

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

NOTICE OF PROPOSED RULEMAKING

Adopted: September 30, 2021

Released: September 30, 2021

Comment Date: [30] days after publication in the Federal Register
Reply Comment Date: [60] days after publication in the Federal Register

By the Commission: Acting Chairwoman Rosenworcel and Commissioner Starks issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION ..... 1
II. BACKGROUND ..... 4
III. DISCUSSION..... 22
A. Strengthening the Commission’s CPNI Rules to Protect Consumers..... 23
B. Strengthening the Commission’s Number Porting Rules to Protect Consumers..... 49
C. Additional Consumer Protection Measures..... 68
IV. PROCEDURAL MATTERS ..... 74
V. ORDERING CLAUSES..... 80
APPENDIX A – Proposed Rules
APPENDIX B – Initial Regulatory Flexibility Analysis

I. INTRODUCTION

1. Cell phones are an essential part of everyday life for most Americans. We use them not just to make phone calls but to conduct much of our daily activities through their broadband connections and by using applications we have installed on our devices. We keep in touch with friends and family through voice calls, text messages, messaging applications, and social media. We manage our financial lives by accessing our bank and brokerage accounts and make payments using a wide array of financial services applications. We apply for jobs and for government benefits. We also use them to monitor and record health information. And, when we sign into certain websites or applications, or need to reset a password, we often receive a one-time passcode sent in a text message to our cell phone that we then input into the website or application to authenticate our identity. As a result, if a bad actor can intercept our text messages, he or she can steal our identities and our money and take control of our digital lives.

2. Today, we focus on putting an end to two methods used by bad actors 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 “subscriber identity module swapping” or “SIM swapping,”<sup>1</sup> a bad actor convinces a victim’s wireless carrier<sup>2</sup> to transfer the

<sup>1</sup> 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 (continued....)

victim's service from the victim's cell phone to a cell phone in the bad actor's possession. This scam is known as "SIM swapping" because it involves an account being fraudulently transferred (or swapped) from a device associated with one SIM to a device associated with a different SIM. In the second method, known as "port-out fraud," the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or "ported out") to the account with the new carrier controlled by the bad actor.

3. We have received numerous complaints from consumers who have suffered significant distress, inconvenience, and financial harm as a result of SIM swapping and port-out fraud. In addition, we note that recently disclosed data breaches have exposed customer information that could potentially make it easier to pull off these kinds of attacks.<sup>3</sup> Today, we take aim at these scams, with the goal of foreclosing the opportunistic ways in which bad actors take over consumers' cell phone accounts and proactively addressing the risk of follow-on attacks using stolen data, so as to mitigate the risk of additional consumer harm from recent data breaches. Section 222 of the Communications Act of 1934, as amended (the Act), and our Customer Proprietary Network Information (CPNI) rules, which govern the use, disclosure, and protection of sensitive customer information to which a telecommunications carrier has access, require carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to customers' private information. Our Local Number Portability (LNP) rules govern the porting of telephone numbers from one carrier to another. Yet, it appears that neither our CPNI rules nor our LNP rules are adequately protecting consumers against SIM swapping and port-out fraud. We, therefore, propose to amend our CPNI and LNP rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. We also propose to require providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts, and we seek comment on other ways to protect consumers from SIM swapping and port-out fraud.

## II. BACKGROUND

4. *SIM Swapping and Port-Out Fraud.* Cell phone numbers are frequently used as a means of authenticating a user for various types of accounts, including accounts with telecommunications carriers, e-mail and social media providers, financial institutions, and retail websites. For example, a consumer logging in to an e-mail account from a new computer might be asked not only to provide her username and password, but also to input a one-time code sent via text message to her cell phone. Similarly, a consumer who has forgotten her password for a social media website may be prompted to enter a one-time code sent via text message to her cell phone before being allowed to reset her password. Because so many consumers have their cell phones with them at all times, text message-based two-factor authentication can be incredibly convenient. Text message-based authentication relies upon a customer's control of her device and her phone number, which is typically achieved through the SIM. Phone calls and text messages are routed to the device that has the SIM associated with the relevant phone number.

(Continued from previous page) \_\_\_\_\_

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 (updated May 21, 2021), <https://www.lifewire.com/what-are-sim-cards-577532>.

<sup>2</sup> In this item, when we use the term "wireless carrier" or "wireless provider," we intend to encompass mobile wireless services.

<sup>3</sup> See, e.g., T-Mobile, *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats* (Aug. 19, 2021), <https://www.tmobile.com/brand/data-breach-2021>. Breaches of customer information can lead to further fraud through SIM swaps and port-out schemes. See, e.g., WSJ Pro Cyber Newsletter, *Cyber Daily: Watch for Identity Theft, SIM Swapping in T-Mobile Hack, Security Researchers Warn* (Aug. 19, 2021), [https://www.wsj.com/articles/cyber-daily-watch-for-identity-theft-sim-swapping-in-t-mobile-hack-security-researchers-warn-11629379373?mod=searchresults\\_pos3&page=1](https://www.wsj.com/articles/cyber-daily-watch-for-identity-theft-sim-swapping-in-t-mobile-hack-security-researchers-warn-11629379373?mod=searchresults_pos3&page=1).

5. When a cell phone owner loses, breaks, or upgrades her cell phone, she can sometimes take the SIM card out of her previous cell phone and insert it into her new phone. Often, however, she needs to contact her wireless carrier, explain that she is changing cell phones, and request that her wireless carrier reassign her account information to the SIM in her new device. When a bad actor successfully impersonates the customer of a wireless carrier and convinces the carrier to redirect the real customer's cell phone service to a new SIM in a device that the bad actor controls, the bad actor gains access to all of the information associated with the customer's account, including CPNI, and gains control over the customer's phone number and receives both text messages and phone calls intended for the victim.

6. When a wireless service customer decides to switch wireless carriers, the customer provides certain identifying information (telephone number, current account number, ZIP code, and any customer-assigned passcode) to the new wireless carrier to request that the customer's existing number be ported to the new service provider. The new service provider then sends a request with this information through the numbering administrator to the current service provider to port the customer's number. Once the current service provider verifies this information (thus "validating the port"), the two service providers coordinate through the numbering administrator to port the customer's number to the new service provider. As in SIM swapping fraud, when a bad actor successfully impersonates the customer of a wireless carrier and convinces the carrier to port the real customer's telephone number to a new service provider and a device that the bad actor controls, the bad actor gains control over the customer's phone number and can intercept both 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 over many more of the victim's accounts. Such account takeover tactics can cause substantial consumer injury. Because text messages are often used by banks, businesses, and payment services to verify a customer's identity when a customer requests updates to accounts, intercepting a text message used to authenticate a customer can allow a bad actor to reset a customer's password and take over the customer's financial, social media, and other accounts. Having taken over these accounts, the bad actor can then change login credentials, drain bank accounts, and, increasingly, steal cryptocurrency and sell or try to ransom social media accounts.<sup>4</sup> Loss of service on a customer's device—the phone going dark or only allowing 911 calls—is typically the first sign of a SIM swapping or port-out scam. There are also media reports that, in some instances, a hacker was able to perpetrate a

---

<sup>4</sup> See, e.g., 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> (reporting that a federal grand jury indicted two individuals on federal charges in connection with their unauthorized takeovers of victims' wireless phone and other electronic accounts and to steal digital currency and valuable social media accounts); 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,* Motherboard, 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, Reuters, *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>.

“partial porting fraud” by changing the carrier for delivery of SMS messages without changing the primary carrier for purposes of voice, data, and accounting.<sup>5</sup>

8. The Commission and our sister agency, the Federal Trade Commission (FTC), have received hundreds of consumer complaints about SIM swapping and port-out fraud.<sup>6</sup> Some of the complaints describe wireless carrier 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 consumers complain that their wireless carriers have refused to provide them with documentation related to the fraudulent SIM swaps, making it difficult for them to pursue claims with their financial institutions or law enforcement. Several consumer complaints filed with the Commission allege that the wireless carrier’s store employees are involved in the fraud, or that carriers completed SIM swaps despite the customer having previously set a PIN or password on the account.

9. A study published last year by a group of Princeton University researchers examined the types of authentication mechanisms in place at five major wireless carriers, AT&T Mobility, LLC (AT&T), T-Mobile US, Inc. (T-Mobile), Tracfone, US Mobile, and Verizon Wireless (Verizon), to identify the weaknesses that allow for SIM swapping.<sup>7</sup> The researchers opened 50 prepaid accounts (10 with each carrier) and called to request a SIM swap on each account. The researchers found that all five carriers “used insecure authentication challenges that could easily be subverted by attackers.”<sup>8</sup> They 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.”<sup>9</sup> In nine instances involving two different carriers, “customer service representatives (CSRs) either did not authenticate the caller or leaked account information prior to authentication.”<sup>10</sup>

10. The researchers identified six types of information used by the carriers to authenticate their customers: (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.<sup>11</sup>

---

<sup>5</sup> See Krebs on Security, *Can We Stop Pretending SMS Is Secure Now?*, Mar. 16, 2021, <https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/>; Joseph Cox, *A Hacker Got All My Texts for \$16*, Vice, Mar. 15, 2021, [https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber?\\_twitter\\_impression=true](https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber?_twitter_impression=true); see also Joseph Cox, *T-Mobile, Verizon, AT&T Stop SMS Hijacks After Motherboard Investigation*, Vice, Mar. 25, 2021, <https://www.vice.com/en/article/5dp7ad/tmobile-verizon-att-sms-hijack-change> (reporting that “[a]ll the mobile carriers have mitigated a major SMS security loophole that allowed a hacker to hijack text messages for just \$16.”) (Cox Mar. 25, 2021).

<sup>6</sup> Federal Trade Commission, *Consumer Sentinel Network Data Book 2020* (Feb. 2021), at Appx. B, p. 88, [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn\\_annual\\_data\\_book\\_2020.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf); see Letter from Ajit V. Pai, Chairman, FCC, to Sen. Ron Wyden, U.S. Senate at 3 (Feb. 14, 2020), <https://docs.fcc.gov/public/attachments/DOC-362599A2.pdf> (stating that the Commission received 218 informal consumer complaints discussing port-out fraud or SIM swapping in 2017, 211 informal consumer complaints in 2018, and 183 informal consumer complaints in 2019).

<sup>7</sup> 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>.

<sup>8</sup> Lee et al. at 1.

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *Id.* at 2.

11. The researchers found that all of these methods of authentication were or could be vulnerable to abuse. For example, authenticating customers through recent payment information was easily exploitable. According to the researchers, three of the wireless carriers were using payment systems that did not require authentication when using a refill card.<sup>12</sup> An attacker could purchase a refill card at a retail store, submit a refill on the victim's account, then request a SIM swap using the known refill as authentication.<sup>13</sup> The researchers also found that "using information about recent calls for authentication is exploitable."<sup>14</sup> A bad actor could bait his victim into placing calls to specific phone numbers, and then provide those phone numbers when the customer service representative requested information about outgoing calls.<sup>15</sup> It appeared to the researchers that the customer service representatives also had the discretion to allow authentication with incoming call information.<sup>16</sup> The researchers also found that some of the wireless carriers authenticated their customers through the use of account information or personal information that would have been readily available to bad actors. For example, four of the five carriers authenticated their customers using device information that could be obtained by bad actors.<sup>17</sup> One carrier used preset "security" answers to authenticate its customers. As the authors explained, "[r]ecent research has demonstrated that security questions are an insecure means of authentication, because answers that are memorable are also frequently guessable by an attacker."<sup>18</sup> Finally, the research team found that three of the five wireless carriers disclosed personal customer information without authentication, including information that could be used to authenticate a customer.<sup>19</sup>

12. The researchers also "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."<sup>20</sup> They found that 17 websites across different industries have implemented authentication policies with logic flaws that would allow an attacker to fully compromise an account with just a SIM swap.<sup>21</sup>

13. *Privacy of Telecommunications Customer Information.* Section 222 of 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.<sup>22</sup> Section 222(a) requires carriers to protect the confidentiality of proprietary information of and relating to their customers.<sup>23</sup> Section 222(b) provides that a carrier that receives or obtains proprietary information from other carriers

---

<sup>12</sup> *Id.*

<sup>13</sup> *Id.* at 2-3.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.* at 3.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> *Id.* at 1.

<sup>21</sup> *Id.*

<sup>22</sup> 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").

<sup>23</sup> 47 U.S.C. § 222(a).

in order to provide a telecommunications service may only use such information for that purpose and may not use that information for its own marketing efforts.<sup>24</sup> Section 222(c)(1) provides that a carrier may only use, disclose, or permit access to CPNI that it has received 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 services necessary to or used in the provision of such telecommunications service.<sup>25</sup> 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."<sup>26</sup> The Commission has not provided an exhaustive list of what constitutes CPNI, but has explained that CPNI includes (but is not limited to) information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.<sup>27</sup>

14. Beginning in 1998, the Commission promulgated rules implementing the express statutory obligations of section 222.<sup>28</sup> In addition to adopting restrictions on the use and disclosure of CPNI, the Commission adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.<sup>29</sup> 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.<sup>30</sup> In addition, the Commission required each carrier to annually certify its compliance with the CPNI requirements and to make this certification publicly available.<sup>31</sup>

---

<sup>24</sup> 47 U.S.C. § 222(b).

<sup>25</sup> 47 U.S.C. § 222(c)(1). 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. 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. 47 U.S.C. § 222(f).

<sup>26</sup> 47 U.S.C. § 222(h)(1).

<sup>27</sup> *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, 6930, 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).

<sup>28</sup> *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*).

<sup>29</sup> *See id.* at 8195, para. 193.

<sup>30</sup> *See* 47 CFR § 64.2009(b); *see also CPNI Order*, 13 FCC Rcd at 8198, para. 198.

<sup>31</sup> 47 CFR § 64.2009(e); *see also CPNI Order*, 13 FCC Rcd at 8198-200, paras. 199-202; *CPNI Reconsideration Order*, 14 FCC Rcd at 14468 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").

15. In 2007, the Commission amended its CPNI rules to address “pretexting,” the practice of pretending to be a particular customer or other authorized person to obtain access to that customer’s call detail or other private communications records.<sup>32</sup> The Commission concluded that “pretexters have been successful at gaining unauthorized access to CPNI”<sup>33</sup> 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.”<sup>34</sup> To prevent fraudsters from impersonating a telephone company’s customer, the Commission amended its CPNI rules to restrict the release of call detail information<sup>35</sup> based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online.<sup>36</sup> The Commission also required carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI<sup>37</sup> 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.<sup>38</sup> 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.<sup>39</sup> In addition, the Commission modified its CPNI rules to require carriers to notify law enforcement and customers of security breaches involving CPNI.<sup>40</sup> The Commission has made clear that carriers are free to bolster their security measures through additional 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.<sup>41</sup> Finally, the Commission also extended the application of its CPNI rules to providers of interconnected VoIP service, finding that it is “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.”<sup>42</sup> Also 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.<sup>43</sup>

16. *Local Number Portability.* The LNP process gives consumers the ability to retain their phone numbers when switching telecommunications service providers and enhances competition by

---

<sup>32</sup> 2007 CPNI Order, 22 FCC Rcd at 6928 n.1.

<sup>33</sup> *Id.* at 6934, para. 12.

<sup>34</sup> *Id.*

<sup>35</sup> 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.

<sup>36</sup> See generally 2007 CPNI Order, 22 FCC Rcd at 6933-46, paras. 12-36; 47 CFR § 64.2010(b)-(e).

<sup>37</sup> See 2007 CPNI Order, 22 FCC Rcd at 6945-46, paras. 33-36; 47 CFR § 64.2010(a).

<sup>38</sup> See 2007 CPNI Order, 22 FCC Rcd at 6942, para. 24; 47 CFR § 64.2010(f).

<sup>39</sup> 47 CFR § 64.2010(f).

<sup>40</sup> 2007 CPNI Order, 22 FCC Rcd at 6943-45, paras. 26-32.

<sup>41</sup> See *id.* at 6929, para. 3. 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.

<sup>42</sup> 2007 CPNI Order, 22 FCC Rcd at 6954-57, paras. 54-59.

<sup>43</sup> Telephone Records and Privacy Protection Act of 2006, Pub. L. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039).

enabling consumers to choose a provider that best suits their needs. 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.”<sup>44</sup> 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.”<sup>45</sup> 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.<sup>46</sup> Although the Act excludes CMRS providers from the statutory definition of “local exchange carrier,” 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.<sup>47</sup>

17. Since 2002, wireless carriers have been required to provide wireless number portability, but the Commission has not codified customer validation requirements for porting phone numbers between wireless carriers in our rules.<sup>48</sup> In 2003, the Commission offered guidance on wireless number portability.<sup>49</sup> Among other things, the Commission found that, absent an agreement setting additional terms, wireless carriers need only share basic contact and technical information with each other sufficient to validate and execute the port.<sup>50</sup> The Commission also found that it did not “see a present need to propose formally incorporating the industry standard [two-and-one-half-hour porting interval] in our rules,” but “view[ed] this industry standard as feasible and [ ]encourage[d] carriers to complete wireless-wireless ports within this timeframe.”<sup>51</sup>

18. 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 the port request and accomplish the port.<sup>52</sup> The Commission observed that the wireless industry had reached an

---

<sup>44</sup> 47 U.S.C. § 251(b)(2).

<sup>45</sup> 47 U.S.C. § 153(30); 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*, 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).

<sup>46</sup> 47 U.S.C. § 251(e)(1).

<sup>47</sup> *See Telephone Number Portability*, 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*, 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). The Commission has defined 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.” 47 CFR § 20.3.

<sup>48</sup> *See First Number Portability Order*, 11 FCC Rcd at 8393, paras. 77-78; *see also Cellular Telecommunications Industry Association’s Petition for Forbearance from Commercial Mobile Radio Services Number Portability Obligations and Telephone Number Portability*, CC Docket No. 95-116 et al., Memorandum Opinion and Order, 14 FCC Rcd 3092 (1999) (extending implementation deadline for CMRS providers).

<sup>49</sup> *See Wireless Number Portability Order*, 18 FCC Rcd 20971.

<sup>50</sup> *See id.* at 20978, para. 24.

<sup>51</sup> *Id.* at 20979-80, para. 26.

<sup>52</sup> *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*

(continued....)



agreement to require only three fields of information to validate a simple port request—the customer telephone number, account number, and password (if applicable).<sup>53</sup> The Commission concluded that for simple<sup>54</sup> 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) 5-digit zip code; and (4) passcode (if applicable).<sup>55</sup> The Commission found that use of these four fields “will sufficiently protect consumers from slamming,” the switching of a consumer’s traditional wireline telephone company for a local, local toll, or long distance service without permission, and explained that data in the record suggested that “complaints about unauthorized ports occur much less frequently for wireless-to-wireless ports, where only three validation fields are used, than for intermodal ports.”<sup>56</sup>

19. To ensure that consumers were able to port their telephone numbers efficiently and to enhance competition for all communications services, in 2009 the Commission adopted the *Porting Interval Order*, which reduced the porting interval for simple wireline and simple intermodal port requests to one business day.<sup>57</sup> The Commission reasoned that delays in porting cost consumers time and money and limit consumer choice and competition because consumers would abandon efforts to switch providers when they got frustrated with slow porting.<sup>58</sup>

20. In 2010, to ensure that customers could easily port numbers between carriers, the Commission adopted an Order standardizing the data exchanged between carriers when service providers execute a wireline or intermodal simple port subject to the one-business day porting interval.<sup>59</sup> The Commission concluded that 14 information fields are necessary to accomplish a simple wireline or intermodal port, and thus mandated that service providers use those 14 fields—and only those fields—to accomplish such ports.<sup>60</sup> The Commission maintained the same three customer-provided information

(Continued from previous page) \_\_\_\_\_  
*Optimization*, Report and Order, Declaratory Ruling, Order on Remand, and Notice of Proposed Rulemaking, 22 FCC Rcd 19531, 19553, para. 42 (2007) (*2007 VoIP LNP Order* or *2007 LNP Four Fields Declaratory Ruling*), *aff’d sub nom. National Telecomms. Cooperative Ass’n v. FCC* (D.C. Cir. Apr. 28, 2009).

<sup>53</sup> *Id.* at 19556-57, para. 47.

<sup>54</sup> 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., 2007 VoIP LNP Order*, 22 FCC Rcd at 19556, n.153.

<sup>55</sup> *2007 VoIP LNP Order*, 22 FCC Rcd at 19557, para. 48.

<sup>56</sup> *Id.* at 19557-58, 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.”).

<sup>57</sup> *See generally 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 (2009) (*Porting Interval Order and FNPRM*).

<sup>58</sup> *See id.* at 6087, para. 6.

<sup>59</sup> *See Local Number Portability Porting Interval and Validation Requirements; Telephone Number Portability*, Report and Order, 25 FCC Rcd 6953, 69659-62, paras. 9-17 (2010) (*LNP Standard Fields Order*). The Commission also codified its long-standing requirement that non-simple ports must be completed within four business days. *See* 47 CFR § 52.35(d).

<sup>60</sup> *See LNP Standard Fields Order*, 25 FCC Rcd 6953, 6959-62, paras. 9-17. 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

(continued....)

fields from the *2007 LNP Four Fields Declaratory Ruling*—the ported telephone number, the customer’s account number, and customer’s zip code—to help protect against fraudulent ports. To further help protect against fraudulent ports, the rules also permit customers to request that a user-created passcode be put on their account, which the consumer must then provide before a port can be accomplished.<sup>61</sup> 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 consumer concerns about unauthorized ports with competitors’ interest in ensuring that porting obligations may not be used in an anticompetitive manner to inhibit consumer choice.<sup>62</sup> Wireless-to-wireless ports continued to be governed by the *2007 LNP Four Fields Declaratory Ruling* for customer-provided fields of information and their own industry agreement regarding technical fields.

21. The members of the non-governmental, multi-stakeholder Number Portability Industry Forum (NPIF) have created “Best Practices” for porting between and within telephony carriers.<sup>63</sup> 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. Best Practice 73 (Unauthorized Port Flow) specifically addresses unauthorized ports, including fraudulent ports.<sup>64</sup> Among other things, Best Practice 73 encourages carriers to review “incident and/or police report details if provided (official document showing case number or other verification that the matter was reported or attempted to be reported to law enforcement by reporting end user is acceptable)” and places priority on resolving unauthorized ports that have a heightened severity of impact, including “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.”<sup>65</sup>

(Continued from previous page)

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 (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. *Id.* 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.

<sup>61</sup> See 47 CFR § 52.36(c).

<sup>62</sup> See generally *LNP Standard Fields Order*, 25 FCC Rcd at 6956-62, paras. 6-10.

<sup>63</sup> NPAC, Number Portability Best Practices, <https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1> (last visited Aug. 20, 2021).

<sup>64</sup> 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*, <https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1> (last visited Aug. 20, 2021).

<sup>65</sup> See Best Practice 73, NPAC, *Number Portability Best Practices*, <https://numberportability.com/industry-info/lnpa-working-group/lnp-best-practices/?page=1> (last visited Aug. 20, 2021).

### III. DISCUSSION

22. We believe that our CPNI and number porting rules are ripe for updates that could help prevent SIM swapping and port-out fraud.<sup>66</sup> In this Notice, we propose to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer. We also propose to amend our CPNI rules to require wireless carriers to develop procedures for responding to failed authentication attempts and to notify customers immediately of any requests for SIM changes. We also seek comment on whether we should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud. We likewise propose to amend our number porting rules to combat port-out fraud while continuing to encourage robust competition through efficient number porting. Finally, we consider whether we should adopt any other changes to our rules to address SIM swap and port-out fraud, including the difficulties encountered by victims of these schemes. We seek comment on our proposals and invite input from stakeholders on how to best tailor the rules to combat this growing, pernicious fraudulent activity.

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

23. *Customer Authentication Requirements for SIM Change Requests.* To reduce the incidence of SIM swap fraud, we propose to prohibit carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer, and to define "SIM" for purposes of these rules as a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network.<sup>67</sup> We seek comment on these proposals. Consistent with the recommendations made last year by the Princeton Research team that studied SIM swapping, we propose that use of a pre-established password;<sup>68</sup> a one-time passcode sent via text message to the account phone number or a pre-registered backup number; a one-time passcode sent via e-mail to the e-mail address associated with the account; or a passcode sent using a voice call to the account phone number or a preregistered back-up telephone number would each constitute a secure method of authenticating a customer prior to a SIM change.<sup>69</sup> We seek comment on this proposal and whether it will serve as an effective deterrent to SIM swapping fraud.

24. Are each of these authentication methods secure? Since 2016, the National Institute of Standards and Technology (NIST) has recognized known risks associated with SMS-based authentication, distinguishing "SMS-based authentication from other out-of-band authentications methods due to heightened security risks including 'SIM change.'"<sup>70</sup> In addition, recent media reports call into question the security of using text messages for authentication purposes. For example, a recent investigation found that SMS-based text messages could be easily intercepted and re-routed using a low-cost, online marketing service that helps businesses do SMS marketing and mass messaging.<sup>71</sup> As with

---

<sup>66</sup> At the same time, we emphasize that carriers have statutory duties to protect the confidentiality of their customers' private information and to maintain just and reasonable practices and that these statutory duties are not necessarily coterminous with our rules. See 47 U.S.C. §§ 222(a), 201(b); *TerraCom, Inc., and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014). Recent breaches appear to demonstrate that current safeguards are not sufficient to protect consumers' data.

<sup>67</sup> As used in our proposed rules, the term "carrier" includes "any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment." See 47 U.S.C. § 217.

<sup>68</sup> As used here, a "pre-established password" is a password chosen by the customer for future use to authenticate a customer for access to account information or to make account changes.

<sup>69</sup> See generally Lee et al.

<sup>70</sup> See Lee et al. at 1, 9.

<sup>71</sup> See Lucky225, *It's time to stop using SMS for anything*, Mar. 15, 2021, <https://lucky225.medium.com/its-time-to-stop-using-sms-for-anything-203c41361c80>; Joseph Cox, *A Hacker Got All My Texts for \$16*, Vice, Mar. 15, 2021, <https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber>; Krebs on Security,

(continued....)

SIM swap fraud, once the hacker was able to re-route a target's text messages, the hacker was also able to access other accounts associated with that phone number. Wireless carriers reportedly have mitigated the security vulnerability uncovered in this investigation.<sup>72</sup> Has this vulnerability been fixed so that it is no longer a threat to customers of any carrier? What rules could we adopt to ensure that authentication using text messages is secure and effective to protect consumers from SIM swap fraud? Or alternatively, should we prohibit carriers from using text messaging, or specifically SMS text messaging, to authenticate customers requesting SIM swaps? What steps could we take to prevent a customer's text messages from being forwarded without authorization? Should we, for example, require companies offering the text forwarding services to call the customer whose texts will be forwarded to confirm consent prior to forwarding? If so, what authority may we rely upon to adopt such a rule? Are such methods effective? What other steps should we take to help secure customers' accounts and text messages?

25. All of the methods of authentication that we propose to include in the requirement to authenticate a wireless customer before allowing for a SIM swap are familiar ones, already used by consumers and companies in various other circumstances. Based on stakeholder experience with these methods of authentication, how burdensome would our proposed authentication requirement be on customers making legitimate SIM change requests? Would they pose particular challenges to customers whose phone associated with their account has been lost, stolen, or destroyed, or customers who are not comfortable with technology, or to customers with disabilities? Should customers be able to opt-in or opt-out of certain methods of authentication?

26. We also invite comment on whether there are other secure methods of authentication that we should allow carriers to use to authenticate their customers in advance of effectuating a SIM change. What practices and safeguards do carriers currently employ to authenticate customers when SIM change requests are made? Have carriers implemented any processes and protections to address SIM swap fraud specifically? If so, have those practices been effective? Do carriers use multi-factor authentication and has it been effective in preventing SIM swap fraud? If so, should we adopt a multi-factor authentication requirement to prevent SIM swap fraud? If we do require multi-factor authentication, is texting sufficiently secure to permit it as an authentication method for use in multi-factor authentication? Are there emerging technologies or authentication methods in development that could potentially be implemented to protect customers from SIM swap fraud? Are there other security measures incorporated into handsets or operating systems that can be used to authenticate or otherwise prevent SIM swap fraud? Could blockchain technologies that store data in a decentralized manner offer additional security when authenticating customers requesting SIM changes? Are there limitations in these technologies, such as security, storage, scalability, and cost that could place a burden on providers and manufacturers of SIMs? What privacy risks are associated with any of these methods or others suggested by commenters? How effective would any of these methods be at deterring SIM swap fraud? As with the methods we have proposed, what challenges do other secure methods of authentication pose to customers and how burdensome would they be on customers making legitimate SIM change requests, particularly those customers who are no longer in possession of their cell phone because it was lost, stolen, or destroyed, or customers who are not comfortable with technology, or customers with disabilities? What are the costs to carriers for any alternative secure authentication methods?

27. If we adopt a specific set of authentication practices that carriers must employ before effectuating a SIM change, how can we account for changes in technology, recognizing that some of these methods may become hackable over time, while additional secure methods of authentication will likely be

(Continued from previous page) \_\_\_\_\_

*Can We Stop Pretending SMS Is Secure Now?*, Mar. 16, 2021, <https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/>.

<sup>72</sup> See Cox Mar. 25, 2021 at 1 (reporting that “[a]ll the mobile carriers have mitigated a major SMS security loophole that allowed a hacker to hijack text messages for just \$16”).

developed over time? We seek comment on whether instead of requiring specific methods of authentication, we should adopt a flexible standard requiring heightened authentication measures for SIM swap requests. The Commission has previously found that “techniques for fraud vary and tend to become more sophisticated over time” and that carriers “need leeway to engage emerging threats.”<sup>73</sup> The Commission has allowed carriers to determine which specific measures will best enable them to ensure compliance with the requirement that carriers take reasonable measures to discover and protect against fraudulent activity.<sup>74</sup> We observe that to the extent carriers have already implemented or are considering implementing additional protections against SIM swap fraud, we want to ensure that any rules we adopt do not inhibit carriers from using and developing creative and technical solutions to prevent SIM swap fraud or impose unnecessary costs. Would codifying a limited set of methods for authenticating customers in advance of approving SIM swapping requests reduce carriers’ flexibility to design effective measures and, in effect, reduce their ability to take aggressive actions to detect and prevent fraudulent practices as they evolve? Could requiring specific methods of authentication provide a “roadmap” to bad actors? What costs would such requirements impose on carriers, particularly smaller carriers?

28. To that end, we seek comment whether we should instead require carriers to comply with the NIST Digital Identity Guidelines, which are updated in response to changes in technology, in lieu of other proposals.<sup>75</sup> The NIST Digital Identity Guidelines are a set of guidelines that provide technical requirements for federal agencies “implementing digital identity services,” focusing on authentication.<sup>76</sup> Would requiring carriers to adopt and comply with these guidelines “future proof” authentication methods? Would these guidelines effectively protect consumers in the context of SIM swap fraud? Are these guidelines generally applicable in the telecommunications context, and do the guidelines provide sufficient flexibility to carriers? Would requiring carriers to comply with the guidelines pose any difficulties for smaller providers, and would the authentication methods recommended in the guidelines pose any particular challenges to customers? We also seek comment on whether there are other definitive government sources that we could consider adopting as appropriate authentication methods.

29. We also seek comment on what would be an appropriate implementation period for wireless carriers to implement any changes to their customer authentication processes. Because of the serious harms associated with SIM swap fraud, we believe that a speedy implementation is appropriate. Are there any barriers to a short implementation timeline and, if so, what are they? What could we do to eliminate or reduce potential obstacles? Will smaller wireless carriers need additional time to implement the requirements we propose?

30. Are there other ways we can strengthen the Commission’s customer authentication rules to better protect customers from SIM swap fraud? For example, for online access to CPNI, our rules require a carrier to authenticate a customer “without the use of readily available biographical information[] or account information.”<sup>77</sup> Given evidence of the ease with which bad actors can create recent payment or call detail information,<sup>78</sup> we propose to make clear that carriers cannot rely on such information to authenticate customers for online access to CPNI. We invite comment on that proposal.

---

<sup>73</sup> 2007 CPNI Order, 22 FCC Rcd at 6945, para. 33.

<sup>74</sup> *Id.*

<sup>75</sup> National Institute of Standards and Technology, Department of Commerce, NIST Special Publication 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management, at <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf>.

<sup>76</sup> *Id.*

<sup>77</sup> 47 CFR § 64.2010(c).

<sup>78</sup> *See* Lee et al. at 2-3.

31. We also seek comment on whether there are other methods of authentication that carriers should be allowed to implement to prevent SIM fraud that originates in retail locations. Our rules currently allow carriers to disclose CPNI to a customer at a carrier's retail location if the customer presents a valid photo ID.<sup>79</sup> We seek comment on whether a government-issued ID alone is sufficient for in-person authentication. How prevalent is in-person fraud using fake IDs as a source of SIM swap fraud? What role can, and should, retail stores play in authentication, particularly in situations where customers do not have access to technology or are not tech savvy? Should customer authentication requirements be the same for SIM changes initiated by telephone, online, or in store?

32. We also invite comment on whether we should amend our rule on passwords and back-up authentication methods for lost or forgotten passwords.<sup>80</sup> Our rules require a carrier to authenticate the customer without the use of readily available biographical information or account information to establish the password.<sup>81</sup> We permit carriers to create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information or account information.<sup>82</sup> Should we make changes to this requirement? If so, what changes are needed? Do the existing rules create vulnerabilities that should be addressed? Should these requirements be updated to reflect any changes in technology? How would they enhance the protections already provided to consumer passwords?

33. *Response to Failed Authentication Attempts.* We propose to require wireless carriers to develop procedures for responding to failed authentication attempts, and we seek comment on this proposal. We seek comment on what processes carriers can implement to prevent bad actors from attempting multiple authentication methods while at the same time ensuring that protections do not negatively impact legitimate customer requests. For example, would a requirement that SIM swaps be delayed for 24 hours in the case of multiple failed authentication attempts while notifying the customer via text message and/or e-mail, be effective at protecting customers from fraudulent SIM swaps? If we adopt such a rule, should we specify the number of attempts, and if so, how many attempts should trigger the 24-hour delay? How burdensome would this be for customers, and what costs would this impose on carriers? How long would it take carriers to develop and implement procedures for responding to failed authentication attempts? Would such a requirement have anti-competitive effects?

34. *Customer Notification of SIM Change Requests.* As part of our effort to protect consumers from fraudulent SIM swapping, we propose to require wireless providers to notify customers immediately of any requests for SIM changes. We seek comment on this proposal. Is it unnecessary if we adopt specific heightened authentication requirements prior to providing a SIM swap? Or will it provide a worthwhile second line of protection against fraudulent SIM swaps?

35. Our CPNI rules currently require 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.<sup>83</sup> This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.<sup>84</sup> As the Commission found with respect to these other types of account changes, we believe that notification of SIM change requests could be an important tool for customers to monitor their account's security, and

---

<sup>79</sup> See 47 CFR § 64.2010(d).

<sup>80</sup> See 47 CFR § 64.2010(e).

<sup>81</sup> See 47 CFR § 64.2010(b), (c).

<sup>82</sup> See 47 CFR § 64.2010(e).

<sup>83</sup> 47 CFR § 64.2010(f).

<sup>84</sup> *Id.*

could help protect customers from bad actors “that might otherwise manage to circumvent [authentication protections]” and enable customers “to take appropriate action in the event” of fraudulent activity.<sup>85</sup> Do commenters agree?

36. We also seek comment on how this notification should be provided to customers. We believe that the verification methods provided in our rules for other types of account changes may be insufficient to protect customers from SIM swap fraud because in these situations, the bad actor has taken control of the customer’s account and any verification communications sent after the transfer by voicemail or text may be directed to the bad actor rather than to the victim. Moreover, mail to the address of record will likely be too slow to stop the ongoing fraud that may involve financial accounts, social media profiles, and other services. We therefore propose to amend our rules to include notification requirements that would more effectively alert customers to SIM fraud on their accounts and seek comment on what types of notification would be most effective in alerting customers to SIM swap fraud in progress. Would e-mail notification be more effective? Should we retain the option to send such notifications by mail even though this method involves significant delay? Should carriers be required to give customers the option of listing a personal contact (e.g., a spouse or family member) and then inform that contact that the customer is requesting a SIM swap? What other methods of communication could be used to get timely notification to customers, particularly those customers who are no longer in possession of their device because it has been lost or stolen?

37. In addition to immediate customer notification of requests for SIM swaps, we seek comment on requiring up to a 24-hour delay (or other period of time) for SIM swap requests while notifying the customer via text message, e-mail, through the carrier’s app, or other push notification<sup>86</sup> and requesting verification of the request. Once a customer verifies the SIM change request either via text, the carrier’s app (if the device is in the customer’s possession), an e-mail response, or the customer’s online account, the carrier would be free to process the SIM change. If we adopt heightened authentication requirements, is a temporary delay in transferring the account to a new SIM necessary to ensure sufficient time for a customer to receive the notification of activity on the account and take action if the customer has not initiated the changes? Would this requirement be effective in preventing SIM swap fraud? How burdensome would such a delay be for customers? Are there safety implications for customers who legitimately need a new SIM? Could such a delay prevent the customer from completing 911 calls during the waiting period? What costs would this requirement impose on carriers, and how long would it take carriers to develop, test, and implement such a process? Would such a requirement be anti-competitive? Should we consider other approaches to customer notifications of SIM transfers?

38. *Customer Service, Training, and Transparency.* Additionally, we seek comment on whether we should impose customer service, training, and/or transparency requirements specifically focused on preventing SIM swap fraud. For example, should we require carriers to modify customer record systems so that customer service representatives are unable to access CPNI until after the customer has been properly authenticated? Would this approach be effective in preventing customer service representatives from assisting with authentication through the use of leading questions or other more nefarious employee involvement in SIM swap fraud? Would a requirement for record-keeping of the authentication method used for each customer deter employee involvement in SIM swapping fraud? Are there ways to avoid employee malfeasance, such as requiring two employees to sign off on every SIM change? What burdens would be associated with these possible requirements? Anecdotal evidence suggests that, in some cases, customer service representatives are not trained on procedures to deal with customers who have been victims of SIM swap fraud, and as a result, customers who are already victims

---

<sup>85</sup> 2007 CPNI Order, 22 FCC Rcd at 6942, para. 24.

<sup>86</sup> A push notification is “a message sent to a smartphone relating to one of its apps, even when it is not running, or the act of sending such messages.” Cambridge Dictionary (visited Aug. 20, 2021), available at <https://dictionary.cambridge.org/us/dictionary/english/push-notification>.

have difficulty getting help from their carriers. To address this concern, we seek comment on whether we should impose training requirements for customer service representatives to address SIM swap fraud attempts, complaints, and remediation. What costs would these measures impose on carriers? Is there a way to reduce the burdens of these proposals while still achieving the policy aims? Would these proposals reduce SIM swap fraud or otherwise impact the customer experience? How long would it take wireless carriers to implement any new training requirements? Are there alternative approaches that might be more effective or efficient?

39. We also seek comment on whether we should require wireless providers to offer customers the option to disable SIM changes requested by telephone and/or online access (i.e., account freezes or locks).<sup>87</sup> We believe that offering these protections would impose minimal burdens on carriers while offering significant protection to customers. Do commenters agree? Whether or not we require wireless providers to offer such services, we also seek comment on whether we should require carriers to provide a transparent, easy-to-understand, yearly notice to customers of the availability of any account protection mechanisms the carrier offers (e.g., SIM transfer freeze, port request freezes, PINs, etc.). What costs would such notification requirements impose on carriers? We believe that any customer notifications should be brief, use easy-to-understand language, and be delivered in a manner that is least burdensome to customers. We seek comment on what form such notifications could take and how they could be delivered to customers to provide meaningful notice of such services while imposing minimal burden on carriers. Do we need to prescribe a method or methods for customers to unfreeze or unlock their accounts? What methods would be sufficiently secure? Would an unfreeze or unlock be immediate or should there be a waiting period before an unlocked account can be transferred?

40. *Accounts with Multiple Lines.* We seek comment on how these proposed CPNI rule changes impact wireless accounts with multiple lines, such as shared or family accounts. If we require the customer to provide a one-time passcode for the carrier to execute a SIM change, should each line on the shared or family account have its own passcode? If the account owner elects to freeze the account to protect against unauthorized changes, how can we ensure that another member of the shared or family account remains able to port-out his or her number? Should the freeze option apply only to individual lines and not to entire accounts? Do our proposed rules impact these types of accounts with multiple lines in any other ways?

41. *Remediation of SIM Swap Fraud.* We seek comment on how we can enable timely resolution of SIM swap fraud to minimize financial and other damage to customers who are victims of SIM swap fraud. How can we encourage and/or ensure that carriers quickly resolve complaints in cases of SIM swap fraud? Should we require carriers to respond to customers and offer redress within a certain time frame? What would be the costs to carriers, and what are the costs to customers if we do not do so? We seek comment on the methods wireless carriers have established to help victims of SIM swap fraud halt an unauthorized SIM swap request or to recover their phone numbers from bad actors.<sup>88</sup>

42. *Carriers' Duty to Protect CPNI.* We also seek comment on codifying the Commission's expectation that carriers must take affirmative measures to discover and protect against fraudulent activity beyond the measures specifically dictated by our rules and that additional measures (e.g., self-monitoring) are required to comply with section 222's mandate to protect the confidentiality of customer information. In the *2007 CPNI Order*, the Commission codified the requirement that carriers take reasonable measures to discover and protect against unauthorized access to CPNI,<sup>89</sup> and specified that adoption of the rules in

---

<sup>87</sup> Cf., e.g., 47 CFR § 64.1190 (governing preferred carrier freezes).

<sup>88</sup> See also *infra* Part III.C.

<sup>89</sup> 47 CFR § 64.2010(a) ("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.").



that *Order* does not relieve carriers of their fundamental statutory duty to remain vigilant in their protection of CPNI,<sup>90</sup> nor does it insulate them from enforcement action for unauthorized disclosure of CPNI. The Commission allowed carriers flexibility in how they would satisfy their statutory obligations but expressed an expectation that carriers would take affirmative measures to discover and protect against fraudulent activities beyond what is expressly required by the Commission's rules.<sup>91</sup> We seek comment on whether codifying a requirement to take affirmative measures to discover and protect against fraudulent activities would lead to more effective measures to detect and prevent SIM swap fraud. Has the expectation expressed in 2007 been effective?<sup>92</sup> Would the additional threat of enforcement of a codified rule create additional incentives for carriers to take more aggressive action to detect and prevent fraudulent access to CPNI? We seek comment on whether there are additional requirements needed to ensure that carriers comply with their legal obligations under section 222 to detect and prevent SIM swap fraud.

43. *Tracking the Effectiveness of Authentication Measures.* We seek comment on what data carriers collect about SIM swap fraud, and whether we should require that carriers track data regarding SIM swap complaints to measure the effectiveness of their customer authentication and account protection measures. What would be the burdens of requiring wireless carriers to internally track customer SIM swap complaints? Do wireless carriers already report this information to the U.S. Secret Service and Federal Bureau of Investigation (FBI) pursuant to the Commission's rules?<sup>93</sup> We also seek comment on whether we should modify our breach reporting rules to require wireless carriers to report SIM swap and port-out fraud to the Commission, and what the costs would be to carriers of doing so, including the timeframe for implementing such a requirement. Should we require carriers to inform the Commission of the authentication measures that they have in place and when those measures change? Would requiring carriers to update the Commission about changes to authentication measures, along with the frequency of customer SIM swap complaints, be sufficient to enable the Commission to evaluate the efficacy of a carrier's authentication measures, or should the Commission require carriers to provide additional information? We also seek comment on how we should ensure carrier compliance with any proposed obligations that we adopt. For example, should we specifically direct the Commission's Enforcement Bureau, or another Bureau or Office, to conduct compliance audits? Are there other audits or models that we should use as guidelines to ensure compliance? We seek comment on the best method to enforce our proposals.

44. *Applicability of Customer Authentication Measures.* We seek comment on whether any new or revised customer authentication measures we adopt should apply only to wireless carriers and only with respect to SIM swap requests, or whether such expanded authentication requirements would offer benefits for all purposes and with respect to all providers covered by our CPNI rules. Is there anything unique about VoLTE service or the upcoming Voice over New Radio (VoNR) that we need to

---

<sup>90</sup> 47 U.S.C. § 222(a) (imposing a general duty on carriers to "protect the confidentiality of proprietary information of, and relating to . . . customers").

<sup>91</sup> 2007 CPNI Order, 22 FCC Rcd at 6946, para. 35.

<sup>92</sup> The frequency of customer data breaches since 2007 appears to indicate that current safeguards are not sufficient to protect consumers' data. See, e.g., *AT&T Services, Inc.*, Order, 30 FCC Rcd 2808 (EB 2015) (reaching \$25 million settlement of investigation into three breaches); T-Mobile, *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats* (Aug. 19, 2021), <https://www.t-mobile.com/brand/data-breach-2021> (providing notice of an August 2021 breach that exposed names, dates of birth, and social security numbers for more than 50 million current, former, and prospective customers); Selena Larson, *Verizon data of 6 million users leaked online*, CNN Business (July 12, 2017), <https://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html>.

<sup>93</sup> See 47 CFR § 64.2011 (requiring telecommunications carriers to notify law enforcement when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI).

consider?<sup>94</sup> Further, as the nation's networks migrate from 2G and 3G to 4G and 5G, are there particular technical features that should be taken into consideration regarding authentication requirements? Is the type of phone number takeover that occurs through SIM swap fraud only relevant to mobile phone numbers (due to SIM swaps and text message-based text authentication)? Are there also concerns with respect to account takeovers of interconnected Voice over Internet Protocol (VoIP) services,<sup>95</sup> one-way VoIP services, and landline telephone services? Even if the same concerns are not present (or as strongly present), should we apply any stronger authentication requirements to all providers to protect customers' privacy and to provide uniform rules across all providers? If so, under what legal authority could we extend the proposed authentication requirements to services other than wireless? Is there value to uniformity with other categories of providers? Would costs imposed on these carriers outweigh the limited benefit of these requirements related to non-wireless carriers? Are there any other rules that would need to be aligned for consistency if we make changes to the CPNI rules to address SIM swap fraud? In addition, if limited to wireless providers only, we believe that any new rules we adopt should apply to all providers of wireless services, including resellers. Do commenters agree?

45. We also seek comment on whether any new rules should apply only to certain wireless services, such as pre-paid services. Is SIM swap fraud limited to, or more prevalent with, pre-paid or post-paid wireless accounts? Do wireless resellers (many of which offer pre-paid services) encounter this type of fraud more or less often than facilities-based carriers? We invite comment on whether some or all changes discussed here should apply to all mobile accounts or whether certain changes should be limited to pre-paid or post-paid accounts only. We note that pre-paid plans generally do not require credit checks and therefore subscribers to prepaid plans may be more low-income and economically vulnerable individuals. Would such requirements impose disproportionate burdens on these customers?

46. We also seek comment on the scope of any changes that we may make to the CPNI rules to address SIM swap fraud. Specifically, should any new rules be narrowly tailored to deal only with SIM swap fraud, or should they be broader to ensure that they cover the evolving state of fraud on wireless customers?<sup>96</sup> Outside of the account takeover context, are there benefits to providing expanded authentication requirements before providing access to CPNI to someone claiming to be a carrier's customer? We seek comment on 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.

47. In addition, we seek comment on the impact that our proposed rules could have on smaller carriers. Would the proposed requirements impose additional burdens on smaller carriers? Would they face different costs than larger carriers in implementing the new requirements, if adopted? Would smaller carriers need more time to comply with new authentication rules? Do they face other obstacles that we have not considered here?

48. We believe that we have authority to adopt the proposed rules discussed in this section pursuant to our authority under sections 4, 201, 222, 303, and 332 of the Act,<sup>97</sup> and we seek comment on

---

<sup>94</sup> See 5G Americas, *The Future of Voice in Mobile Wireless Communications* at 25, Feb. 2021, [www.5gamericas.org/wp-content/uploads/2021/02/InDesign-Future-of-Voice-Feb-2021-1.pdf](http://www.5gamericas.org/wp-content/uploads/2021/02/InDesign-Future-of-Voice-Feb-2021-1.pdf).

<sup>95</sup> 47 CFR § 9.3.

<sup>96</sup> See, e.g., T-Mobile, *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats* (Aug. 19, 2021), <https://www.t-mobile.com/brand/data-breach-2021> (providing notice that personal information was stolen from T-Mobile systems).

<sup>97</sup> See *2007 CPNI Order*, 22 FCC Rcd at 6930, para. 4; *id.* at 6955-58, paras. 54-59 (relying on "our Title I ancillary jurisdiction" to the extent necessary to apply CPNI rules to interconnected VoIP). 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.

(continued....)

this conclusion. Do we have additional sources of authority on which we may rely here?<sup>98</sup> To the extent that we have not already done so, we also solicit input on the relative costs and benefits of our proposals to amend the CPNI rules to address SIM swap fraud. How many legitimate SIM swap requests do carriers receive yearly, and what are customers' most common reasons for requesting a legitimate SIM swap? Is there any evidence concerning the degree to which authentication measures limit legitimate SIM swaps, or the degree to which they successfully prevent fraud? We ask commenters for input on how any of these proposals could positively or negatively affect the customer experience and whether they foresee any unintended consequences from the changes we propose here.

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

49. We next seek comment on proposals to strengthen our number porting rules to protect customers from unauthorized ports and port-out fraud. One reason that number porting can be used to subvert two-factor authentication may be the relative ease with which carriers fulfill port order requests from other carriers.<sup>99</sup> The Commission has, in the past, been concerned that adding "additional steps for the customer would also add a layer of frustration and complexity to the number porting process, with anticompetitive effects."<sup>100</sup> While the Commission remains committed to "facilitat[ing] greater competition among telephony providers by allowing customers to respond to price and service changes . . . ,"<sup>101</sup> we seek comment below on what additional measures we can adopt to protect customers from port-out fraud.

50. *Notification of Wireless Port Requests and Customer Authentication Processes.* We propose to require wireless carriers to provide notification to customers through text message or other push notification to the customer's device whenever a port-out request is made to ensure that customers may take action in the event of an unauthorized port request, and seek comment on our proposal. For example, Verizon sends its customers a text message letting the customer know that a port-out request has been initiated.<sup>102</sup> When the request is completed, Verizon will send the customer an e-mail stating that the port to the new service was successful.<sup>103</sup> AT&T may also "send customers a text message to help protect them from illegal porting. This notification will not prevent or delay the customer's request. It just adds

(Continued from previous page) \_\_\_\_\_  
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)").

<sup>98</sup> *See, e.g.*, 47 U.S.C. § 1004 ("A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.").

<sup>99</sup> We note that though the Act makes it unlawful for any telecommunications carrier to "submit or execute a change in a subscriber's selection of a provider of telephone exchange service . . . except in accordance with such verification procedures as the Commission shall prescribe," the Commission's slamming rules implementing this provision do not currently apply to wireless carriers. As a result, wireless subscribers are not afforded the same protections as wireline customers when their service is switched to another carrier without their authorization. *See* 47 U.S.C. § 258(a); 47 CFR § 64.1120(a)(3) (excluding CMRS providers from the verification requirements of the slamming rules).

<sup>100</sup> *LNP Standard Fields Order*, 25 FCC Rcd at 6962, para. 16.

<sup>101</sup> *2007 LNP Four Fields Declaratory Ruling*, 22 FCC Rcd at 19532, para. 1.

<sup>102</sup> Verizon, *Transfer (port-out) your number to another carrier FAQs*, <https://www.verizon.com/support/port-out-faqs/> (last visited Aug. 20, 2021).

<sup>103</sup> *Id.*

a simple step to better protect against fraud.”<sup>104</sup> We believe that requiring customer notice of port requests could be a minimally intrusive protective measure that could be automated to minimize delays while providing significant protections for customers. Do commenters agree? Do other carriers currently notify their customers of port-out requests? What would be the costs for carriers to implement such a requirement, particularly for smaller carriers? How much time would carriers need to implement such a requirement? Would requiring notification of port requests to customers harm competition? Is there a particular method of notification that is most effective? For this and other potential rules that may require text messages and/or push notifications, should we define the scope of permissible text messages or other push notifications and, if so, what definition or definitions should we use?<sup>105</sup>

51. We also seek comment on whether a port request notification requirement is sufficient to protect customers from port-out fraud, or whether we should also require customer verification or acknowledgement of the text message or push notification through a simple Yes/No response mechanism. Would a customer port verification requirement unreasonably hinder the porting process, and could it be used anticompetitively by carriers? Should we require that customers respond within a certain amount of time before the carrier can execute the port? We recognize that some customers may not frequently check their text messages or push notifications, which could lead to a delay if we require the customer to verify the port. Should we require carriers to send follow-up messages to the customer via e-mail or a phone call? What other processes have wireless carriers adopted to protect customers from port-out fraud, and have they been effective in reducing port-out fraud?

52. As discussed above, the National Institute of Standards and Technology and recent media reports call into question the security of using text messages for authentication purposes.<sup>106</sup> Is notification and/or verification of a port request via text message a secure means of authenticating the validity of a customer’s wireless port request? Should we instead require an automated notification call and verification response through a voice call or other method, such as e-mail or carrier app? What methods would ensure that customers who have voice-and-text-only service, or whose devices are incapable of accessing a carrier’s app or website, are not hindered in their porting choices? Are there any barriers for smaller carriers implementing any of these changes to protect customers’ accounts from port-out fraud?

53. We seek comment whether we should require customers’ existing wireless carriers to authenticate a customer’s wireless port request through means other than the fields used to validate simple port requests. Are the benefits of potentially protecting customers from port-out fraud outweighed by the potential harms to competition from delaying or impeding customers’ valid wireless number port requests? We seek comment on the processes that wireless carriers, including MVNO providers, resellers, and smaller carriers, currently use to authenticate customer port-out requests, and whether those methods are effective in preventing port-out fraud. According to CTIA, “[w]ireless providers are constantly improving internal processes to stay ahead of . . . bad actors, while protecting the rights of legitimate customers to transfer their phone number to a new device or wireless provider,” including “[s]ending one-time passcodes via text message or e-mail to the account phone number or the e-mail associated with the account when changes are requested . . . .”<sup>107</sup> Verizon will not allow its customers to transfer their number to a different carrier unless that customer first requests a Number Transfer Pin.<sup>108</sup>

<sup>104</sup> AT&T, *Prevent Porting to Protect Your Identity*, <https://about.att.com/pages/cyberaware/ni/blog/porting> (last visited Aug. 20, 2021).

<sup>105</sup> See, e.g., 47 U.S.C. § 227(e)(8)(C) (defining “text message” in the Truth in Caller ID context); 47 CFR § 9.10(q)(9), (10)(iv) (defining “911 text message” and setting forth certain exclusions).

<sup>106</sup> See *supra* para. 24.

<sup>107</sup> CTIA, *Protecting Your Wireless Account Against SIM Swap Fraud*, <https://www.ctia.org/protecting-against-sim-swap-fraud> (last visited Aug. 20, 2021).

<sup>108</sup> Verizon, *Transfer (port-out) your number to another carrier FAQs*, <https://www.verizon.com/support/port-out-faqs/> (last visited Aug. 20, 2021).

When a Verizon customer requests a port from its new service provider, the customer must present the Verizon account number and Number Transfer Pin in order to authenticate the request.<sup>109</sup> AT&T customers can create a unique passcode that in most cases the customer is required to provide “before any significant changes can be made including porting through another carrier,”<sup>110</sup> and starting September 30, 2021, will require customers to request a Number Transfer PIN to transfer their number to another service provider, which will replace the account passcode customers currently use.<sup>111</sup> T-Mobile assigns each of its customer accounts a 6-15 digit PIN that must be provided whenever an individual requests to port-out the phone number associated with that account.<sup>112</sup> Have such port-out PINs been effective at protecting customers from port-out fraud? Have carriers noticed any effect from adopting port-out PINs or other additional security measures on their customers’ likelihood of switching carriers? Is there any evidence indicating how security measures affect porting frequency? Should we require wireless carriers to authenticate customers for wireless port requests under the same standard as we require carriers to authenticate customers for SIM change requests, recognizing that in the porting context, the Act sets forth competing goals of protecting customer information and promoting competition through local number porting? What would be the benefits and costs of doing so?

54. We seek comment on any other technical or innovative solutions for customer authentication for port requests that carriers could implement to reduce port-out fraud. For example, are there technologies developed out of the Mobile Authentication task force, a collaboration among the three major U.S. wireless carriers, that could be easily implemented into the port authentication process? ZenKey, which was developed under the auspices of the Mobile Authentication task force, “collects and shares device and account data with your wireless carrier . . . [to] easily and more securely authenticate, sign up, and sign in,”<sup>113</sup> and “uses multi-factor authentication, including unique network signals, to not only verify a user’s device but also allow verification that the user is who they say they are.”<sup>114</sup> Could carriers use similar technology to authenticate wireless customer port requests? What would be the costs of doing so and what are the challenges to implementation, including customer privacy and consent implications? What other technologies exist that carriers could use to quickly and effectively authenticate wireless port requests to reduce port-out fraud? As the nation’s networks migrate from 2G and 3G to 4G and 5G, are there particular technical features that should be taken into consideration for protecting customers from port-out fraud?

55. We seek comment on whether we should require all carriers to implement any of the additional authentication processes for wireless port requests some providers have already developed and implemented. Is there value in uniformity? Would it reduce consumer confusion if we mandate the same authentication requirements on all wireless port-out requests regardless of the providers involved? Would that potential reduction in consumer confusion outweigh the benefits of enabling carriers to create innovative procedures to protect against port-out fraud attempts as they evolve? Would requiring specific additional customer authentication procedures, as opposed to simply making it clear that carriers are responsible for preventing port-out fraud, provide a roadmap to bad actors? Should we instead require

---

<sup>109</sup> *Id.*

<sup>110</sup> AT&T, *Prevent Porting to Protect Your Identity*, [https://about.att.com/pages/cyber-aware/news-information/blog/prevent\\_porting.html](https://about.att.com/pages/cyber-aware/news-information/blog/prevent_porting.html) (last visited Aug. 23, 2021).

<sup>111</sup> AT&T, *Transfer Your Wireless Number to Another Provider*, <https://www.att.com/support/article/wireless/KM1447526/> (last visited Sept. 23, 2021).

<sup>112</sup> T-Mobile, *How T-Mobile Helps Customers Fight Account Takeover Fraud* (Oct. 29, 2019), <https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud>.

<sup>113</sup> AT&T, *Learn about ZenKey*, <https://www.att.com/support/article/wireless/KM1375558/> (last visited Aug. 23, 2021).

<sup>114</sup> AT&T, *Mobile Authentication Taskforce to Unveil ZenKey at MWC Los Angeles*, [https://about.att.com/story/2019/mobile\\_authentication\\_taskforce\\_zenkey.html](https://about.att.com/story/2019/mobile_authentication_taskforce_zenkey.html) (last visited Aug. 23, 2021).

carriers to develop heightened customer authentication procedures like those already initiated by the three nationwide wireless carriers, but provide flexibility to the individual carriers to create and employ what works best for their service? Should we require different authentication procedures for pre-paid wireless account port-out requests than we do for post-paid wireless account port-out requests? We also seek comment on what implementation period the wireless industry would need to implement any additional validation requirements and processes we adopt.

56. We seek comment on how additional port authentication requirements would affect the timing of simple wireless-to-wireless ports. Would allowing additional authentication procedures cause unreasonable delay to the wireless porting process or cause harm to competition? In adopting any additional customer authentication requirements, we want to ensure that we leave carriers in a position to innovate and address new problems as they arise. Relatedly, we seek comment on whether it is necessary to codify a simple wireless-to-wireless porting interval to ensure that any new port authentication requirements do not lead to delay in the current porting process. The wireless industry has voluntarily established an industry standard of two and one-half hours for simple wireless-to-wireless ports.<sup>115</sup> Should we codify this interval in our rules?

57. *Port-Freeze Offerings.* We propose to require all wireless providers, including resellers, to offer customers the option to place a “port-freeze” on their accounts at no cost to the customer to help deter port-out fraud. We observe that our rules currently permit local exchange carriers (LECs) to offer their customers the ability to “prevent[] a change in a subscriber’s preferred carrier selection unless the subscriber gives the carrier from whom the freeze was requested his or her express consent.”<sup>116</sup> Should we require wireless providers to offer a similar option, and would making this option available to wireless customers deter wireless port-out fraud? Verizon offers customers the option to lock their number, blocking all port-out requests unless the account owner turns off the Number Lock feature through the Verizon mobile app, on Verizon’s website, or by calling customer service.<sup>117</sup> Do other wireless carriers currently offer a similar feature? Has this feature, and others like it, been successful at deterring port-out fraud? What costs would offering this feature impose on carriers? How can we make sure that customers are easily notified of this feature? Would a one-time notice for existing customers, and notice at the time service is started, be effective at notifying customers? How often should carriers provide this notice to customers? What method would be least burdensome on carriers while also notifying all customers, including those that do not access their accounts through online services or carrier apps, of the availability of this feature? Local exchange carriers who offer their customers the “preferred carrier freeze” option must follow specific requirements regarding the solicitation and imposition of this option.<sup>118</sup> Should we extend similar requirements to wireless carriers? If we impose these requirements, would the benefits gained by deterring port-out fraud outweigh the costs of this measure?<sup>119</sup> What happens when a customer

---

<sup>115</sup> See North American Numbering Council Local Number Portability Administration Working Group Report on Wireless Wireline Integration, May 8, 1998, CC Docket No. 95-116 (filed May 18, 1998); 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 (filed Sept. 26, 2000); ATIS Operations and Billing Forum, Wireless Intercarrier Communications: Interface Specification for Local Number Portability, Version 2, at 6, para. 2 (Jan. 2003).

<sup>116</sup> See 47 CFR § 64.1190(a).

<sup>117</sup> Verizon, *Transfer (port-out) your number to another carrier FAQs*, <https://www.verizon.com/support/port-out-faqs/> (last visited Aug. 23, 2021).

<sup>118</sup> See 47 CFR § 64.1190(d).

<sup>119</sup> See *Protecting Consumers from Unauthorized Carrier Changes and Related Unauthorized Charges*, CG Docket No. 17-169, Report and Order, 33 FCC Rcd 5773, 5784, para. 31 (2018). The Commission declined to adopt a default preferred carrier freeze requirement, finding that default freezes could potentially inhibit consumer switching and competition and the ability of carriers to quickly port customers. *Id.*

locks his or her account but is unable to recall the information necessary to unlock their account? Should there be a back-up authentication method available? Are there other methods wireless carriers use to prevent unauthorized port requests that we should consider requiring?

58. *Wireless Port Validation Fields.* We also propose to codify the types of information carriers must use to validate simple wireless-to-wireless port requests. Pursuant to the Commission's 2007 LNP *Four Fields Declaratory Ruling*, the wireless industry agreed to use three fields of customer-provided information—telephone number, account number, and ZIP code—plus a passcode field (if customer-initiated) to validate requests for simple wireless-to-wireless ports. We propose to codify this requirement in our rules for simple wireless-to-wireless ports, just as we have codified field requirements for simple wireline and intermodal ports.<sup>120</sup> We preliminarily believe that standardizing the fields necessary to complete a simple wireless-to-wireless port will allow for quicker and more efficient porting,<sup>121</sup> and we seek comment on this view. We propose adopting the existing fields because we are cognizant that imposing new or different customer-required information fields could complicate the porting process, from both the carrier and customer perspectives, and we seek comment on this view. We seek comment whether codifying the existing fields used for validating simple wireless ports, in combination with immediate customer notification of port-requests and the offering and advertisement of port-freeze options as we propose, would help to protect customers from port-out fraud. Do such measures appropriately balance the competitive benefits of rapid porting with protecting customers' accounts from fraud?

59. Are there additional fields of customer-provided information we should require for validation of wireless-to-wireless ports to minimize port-out fraud, while ensuring the continued rapid execution of valid port-out requests? If we require additional fields of customer-provided information for only wireless-to-wireless simple ports, will that cause unnecessary complications for the telecommunications industry as a whole? Will it impose additional costs on wireless carriers that would reduce competition in the telecommunications marketplace? We seek comment on whether requiring carriers to implement changes to the wireless port validation requirements would significantly impair the customer's ability to perform a legitimate port-out request. Would requiring carriers to implement additional customer-provided fields for wireless port requests stifle the ability of customers to switch carriers while retaining their phone number or keep customers locked into contracts with their current service providers? Would customers still be able to respond to price and service changes in a quick and efficient manner? Finally, we propose to make clear that any customer validation requirements apply to both facilities-based wireless carriers and resellers of wireless service and we seek comment on that proposal.

60. We seek comment on whether we should require carriers to implement a customer-initiated passcode field for all wireless number port requests, or whether it should remain optional. While AT&T, Verizon, and T-Mobile offer this option, it is unclear if all customers are required to participate. What would be the burden on customers and carriers, particularly smaller carriers, were we to mandate passcode fields for wireless number port requests? Could it harm competition and cause customer frustration if a customer has either not set up a passcode or does not know how to set up a passcode? Should we require carriers to make a customer-initiated passcode optional on an opt-out rather than opt-in basis? What steps could carriers take to make it least burdensome on customers to establish an account passcode for wireless number porting purposes? We also seek comment on how we can ensure that a customer can make a legitimate port request if he forgets his passcode.

61. *Remediating Port-Out Fraud.* We seek comment on how we can ensure timely resolution of unauthorized port-out requests to minimize financial and other damage to customers who are victims of such fraud. What information do wireless carriers currently collect about port-out fraud? Are wireless

---

<sup>120</sup> See 47 CFR § 52.36(b)(1)-(3).

<sup>121</sup> LNP *Standard Fields Order*, 25 FCC Rcd at 6958, para. 8.

carriers already tracking instances of customer complaints regarding this issue? Should we require that carriers use this information to measure the effectiveness of their customer authentication and account protection measures? How can we encourage and/or ensure that carriers coordinate and work together to quickly resolve complaints in cases of port-out fraud? Should we require carriers to respond to customers who allege they are victims of port-out fraud and to offer redress to such customers within a certain time frame? What would be the costs to carriers, and what are the costs to customers if we do not do so? We seek comment on the methods wireless carriers have established to help victims of port-out fraud stop an unauthorized port-out request or to recover their phone numbers from bad actors.

62. *Accounts with Multiple Lines.* We seek comment on how the proposed changes to our LNP rules impact wireless accounts with multiple lines, such as shared or family accounts. If we require the customer to provide a one-time passcode for the carrier to execute the port, should each line on the shared or family account have its own passcode? If the account owner elects to freeze the account to protect against unauthorized changes, how can we ensure that another member of the shared or family account remains able to port-out their number? Should the port-freeze option apply only to individual lines and not to entire accounts? Do our proposed rules impact these types of accounts with multiple lines in any other ways?

63. *Role of Administrator.* We also seek comment on whether the Local Number Portability Administrator (LNPA) can play a role in thwarting port-out fraud by serving as an authorized neutral third-party to verify customer identification prior to authorizing a port-out request. The LNPA operates the Number Portability Administration Center (NPAC), which “is the system that supports the implementation of LNP and is used to facilitate number porting in the United States.”<sup>122</sup> The LNPA, through the NPAC, currently works with a customer’s new service provider to create a number port and sends a notification to the old service provider, once the existing service provider validates and confirms the subscriber’s information.<sup>123</sup> What information regarding port requests does the NPAC retain? Is there additional information regarding port requests the NPAC should retain to help prevent port-out fraud? What records could be helpful if provided to customers who have been victims of unauthorized port-out fraud? Through what means and under what conditions, if any, should wireless providers permit their customers to access NPAC data regarding port requests that pertain to the customer’s telephone number? Are there additional obligations that we should direct or encourage North American Portability Management, LLC, which oversees the LNPA contract, to impose on the LNPA to safeguard against port-out fraud?

64. As discussed above, the Number Portability Industry Forum has created “Best Practices” for porting between and within telephony carriers.<sup>124</sup> Best Practice 73 (Unauthorized Port Flow) specifically addresses carrier processes for responding to unauthorized ports, including fraudulent ports, which are ports “which occurred as the result of an intentional act of fraud, theft, and/or misrepresentation.”<sup>125</sup> We seek comment on the extent to which wireless providers have adopted Best Practice 73. If wireless carriers have adopted Best Practice 73, is it effective in addressing port-out fraud? Are there changes we can make to the process flow to better protect customers? If wireless carriers have not implemented Best Practice 73, we seek comment on other methods they use to investigate potentially fraudulent ports and how they restore service to the customer. Should we require mobile carriers to adopt Best Practice 73 to help speed resolution of fraudulent port complaints? We also seek comment on what

---

<sup>122</sup> See NPAC, *About NPAC*, <https://numberportability.com/about-us/about-npac/> (last visited Aug. 20, 2021).

<sup>123</sup> NPAC, *How LNP Works*, <https://numberportability.com/about-us/how-lnp-works/> (last visited Aug. 20, 2021).

<sup>124</sup> NPAC, *Number Portability Best Practices*, <https://numberportability.com/industry-info/lmpa-working-group/lmpa-best-practices/?page=1> (last visited Aug. 20, 2021).

<sup>125</sup> NPAC, *Number Portability Best Practices*, <https://numberportability.com/industry-info/lmpa-working-group/lmpa-best-practices/?page=1> (last visited Aug. 20, 2021).



role the North American Numbering Council (NANC) can play in establishing updated best practices to protect customers from port-out fraud and in reaching industry consensus.

65. *Partial Porting Fraud.* We seek comment on whether the proposals on which we seek comment above would also be effective against partial porting fraud, where the bad actor changes the consumer's carrier for delivery of SMS messages without changing their primary carrier. Would our proposed customer notification and authentication rule prevent routing of SMS messages through an alternate provider without customer notification? Would a port freeze prevent changing the delivery provider and destination of SMS messages? If not, what changes to the proposed rules would be required to ensure they also apply to partial porting fraud? What additional measures would be necessary to prevent partial porting fraud in addition to the fraud that may occur when a wireless provider completely ports a consumer's mobile service?

66. *Impact on Smaller Carriers.* We seek comment on the impact the LNP rule changes that we discuss above could have on smaller carriers. Would these new requirements impose undue burdens on smaller carriers? Would smaller carriers face different costs from larger carriers in implementing the new requirements, if adopted? Would smaller carriers need more time to comply with revised number porting rules? Do they face other obstacles that we have not considered here?

67. *Legal Authority.* Finally, we seek comment on our legal authority to adopt the possible rules discussed in this section. We propose to rely on authority derived from sections 4, 201, 251(b)(2), 251(e), 303, and 332 of the Act to implement the proposed changes to our number porting rules to address port-out fraud, and seek comment on our proposal.<sup>126</sup> Are there additional sources of authority on which the Commission can rely to implement these proposals? Should we extend any of the LNP rules on which we seek comment to any entities other than wireless carriers, such as landline carriers or VoIP providers? If so, we propose concluding that we have authority to do so pursuant to section 251(e), and we seek comment on this view.<sup>127</sup> We also seek comment on whether we should update the references to "CMRS" in the Commission's number porting rules to reflect evolving technology. Finally, we solicit input on the relative costs and benefits of our proposals to amend the LNP rules to address port-out fraud.

### C. Additional Consumer Protection Measures

68. Finally, we seek comment on any additional rules that would help protect customers from SIM swap or port-out fraud or assist them with resolving problems resulting from such incidents. We are aware 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. 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. To provide support for customers who have become victims, we seek comment on requiring wireless carriers to provide to customers (upon request) documentation of SIM swap or port-out fraud on accounts that the customer may then provide to law enforcement, financial institutions, or others. We seek comment on what information should be included in the documentation provided by carriers. We also seek comment on the potential benefits and projected costs of this proposal, including on smaller providers. Further, we invite input on how the proposed rule would affect the customer experience, either positively or negatively.

69. Next, we seek comment on other measures we can adopt to ensure that customers have easy access to information they need to report SIM swap, port-out, or other fraud. As discussed above,

---

<sup>126</sup> See generally *First Number Portability Order*, 12 FCC Rcd at 7232, 7242, 7273, paras. 2, 11, 61; *Porting Interval Order and FNPRM*, 24 FCC Rcd at 6084, para. 1; *LNP Standard Fields Order*, 25 FCC Rcd at 6954-55, paras. 2-3.

<sup>127</sup> See, e.g., *Implementation of the National Suicide Hotline Improvement Act of 2018*, Report and Order, 35 FCC Rcd 7373, 7394, para. 40 (2020) (relying on section 251(e) to apply requirements to interconnected and one-way VoIP).

we believe that customer service representatives should be trained on how to assist customers who have been victims of SIM swap or port-out fraud, and carriers should have procedures in place for a response. Identity 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. Thus, in addition to providing documentation, we believe 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 fraud. As such, we seek comment on whether we should adopt rules addressing how wireless carriers deal with customers once they have become victims of SIM swapping and port-out fraud. What procedures do carriers have in place to assist customers in these circumstances and are these procedures effective? What additional steps can carriers take to recover the account and stop the ongoing fraudulent activity? How can carriers ensure that customers have easy access to the information they need to report SIM swap fraud? Should we require wireless carriers to establish a dedicated point or method of contact that is easily accessible by customers and is made available on the carrier's website so that customers can get timely assistance from their carriers?<sup>128</sup> Or, given the time-sensitive nature of most fraud, would it make sense to require carriers to have a dedicated and publicized fraud hotline that customers can call directly in the case of suspected fraud? What costs would such a requirement impose on carriers, and how long would it take for carriers to implement? Are any of the Commission's existing rules obstacles to helping customers recover following a SIM swap or port-out fraud incident?

70. We seek comment on whether there are other customer protections we could adopt to address the problems associated with SIM swap and port-out fraud. For example, should the Commission require wireless carriers to enable "fraud alerts" on accounts and publicize these services to customers? Such fraud alerts could trigger additional protections when changes are requested on the accounts. Would such a requirement be effective at deterring SIM swap and port-out fraud? Would it have any unintended consequences for customers? What would such a requirement cost? Are there any other consumer protections that would be effective in combatting SIM swap and port-out fraud and, if so, how would they operate? What would be their relative costs and benefits? For example, we understand that in other countries, carriers and financial institutions share information about SIM transfers to limit damages to consumers resulting from incidents of SIM swap fraud.<sup>129</sup> As discussed above, section 222 strictly limits carriers' ability to share a customer's CPNI without the customer's consent. Can we, and should we, encourage carriers to establish a mechanism based on express customer consent that would enable a financial institution to determine whether a SIM transfer had been recently completed to help protect customers from the financial harms of SIM swap and port-out fraud? If so, should we require or encourage carriers to ask for customer permission upon set up of accounts (and to send out one-time notice to all existing customers asking if they want to permit this)? Should such a rule require retention of the record of this permission for some designated period of time? Should carriers be permitted to charge a fee for this service either to the wireless customer or to the financial institution? Are there other types of institutions that might need access to the same type of information to prevent fraud? Should our rules expressly permit or prohibit this type of service? What are the potential risks and benefits to consumers? We seek comment on how we can ensure that customers are able to take advantage of third-party fraud services to protect against SIM swap and port-out fraud.

71. We tentatively conclude that our broad Title III authority would support imposing additional consumer protection obligations such as those discussed in this section on wireless carriers. We also seek comment on whether authority derived from sections 4, 201, 222, 251, 303, and 332 would support such additional consumer protection measures. Should we extend any new consumer protection

---

<sup>128</sup> Cf., e.g., 47 CFR § 64.2113 (requiring covered providers to make contact information for the receipt and handling of rural call completion issues available on their websites, and requiring that the contact information must be easy to find and use).

<sup>129</sup> See Andy Greenberg, *Wired*, *The SIM Swap Fix That the US Isn't Using*, Apr. 26, 2019, <https://www.wired.com/story/sim-swap-fix-carriers-banks/>.

requirements to interconnected VoIP services, one-way VoIP services, or landline services? If so, pursuant to what legal authority would the Commission adopt such rules? We invite commenters to discuss the relative costs and benefits of these proposals and any foreseeable unintended consequences of the measures we discuss.

72. We seek comment on whether there are standards-setting bodies, industry organizations, or consumer groups that could evaluate this issue to augment our understanding and present possible solutions. For example, could the Alliance for Telecommunications Industry Solutions (ATIS) provide technical expertise that would be useful in determining the best course of action by the Commission to protect customers from SIM swap or port-out fraud? Could relevant trade associations work to develop industry consensus solutions to the problem?

73. *Digital Equity and Inclusion.* Finally, the Commission, as part of its continuing effort to advance digital equity for all,<sup>130</sup> 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<sup>131</sup> 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 the scope of the Commission's relevant legal authority.

#### IV. PROCEDURAL MATTERS

74. *Ex Parte Rules.* This proceeding shall be treated as a “permit-but-disclose” proceeding in accordance with the Commission's *ex parte* rules.<sup>132</sup> 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,

---

<sup>130</sup> 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.

<sup>131</sup> 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).

<sup>132</sup> 47 CFR §§ 1.1200 *et seq.*

.xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

75. *Initial Regulatory Flexibility Analysis.* Pursuant to the Regulatory Flexibility Act (RFA),<sup>133</sup> the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and actions considered in this *Notice of Proposed Rulemaking*. The text of the IRFA is set forth in Appendix B. Written public 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 *Notice of Proposed Rulemaking*. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of the *Notice of Proposed Rulemaking*, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration.<sup>134</sup>

76. *Comment 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). See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: <https://www.fcc.gov/ecfs/>.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.

Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- 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 DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020). <https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy>

77. *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](mailto:fcc504@fcc.gov) or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice), 202-418-0432 (TTY).

78. *Paperwork Reduction Act of 1995 Analysis.* This document may contain proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB)

---

<sup>133</sup> See 5 U.S.C. § 603.

<sup>134</sup> See 5 U.S.C. § 603(a).

to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.<sup>135</sup>

79. *Contact Person.* For further information about this rulemaking proceeding, please contact Melissa Kirkel, Competition Policy Division, Wireline Competition Bureau, at (202) 418-7958 or melissa.kirkel@fcc.gov.

## V. ORDERING CLAUSES

80. Accordingly, IT IS ORDERED that, pursuant to the authority contained in 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, this Notice of Proposed Rulemaking in WC Docket No. 21-341 IS ADOPTED.

81. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch  
Secretary

---

<sup>135</sup> See 44 U.S.C. § 3506(c)(4).

**APPENDIX A**  
**Proposed Rules**

The Federal Communications Commission proposes to amend 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) A wireless provider, including a reseller of wireless service, may only require the data described in paragraphs (b) and (c) of this section to accomplish a simple wireless-to-wireless port order request from an end user customer's new wireless provider.

(b) *Required standard data fields.*

(1) Ported telephone number;

(2) Account number;

(3) Zip code;

(c) *Optional standard data field.* A Passcode field shall be optional unless the passcode has been requested and assigned by the end user, in which case it is required.

(d) *Notification required after port request.* A wireless provider, including a reseller of wireless service, shall notify an end user customer that a port request has been received for the customer's account before executing a simple wireless-to-wireless port request. A wireless provider shall provide this notification to the end-user customer via text message to the telephone number of record for the customer's account or via push notification.

(e) *Account freezes.* A wireless provider, including a reseller of wireless service, shall offer customers the option to lock their accounts to prohibit unauthorized port requests. If the customer chooses to lock the customer's account, the wireless provider shall not fulfill a simple wireless-to-wireless port order request until the customer deactivates the lock on the account.

**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, 403(b)(2)(B), (c), 616, 620, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

4. Revise § 64.2010 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.

(b) *Telephone access to CPNI.* Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (g) of this section, that is not prompted by the carrier asking for readily available biographical information or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, account information, recent payment information, or call detail information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (g) of this section, that is not prompted by the carrier asking for readily available biographical information, account information, recent payment information, or call detail information.

(d) *In-store access to CPNI.* A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e) *Subscriber Identity Module (SIM) changes.* Telecommunications carriers shall not effectuate a SIM change unless the carrier uses a secure method of authenticating its customer. For purposes of this paragraph, the following shall be considered secure methods of authenticating a customer: (1) use of a pre-established password; (2) a one-time passcode sent via text message to the account phone number or a pre-registered backup number; (3) a one-time passcode sent via e-mail to the e-mail address associated with the account; or (4) a one-time passcode sent using a voice call to the account phone number or a pre-registered backup number. These methods shall not be considered exhaustive and an alternative customer authentication measure used by a carrier must be a secure method of authentication. For purposes of this section, SIM means a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network.

(f) *Procedures for failed authentication for SIM changes.* Wireless carriers shall develop, maintain, and implement procedures for responding to multiple failed authentication attempts.

(g) *Establishment of a password and back-up authentication methods for lost or forgotten passwords.* To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, account information, recent payment information, or call detail information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, account information, recent payment information, or call detail information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(h) *Notification of account changes.* Telecommunications carriers must 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. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information. Telecommunications carriers shall notify customers immediately of any requests for SIM changes through means that effectively alert customers in a timely manner.

(i) *Business customer exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.



**APPENDIX B****Initial Regulatory Flexibility Analysis**

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),<sup>1</sup> 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 Notice of Proposed Rulemaking (NPRM). 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 NPRM provided on the first page of the item. The Commission will send a copy of the NPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).<sup>2</sup> In addition, the NPRM and IRFA (or summaries thereof) will be published in the Federal Register.<sup>3</sup>

**A. Need For, and Objectives of, the Proposed Rules**

2. This item focuses developing protections to address SIM swapping and port-out fraud. In SIM swapping, the bad actor targets a consumer's subscriber identity module (SIM) and convinces the victim's wireless carrier to transfer the victim's service from the original device (and that device's SIM) to a cell phone in the bad actor's possession. A consumer's wireless phone number is associated with the SIM in that consumer's cell phone; by "swapping" the SIM associated with a phone number, the bad actor can take control of a consumer's cell phone account. In "port-out fraud," the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or "ported out") to the account with the new carrier controlled by the bad actor.

3. We have received numerous consumer complaints from people who have suffered significant distress, inconvenience, and financial harm as a result of SIM swapping and port-out fraud. Today, we take aim at these scams, with the goal of foreclosing these opportunistic ways in which bad actors take over consumers' cell phone accounts. Section 222 of the Communications Act of 1934, as amended (the "Act"), and our Customer Proprietary Network Information (CPNI) rules, which govern the use, disclosure, and protection of sensitive customer information to which a telecommunications carrier has access, require carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to customers' private information. Our Local Number Portability (LNP) rules govern the porting of telephone numbers from one carrier to another. Yet, it appears that neither our CPNI rules nor our LNP rules are adequately protecting consumers against SIM swap and port-out fraud. We, therefore, propose to amend our CPNI and LNP rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. We also propose to require providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts, and we seek comment on other ways to protect consumers from SIM swapping and port-out fraud.

**B. Legal Basis**

4. The legal basis for any action that may be taken pursuant to this NPRM is contained in sections 1, 4(i), 4(j), 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), 332.

---

<sup>1</sup> 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).

<sup>2</sup> See 5 U.S.C. § 603(a).

<sup>3</sup> See *id.*

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

5. 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 and policies, if adopted.<sup>4</sup> The RFA generally defines the term “small entity” as having the same meaning as the terms “small business,” “small organization,” and “small governmental jurisdiction.”<sup>5</sup> In addition, the term “small business” has the same meaning as the term “small business concern” under the Small Business Act.<sup>6</sup> 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.<sup>7</sup>

6. *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 here, at the outset, three broad groups of small entities that could be directly affected herein.<sup>8</sup> 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.<sup>9</sup> These types of small businesses represent 99.9 percent of all businesses in the United States, which translates to 30.7 million businesses.<sup>10</sup>

7. 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.”<sup>11</sup> 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.<sup>12</sup> Nationwide, for tax year 2018, there were approximately 571,709 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.<sup>13</sup>

---

<sup>4</sup> 5 U.S.C. § 603(b)(3).

<sup>5</sup> 5 U.S.C. § 601(6).

<sup>6</sup> 5 U.S.C. § 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.”

<sup>7</sup> 15 U.S.C. § 632.

<sup>8</sup> See 5 U.S.C. § 601(3)-(6).

<sup>9</sup> See U.S. Small Business Administration, Office of Advocacy, *What’s New With Small Business?* (Sept. 2019), <https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/23172859/Whats-New-With-Small-Business-2019.pdf>.

<sup>10</sup> *Id.*

<sup>11</sup> 5 U.S.C. § 601(4).

<sup>12</sup> 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 small organizations in this small entity description. See IRS, *Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), Who May File Form 990-N to Satisfy Their Annual Reporting Requirement*, <https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard> (last visited Aug. 2, 2021). 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.

<sup>13</sup> 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....)

8. 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.”<sup>14</sup> U.S. Census Bureau data from the 2017 Census of Governments<sup>15</sup> indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.<sup>16</sup> Of this number there were 36,931 general purpose governments (county,<sup>17</sup> municipal and town or township<sup>18</sup>) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts<sup>19</sup> with enrollment populations of less than 50,000.<sup>20</sup>

### 1. Providers of Telecommunications and Other Services

9. *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. 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. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.”<sup>21</sup> The SBA has developed a small

(Continued from previous page) \_\_\_\_\_

BMF data for Region 1-Northeast Area (76,886), Region 2-Mid-Atlantic and Great Lakes Areas (221,121), and Region 3-Gulf Coast and Pacific Coast Areas (273,702) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

<sup>14</sup> 5 U.S.C. § 601(5).

<sup>15</sup> See 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>.

<sup>16</sup> See 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 Table 2. CG1700ORG02 Table Notes\_Local Governments by Type and State\_2017.

<sup>17</sup> See *id.* at Table 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.

<sup>18</sup> See *id.* at Table 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.

<sup>19</sup> See *id.* at Table 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 Table 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.

<sup>20</sup> 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 Tables 5, 6, and 10.

<sup>21</sup> See U.S. Census Bureau, 2017 NAICS Definition, “517311 Wired Telecommunications Carriers,” <https://www.census.gov/naics/?input=517311&year=2017&details=517311>.

business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.<sup>22</sup> U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.<sup>23</sup> Of this total, 3,083 operated with fewer than 1,000 employees.<sup>24</sup> Thus, under this size standard, the majority of firms in this industry can be considered small.

10. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers.<sup>25</sup> Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.<sup>26</sup> U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated for the entire year.<sup>27</sup> Of that total, 3,083 operated with fewer than 1,000 employees.<sup>28</sup> Thus under this category and the associated size standard, the Commission estimates that the majority of local exchange carriers are small entities.

11. *Incumbent Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers.<sup>29</sup> Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.<sup>30</sup> U.S. Census Bureau data for 2012 indicate that 3,117 firms operated the entire year.<sup>31</sup> Of this total, 3,083 operated with fewer than 1,000 employees.<sup>32</sup> Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.<sup>33</sup> Of this total, an estimated 1,006 have 1,500 or

<sup>22</sup> See 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

<sup>23</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>24</sup> *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.

<sup>25</sup> See U.S. Census Bureau, *2017 NAICS Definition*, “517311 Wired Telecommunications Carriers,” <https://www.census.gov/naics/?input=517311&year=2017&details=517311>.

<sup>26</sup> See 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

<sup>27</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>28</sup> *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.

<sup>29</sup> See U.S. Census Bureau, *2017 NAICS Definition*, “517311 Wired Telecommunications Carriers,” <https://www.census.gov/naics/?input=517311&year=2017&details=517311>.

<sup>30</sup> See 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

<sup>31</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>32</sup> *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.

<sup>33</sup> See *Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

fewer employees.<sup>34</sup> Thus, using the SBA's size standard the majority of incumbent LECs can be considered small entities.

12. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers.<sup>35</sup> The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.<sup>36</sup> U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year.<sup>37</sup> Of that number, 3,083 operated with fewer than 1,000 employees.<sup>38</sup> According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.<sup>39</sup> Of this total, an estimated 317 have 1,500 or fewer employees.<sup>40</sup> Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

13. *Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers<sup>41</sup> and under that size standard, such a business is small if it has 1,500 or fewer employees.<sup>42</sup> U.S. Census Bureau data for 2012 indicate that 3,117 firms operated during that year.<sup>43</sup> Of that number, 3,083 operated with fewer than 1,000 employees.<sup>44</sup> Based on these data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services.<sup>45</sup> Of these 1,442 carriers, an

---

<sup>34</sup> *Id.*

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

<sup>36</sup> See 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

<sup>37</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>38</sup> *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.

<sup>39</sup> See *Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010), [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-301823A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf) (*Trends in Telephone Service*).

<sup>40</sup> *Id.*

<sup>41</sup> See U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* <https://www.census.gov/naics/?input=517311&year=2017&details=517311>.

<sup>42</sup> See 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

<sup>43</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>44</sup> *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.

<sup>45</sup> See Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division, *Trends in Telephone Service* at Table 5.3 (Sept. 2010), [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-301823A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf) (*Trends in Telephone Service*).

estimated 1,256 have 1,500 or fewer employees.<sup>46</sup> In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees.<sup>47</sup> Also, 72 carriers have reported that they are Other Local Service Providers.<sup>48</sup> Of this total, 70 have 1,500 or fewer employees.<sup>49</sup> Consequently, based on internally researched FCC data, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.<sup>50</sup>

14. *Local Resellers.* The SBA has not developed a small business size standard specifically for Local Resellers. The closest NAICS Code Category is Telecommunications Resellers. 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. MVNOs are included in this industry.<sup>51</sup> The SBA has developed a small business size standard for the category of Telecommunications Resellers.<sup>52</sup> Under that size standard, such a business is small if it has 1,500 or fewer employees.<sup>53</sup> 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.<sup>54</sup> Of that number, 1,341 operated with fewer than 1,000 employees.<sup>55</sup> Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.<sup>56</sup> Of this total, an estimated 857 have 1,500 or fewer employees.<sup>57</sup> Consequently, the Commission estimates that the majority of local resellers are small entities.

---

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

<sup>50</sup> We have included small incumbent LECs in this present RFA analysis. As noted above, a “small business” under the RFA is one that, *inter alia*, meets the pertinent small business size standard (e.g., a telephone communications business having 1,500 or fewer employees), and “is not dominant in its field of operation.” The SBA’s Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not “national” in scope. We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

<sup>51</sup> See U.S. Census Bureau, *2017 NAICS Definition*, “517911 Telecommunications Resellers,” <https://www.census.gov/naics/?input=517911&year=2017&details=517911>.

<sup>52</sup> See 13 CFR § 121.201, NAICS Code 517911.

<sup>53</sup> *Id.*

<sup>54</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517911, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>55</sup> *Id.* Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA’s size standard.

<sup>56</sup> See *Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

<sup>57</sup> See *id.*

15. *Toll Resellers.* The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. 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. MVNOs are included in this industry.<sup>58</sup> The SBA has developed a small business size standard for the category of Telecommunications Resellers.<sup>59</sup> Under that size standard, such a business is small if it has 1,500 or fewer employees.<sup>60</sup> 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.<sup>61</sup> Of that number, 1,341 operated with fewer than 1,000 employees.<sup>62</sup> Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.<sup>63</sup> Of this total, an estimated 857 have 1,500 or fewer employees.<sup>64</sup> Consequently, the Commission estimates that the majority of toll resellers are small entities.

16. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. 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.<sup>65</sup> The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.<sup>66</sup> For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.<sup>67</sup> Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed 1000 employees or more.<sup>68</sup> Thus under this category and the associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

---

<sup>58</sup> See U.S. Census Bureau, *2017 NAICS Definition, "517911 Telecommunications Resellers,"* <https://www.census.gov/naics/?input=517911&year=2017&details=517911>.

<sup>59</sup> See 13 CFR § 121.201, NAICS Code 517911.

<sup>60</sup> *Id.*

<sup>61</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517911, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>62</sup> *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.

<sup>63</sup> See *Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

<sup>64</sup> See *id.*

<sup>65</sup> See U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* <https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517312&search=2017%20NAICS%20Search>.

<sup>66</sup> See 13 CFR § 121.201, NAICS Code 517312 (previously 517210).

<sup>67</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517210, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517210&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false&vintage=2012>.

<sup>68</sup> *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.

17. The Commission's own data—available in its Universal Licensing System—indicate that, as of August 31, 2018 there are 265 Cellular licensees that will be affected by our actions.<sup>69</sup> The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services.<sup>70</sup> Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees.<sup>71</sup> Thus, using available data, we estimate that the majority of wireless firms can be considered small.

18. *Satellite Telecommunications.* This category 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.”<sup>72</sup> Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of \$35 million or less in average annual receipts, under SBA rules.<sup>73</sup> For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.<sup>74</sup> Of this total, 299 firms had annual receipts of less than \$25 million.<sup>75</sup> Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

19. *All Other Telecommunications.* The “All Other Telecommunications” category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.<sup>76</sup> 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.<sup>77</sup> Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.<sup>78</sup> The SBA has developed a small business size standard for “All Other

---

<sup>69</sup> See <http://wireless.fcc.gov/uls>. For the purposes of this IRFA, consistent with Commission practice for wireless services, the Commission estimates the number of licensees based on the number of unique FCC Registration Numbers.

<sup>70</sup> See Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division, Trends in Telephone Service at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*), [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-301823A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf).

<sup>71</sup> See *id.*

<sup>72</sup> See U.S. Census Bureau, 2017 NAICS Definition, “517410 Satellite Telecommunications”, <https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017>.

<sup>73</sup> See 13 CFR § 121.201, NAICS Code 517410.

<sup>74</sup> See U.S. Census Bureau, 2012 Economic Census of the United States, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517410, <https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517410&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false&vintage=2012>.

<sup>75</sup> *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 of annual receipts of \$35 million or less.

<sup>76</sup> See U.S. Census Bureau, 2017 NAICS Definition, “517919 All Other Telecommunications”, <https://www.census.gov/naics/?input=517919&year=2017&details=517919>.

<sup>77</sup> *Id.*

<sup>78</sup> *Id.*



Telecommunications,” which consists of all such firms with annual receipts of \$35 million or less.<sup>79</sup> For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.<sup>80</sup> Of those firms, a total of 1,400 had annual receipts less than \$25 million and 15 firms had annual receipts of \$25 million to \$49,999,999.<sup>81</sup> Thus, the Commission estimates that the majority of “All Other Telecommunications” firms potentially affected by our action can be considered small.

## 2. Internet Service Providers

20. *Internet Service Providers (Broadband)*. Broadband Internet service providers include wired (e.g., cable, DSL) and VoIP service providers using their own operated wired telecommunications infrastructure fall in the category of Wired Telecommunication Carriers.<sup>82</sup> Wired Telecommunications Carriers are comprised of 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 telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies.<sup>83</sup> The SBA size standard for this category classifies a business as small if it has 1,500 or fewer employees.<sup>84</sup> U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.<sup>85</sup> Of this total, 3,083 operated with fewer than 1,000 employees.<sup>86</sup> Consequently, under this size standard the majority of firms in this industry can be considered small.

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

21. In this NPRM, we propose to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer. We also propose to amend our CPNI rules to require wireless carriers to develop procedures for responding to failed authentication attempts and to notify customers immediately of any requests for SIM changes. We also seek comment on whether we should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud. We likewise propose to amend our number porting rules to combat port-out fraud while continuing to encourage robust competition through efficient number porting. Specifically, the Commission also proposes to amend the LNP rules to require carriers to send customers a text message or push notification whenever a porting request is made; to require carriers to allow customers the option to freeze their accounts to prevent any unauthorized port-out requests; and to codify the data fields wireless carriers must use to validate a port request. Finally, we also seek comment

<sup>79</sup> See 13 CFR § 121.201, NAICS Code 517919.

<sup>80</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517919, <https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517919&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false>.

<sup>81</sup> *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.

<sup>82</sup> See U.S. Census Bureau, *2017 NAICS Definition*, “517311 Wired Telecommunications Carriers”, <https://www.census.gov/naics/?input=517311&year=2017&details=517311>.

<sup>83</sup> *Id.*

<sup>84</sup> See 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

<sup>85</sup> See U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517110, <https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false>.

<sup>86</sup> *Id.* The largest category provided by the census data is “1000 employees or more” and a more precise estimate for firms with fewer than 1,500 employees is not provided.

whether we should adopt any other changes to our rules to address SIM swap and port-out fraud, including the difficulties encountered by victims of these schemes.

22. Should the Commission decide to modify existing rules or adopt new rules to protect customers from SIM swap or porting-out 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.

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

23. 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.”<sup>87</sup>

24. In this NPRM, we seek comment whether the Commission should modify its CPNI or LNP rules to protect customers from SIM swap and port-out fraud, and, if so, whether our proposals would be effective to do so. In this NPRM, we seek comment on the impact that any proposed rules could have on smaller carriers. We also seek comment on the benefits and burdens, especially the burdens on small entities, of adopting any new or revised rules regarding the customer authentication and porting process. Specifically, we seek comment whether the proposed requirements would impose additional burdens on smaller carriers; whether smaller carriers would face different costs than larger carriers in implementing the new requirements, if adopted; whether smaller carriers would need more time to comply with any new or modified authentication or port-out rules; and whether smaller providers face other obstacles that we have not considered here. The Commission expects to consider the economic impact on small entities, as identified in comments filed in response to the NPRM, in reaching its final conclusions and taking action in this proceeding.

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

25. None.

---

<sup>87</sup> See 5 U.S.C. § 603(c).

**STATEMENT OF  
ACTING CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

We download so much of our daily lives into our mobile devices. Those devices are in our palms, pockets, and purses—they're with us always. They provide us with connections a million times more powerful than what was available on Apollo 11. It's pretty incredible. It also makes them a terrific target for fraud.

One of the most dangerous scams is called SIM swapping fraud. SIM cards are small plastic chips, about the size of a dime, that are inserted into a mobile phone to identify and authenticate the subscriber.

SIM cards are increasingly at the center of scams involving our mobile devices. Here's how it works: A fraudster calls up your wireless provider and convinces the customer service representative that they are you and need your phone number switched to a new SIM card that they control. These cybercrooks do not need your phone to do this, they simply need to convince your carrier to make a change to your account. Once they do, they can use your phone number to divert your incoming messages and easily complete the kind of two-factor authentication checks that financial institutions and social media companies use. They also can be used to take over your e-mail and drain your bank accounts.

By all accounts, including a big, recent Princeton University study, this type of fraud is growing. At the Federal Communications Commission, we've seen complaints from consumers who have suffered significant distress, inconvenience, and financial harm because of SIM swapping. To make matters worse, recent carrier data breaches that have made headlines may have exposed the very kind of customer information that could make it easier to pull off these kinds of attacks.

As Senator Ron Wyden has said, "Consumers are at the mercy of wireless carriers when it comes to being protected against SIM swaps." He's right. But we have tools at this agency we can use so consumers are better protected, and their devices are more secure. In fact, we have rules on the books designed to prevent your carrier from sharing personal and private information. These rules govern how carriers are supposed to protect what is known in the law as customer proprietary network information, or CPNI. But these rules need an update to address new types of fraud like SIM swapping.

That's what we start here today. We propose to update our CPNI and related local number portability rules to require carriers to securely authenticate a customer before transferring a phone number to a new device or carrier, and we seek comment on the best way to do that. We also propose that carriers immediately notify customers whenever a SIM change or port request has been made. These proposals will help protect consumers from both SIM swaps and a related kind of fraud known as "port-out fraud," where fraudsters pose as their victims and then arrange to transfer their victim's phone number to a new account that they control.

It's important we do this now. The Princeton University study I mentioned found that four out of five SIM swap attempts in the United States are successful. We can help fix this. I look forward to the record that develops and putting an end to this cyber fraud.

For their efforts to protect consumers and their privacy, thank you to Pam Arluk, Brian Cruikshank, Justin Faulb, Lisa Hone, Dan Kahn, Melissa Kirkel, Kris Monteith, and Christi Shewman of the Wireline Competition Bureau; Eduard Bartholme, Zac Champ, Aaron Garza, Eliot Greenwald, Kurt Schroeder, Mark Stone, Patrick Webre, and Kimberly Wild of the Consumer and Governmental Affairs Bureau; Ken Carlberg, Lisa Fowlkes, Jeffery Goldthorp, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Zenji Nakazawa, Erika Olsen, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Michael Epshteyn, James Graves, Phillip Rosario, Kimbarly Taylor, Kristi Thompson,

and Shana Yates of the Enforcement Bureau; Mark Azic, Patrick Brogan, Eugene Kiselev, Eric Ralph, and Emily Talaga of the Office of Economics and Analytics; and Doug Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel.

**STATEMENT OF  
COMMISSIONER GEOFFREY STARKS**

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

You may not know exactly how SIM swapping works, but you have probably heard about its harmful results. In 2019, hackers used a SIM swap to take control of Twitter CEO Jack Dorsey’s singular twitter handle, @jack. In just 20 minutes, the hackers sent out two dozen tweets and retweets to @jack’s millions of followers, including many toxic messages.<sup>1</sup> For Mr. Dorsey and his followers, the security breach caused alarm and offense. For other victims, there have been even more devastating consequences, from drained bank balances to lost email accounts containing years of communication.

SIM swapping and port-out fraud, a related scam, occur when a bad actor successfully poses as the victim in a transaction with the victim’s phone company. The scammer can then take control of the Customer Proprietary Network Information associated with the victim’s account, leverage that control to access bank accounts and other private information, and impersonate the victim in other harmful ways. These attacks are especially insidious because they are difficult for individuals—even those with all the security resources a large tech company can provide its senior leaders—to prevent on their own.

Protecting consumers from these kinds of scams will require systemic changes. I am pleased to support this Notice of Proposed Rulemaking because it begins the process of modernizing our CPNI and Local Number Portability rules to require carriers to act. I thank my colleagues for agreeing to two changes that I believe will make this NPRM even better. First, we have asked commenters to address the possibility of “future proofing” our guidelines for authenticating user identities by incorporating the National Institute of Standards and Technology’s Digital Identity Guidelines or another authoritative source. As authentication technology improves and adapts to new threats, we will want our rules to keep up. Second, we will seek comment on whether and how the Commission should audit compliance with any carrier obligations we decide to adopt. There’s good reason to think consumer complaints alone may not reliably surface problems like improper authentication procedures. After all, a consumer who calls her wireless company and gets the assistance she hoped for could be forgiven for not noticing if the customer service representative skips steps in the authentication process. I look forward to robust comments on these issues and the many other important questions raised in the NPRM, and I thank staff of the Wireline Competition Bureau for their hard work on this item.

---

<sup>1</sup> Brian Barrett, *How Twitter CEO Jack Dorsey's Account Was Hacked* (Aug. 30, 2019), <https://www.wired.com/story/jack-dorsey-twitter-hacked/>.