ("SIM swaps are an increasing attack vector for online account compromises, especially in the financial services sector.").

[352] *See SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14144, para. 68.

[353] NCLC/EPIC Comments at 6.

[354] Section 1 of the Communications Act of 1934 as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex." 47 U.S.C. § 151.

[355] The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (January 20, 2021).

that CCA advised the Commission to "keep in mind the constraints with which many small carriers operate against in adopting security measures," asserting that any rules "should allow carriers to use technologies that are reasonably available and have choice in the approach to take in authenticating their customers."[356] As a general matter, the baseline, flexible rules we adopt reflect our recognition that, in some cases, strict prescriptive requirements to prevent SIM swap and port-out fraud could be technically and economically infeasible for wireless providers to implement, particularly for smaller providers.[357] We emphasize that the record shows that many wireless providers already have in place some of the policies and procedures we adopt today and that our rules may therefore only require them to adapt, refine, or consistently apply those existing practices.[358] Additionally, by setting baseline requirements and giving wireless providers flexibility on how to meet them, we allow providers to adopt the most cost-effective and least burdensome solutions to achieve the level of security needed to protect customers against SIM swap and port-out fraud in a given circumstance.[359] We have further minimized the potential burdens of customer notifications by declining to prescribe particular content and wording and giving wireless providers flexibility on how to deliver such notifications.[360] Similarly, for customer notices, we declined to require a specific format and content, and we declined to require such notices be delivered to customers annually.[361] Further, we mitigated potential burdens of the recordkeeping requirement by declining to require that wireless providers include historic data in their recordkeeping, which we acknowledged would be particularly burdensome for small providers, and declining to require that providers report this data to the Commission regularly.[362]

109. The *Further Notice of Proposed Rulemaking* may contain new or modified information collection(s) subject to the Paperwork Reduction Act of 1995.[363] All such new or modified information collection requirements will be submitted to OMB for review under section 3507(d) of the PRA. OMB, the general public, and other federal agencies are invited to comment on any new or modified information collection requirements contained in this proceeding. In addition, pursuant to the Small Business Paperwork Relief Act of 2002,[364] we seek specific comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees."[365]

110. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA)[366] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[367] Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the potential impact of the rule and policy changes adopted in this *Report and Order* on small entities. The FRFA is set forth in Appendix B.

---

[356] CCA Comments at 6. *See also* RWA Comments at 12-13 (advocating for uniform authentication standards to avoid anticompetitive effects and other costs or burdens on small wireless providers).

[357] *See supra* para. 23.

[358] *See supra* paras. 20, 23, 37, 42, 57, 60, 64, 67, 70.

[359] *See supra* para. 23.

[360] *See* sections III.A.3& III.B.2.

[361] *See supra* section III.C..

[362] *See supra* section III.A.5.

[363] Pub. L. No. 104-13.

[364] Pub. L. No. 107-198.

[365] 44 U.S.C. § 3506(c)(4).

[366] 5 U.S.C. § 603. The RFA, 5 U.S.C. § 601 et seq., has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[367] 5 U.S.C. § 605(b).

111. We have also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of rule and policy change proposals in the *Further Notice* on small entities. The IRFA is set forth in Appendix C. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the *Further Notice* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

112. *Congressional Review Act.* [The Commission will submit this draft *Report and Order* to the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, for concurrence as to whether this rule is "major" or "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2).] The Commission will send a copy of this *Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

113. *Ex Parte Presentations*. The proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must: (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

114. *Comment Period and Filing Procedures*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS) or by paper. Commenters should refer to WC Docket No. 21-341 when filing in response to this *Further Notice*.

- Electronic Filers: Comments may be filed electronically by accessing ECFS at https://www.fcc.gov/ecfs.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. Paper filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings.[368]
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority Mail must be addressed to 45 L Street NE, Washington, D.C. 20554.

[368] *See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, DA 20-304, Public Notice, 35 FCC Rcd 2788 (2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

115. *Providing Accountability Through Transparency Act*. The Providing Accountability Through Transparency Act requires each agency, in providing notice of a rulemaking, to post online a brief plain-language summary of the proposed rule.[369] Accordingly, the Commission will publish the required summary of this *Further Notice of Proposed Rulemaking* on https://www.fcc.gov/proposed-rulemakings.

116. *People with Disabilities.* To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the FCC's Consumer and Governmental Affairs Bureau at (202) 418-0530 (voice).

117. *Additional Information.* For additional information on this proceeding, contact Melissa Kirkel, Wireline Competition Bureau, Competition Policy Division, at 202-418-7958 or melissa.kirkel@fcc.gov.

VI. ORDERING CLAUSES

118. Accordingly, IT IS ORDERED that, pursuant to the authority contained in sections 1, 2, 4, 201, 222, 251, 303, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154, 201, 222, 251, 303, and 332, this *Report and Order* in WC Docket No. 21-341 IS ADOPTED and that Parts 52 and 64 of the Commission's Rules, 47 CFR Parts 52, 64, are AMENDED as set forth in Appendix A.

119. IT IS FURTHER ORDERED that this *Report and Order* SHALL BE EFFECTIVE 30 days after publication in the Federal Register, and that compliance with the rules adopted herein shall be required six months after the effective date of the *Report and Order*, except that the amendments to sections 52.37(c), 52.37(d), 52.37(e), 52.37(g), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8) of the Commission's rules, 47 CFR §§ 52.37(c), 52.37(d), 52.37(e), 52.37(g), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8), which may contain new or modified information collection requirements, will not become effective until the later of i) six months after the effective date of this *Report and Order*; or ii) after the Office of Management and Budget completes review of any information collection requirements associated with this *Report and Order* that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act. The Commission directs the Wireline Competition Bureau to announce the compliance date for sections 52.37(c), 52.37(d), 52.37(e), 52.37(g), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8) by subsequent Public Notice and to cause 47 CFR § 52.37 and § 64.2010 to be revised accordingly.

120. IT IS FURTHER ORDERED that pursuant to the authority contained in sections 1, 2, 4, 201, 222, 251, 303, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154, 201, 222, 251, 303, and 332, this *Further Notice of Proposed Rulemaking* in WC Docket No. 21-341 IS ADOPTED.

121. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, Reference Information Center, SHALL SEND a copy of this *Report and Order* and *Further Notice of Proposed Rulemaking*, including the Final Regulatory Flexibility Analysis and Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

[369] 5 U.S.C. § 553(b)(4). The Providing Accountability Through Transparency Act, Pub. L. No. 118-9 (2023), amended section 553(b) of the Administrative Procedure Act.

122. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance and Program Management, SHALL SEND a copy of this *Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. § 801(a)(1)(A).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

The Federal Communications Commission amends Parts 52 and 64 of Title 47 of the Code of Federal Regulations as follows:

PART 52 – NUMBERING

1. The authority citation for part 52 continues to read as follows:

AUTHORITY: 47 U.S.C. 151, 152, 153, 154, 155, 201-205, 207-209, 218, 225-227, 251-252, 271, 303, 332, unless otherwise noted.

2. Add § 52.37 to subpart C to read as follows:

§ 52.37 Number Portability Requirements for Wireless Providers

(a) *Applicability.* This section applies to all providers of commercial mobile radio service (CMRS), as defined in 47 CFR § 20.3, including resellers of wireless service.

(b) *Authentication of port-out requests.* A CMRS provider shall use secure methods to authenticate a customer that are reasonably designed to confirm the customer's identity before effectuating a port-out request, except to the extent otherwise required by 47 U.S.C. § 345 (Safe Connections Act of 2022) or Part 64 Subpart II of this chapter. A CMRS provider shall regularly, but not less than annually, review and, as necessary, update its customer authentication methods to ensure that its authentication methods continue to be secure.

(c) *Customer notification of port-out requests*. Upon receiving a port-out request, and before executing the request, a CMRS provider shall immediately notify the customer that a port-out request associated with the customer's account was made, delivered in accordance with customer preferences, if indicated, and using means reasonably designed to reach the customer associated with the account and clear and concise language that provides sufficient information to effectively inform a customer that a port-out request involving the customer's number was made, except if the port-out request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. § 345 and Part 64, Subpart II of this chapter.

(d) *Account locks.* A CMRS provider shall offer customers, at no cost, the option to lock their accounts to prohibit the CMRS provider from processing requests to port the customer's number. A CMRS provider shall not fulfill a port-out request until the customer deactivates the lock on the account, except if the port-out request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. § 345 and Part 64, Subpart II of this chapter. The process to activate and deactivate an account lock must not be unduly burdensome for customers such that it effectively inhibits customers from implementing their choice. A CMRS provider may activate a port-out lock on a customer's account when the CMRS provider has a reasonable belief that the customer is at high risk of fraud, but must provide the customer with clear notification that the account lock has been activated with instructions on how the customer can deactivate the account lock, and promptly comply with the customer's legitimate request to deactivate the account lock.

(e) *Notice of Account Protection Measures*. A CMRS provider must provide customers with notice, using clear and concise language, of any account protection measures the CMRS provider offers, including those to prevent port-out fraud. A CMRS provider shall make this notice easily accessible through the CMRS provider's website and application.

(f) *Employee Training.* A CMRS provider shall develop and implement training for employees to specifically address fraudulent port-out attempts, complaints, and remediation. Training shall include, at a minimum, how to identify fraudulent requests, how to recognize when a customer may be the victim of fraud, and how to direct potential victims and individuals making potentially fraudulent requests to employees specifically trained to handle such incidents.

(g) *Procedures to resolve fraudulent ports.* A CMRS provider shall, at no cost to customers:

(1) maintain a clearly disclosed, transparent, and easy-to-use process for customers to report fraudulent number ports;

(2) promptly investigate and take reasonable steps within its control to remediate fraudulent number ports; and

(3) promptly provide customers, upon request, with documentation of fraudulent number ports involving their accounts.(h) This section may contain information-collection and/or recordkeeping requirements. Compliance with this section will not be required until this paragraph is removed or contains a compliance date, which will not occur until the later of: i) [INSERT DATE SIX MONTHS AFTER THE EFFECTIVE DATE OF THIS REPORT AND ORDER]; or ii) after the Office of Management and Budge completes review of any information collection requirements in this section that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act or the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for this section by subsequent Public Notice and to cause this section to be revised accordingly.

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

3. The authority citation for part 64 continues to read as follows:

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 262, 276, 303, 332, 403(b)(2)(B), (c), 616, 620, 1004, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

4. Revise § 64.2010 by revising paragraph (a) and adding paragraphs (h) and (i) to read as follows:

§ 64.2010 Safeguards on the disclosure of customer proprietary network information.

(a) *Safeguarding CPNI.* Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit. Telecommunications carriers shall establish safeguards and processes so that employees who interact directly with customers are unable to access CPNI until after a customer has been properly authenticated.

* * * * *

(h) *Subscriber Identity Module (SIM) changes.* A provider of commercial mobile radio service (CMRS), as defined in 47 CFR § 20.3, including resellers of wireless service, shall only effectuate SIM change requests in accordance with this section. For purposes of this section, SIM means a physical or virtual card associated with a device that stores unique information that can be identified to a specific mobile network.

(1) *Customer authentication.* A CMRS provider shall use secure methods to authenticate a customer that are reasonably designed to confirm the customer's identity before executing a SIM change request, except to the extent otherwise required by 47 U.S.C. § 345(Safe Connections Act of 2022) () or Part 64, Subpart II of this chapter. Authentication methods shall not rely on readily available biographical information, account information, recent payment information, or call detail information unless other permitted under 47 U.S.C. § 345 or Part 64, Subpart II of this chapter. A CMRS provider shall regularly, but not less than annually, review and, as necessary, update its customer authentication methods to ensure that its authentication methods continue to be secure.

(2) *Response to failed authentication attempts.* A CMRS provider shall immediately notify a customer of a failed authentication attempt associated with the customer's account in connection with a SIM change request, using clear and concise language and means reasonably designed to reach the customer associated with the account, except to the extent otherwise required by 47 U.S.C. § 345 (Safe

Connections Act of 2022) or Part 64, Subpart II of this chapter. A CMRS provider shall also develop, maintain, and implement procedures for addressing failed authentication attempts in connection with a SIM change request that are reasonably designed to prevent unauthorized access to a customer's account, which, among other things, take into consideration the needs of survivors pursuant to 47 U.S.C. § 345 and Part 64, Subpart II of this chapter.

(3) *Customer notification of SIM change requests*. Upon receiving a SIM change request, and before effectuating the request, a CMRS provider shall immediately notify the customer that a SIM change request associated with the customer's account was made, delivered in accordance with customer preferences, if indicated, and using means reasonably designed to reach the customer associated with the account and clear and concise language that provides sufficient information to effectively inform a customer that a SIM change request involving the customer's SIM was made, except if the SIM change request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. § 345 and Part 64, Subpart II of this chapter.

(4) *Account locks.* A CMRS provider shall offer customers, at no cost, the option to lock their accounts to prohibit the CMRS provider from processing requests to change the customer's SIM. A CMRS provider shall not fulfill a SIM change request until the customer deactivates the lock on the account, except if the SIM change request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. § 345 and Part 64, Subpart II of this chapter. The process to activate and deactivate an account lock must not be unduly burdensome for customers such that it effectively inhibits customers from implementing their choice. A CMRS provider may activate a SIM change lock on a customer's account when the CMRS provider has a reasonable belief that the customer is at high risk of fraud, but must provide the customer with clear notification that the account lock has been activated with instructions on how the customer can deactivate the account lock, and promptly comply with the customer's legitimate request to deactivate the account lock.

(5) *Notice of account protection measures.* A CMRS provider must provide customers with notice, using clear and concise language, of any account protection measures the CMRS provider offers, including those to prevent SIM swap fraud. A CMRS provider shall make this notice easily-accessible through the CMRS provider's website and application.

(6) *Procedures to resolve fraudulent SIM changes.* A CMRS provider shall, at no cost to customers:

(i) maintain a clearly disclosed, transparent, and easy-to-use process for customers to report fraudulent SIM changes;

(ii) promptly investigate and take reasonable steps within its control to remediate fraudulent SIM changes; and

(iii) promptly provide customers, upon request, with documentation of fraudulent SIM changes involving their accounts.

(7) *Employee training.* A CMRS provider shall develop and implement training for employees to specifically address fraudulent SIM change attempts, complaints, and remediation. Training shall include, at a minimum, how to identify potentially fraudulent SIM change requests, how to identify when a customer may be the victim of SIM swap fraud, and how to direct potential victims and individuals making potentially fraudulent requests to employees specifically trained to handle such incidents.

(8) *SIM change recordkeeping.* A CMRS provider shall track, and maintain for a minimum of three years, the total number of SIM change requests it received, the number of successful SIM change requests, the number of failed SIM change requests, the number of successful fraudulent SIM change requests, the average time to remediate a fraudulent SIM change, the total number of complaints received regarding fraudulent SIM change requests, the authentication measures the CMRS provider has implemented, and when those authentication measures change. A CMRS provider shall provide such data and information to the Commission upon request.

(9) *Compliance.* Paragraph (h) may contain information-collection and/or recordkeeping requirements. Compliance with paragraph (h) will not be required until this subparagraph is removed or contains a compliance date, which will not occur until the later of: i) [INSERT DATE SIX MONTHS AFTER THE EFFECTIVE DATE OF THIS REPORT AND ORDER]; or ii) after the Office of Management and Budge completes review of any information collection requirements in paragraph (h) that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act or the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for this paragraph (h) by subsequent Public Notice and to cause this paragraph to be revised accordingly.

APPENDIX B

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Protecting Consumers from SIM Swap and Port-Out Fraud Notice of Proposed Rulemaking* (*SIM Swap and Port-Out Fraud Notice*) released in September 2021.[2] The Commission sought written public comment on the proposals in the *SIM Swap and Port-Out Fraud Notice*, including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Report and Order

2. The *Report and Order* establishes protections to address SIM swap and port-out fraud. With SIM swap fraud, a bad actor impersonates a customer of a wireless provider and convinces the provider to reassign the customer's SIM from the customer's device to a device controlled by the bad actor. Similarly, with port-out fraud, the bad actor impersonates a customer of a wireless provider and convinces the provider to port the customer's telephone number to a new wireless provider and a device that the bad actor controls.[4] Both fraudulent practices transfer the victim's wireless service to the bad actor, allow the bad actor to gain access to information associated with the customer's account, and permit the bad actor to receive the text messages and phone calls intended for the customer.

3. The rules adopted in the *Report and Order* aim to foreclose these fraudulent practices while preserving the relative ease with which customers can obtain legitimate SIM changes and number ports. Specifically, the *Report and Order* revises the Commission's CPNI and LNP rules to require that wireless providers use secure methods of authenticating customers prior to performing SIM changes and number ports. This requirement is reinforced by other rules, including that wireless providers 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 interact with customers from accessing CPNI until after customers have 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 that wireless providers 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. Additionally, the *Report and Order* establishes requirements to minimize the harms of SIM swap and port-out fraud when it occurs, including requiring wireless providers to maintain a clear process for customers to report fraud, 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.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

4. There were no comments that directly addressed the proposed rules and policies presented in the *SIM Swap and Port-Out Fraud Notice* IRFA. However two commenters discussed the potential impact of rules on small carriers. The Competitive Carriers Association (CCA) advocated that the Commission adopt security measures that give providers flexibility to account for the constraints with

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *SIM Swap and Port-Out Fraud Notice*, 36 FCC Rcd at 14152-14161, para. 6., Appx. B.

[3] 5 U.S.C. § 604.

[4] FCC, *Port-Out Fraud Targets Your Private Accounts*, https://www.fcc.gov/port-out-fraud-targets-your-private-accounts (last updated July 10, 2023).

which many small providers operate.[5] The Rural Wireless Association (RWA) called for uniform standards for port-out authentication to prevent potential anticompetitive activities and increased costs for small providers in the event that larger providers hold small providers to standards that are difficult or costly to implement.[6] The approach taken by the *Report and Order* addresses these comments by setting baseline requirements that build on existing mechanisms that many wireless providers already use to establish a uniform framework across the mobile wireless industry, while giving wireless providers the flexibility to deliver the most advanced, appropriate, and cost-effective fraud protection measures available.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

5. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[7] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[8] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[9] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[10] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[11]

7. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[12] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[13] These types of small

[5] *See* CCA Comments at 6.

[6] *See* RWA Comments at 12-14.

[7] 5 U.S.C. § 604(a)(3).

[8] *Id.* § 604 (a)(4).

[9] *Id.* § 601(6).

[10] *Id.* § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[11] 15 U.S.C. § 632.

[12] *See* 5 U.S.C. § 601(3)-(6).

[13] SBA, Office of Advocacy, "What's New With Small Business?," https://advocacy.sba.gov/wp-content/uploads/2023/03/Whats-New-Infographic-March-2023-508c.pdf (Mar. 2023).

businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.[14]

8. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[15] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[16] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[17]

9. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[18] U.S. Census Bureau data from the 2017 Census of Governments[19] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[20] Of this number, there were 36,931 general purpose governments (county,[21] municipal, and town or township[22]) with populations of

[14] *Id*.

[15] *See* 5 U.S.C. § 601(4).

[16] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number of small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file," https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[17] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000 for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[18] 5 U.S.C. § 601(5).

[19] 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[20] U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[21] *Id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[22] *Id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

less than 50,000 and 12,040 special purpose governments—independent school districts[23] with enrollment populations of less than 50,000.[24] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[25]

1. Providers of Telecommunications and Other Services

10. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[26] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband Internet services.[27] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[28] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[29]

11. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[30] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[31] Of this number, 2,964 firms operated with fewer than 250 employees.[32] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged

---

[23] *Id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[24] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[25] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[26] U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[27] *Id.*

[28] *Id.*

[29] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[30] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[31] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[32] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

in the provision of fixed local services.[33] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[34] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

12. *Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers[35] is the closest industry with an SBA small business size standard.[36] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[37] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[38] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[39] Of this number, 2,964 firms operated with fewer than 250 employees.[40] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were fixed local exchange service providers.[41] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[42] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. *Incumbent Local Exchange Carriers (Incumbent LECs).* Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[43] is the closest industry with an SBA small business size standard.[44] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[45] U.S. Census Bureau data for 2017 show that there were 3,054 firms

---

[33] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[34] *Id.*

[35] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[36] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[37] Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[38] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[39] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[40] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[41] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[42] *Id.*

[43] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[44] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[45] *Id.*

in this industry that operated for the entire year.[46] Of this number, 2,964 firms operated with fewer than 250 employees.[47] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers.[48] Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees.[49] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

14. *Competitive Local Exchange Carriers (Competitive LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers.[50] Wired Telecommunications Carriers[51] is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[52] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[53] Of this number, 2,964 firms operated with fewer than 250 employees.[54] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local exchange service providers.[55] Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees.[56] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications

[46] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[47] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[48] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[49] *Id.*

[50] Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[51] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[52] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[53] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[54] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[55] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[56] *Id.*

Carriers[57] is the closest industry with an SBA small business size standard.[58] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[59] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[60] Of this number, 2,964 firms operated with fewer than 250 employees.[61] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees.[62] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

16. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard.[63] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[64] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[65] Mobile virtual network operators (MVNOs) are included in this industry.[66] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[67] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[68] Of that number, 1,375 firms operated with fewer than 250 employees.[69] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported

[57] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[58] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[59] *Id.*

[60] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[61] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[62] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[63] *See* U.S. Census Bureau, *2017 NAICS Definition*, *"517911 Telecommunications Resellers,"* https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[64] *Id.*

[65] *Id*.

[66] *Id*.

[67] 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[68] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[69] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

they were engaged in the provision of local resale services.[70] Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees.[71] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

17. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[72] is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[73] Mobile virtual network operators (MVNOs) are included in this industry.[74] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[75] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[76] Of that number, 1,375 firms operated with fewer than 250 employees.[77] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 457 providers that reported they were engaged in the provision of toll services.[78] Of these providers, the Commission estimates that 438 providers have 1,500 or fewer employees.[79] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[80] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless Internet access, and wireless video services.[81] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[82] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this

[70] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[71] *Id.*

[72] *See* U.S. Census Bureau, *2017 NAICS Definition*, *"517911 Telecommunications Resellers,"* https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[73] *Id.*

[74] *Id*.

[75] 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[76] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[77] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[78] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[79] *Id.*

[80] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[81] *Id.*

[82] 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

industry that operated for the entire year.[83] Of that number, 2,837 firms employed fewer than 250 employees.[84] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services.[85] Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees.[86] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

19. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[87] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small.[88] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[89] Of this number, 242 firms had revenue of less than $25 million.[90] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 65 providers that reported they were engaged in the provision of satellite telecommunications services.[91] Of these providers, the Commission estimates that approximately 42 providers have 1,500 or fewer employees.[92] Consequently, using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

20. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[93] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from,

---

[83] U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[84] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[85] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[86] *Id.*

[87] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[88] 13 CFR § 121.201, NAICS Code 517410.

[89] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[90] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[91] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[92] *Id.*

[93] *See* U.S. Census Bureau, *2017 NAICS Definition*, *"517919 All Other Telecommunications,"* https://www.census.gov/naics/?input=517919&year=2017&details=517919.

satellite systems.[94] Providers of Internet services (e.g. dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[95] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[96] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[97] Of those firms, 1,039 had revenue of less than $25 million.[98] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

2. Internet Service Providers

21. *Wired Broadband Internet Access Service Providers (Wired ISPs)*.[99] Providers of wired broadband Internet access service include various types of providers except dial-up Internet access providers. Wireline service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[100] Wired broadband Internet services fall in the Wired Telecommunications Carriers industry.[101] The SBA small business size standard for this industry classifies firms having 1,500 or fewer employees as small.[102] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[103] Of this number, 2,964 firms operated with fewer than 250 employees.[104]

22. Additionally, according to Commission data on Internet access services as of December 31, 2018, nationwide there were approximately 2,700 providers of connections over 200 kbps in at least one direction using various wireline technologies.[105] The Commission does not collect data on the

---

[94] *Id.*

[95] *Id*.

[96] 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[97] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[98] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[99] Formerly included in the scope of the Internet Service Providers (Broadband), Wired Telecommunications Carriers and All Other Telecommunications small entity industry descriptions.

[100] 47 CFR § 1.7001(a)(1).

[101] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[102] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[103] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[104] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[105] *IAS Status 2018*, Fig. 30 (The technologies used by providers include aDSL, sDSL, Other Wireline, Cable Modem and FTTP). Other wireline includes: all copper-wire based technologies other than xDSL (such as Ethernet over copper, T-1/DS-1 and T3/DS-1) as well as power line technologies which are included in this category to maintain the confidentiality of the providers.

number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, in light of the general data on fixed technology service providers in the Commission's *2022 Communications Marketplace Report*,[106] we believe that the majority of wireline Internet access service providers can be considered small entities.

23. *Wireless Broadband Internet Access Service Providers (Wireless ISPs or WISPs)*.[107] Providers of wireless broadband Internet access service include fixed and mobile wireless providers. The Commission defines a WISP as "[a] company that provides end-users with wireless access to the Internet[.]"[108] Wireless service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[109] Neither the SBA nor the Commission have developed a size standard specifically applicable to Wireless Broadband Internet Access Service Providers. The closest applicable industry with an SBA small business size standard is Wireless Telecommunications Carriers (except Satellite).[110] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[111] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[112] Of that number, 2,837 firms employed fewer than 250 employees.[113]

24. Additionally, according to Commission data on Internet access services as of December 31, 2018, nationwide there were approximately 1,209 fixed wireless and 71 mobile wireless providers of connections over 200 kbps in at least one direction.[114] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, based on data in the Commission's *2022 Communications Marketplace Report* on the small number of large mobile wireless nationwide and regional facilities-based providers, the dozens of small regional facilities-based providers and the number of wireless mobile virtual network providers in general,[115] as well as on terrestrial fixed wireless broadband providers in general,[116] we believe that the majority of wireless Internet access service providers can be considered small entities.

---

[106] *See Communications Marketplace Report*, GN Docket No. 22-203, 2022 WL 18110553 at 10, paras. 26-27, Figs. II.A.5-7. (2022) (*2022 Communications Marketplace Report*).

[107] Formerly included in the scope of the Internet Service Providers (Broadband), Wireless Telecommunications Carriers (except Satellite) and All Other Telecommunications small entity industry descriptions.

[108] Federal Communications Commission, Internet Access Services: Status as of December 31, 2018 *(IAS Status 2018)*, Industry Analysis Division, Office of Economics & Analytics (September 2020). The report can be accessed at https://www.fcc.gov/economics-analytics/industry-analysis-division/iad-data-statistical-reports.

[109] *See* 47 CFR § 1.7001(a)(1).

[110] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[111] 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[112] U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[113] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[114] *See IAS Status 2018*, Fig. 30.

[115] *2022 Communications Marketplace Report* , 2022 WL 18110553 at 27, paras. 64-68.

[116] *Id.* at 8, para. 22.

25. *Internet Service Providers (Non-Broadband).* Internet access service providers using client-supplied telecommunications connections (e.g., dial-up ISPs) as well as VoIP service providers using client-supplied telecommunications connections fall in the industry classification of All Other Telecommunications.[117] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[118] For this industry, U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[119] Of those firms, 1,039 had revenue of less than $25 million.[120] Consequently, under the SBA size standard a majority of firms in this industry can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

26. This *Report and Order* adopts rules that could result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance requirements for affected providers of service, including small wireless providers. Specifically, it requires that wireless providers use secure methods of authenticating customers prior to performing SIM changes and number ports, and to review and update these authentication methods as needed, but at least annually. It requires wireless providers to adopt processes for customer notification and response to failed authentication attempts, institute employee training for handling SIM swap and port-out fraud, and establish safeguards to prevent employees who interact with customers from accessing CPNI until after customers have been authenticated. The *Report and Order* also adopts rules requiring that wireless providers 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. Additionally, the *Report and Order* requires wireless providers to maintain a clear process for customers to report fraud, promptly investigate and remediate fraud, and promptly provide customers with documentation of fraud involving their accounts. Finally, the *Report and Order* requires that providers keep records of SIM change requests and the authentication measures they use.

27. We are cognizant that, in some instances, strict prescriptive requirements to prevent SIM swap and port-out fraud could be technically and economically infeasible for wireless providers to implement, particularly for smaller providers. The Commission does not have sufficient information on the record to determine whether small entities will be required to hire professionals to comply with its decisions or to quantify the cost of compliance for small entities. However, the record reflects that many wireless providers have already developed and implemented some form of the customer authentication requirements in the *Report and Order*, minimizing cost implications for small entities. We also permit wireless providers to use existing methods of notification that are reasonably designed to reach the affected customer. Several of our rules build on existing mechanisms that many wireless providers already use, and therefore, we expect that our new rules will further minimize the costs and burdens for those providers, and should significantly reduce compliance requirements for small entities that may have smaller staff and fewer resources.

---

[117] *See* U.S. Census Bureau, *2017 NAICS Definition, "517919 All Other Telecommunications,"* https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[118] 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[119] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[120] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

28. The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . .including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[121]

29. The requirements established in this *Report and Order* are designed to minimize the economic impact on wireless providers, including small providers. The baseline, flexible rules adopted reflect a recognition that, in some cases, strict prescriptive requirements to prevent SIM swap and port-out fraud could be technically and economically infeasible for wireless providers to implement, particularly for smaller providers. We therefore decline to adopt certain specific authentication methods mentioned in the *SIM Swap and Port-Out Fraud Notice* because they may discourage carriers from adopting new methods to address evolving techniques used by bad actors. The record shows that many wireless providers already have in place some of the policies and procedures this *Report and Order* adopts and that the rules may therefore only require them to adapt, refine, or consistently apply those existing practices. Additionally, by setting baseline requirements and giving wireless providers flexibility on how to meet them, this *Report and Order* allows providers to adopt the most cost-effective and least burdensome solutions to achieve the level of security needed to protect customers against SIM swap and port-out fraud in a given circumstance. The *Report and Order* further minimizes any potential burdens of customer notifications by declining to prescribe particular content and wording and giving wireless providers flexibility on how to deliver such notifications. Similarly, for customer notices, the *Report and Order* declines to require a specific format and content and declines to require such notices be delivered to customers annually. With respect to employee training, we decline to adopt overly prescriptive safeguards, such as two-employee sign off. Instead, the requirement this *Report and Order* adopts minimizes potential burdens because it builds on the Commission's existing CPNI training rule and gives wireless providers flexibility on how to develop their training programs. Further, the *Report and Order* mitigates the potential burdens of the recordkeeping requirement by declining to require that wireless providers include historic data in their recordkeeping, which the *Report and Order* acknowledged would be particularly burdensome for small providers, and declining to require that providers report this data to the Commission regularly.

G. Report to Congress

30. The Commission will send a copy of the *SIM Swap and Port-Out Fraud Report and Order*, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act.[122] In addition, the Commission will send a copy of the *SIM Swap and Port-Out Fraud Report and Order*, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *SIM Swap and Port-Out Fraud Report and Order* (or summaries thereof) will also be published in the Federal Register.[123]

[121] 5 U.S.C. § 604(a)(6).

[122] *Id*. § 801(a)(1)(A).

[123] *Id*. § 604(b).

APPENDIX C

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the *Protecting Consumers from SIM Swap and Port-Out Fraud Further Notice of Proposed Rulemaking* (*Further Notice*). Written comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *Further Notice* provided on the first page of the item. The Commission will send a copy of the *Further Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the *Further Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

2. In the *SIM Swap and Port-Out Fraud Report and Order* (*Report and Order*), the Commission adopts rules to address fraudulent practices that transfer a customer's wireless service to a bad actor, allowing the bad actor to gain access to information associated with the customer's account, and permitting the bad actor to receive the text messages and phone calls intended for the customer.. Specifically, the *Report and Order* revises the Commission's Customer Proprietary Network Information (CPNI) and Local Number Portability (LNP) rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider. The *Report and Order* also requires wireless providers to immediately notify customers whenever a SIM change or port-out request is made on customers' accounts, and take additional steps to protect customers from SIM swap and port-out fraud. This approach sets baseline requirements that establish a uniform framework across the mobile wireless industry while giving wireless providers the flexibility to deliver the most advanced and appropriate fraud protection measures available.

3. In this *Further Notice*, we seek comment on whether to harmonize the existing requirements governing customer access to CPNI[4] with the SIM change authentication and protection measures adopted in the *Report and Order*. This *Further Notice* expands on questions asked in the *SIM Swap and Port-Out Fraud Notice* and several comments in the record, but seeks more targeted feedback on a specific approach. The *Further Notice* explores whether justifications identified by commenters in the record, or any other justifications, provide a rationale for harmonizing the existing CPNI rules with the customer protection measures adopted in the *Report and Order*, as well as any reasons why the Commission should not harmonize its existing CPNI rules with the SIM swap fraud protection measures adopted in the *Report and Order*.

4. Recognizing that there may be other efforts within the government to tackle SIM swap and port-out fraud to address the broader implications of these harmful practices, the *Further Notice* also seeks comment on information about those other efforts and what steps the Commission can take to harmonize government efforts to address SIM swap and port-out fraud.

B. Legal Basis

5. The proposed action is authorized pursuant to sections 1, 4, 201, 222, 251, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 222, 251, 303(r), and 332.

---

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] 5 U.S.C. § 603(a).

[3] *Id.*

[4] *See* 47 CFR § 64.2010.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[5] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[6] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[7] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[8]

7. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[9] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.[11]

8. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[12] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[13] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[14]

---

[5] 5 U.S.C. § 603(b)(3).

[6] *Id.* § 601(6).

[7] *Id*. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[8] 15 U.S.C. § 632.

[9] 5 U.S.C. § 601(3)-(6).

[10] SBA, Office of Advocacy, "What's New With Small Business?," https://advocacy.sba.gov/wp-content/uploads/2023/03/Whats-New-Infographic-March-2023-508c.pdf. (Mar. 2023).

[11] *Id*.

[12] 5 U.S.C. § 601(4).

[13] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number of small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file," https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[14] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO

(continued….)

9. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[15] U.S. Census Bureau data from the 2017 Census of Governments[16] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[17] Of this number, there were 36,931 general purpose governments (county,[18] municipal, and town or township[19]) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts[20] with enrollment populations of less than 50,000.[21] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[22]

1. Providers of Telecommunications and Other Services

10. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[23] Transmission facilities may be based on a single technology or a

---

BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000 for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[15] 5 U.S.C. § 601(5).

[16] 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[17] U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[18] *Id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[19] *Id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[20] *Id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[21] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[22] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[23] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband Internet services.[24] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[25] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[26]

11. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[27] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[28] Of this number, 2,964 firms operated with fewer than 250 employees.[29] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services.[30] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[31] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

12. *Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers[32] is the closest industry with an SBA small business size standard.[33] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[34] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[35] U.S. Census Bureau data for 2017 show that there were 3,054 firms

[24] *Id.*

[25] *Id.*

[26] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[27] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[28] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[29] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[30] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[31] *Id.*

[32] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[33] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[34] Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VoIP Providers, Non-Interconnected VoIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[35] *Id.*

that operated in this industry for the entire year.[36] Of this number, 2,964 firms operated with fewer than 250 employees.[37] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were fixed local exchange service providers.[38] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[39] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. *Incumbent Local Exchange Carriers (Incumbent LECs).* Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[40] is the closest industry with an SBA small business size standard.[41] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[42] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[43] Of this number, 2,964 firms operated with fewer than 250 employees.[44] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers.[45] Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees.[46] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

14. *Competitive Local Exchange Carriers (Competitive LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service

[36] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[37] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[38] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[39] *Id.*

[40] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[41] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[42] *Id.*

[43] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[44] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[45] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[46] *Id.*

providers.[47] Wired Telecommunications Carriers[48] is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[49] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[50] Of this number, 2,964 firms operated with fewer than 250 employees.[51] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local exchange service providers.[52] Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees.[53] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[54] is the closest industry with an SBA small business size standard.[55] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[56] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[57] Of this number, 2,964 firms operated with fewer than 250 employees.[58] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or

[47] Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[48] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[49] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[50] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[51] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[52] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[53] *Id.*

[54] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[55] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[56] *Id.*

[57] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[58] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

fewer employees.[59] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

16. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard.[60] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[61] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[62] Mobile virtual network operators (MVNOs) are included in this industry.[63] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[64] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[65] Of that number, 1,375 firms operated with fewer than 250 employees.[66] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services.[67] Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees.[68] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

17. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[69] is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[70] Mobile virtual network operators (MVNOs) are included in this industry.[71] The SBA small business size standard for Telecommunications Resellers

---

[59] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[60] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[61] *Id.*

[62] *Id*.

[63] *Id*.

[64] 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[65] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[66] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[67] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[68] *Id.*

[69] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[70] *Id.*

[71] *Id*.

classifies a business as small if it has 1,500 or fewer employees.[72] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[73] Of that number, 1,375 firms operated with fewer than 250 employees.[74] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 457 providers that reported they were engaged in the provision of toll services.[75] Of these providers, the Commission estimates that 438 providers have 1,500 or fewer employees.[76] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[77] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless Internet access, and wireless video services.[78] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[79] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[80] Of that number, 2,837 firms employed fewer than 250 employees.[81] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services.[82] Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees.[83] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

19. *Wireless Resellers.* Neither the Commission nor the SBA have developed a small business size standard specifically for Wireless Resellers. The closest industry with an SBA small

[72] 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[73] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[74] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[75] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[76] *Id.*

[77] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[78] *Id.*

[79] 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[80] U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[81] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[82] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[83] *Id.*

business size standard is Telecommunications Resellers.[84] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[85] Establishments in this industry resell telecommunications and they do not operate transmission facilities and infrastructure.[86] Mobile virtual network operators (MVNOs) are included in this industry.[87] Under the SBA size standard for this industry, a business is small if it has 1,500 or fewer employees.[88] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services during that year.[89] Of that number, 1,375 firms operated with fewer than 250 employees.[90] Thus, for this industry under the SBA small business size standard, the majority of providers can be considered small entities.

20. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[91] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small.[92] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[93] Of this number, 242 firms had revenue of less than $25 million.[94] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 65 providers that reported they were engaged in the provision of satellite telecommunications services.[95] Of these providers, the Commission estimates that approximately 42 providers have 1,500 or fewer employees.[96] Consequently, using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

---

[84] *See* U.S. Census Bureau, *2017 NAICS Definition, "517911 Telecommunications Resellers,"* https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[89] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[90] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[91] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[92] 13 CFR § 121.201, NAICS Code 517410.

[93] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[94] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[95] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[96] *Id.*

21. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[97] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[98] Providers of Internet services (e.g. dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[99] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[100] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[101] Of those firms, 1,039 had revenue of less than $25 million.[102] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

2. Internet Service Providers

22. *Wired Broadband Internet Access Service Providers (Wired ISPs).*[103] Providers of wired broadband Internet access service include various types of providers except dial-up Internet access providers. Wireline service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[104] Wired broadband Internet services fall in the Wired Telecommunications Carriers industry.[105] The SBA small business size standard for this industry classifies firms having 1,500 or fewer employees as small.[106] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[107] Of this number, 2,964 firms operated with fewer than 250 employees.[108]

---

[97] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[98] *Id.*

[99] *Id*.

[100] 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[101] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[102] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[103] Formerly included in the scope of the Internet Service Providers (Broadband), Wired Telecommunications Carriers and All Other Telecommunications small entity industry descriptions.

[104] 47 CFR § 1.7001(a)(1).

[105] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[106] 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[107] U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[108] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

23. Additionally, according to Commission data on Internet access services as of December 31, 2018, nationwide there were approximately 2,700 providers of connections over 200 kbps in at least one direction using various wireline technologies.[109] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, in light of the general data on fixed technology service providers in the Commission's *2022 Communications Marketplace Report*,[110] we believe that the majority of wireline Internet access service providers can be considered small entities.

24. *Wireless Broadband Internet Access Service Providers (Wireless ISPs or WISPs).*[111] Providers of wireless broadband Internet access service include fixed and mobile wireless providers. The Commission defines a WISP as "[a] company that provides end-users with wireless access to the Internet[.]"[112] Wireless service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the Internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction is classified as a broadband connection under the Commission's rules.[113] Neither the SBA nor the Commission have developed a size standard specifically applicable to Wireless Broadband Internet Access Service Providers. The closest applicable industry with an SBA small business size standard is Wireless Telecommunications Carriers (except Satellite).[114] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[115] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[116] Of that number, 2,837 firms employed fewer than 250 employees.[117]

25. Additionally, according to Commission data on Internet access services as of December 31, 2018, nationwide there were approximately 1,209 fixed wireless and 71 mobile wireless providers of connections over 200 kbps in at least one direction.[118] The Commission does not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, based on data in the Commission's *2022 Communications Marketplace Report* on the small number of

---

[109] *See IAS Status 2018,* Fig. 30 (The technologies used by providers include aDSL, sDSL, Other Wireline, Cable Modem and FTTP). Other wireline includes: all copper-wire based technologies other than xDSL (such as Ethernet over copper, T-1/DS-1 and T3/DS-1) as well as power line technologies which are included in this category to maintain the confidentiality of the providers.

[110] *Communications Marketplace Report*, GN Docket No. 22-203, 2022 WL 18110553 at 10, paras. 26-27, Figs. II.A.5-7. (2022) (*2022 Communications Marketplace Report*).

[111] Formerly included in the scope of the Internet Service Providers (Broadband), Wireless Telecommunications Carriers (except Satellite) and All Other Telecommunications small entity industry descriptions.

[112] Federal Communications Commission, Internet Access Services: Status as of December 31, 2018 *(IAS Status 2018)*, Industry Analysis Division, Office of Economics & Analytics (September 2020). The report can be accessed at https://www.fcc.gov/economics-analytics/industry-analysis-division/iad-data-statistical-reports.

[113] 47 CFR § 1.7001(a)(1).

[114] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[115] 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[116] U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[117] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[118] *See IAS Status 2018*, Fig. 30.

large mobile wireless nationwide and regional facilities-based providers, the dozens of small regional facilities-based providers and the number of wireless mobile virtual network providers in general,[119] as well as on terrestrial fixed wireless broadband providers in general,[120] we believe that the majority of wireless Internet access service providers can be considered small entities.

26. *Internet Service Providers (Non-Broadband).* Internet access service providers using client-supplied telecommunications connections (e.g., dial-up ISPs) as well as VoIP service providers using client-supplied telecommunications connections fall in the industry classification of All Other Telecommunications.[121] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[122] For this industry, U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[123] Of those firms, 1,039 had revenue of less than $25 million.[124] Consequently, under the SBA size standard a majority of firms in this industry can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

27. In this *Further Notice*, we seek comment on whether to harmonize the existing requirements governing customer access to CPNI[125] with the SIM change authentication and protection measures adopted in the *Report and Order*, and if so, the extent to which the rules should be harmonized. We tentatively conclude that harmonized authentication and protection requirements will be easier for wireless providers to implement and therefore will reduce costs and burdens on carriers, including small carriers. Recognizing that there may be other efforts within the government to tackle SIM swap and port-out fraud to address the broader implications of these harmful practices, the *Further Notice* also seeks comment on information about those other efforts and what steps the Commission can take to harmonize government efforts to address SIM swap and port-out fraud.

28. Should the Commission decide to modify existing rules or adopt new rules to harmonize its existing CPNI rules with rules to protect customers from SIM swap fraud, such action could potentially result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance requirements for affected providers of service. We seek comment on the effect of any proposals on small entities. Entities, especially small businesses, are encouraged to quantify the costs and benefits of any reporting, recordkeeping, or compliance requirement that may be established in this proceeding. We anticipate the information we receive in comments including, where requested, cost and benefit analyses, will help the Commission identify and evaluate relevant compliance matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries we make in the *Further Notice*.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and

[119] *2022 Communications Marketplace Report*, 2022 WL 18110553 at 27, paras. 64-68.

[120] *Id.* at 8, para. 22.

[121] *See* U.S. Census Bureau, *2017 NAICS Definition, "517919 All Other Telecommunications,"* https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[122] 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[123] U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[124] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[125] 47 CFR § 64.2010.

Significant Alternatives Considered

29. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[126]

30. In this *Further Notice*, we seek comment on whether we should harmonize the existing requirements governing customer access to CPNI[127] with the SIM change authentication and protection measures adopted in the *Report and Order*, and if so, the extent to which the rules should be harmonized. Among the justifications on which we seek comment are whether inconsistent rules are more burdensome on carriers and whether carriers need flexibility to implement more secure authentication measures. We also tentatively conclude that harmonized authentication and protection requirements will be easier for wireless providers to implement and therefore will reduce costs and burdens on carriers. In considering additional alternatives, we also ask whether it would it be costly and burdensome for carriers to adjust the CPNI authentication and protection practices they have already implemented to comply with the authentication requirements adopted in the *Report and Order*, and whether there are other reasons harmonized rules could increase the costs or burdens on carriers, including small carriers. The Commission expects to consider the economic impact on small entities, as identified in comments filed in response to the *Further Notice* and this IRFA, in reaching its final conclusions and taking action in this proceeding.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

31. None.

[126] 5 U.S.C. § 603(c)(1)–(4).

[127] 47 CFR § 64.2010.