This document is scheduled to be published in the
Federal Register on 12/08/2023 and available online at
https://federalregister.gov/d/2023-26338, and on **https://govinfo.gov**

6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 52 and 64

[WC Docket No. 21-341; FCC 23-95, FR ID 186823]

Protecting Consumers from SIM-Swap and Port-Out Fraud

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission adopted a *Report and Order* that adopts measures designed to address two fraudulent practices bad actors use to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone. The *Report and Order* revises the Commission's Customer Proprietary Network Information (CPNI) and Local Number Portability (LNP) rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider. The *Report and Order* also require wireless providers to immediately notify customers whenever a SIM change or port-out request is made on customers' accounts, and take additional steps to protect customers from SIM swap and port-out fraud.

DATES: Effective [[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]], except for revisions to 47 CFR 52.37(c), 52.37(d), 52.37(e), 52.37(g) (instruction 3), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8) (instruction 6), which contain information collection requirements and are delayed indefinitely. The FCC will publish a document in the *Federal Register* announcing the effective date for those Sections.

ADDRESSES: Federal Communications Commission, 45 L Street, SW, Washington, DC 20554. In addition to filing comments with the Office of the Secretary, a copy of any comments on the Paperwork Reduction Act information collection requirements contained herein should be

submitted to Nicole Ongele, Federal Communications Commission, 45 L Street, SW, Washington, DC 20554, or send an email to PRA@fcc.gov.

FOR FURTHER INFORMATION CONTACT: For further information, contact Melissa Kirkel at melissa.kirkel@fcc.gov. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele, Nicole.Ongele@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order in WC Docket No. 21-341, FCC 23-95, adopted on November 15, 2023 and released on November 16, 2023. The full text of the document is available on the Commission's website at https://docs.fcc.gov/public/attachments/FCC-23-95A1.pdf. To request materials in accessible formats for people with disabilities (e.g. braille, large print, electronic files, audio format, etc.), send an email to FCC504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice).

Compliance with the rule changes adopted in this *Report and Order* shall not be required until the later of: i) six months after the effective date of this *Report and Order*; or ii) after the Office of Management and Budget (OMB) completes review of any information collection requirements associated with this *Report and Order* that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act.

Paperwork Reduction Act of 1995 Analysis

This document contains new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, will invite the general public to comment on the information collection requirements contained in this Report and Order as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the

Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

In this *Report and Order*, we have assessed the effects of required customer notifications and notices, and related recordkeeping requirements, to protect customers from SIM swap and port-out fraud, and find that they do not place a significant burden on small businesses. Although no commenters specifically addressed whether such requirements may place burdens on small wireless providers, we note that CCA advised the Commission to "keep in mind the constraints with which many small carriers operate against in adopting security measures," asserting that any rules "should allow carriers to use technologies that are reasonably available and have choice in the approach to take in authenticating their customers." As a general matter, the baseline, flexible rules we adopt reflect our recognition that, in some cases, strict prescriptive requirements to prevent SIM swap and port-out fraud could be technically and economically infeasible for wireless providers to implement, particularly for smaller providers. We emphasize that the record shows that many wireless providers already have in place some of the policies and procedures we adopt today and that our rules may therefore only require them to adapt, refine, or consistently apply those existing practices. Additionally, by setting baseline requirements and giving wireless providers flexibility on how to meet them, we allow providers to adopt the most cost-effective and least burdensome solutions to achieve the level of security needed to protect customers against SIM swap and port-out fraud in a given circumstance. We have further minimized the potential burdens of customer notifications by declining to prescribe particular content and wording and giving wireless providers flexibility on how to deliver such notifications. Similarly, for customer notices, we declined to require a specific format and content, and we declined to require such notices be delivered to customers annually. Further, we mitigated potential burdens of the recordkeeping requirement by declining to require that wireless providers include historic data in their recordkeeping, which we acknowledged would

be particularly burdensome for small providers, and declining to require that providers report this data to the Commission regularly.

Congressional Review Act

The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

I. Synopsis

1. Today we revise our CPNI and LNP rules to provide greater protection to customers from SIM swap and port-out fraud. The cornerstone of our action is a requirement that wireless providers use secure methods of authenticating customers prior to performing SIM changes and number ports. Other rules we adopt reinforce that requirement, including that wireless providers adopt processes for responding to failed authentication attempts, institute employee training for handling SIM swap and port-out fraud, and establish safeguards to prevent employees who interact with customers from accessing CPNI until after customers have been authenticated. We also adopt rules that will enable customers to act to prevent and address fraudulent SIM changes and number ports, including requiring that wireless providers notify customers regarding SIM change and port-out requests, offer customers the option to lock their accounts to block processing of SIM changes and number ports, and give advanced notice of available account protection mechanisms. We further establish requirements to minimize the harms of SIM swap and port-out fraud when it occurs, including requiring wireless providers to maintain a clear process for customers to report fraud, promptly investigate and remediate fraud, and promptly provide customers with documentation of fraud involving their accounts. Finally, to ensure wireless providers track the effectiveness of authentication measures used for SIM change requests, we require that they keep records of SIM change requests and the authentication

measures they use.

2. In adopting these rules, we balance the need to protect customers from the harms of SIM swap and port-out fraud with the goal of preserving the relative ease with which customers can obtain legitimate SIM changes and number ports. The record reflects that the vast majority of SIM change and port-out requests are legitimate. It also shows that the efficient and effective processing of SIM changes and port-out requests promotes customer choice and competition and prevents interruptions in access to wireless services that are vital to customers' everyday lives. Service interruptions can be particularly problematic when they hamper the ability of customers to access emergency services. We agree with the Competitive Carriers Association (CCA) that "enhanced requirements for SIM swap and port-out requests can implicate the customer experience and can intentionally or unintentionally serve as impediments to legitimate requests to change devices or change providers." We are wary of setting rigid requirements that would impose significant burdens on customers without substantially protecting against SIM swap and port-out fraud. We also recognize that prescribing particular security methods can place greater burdens on some customers because of their technical and financial means, digital literacy, accessibility needs, and other particularized circumstances. We anticipate that the approach we take today will provide meaningful protection to customers while preserving the competition and customer choice that SIM changes and number porting are meant to facilitate and avoiding undue burdens that hinder access to wireless services.

3. To that end, we set baseline rules, rather than prescriptive requirements, that establish a uniform framework across the mobile wireless industry for the types of policies and procedures providers must employ to combat SIM swap and port-out fraud. The record indicates that several wireless providers already rely, at least partly, on some of these policies and procedures. We are concerned, however, that a lack of consistency in how wireless providers apply these measures and a lack of uniformity in the use of these measures industry-wide leaves some customers vulnerable to SIM swap and port-out fraud. The rules we adopt ensure that all

wireless providers are taking consistent and comprehensive steps to address this fraud. For wireless providers that already employ the measures we require, in many cases our rules simply raise the bar by requiring them to adapt, refine, or consistently apply those existing practices. For wireless providers that do not, our new rules require them to implement new practices to meet the baseline standards. We anticipate that our approach will ensure that customers receive effective protection from SIM swap and port-out fraud regardless of the wireless telecommunications services they purchase or the wireless provider from whom they purchase them.

4. In setting baseline requirements, rather than prescriptive rules, our approach also gives wireless providers the flexibility to establish the specific fraud protection measures they use so that they can deliver the most advanced protections available. The record provides substantial evidence that to best combat SIM swap and port-out fraud, wireless providers need flexibility. In particular, we are persuaded that wireless providers need such flexibility so that they can adapt their security methods to keep pace with the evolving threat landscape. Verizon notes that "fraudsters are sophisticated and constantly look to circumvent any protections, no matter how robust." We also recognize that "[r]apid technological changes introduce new vulnerabilities that existing rules may be unequipped to address." We are therefore concerned by record evidence that a static set of prescriptive requirements may incentivize some wireless providers to rely exclusively on those security methods and discourage them from innovating and adopting new and improved practices to address evolving fraud techniques used by bad actors. We also share concerns that setting specific requirements could either provide a roadmap for bad actors seeking to commit fraud or lock in measures that quickly prove to be ineffective or obsolete. The aim of our action today is to better protect telecommunications customers from fraudulent schemes; in doing so, it is important that our rules, while functioning as baseline safeguards, do not serve as obstacles to adoption of better security practices. Indeed, the record asserts that establishing rules that provide flexibility will incentivize wireless providers to

develop and adopt new and improved methods to protect against SIM swap and port-out fraud and enable them to quickly adapt their security measures to respond to evolving techniques and technologies used by bad actors. Accordingly, we agree with AT&T that "[t]he best way to combat ever-evolving fraud tactics is to allow industry players the ability to adapt and respond to these changing threats in real-time," and we afford wireless providers this flexibility with the rules we adopt in this *Report and Order*.

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

6. We further anticipate that our flexible approach will enhance protections for customers without placing undue costs and burdens on wireless providers. We are cognizant that in some instances, strict prescriptive requirements to prevent SIM swap and port-out fraud could be technically and economically infeasible for wireless providers to implement, particularly for

smaller providers. Even in the instances when wireless providers do have the means to implement prescriptive requirements, those requirements could prove burdensome on providers if they become obsolete or ineffective and providers are compelled to maintain them alongside new and better practices they adopt to address the evolving threat landscape. By setting baseline requirements and giving wireless providers flexibility on how to meet them, we allow providers to adopt the most cost-effective and least burdensome solutions to achieve the level of security needed to protect customers against SIM swap and port-out fraud in a given circumstance. Additionally, because many of our rules build on existing mechanisms that many wireless providers already use, we expect that our new rules will further minimize the costs and burdens for those providers.

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

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

8. The record makes clear that because SIMs are only used to facilitate service for mobile wireless devices, SIM swap fraud is a practice that is exclusive to mobile wireless

services. Thus, we apply these new requirements to providers of commercial mobile radio service (CMRS), as defined in Section 20.3 of Title 47 of the Code of Federal Regulations, including resellers of CMRS. We apply these new requirements to all SIM changes that wireless providers perform. Further, we require wireless providers to implement these rules with respect to customers of both pre-paid and post-paid services, consistent with the protections afforded by Section 222. We see no reason why the protections should not apply to all customers of CMRS, including customers of resellers, particularly considering indications in the record that pre-paid customers are disproportionately impacted by fraud and that many customers impacted by such fraud are low-income customers who can ill afford such losses. Under this definition, our new rules apply to both facilities-based wireless providers as well as resellers of wireless services. Additionally, given that Section 332(c)(1)(A) of the Act requires that providers of commercial mobile service be treated as common carriers, 47 U.S.C. 332(c)(1)(A), our rules cover "any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment." We make clear, however, that the rules we adopt today do not require providers to collect more information about pre-paid customers than they otherwise do in the normal course of business, nor should they be interpreted to impose disparate burdens on pre-paid customers related to information collection or authentication.

1. Customer Authentication Requirements

9. We update our CPNI rules to protect customers from the risk of fraudulent SIM swaps by requiring wireless providers, prior to conducting a SIM change, to use secure methods to authenticate a customer that are reasonably designed to confirm a customer's identity, except to the extent otherwise required by the Safe Connections Act or the Commission's rules implementing that statute. We define "SIM," for purposes of these rules, as "a physical or virtual card associated with a device that stores unique information that can be identified to a specific mobile network." The record reflects significant support for strengthening authentication requirements for SIM change requests, and we find that the requirement we adopt

today most appropriately balances the need to increase protection for customers from these types of fraudulent schemes while providing wireless providers the flexibility the record shows they need to respond to new and emerging threats. We encourage wireless providers to use secure authentication methods that accommodate the needs of the broad spectrum of customers they may serve. We are persuaded by commenters that a general security authentication standard will afford customers the highest level of protection by allowing wireless providers to implement the authentication methods raised in the record, or develop new authentication methods, in ways that both account for advances in the technology and tactics used by bad actors and that work best for their customers and the particular services they offer. Additionally, we believe this flexibility alleviates record concerns about the limited information wireless providers may have to authenticate customers of pre-paid accounts.

10. The Safe Connections Act of 2022, Pub. L. No. 117-223, 136 Stat. 2280 (Safe Connections Act), which is codified at 47 U.S.C. 345, requires wireless providers to separate lines from a multi-line account upon request of a survivor of domestic violence and other related crimes and abuses. 47 U.S.C. 345(b)(1). In an Order adopted today implementing the Safe Connections Act, the Commission adopted rules to require covered providers to attempt to authenticate, using multiple authentication methods if necessary, that a survivor requesting a line separation is a user of a specific line or lines. Covered providers must use methods that are reasonably designed to confirm the survivor is actually a user of the specified line(s) on the account when the survivor is not the primary account holder or a designated user, and this authentication shall be sufficient for requesting a SIM change when made in connection with a line separation request. To the extent this requirement differs from other authentication requirements, including those in 47 CFR 64.2010, the line separation authentication requirements the Commission adopts to implement 47 U.S.C. 345 serve as an exception to those other requirements. We also make clear that the Safe Connections Act-related exceptions to our new SIM change and LNP rules for any SIM change or port-out requests made in connection with a

legitimate line separation request apply regardless of whether a line separation request is technically or operationally infeasible.

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

12. Because we impose a general requirement for secure and reasonably designed customer authentication, both permitting and obligating wireless providers to design effective methods to authenticate customers, we decline to enumerate the four specific authentication methods the Commission specified in the *SIM Swap and Port-Out Fraud Notice* as those that would meet the standard of secure authentication methods. Those four methods were: (i) the use of a pre-established password; (ii) a one-time passcode sent via text message to the account phone number or a pre-registered backup number; (iii) a one-time passcode sent via e-mail to the e-mail address associated with the account; or (iv) a passcode sent using a voice call to the account phone number or a preregistered back-up telephone number. No commenters supported our imposing these as the exclusive forms of authentication. We are convinced by the record that specifying approved authentication methods may incentivize wireless providers to rely exclusively on those methods or discourage them from adopting new methods to address evolving techniques used by bad actors. Further, some commenters assert that requiring specific authentication methods would be burdensome for wireless providers. Additionally, the record

reflects that setting specific authentication methods could provide a roadmap for bad actors seeking to commit fraud. The record also highlights potential vulnerabilities of the four authentication methods we proposed, which counsels against us codifying these as secure methods of authentication in perpetuity. For these reasons, we conclude it is most appropriate to allow wireless providers to analyze and implement the most effective and secure methods of authenticating customers requesting a SIM change. For similar reasons, we also decline to require carriers to comply with the National Institute of Standards and Technology (NIST) Digital Identity Guidelines or other standards proposed in the record.

13. We nevertheless place boundaries on the use of certain information for customer authentication for SIM change requests in light of evidence in the record of their particular vulnerability. Namely, we conclude, consistent with our proposal, that methods of authentication that use readily available biographical information, account information, recent payment information, and call detail information do not constitute secure methods of authentication. We decline to establish an exigent circumstances exception on the use of this information for authentication for when customers are traveling and may not have access to or remember a PIN, as CTIA asked us to consider. We believe that such an exception would establish a significant loophole for fraudulent activity and note that in these circumstances, customers can use alternative methods of authentication, such as email. We strongly encourage providers to work with customers to develop backup authentication practices for use in these types of scenarios. We seek comment in the *Further Notice* on whether we should harmonize our CPNI rules with the SIM change rules we adopt today, and we therefore take no action, at this time, to amend our existing rules to prohibit providers from relying on recent payment and call detail information to authenticate customers for online, telephone, or in-person access to CPNI.

14. We decline to restrict the use of SMS-based customer authentication for SIM change requests, but we strongly encourage wireless providers to use this mechanism only when paired with other secure methods of authentication, i.e., as part of multi-factor authentication

(MFA). In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on the potential security vulnerabilities of SMS-based authentication. The record clearly expresses concern about the security risks of SMS-based authentication when used by third parties, such as financial institutions, largely because this authentication method becomes vulnerable following fraudulent SIM swaps. The record evidence is less clear that SMS-based authentication is an insecure mechanism in every instance it is used, such as to authenticate the identity of individuals requesting a SIM change, particularly when sent over a provider's own network, rather than the Public Switched Telephone Network (PSTN). We also acknowledge that, in some instances, it may be the most practical means a provider can authenticate a customer, particularly when considering the needs of a particular customer. We anticipate that the approach we take here strikes the right balance between protecting customers against SIM swap fraud while preserving the relative ease with which customers can obtain legitimate SIM changes. We emphasize, however, that our rules create an ongoing obligation that wireless providers ensure the authentication methods they use are secure. Accordingly, permitting wireless providers to use SMS-based authentication does not create a safe harbor for use of this authentication method. We will continue to monitor the use of SMS-based authentication and may later revisit our decision to permit its continued use.

2. Response to Failed Authentication Attempts

15. We require wireless providers to develop, maintain, and implement procedures for responding to failed authentication attempts in connection with a SIM change request that are reasonably designed to prevent unauthorized access to a customer's account, which, among other things, take into consideration the needs of survivors pursuant to the Safe Connections Act and our implementing rules. We are bolstered by the Princeton University researchers who found evidence that wireless providers' procedures to respond to suspicious authentication attempts may be inadequate or nonexistent. Specifically, they determined that some wireless providers only required callers to successfully respond to one authentication challenge to obtain a SIM

change even if the caller had failed numerous previous authentication attempts. While the *SIM Swap and Port-Out Fraud Notice* raised these issues, no commenters offered evidence to counter the researchers' findings. Without procedures in place to respond to failed authentication attempts, bad actors can seek to circumvent wireless provider authentication mechanisms to fraudulently obtain a SIM change. We anticipate that requiring wireless providers to establish procedures to respond to failed authentication attempts that are reasonably designed to prevent unauthorized access to a customer's account will impede these fraud attempts. We conclude that whatever burdens may be associated with this requirement are outweighed by the Commission's interest in protecting customers against fraudulent activity.

16. At the same time, we are persuaded by T-Mobile's argument that wireless providers need flexibility with respect to failed authentication attempts because it is common for customers to lose or forget their authentication data, leading to multiple failed attempts. As such, we decline at this time to adopt prescriptive requirements for how wireless providers must respond to failed authentication attempts in connection with a SIM change request. We find that anchoring this rule in a reasonableness standard will give wireless providers flexibility to design procedures to handle failed authentication attempts that protect against fraudulent activity while preventing unnecessary burdens on legitimate customer activity. We decline, however, to adopt CTIA's suggestion to require the development and implementation of such procedures only where a wireless provider has reason to believe multiple authentication attempts are fraudulent; CTIA does not address how such determinations would be made absent the very procedures we require.

17. We decline, at this time, to adopt a requirement that wireless providers immediately notify customers in the event of multiple failed authentication attempts in connection with SIM change requests. Industry commenters assert that "in many cases, providers will not be able to discern whether a failed authentication attempt is 'in connection with a SIM change request' or some other type of transaction involving account access for which

authentication is needed and fails," and that "a carrier does not typically know why a customer authenticates until after the customer has successfully authenticated." Further, commenters raise concerns that tracking such attempts across platforms could be technically challenging, though we are not persuaded that doing so is technically infeasible. For example, CTIA's proposal that carriers should only be required to develop and implement procedures for responding to multiple failed authentication attempts "where a carrier has reason to believe such attempts are fraudulent" implies that wireless carriers can and do track multiple authentication attempts, or, at a minimum, are technically capable of doing so. Given these concerns, we find that requiring wireless providers to notify customers immediately of multiple failed authentication attempts associated with a SIM change request is not appropriate at this time. However, we seek comment in the *Further Notice* below whether we should require wireless providers, or all telecommunications carriers, to notify customers immediately of all failed authentication attempts to help protect customers from account fraud, as well as how wireless providers could implement a customer notice requirement for multiple failed authentication attempts.

18. We also decline to require that wireless providers delay SIM changes for 24 hours in the event of failed authentication attempts while notifying customers via text message and/or email regarding the failed authentication attempts. The record reflects that strict requirements involving 24-hour delays or account locks could be overly burdensome for customers that are engaged in legitimate SIM changes. We also anticipate that the requirement to develop, maintain, and implement procedures for responding to failed authentication attempts in connection with a SIM change request that are reasonably designed to prevent unauthorized access to a customer's account, coupled with the requirement we adopt below that wireless providers immediately notify customers upon receiving a SIM change request, will be sufficient to empower customers to quickly address unauthorized SIM change attempts.

3. Customer Notification of SIM Change Requests

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

20. We therefore disagree with AT&T's contention that notification of all SIM change requests is unnecessary because "AT&T employs various tools to assess the risk level of a particular postpaid SIM change or port-out request and very often can determine at the outset that a request is legitimate." The notification requirement we adopt today will provide a uniform safety measure for all requests across the mobile wireless industry, which we anticipate will reduce the instances and mitigate the harms of SIM swap fraud. We also disagree with AT&T's assertion that customers will become so inundated with SIM change notifications that they will "eventually become numb or immune to them or tire of and consciously choose to ignore them, thus undermining all value they might otherwise have when the threat of fraud is real." Nothing in the record, or our understanding of the SIM change process, supports the notion that

customers request SIM changes at such a rate that, upon the adoption of this rule, wireless providers will be forced to inundate their customers with the required notifications. For the same reasons, we decline AT&T's request that we modify the mandatory SIM change request notification requirement "either to 1) standalone SIM transactions—i.e., SIM swaps that do not include a device change or upgrade—based on the lower propensity for fraud in transactions involving new devices, or 2) SIM transactions that a carrier identifies as having a high propensity for fraud," on the basis such notifications could cause customer confusion, concern, and fatigue, and could increase costs for carriers because such notifications increase customer calls.

21. Also contrary to AT&T's assertions, we do not anticipate that the notification requirement we adopt today will be overly burdensome for wireless providers to implement. As an initial matter, wireless providers should already have processes in place to immediately notify customers of certain account changes involving CPNI in accordance with our existing rules, so they should be able to build on these processes to provide immediate notification regarding SIM change requests. The record also demonstrates that some wireless providers already notify customers of SIM change requests in most instances and therefore will only need to update their processes to notify customers in all cases. Additionally, as discussed below, we give wireless providers flexibility on how to provide the required notifications, which we expect further minimizes any potential burdens associated with our new rule. For the same reasons, we decline CTIA's request "to let providers determine whether a notice is warranted or effective in the first instance" on the basis that such flexibility is needed to deal with instances, for example, when a phone is lost or stolen and expedient forms of notification may not be available. We do not prohibit wireless providers from processing SIM change requests after the notification is sent, and because bad actors may attempt to commit SIM swap fraud by claiming that a device is lost or stolen, that is precisely the type of situation when we want to ensure customers are provided a notification of a SIM change request. In any event, we find that the benefits of our notification requirement outweigh the potential burdens.

22. We permit wireless providers to determine the method of providing notifications regarding SIM change requests involving a customer's account, but specify that the notifications must be reasonably designed to reach the customer associated with the account, and sent in accordance with customer preferences, if indicated. For example, this would include delivering a notification in the language of the customer's choosing, if the wireless provider permits communications preferences in other languages and the customer has previously indicated such choice. Although some commenters suggest that we should specify the means by which a wireless provider should deliver SIM change request notifications, we agree with industry commenters that providers need flexibility to determine the most appropriate method to notify their customers of a pending SIM change request, so that providers can account for "the complexities of notifications in various contexts," as well as the technical capabilities, accessibility needs, or broadband access of individual customers. For example, when a customer is requesting a SIM change because the customer's phone is lost or stolen, our flexible approach enables wireless providers to use methods of notification that are most likely to reach the customer under those circumstances, such as an email or a text or call to a pre-determined back-up phone number. We also aim to enable wireless providers to send notifications in accordance with customer preferences, needs, and established expectations. As such, we permit wireless providers to use existing methods of notification that are reasonably designed to reach the customer associated with the account, and we encourage them to adopt new notification methods as they are developed to stay responsive to evolving fraud schemes. Such methods include, but are not limited to, live or automated telephone calls, text messages, emails, or push notification through wireless provider software applications. We acknowledge that our new rule differs from our existing rule that providers deliver notification of other account changes involving CPNI, which specifies that those notifications may be delivered through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record. We find that departing from the existing rule's approach is appropriate given the depth of harm that can

occur from SIM swap fraud, the need for wireless providers to be able to choose the most effective method of quickly alerting customers so that customers can take action to mitigate harm, and the importance of providers adopting new forms of notification.

23. Our rule also gives carriers the flexibility to design a notification process that accommodates scenarios beyond individual customers, such as a business customer seeking bulk SIM changes to upgrade their equipment. We note that nothing in the customer safeguard rules we adopt today is inconsistent with or intended to supersede the Commission's existing business customer exemption, which permits telecommunications carriers to "bind themselves contractually to authentications 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."

24. We also decline to prescribe particular content or wording of SIM change notifications, recognizing that wireless providers are in the best position to determine what will most effectively notify customers of SIM change requests and potential fraud and will need to tailor notifications to customers' service plans and circumstances. Nevertheless, consistent with the record and our CPNI rules, we specify that such notifications must use clear and concise language that provides sufficient information to effectively inform a customer that a SIM change request involving the customer's SIM was made. We observe that our rule does not prohibit wireless providers from using different content and wording for notifications depending on a provider's risk assessment of a given SIM change request, so long as the notification uses clear and concise language and is reasonably designed to reach the actual customer.

25. We further decline to require a delay for customer verification or acknowledgement in connection with notifications prior to completing a SIM change request. In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on whether we should require a 24-hour delay (or other period of time) before a wireless provider effectuates a SIM change while notifying the customer via text message, email, the provider's app, or push notification,

and requesting verification of the request. This approach received minimal support in the record, and we are convinced by other record evidence that the burdens of delay and verification requirements outweigh the benefits, particularly given how regularly customers seek legitimate SIM changes. For instance, CTIA explains that a blanket delay would "make it exceedingly difficult for a consumer to obtain a new phone and continued service when a device breaks or is lost, representing a full day where that consumer could not rely on their wireless service for . . . 'keeping in touch with friends through voice calls and text messages' [and] placing life-saving public safety calls." AT&T and T-Mobile echoed these concerns. We also anticipate that the authentication, notification, and remediation requirements we adopt today will sufficiently mitigate fraudulent SIM change requests without the need for a burdensome delay and verification process. While we do not require wireless providers to implement a delay and verification process, we permit them to do so in instances when they determine these measures are necessary to protect against fraud, but stress that this process should not be used to delay legitimate SIM change requests.

4. Account Locks for SIM Changes

26. We require wireless providers to offer all customers, at no cost, the option to lock or freeze their account to stop SIM changes. We anticipate that this requirement will provide customers with more consistent and meaningful protection against SIM swap fraud, and this expectation is supported by the record, which reflects that account locks can be powerful tools against SIM swap fraud, particularly for customers that are at high-risk of being a target of the practice. We adopt our proposal that account locks must be offered to all customers at no cost because we find that a customer's financial means should not dictate their access to this enhanced security measure, particularly since customers with lesser financial means may suffer the greatest consequences of SIM swap fraud. This requirement is consistent with other Commission rules governing preferred carrier freezes for Local Exchange Carriers, *see* 47 CFR 64.1190, as well as the requirements adopted for port-out locks. To simplify the ability for

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

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

28. Consistent with this flexible approach, we permit wireless providers to proactively initiate a SIM swap lock on a customer's account when a provider believes the customer may be at high risk of fraud. We are persuaded by T-Mobile's assertion that such capability is valuable because wireless providers are sometimes positioned to know when a customer is at high risk of SIM swap fraud and that this tool allows them to help customers secure their accounts. However, we require that wireless providers promptly provide clear notification to the customer that the lock has been activated with instructions on how the

customer can deactivate the account lock if the customer chooses, and to promptly comply with the customer's legitimate request to deactivate the account lock. We also caution wireless providers that any proactive initiation of a SIM change lock must be limited in duration and extend only so long as the high risk of fraud is evident to the provider. In establishing this limitation, we intend to prohibit wireless provider abuse of SIM change locks to avoid, among other outcomes, preventing the customer from terminating service with the provider or moving to another competing provider.

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

30. We also disagree with AT&T that an account lock option "should remain a tool that carriers can choose, but are not required, to offer." AT&T acknowledges that "[a]ccount locks can be an effective tool to increase the security of customer accounts on occasion," but it suggests that because "they are not needed to manage the risk of fraud in every case and for every customer," wireless providers should not be required to offer them to all customers. While AT&T's approach would leave the choice of whether an account lock is necessary exclusively in the hands of wireless providers, we conclude this choice should be placed principally in the hands of the customer, the party that is potentially at risk for SIM swap fraud, and therefore we require providers to offer the option to all customers. Likewise, AT&T's concern that "an account lock can be a source of friction" even for a postpaid customer when the "customer forgets having placed the freeze on the account or dislikes the efforts needed to unfreeze the

account" is not, we conclude, a valid basis for declining to require that wireless providers offer SIM change locks. The benefits of this account security measure outweigh any potential friction, and we expect that wireless providers can take steps to mitigate any such friction if they choose, such as by providing customers with periodic reminders that they have activated the account lock and on how they can deactivate the lock. Because of the authentication challenges for pre-paid customers and the potential friction for customers who may not want SIM changes to be more difficult, we decline to require account locks be activated by default, on an opt-out basis, as BPI/BITS suggests. We are also unconvinced by comments claiming that SIM change locks may be of limited value to customers. This requirement empowers high-risk and security-minded customers to enable additional protections beyond the enhanced authentication requirements and other security measures we adopt today, and it need not be activated by a large percentage of customers for it to be valuable.

5. Tracking Effectiveness of SIM Change Protection Measures

31. We require wireless providers to establish processes to reasonably track and maintain information regarding SIM change requests and their authentication measures, and to retain that information for a minimum of three years. We agree with the Princeton University researchers that a tracking requirement will equip wireless providers "to measure the effectiveness of their customer authentication and account protection measures," and find that they would not otherwise be able to do so effectively without collecting such information. Consistent with recommendations in the record by the Princeton University researchers, we specifically require wireless providers to collect and maintain the following information regarding SIM change requests and authentication measures: the total number of SIM change requests, the number of successful SIM changes requests, the number of failed SIM change requests, the number of successful fraudulent SIM change requests, the average time to remediate a fraudulent SIM change, the total number of complaints received regarding fraudulent SIM changes, the authentication measures the wireless provider has implemented, and when

those authentication measures change. We also strongly encourage them to collect and retain any additional information that will help them measure the effectiveness of their customer authentication and account protection measures. We find that the three-year retention period is appropriate because it allows providers to track the effectiveness of their measures over time and ensures the information is available for a sufficient time should the Commission request it for review. The requirement that wireless providers collect and maintain information regarding when authentication measures change simply means that providers must track the introduction and removal of such measures, and not updates or refinements to existing measures.

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

33. We agree with CTIA that the data tracking and retention requirements should only be prospective in nature, and as such, we make clear that our rule does not obligate wireless providers to research and collect historic data. We conclude that including historic data in the data tracking requirements we adopt would be burdensome, or even impossible, for small wireless providers and those who do not already track this information. We decline to adopt reporting and audit requirements in conjunction with our data tracking requirement, but we do require wireless providers to make the information they collect available to the Commission upon request. Because the information we require wireless providers to collect does not include personally identifiable information (PII) or CPNI, wireless providers will not be required to

provide PII or CPNI in response to Commission requests for this information, but the Enforcement Bureau may request PII or CPNI in the course of a specific investigation. Although regular reporting and audit requirements can improve wireless provider incentives and accountability, we do not find that such measures are necessary at this time in light of the other measures we adopt today and providers' ongoing commitment to be vigilant in combating fraud. We maintain the ability to obtain collected information from wireless providers as needed, not only as a potential tool to evaluate whether providers are implementing sufficient measures to address SIM swap fraud, but also to evaluate whether the specific requirements we adopt today continue to be effective or in need of updates to address the evolution of fraud techniques. Consequently, we find that there are insufficient benefits of a regular reporting requirement to outweigh the potential costs.

6. Safeguards on Employee Access to CPNI

34. We require wireless providers to establish safeguards and processes so that employees who receive inbound customer communications are unable to access CPNI in the course of that customer interaction until after a customer has been properly authenticated. We find, based on the record before us, that requiring wireless providers to limit access to CPNI by employees who receive inbound customer communications until after the customer has been properly authenticated will help to minimize the incidences of SIM swap fraud by preventing customer service representatives from inadvertently or intentionally assisting bad actors in fraudulent schemes. We are persuaded that, even with the customer service representative training requirements we adopt today, allowing employees who receive inbound customer communications to access CPNI prior to proper authentication of the customer is unnecessary and possibly "invites adversaries to exploit sympathetic, inattentive, or malicious customer service representatives for account access." While we anticipate that employees will comply with training requirements in good faith, "[t]here should be no opportunity for a representative to give a hint or a free pass" that will help bad actors commit fraud. We therefore conclude that

requiring wireless providers to establish safeguards and processes so that employees who receive inbound customer communications are unable to access CPNI in the course of that customer interaction until after the customer has been properly authenticated—"a straightforward fix" and standard data security best practice—will provide meaningful protection in helping to combat SIM swap fraud. We find that the benefits of this requirement outweigh any potential costs, and that any such costs will be mitigated by allowing telecommunications carriers flexibility to determine the particular safeguards and processes that will prevent employees who receive inbound customer communications from accessing CPNI in the course of that customer interaction until after a customer has been properly authenticated. Below, we seek comment on whether to require all telecommunications carriers to limit access to CPNI by employees who receive inbound customer communications until after the customer has been properly authenticated to minimize customer account fraud.

35. We decline to adopt other suggested employee safeguards that are overly prescriptive and for which the costs outweigh the benefits. In the *SIM Swap and Port-Out Fraud Notice* we sought comment on other ways to avoid employee malfeasance, such as requiring two employees to sign off on every SIM change. Although we anticipate that two-employee sign off could be an effective account protection mechanism and encourage wireless providers to use this procedure when appropriate, we are persuaded by AT&T's argument that requiring this procedure for every SIM change would be a significant burden on legitimate SIM change requests given the uncertainty regarding whether it would prevent SIM swap fraud in most instances, and therefore decline to adopt it. We also reject several other requirements proposed in the record concerning customer service representatives who perform SIM changes. Specifically, a mandate that employees who perform SIM swaps be subject to enhanced background checks may be financially and practically infeasible for large and small wireless providers alike, and could create an incentive for providers to reduce the number of employees capable of performing SIM changes, which would slow the processing of legitimate changes.

Requiring employees to swipe a company badge when entering secure facilities is a good practice that we encourage wireless providers to adopt, but the record does not address how this requirement would serve to prevent SIM swap fraud. The proposal to require employees to sign a restrictive confidentiality agreement is faulty for the same reason. Moreover, a proposed restriction on use of performance incentives is overly broad, could stifle competition, and might prevent customers from accessing special offers. Finally, we decline to adopt a proposal that wireless providers "be required to have heightened SIM swap customer care during [weekends and evenings]." We find that providers are best positioned to implement procedures tailored to the level of risk at any given time and should have the flexibility to adjust their practices to address the evolving nature of fraudulent activity.

7. Telecommunications Carriers' Duty to Protect CPNI

36. While the record shows that some wireless providers have implemented CPNI security practices beyond those required by current rules, SIM swap fraud persists. We are also concerned that some wireless providers may view the protection measures we adopt today as sufficient, rather than baseline, protections against SIM swap fraud. To ensure that wireless providers adapt their security practices on an ongoing basis to address evolving techniques used by bad actors to commit SIM swap fraud, we take this opportunity to remind all telecommunications carriers of their statutory duty to "protect the confidentiality of proprietary information of, and relating to . . . customers," and their continuing preexisting legal obligation to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." Consistent with the Commission's approach in the *2007 CPNI Order*, we conclude that these existing legal obligations necessarily obligate telecommunications carriers to proactively and regularly review and monitor their policies and procedures to ensure that they continue to be effective at addressing evolving fraud techniques against customer accounts and services—including SIM swap and port-out fraud—and to conduct analyses of fraud incidents to determine how the fraud occurred and implement measures to prevent such tactics from being

successful again in the future.

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

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

1. Customer Authentication Requirements

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

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

40. As in the SIM change context, we are persuaded by commenters that a general security authentication standard will best allow wireless providers the flexibility to respond to advances in the technology and tactics used by bad actors, providing the greatest protection for customers, and enabling providers to implement authentication methods in ways that work best for the particular services they offer. The record reflects that the benefits of allowing wireless providers to determine the best method for authenticating customers outweigh speculative concerns that absent standardized authentication methods, nationwide providers could arbitrarily determine which authentication methods or controls are sufficient before effectuating ports. We note also that under the Act and our existing rules, all carriers are required to complete legitimate ports, and that our new customer authentication requirements do not give carriers the authority to make determinations about the sufficiency of another carrier's authentication methods—that responsibility will belong to the Commission, and we will address any concerns regarding the adequacy of authentication methods, as well as inappropriate port denials, as needed. We also agree with CCA that our approach will better serve small wireless providers by permitting them to "use technologies that are reasonably available and have choice in the approach to take in

authenticating their customers." Additionally, as we concluded with regard to authentication for SIM changes, this flexible approach should resolve concerns about authenticating customers of pre-paid accounts.

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

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

2. Customer Notification of Port-Out Requests

43. We also revise our numbering rules to require wireless providers to provide

immediate notification to their customers whenever a port-out request is made, sent in accordance with customer preferences, if indicated, and specify that the notification must be sent before a provider effectuates a port, except to the extent otherwise required by the Safe Connections Act of 2022 (47 U.S.C. 345) or the Commission's rules implementing that Act. For example, this would include delivering a notification in the language of the customer's choosing, if the wireless provider permits communications preferences in other languages and the customer has previously indicated such choice. We require that wireless providers notify their customers "immediately" of a porting request to not only ensure that porting requests are processed efficiently, but also help alert customers quickly to potential fraud to allow them to mitigate damages and inconvenience resulting from fraudulent or inadvertent port-outs. The notification requirement will provide a uniform safety measure for all port-out requests across the mobile wireless industry, which we anticipate will reduce the instances of port-out fraud. For the same reasons we raised in the SIM change context, we decline to impose a blanket yes/no verification requirement for authentication attempts.

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

developed to stay responsive to evolving fraud schemes.

45. On balance, we find that benefits accrued from early warning to customers of potential fraudulent account activity outweigh any potential burdens imposed on wireless providers by this notification requirement. First, we find that customer notification of port-out requests is unlikely to prevent or unreasonably delay customer porting requests, as we require "immediate" notification and do not require a delay or customer verification or acknowledgement of that notification before continuing the porting-out process. Second, because wireless providers are already familiar with notifying customers regarding changes to their accounts, and in many cases likely already notify customers of port-out requests, we anticipate that wireless providers will face low burdens in implementing today's customer notification requirement for port-out requests. We also expect that these existing notification systems can be leveraged to help minimize any potential costs associated with notifying customers of port-out requests. Third, we disagree with AT&T's assertion that customer notification of port-out requests will result in notice fatigue, undermining its efficacy. Nothing in the record supports the notion that customers request port-outs at such a rate that, upon the adoption of this rule, wireless providers will be forced to inundate their customers with the required notifications. For the same reasons, we decline CTIA's request that customer notification of port-out requests be "limited to situations where the carrier determines that there is an increased risk of fraud" on the basis that the notification requirements "threaten to cause customer confusion, concern, and fatigue," and could increase costs for carriers because such notifications increase customer calls. As such, we conclude that the significant benefits of alerting customers to potential fraudulent account activity outweighs any speculative negative impacts on wireless providers or customers.

3. Account Locks for Port-Outs

46. For the same reasons explained above with respect to SIM change requests, we require wireless providers to offer their customers, at no cost, the ability to lock or freeze their

accounts to stop port-outs. We anticipate that this requirement will provide customers with more consistent and meaningful protection against fraudulent port-outs. The record reflects that account locks can be powerful tools against fraudulent port-outs, particularly for customers that are at high-risk of being a target of the practice. As in the SIM swap context, we conclude that it should be offered to customers of both pre-paid and post-paid services, and that this requirement is feasible for both categories of customers despite assertions to the contrary. Because the account lock is an optional security measure for customers, carriers can, if necessary, require customers to provide information to use for authentication purposes to activate and deactivate the account lock.

47. Like the other rules we adopt today, we give wireless providers flexibility on how to comply with the measure. In particular, the record does not evince a need for us to prescribe a method or methods for customers to unlock or unfreeze their accounts or impose a waiting period before an unlocked account can be transferred, and as such, we decline to do so at this time. Although we do not prescribe the exact form of the account lock mechanism wireless providers must adopt, the process to activate and deactivate an account lock must not be unduly burdensome for customers such that it effectively inhibits them from implementing their choice. We stress that when activated, wireless providers must not fulfill port-out requests until the customer deactivates the lock, except to the extent otherwise required by the Safe Connections Act or the Commission's rules implementing that statute. We decline CTIA's request that the Commission find that mandatory port-out PINs satisfy this requirement. We discuss the benefits and drawbacks of port-out PINs as a method of *customer authentication*, above. We disagree that a mandatory port-out PIN has the same effect as an optional account lock; while the two protections serve complementary functions, one is focused on customer authentication for a specific one-time request, and the other functions as a customer directed general account security feature.

48. Consistent with this flexible approach, and as we did with the SIM change rules,

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

49. As with account locks for SIM changes, given that several wireless providers already voluntarily offer account locks to all their customers, and coupled with the flexible approach we adopt, we are unpersuaded by AT&T's claim that implementing account lock offerings will be unduly costly and time-consuming for wireless providers. To the extent there are costs associated with the requirement, we find that they are outweighed by the benefits.

4. Wireless Port Validation Fields

50. After review of the record, we decline to codify the wireless port validation fields. We also decline to require wireless providers to implement a customer-initiated passcode field for all wireless-to-wireless number porting requests. Currently, the mobile wireless industry uses four data fields of customer-provided information to validate a wireless-to-wireless porting request: telephone number, account number, five-digit ZIP code, and passcode (if applicable). In the *SIM Swap and Port-Out Fraud Notice*, we sought comment on whether we should "codify the types of information carriers must use to validate simple wireless-to-wireless port requests." While some commenters did not oppose codification of some of the customer-provided wireless data fields, they preferred that the Commission continue to give wireless providers the flexibility to adjust to business and customer needs. We are persuaded by the record that separate

codification of the customer-provided data fields for validation of wireless-to-wireless ports is not necessary at this time, as we have been provided no evidence that wireless providers are not complying with the validation obligations imposed in the *Four Fields Declaratory Ruling*. As such, we decline to separately codify the customer-provided wireless-to-wireless port validation fields at this time.

C. Additional Consumer Protection Measures

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

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

providers have already developed content to educate customers about some account protection measures.

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

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

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

similarly conclude that the employee training requirement we adopt today is necessary to ensure customer service representatives are prepared to identify, prevent, and remediate fraudulent SIM change and port-out activity.

56. In applying this requirement, we give wireless providers flexibility on designing their training programs. But we do require that all employees who may communicate with customers regarding SIM changes and number ports must be trained on how to recognize potentially fraudulent requests, how to recognize when a customer may be the victim of fraud, and how to direct potential victims and individuals making potentially fraudulent requests to employees specifically trained to handle such incidents. Given that (1) some wireless providers already train employees on how to address fraud, (2) our new training requirement builds upon our existing CPNI training rule, and (3) we are providing wireless providers with flexibility on how to design their training programs, we do not anticipate that imposing this training requirement will be overly costly for wireless providers.

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

58. Our requirement that wireless providers maintain a clearly disclosed, transparent, and easy-to-use process for customers to report SIM swap and port-out fraud rests on our concern that customers currently struggle to report SIM swap and port-out fraud to their wireless

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

59. We require wireless providers to establish procedures to promptly investigate and take reasonable steps within their control to remediate SIM swap and port-out fraud because the record demonstrates that even when victims of SIM swap and port-out fraud are successful in reporting such fraud to their providers, they have difficulty obtaining assistance from their providers to remediate the fraud. This is consequential because "[i]dentity theft, including SIM swap fraud, can cause intense anxiety for victims and must be addressed in a timely manner to prevent financial losses and exposure of personal information." Thus, we conclude that "it should be easy for a customer to get access to appropriate carrier resources that can help mitigate the significant harms caused by SIM swap or port-out fraud." Although we do not specify the procedures that wireless providers must adopt, we agree with commenters that investigations must be instigated and resolved expeditiously.

60. To ensure victims of SIM swap and port-out fraud have additional means to resolve other consequences that result from SIM swap and port-out fraud, we require wireless providers to give customers documentation regarding such fraud on their accounts, upon request. In the *SIM Swap and Port-Out Fraud Notice*, we recognized that "customers sometimes need documentation of the fraud incident to provide to law enforcement, financial institutions, or others to resolve financial fraud or other harms of the incident" and acknowledged that "[a] SIM

swap or port-out fraud victim may have difficulty obtaining such documentation from the carrier because the carrier may not have processes in place to produce such documentation." Requiring wireless providers to give fraud victims supporting documentation will enable those victims to seek remedies from other institutions for additional fraud that bad actors achieve using a victim's SIM or phone number. We do not specify the form that such documentation must take or exactly what information it must contain, but it should be reasonably designed to permit customers to demonstrate to other entities that they were victims of SIM swap or port-out fraud and that bad actors may have used access to a victim's telecommunications services to carry out additional fraud. Such documentation must address the customer's interest in protecting his or her account(s) or identity but may be tailored not to include other proprietary, confidential, or law-enforcement-related information regarding the SIM swap or port-out fraud or the account. Additionally, because of the potential harms that can flow from SIM swap and port-out fraud, we also require wireless providers to provide this documentation promptly.

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

62. To maintain the flexibility we believe will be required for wireless providers to adequately tailor and adapt their practices to address SIM swap and port-out fraud, we decline to impose prescriptive measures raised in the *SIM Swap and Port-Out Fraud Notice* and the record. Specifically, although we encourage wireless providers to establish a dedicated hotline for customers to report SIM swap and port-out fraud and respond within 24 hours of a customer

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

63. *Working Group.* While we recognize that the harmful effects of SIM swap and port-out fraud may extend beyond the control of wireless providers and that the incentives to engage in such fraud implicate the security practices of other industries, we decline at this time to direct or rely on standard-setting bodies, industry organizations, or consumer groups to evaluate SIM swap and port-out fraud "to augment our understanding and present possible solutions." Instead, we find it most appropriate to focus on solutions within the scope of the Commission's authority that we anticipate will mitigate the harmful consequences of this fraud. Additionally, to the extent that commenters advocated that we direct this issue to a working group before taking action, we disagree with that approach and find that doing so would only delay solutions that we expect will benefit customers now. Although we decline to rely on a working group, we also do not foreclose wireless providers from forming or entering into cross-sector, multi-stakeholder efforts, independent of Commission direction, to seek broader solutions to the harms that may ultimately result from SIM swap and port-out fraud.

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

65. NCLC and EPIC argue that the Commission should "[r]equire carriers to offer a redress program that . . . provides full coverage of losses to customers who have been the victims of a fraudulent SIM swap or port-out fraud," which they say would "[p]rovide strong financial incentives to providers to stop SIM swapping and port-out fraud." We agree with CTIA, however, that telecommunications carriers are "but one link in the chain of consumer and business protection from account takeover fraud," and therefore that the responsibility for financial harms that a bad actor may be able to perpetuate following such fraud is borne by several parties, including, significantly, the bad actor. Imposing such liability on wireless providers would be inequitable and would reduce the incentives for e-mail and social media providers, financial institutions, healthcare providers, retail websites, and other entities that rely

on cell phone-based identity authentication to improve their security practices, as well as reduce the incentive for customers to act responsibly. We note, however, that compliance with our rules is not a safe harbor for wireless providers; customers will still be able to pursue any existing remedies available by law.

66. Similarly, we decline to specify, as NCLC and EPIC request, that wireless providers are "fully responsible for any abuse committed by its employees, whether the employees acted either intentionally or negligently," although we make clear that this statement does not absolve wireless providers of any liability for employee actions that already exists. We anticipate that the requirements we adopt today—including employee training regarding SIM swap and port-out fraud and restrictions on the ability of employees to access CPNI prior to authentication—will ensure that wireless providers implement adequate procedures to prevent employees from perpetuating SIM swap and port-out fraud.

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

D. Implementation Timeframe

68. We require wireless providers to comply with the requirements we adopt today six months after the effective date of the *Report and Order* or, for those requirements subject to review by the Office of Management and Budget (OMB), upon completion of that review, whichever is later. We conclude that providing six months to achieve compliance with rules that are not subject to OMB review accounts for the urgency of safeguarding customers from these fraudulent schemes, and will allow wireless providers to coordinate any updates needed to their systems and processes to comply with the Safe Connections Act and the rules we adopt to implement that statute. SIM swap and port-out fraud can result in substantial harm to the customer, including loss of service on their devices. Fraudulent SIM swaps and port-outs allow bad actors to perpetrate greater fraud by giving them the means to complete text and voice authentications to access the victim's other accounts, and as such, we find that an aggressive implementation timeframe is appropriate to provide these important consumer protections without substantial delay. We agree with some commenters that while many wireless providers can immediately implement the revisions to our CPNI and number porting rules, other providers may require this additional time. Some wireless providers already employ authentication and notification measures to process SIM change and port-out requests, offer account change locks, provide notice to customers about available fraud protection measures, and train employees on how to address SIM swap and port-out fraud, and may simply need to refine those practices to align with our rules. Other providers, particularly smaller providers, may need the additional time to upgrade their systems, implement modifications to their policies and procedures, and conduct new customer service representative training. We conclude that providing six months after the effective date of the *Report and Order* to implement these revisions to our CPNI and number porting rules strikes the right balance between time for wireless providers to implement these changes and accounting for the urgency of safeguarding customers from these fraudulent schemes. We also find that this implementation timeframe is consistent with other proceedings

and regulatory frameworks adopted by the Commission where consumer protection and numbering requirements were at issue. While we acknowledge industry's concerns that implementing these new rules will be a multistep process for many providers, providers themselves acknowledge the necessity of implementing today's revisions to our CPNI and LNP rules concurrently with our rules implementing the Safe Connections Act, given how both frameworks address many of the same actions (e.g., account locks, customer notifications, customer authentication). And as we explain in the *Safe Connections Order*, "permitting a more extended compliance timeframe for implementing the line separation provisions, as advocated for by industry commenters, would be inconsistent with the urgency Congress demonstrated with the underlying statutory obligation as well as with the critical wireless communications needs of survivors well-documented in the record." For all of these reasons, we require wireless providers to implement the rules we adopt today six months after the effective date of this *Report and Order*, subject to review by OMB.

E. Legal Authority

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

70. *SIM Changes.* Congress, through Section 222 of the Act, requires telecommunications carriers to protect the privacy and security of customers' proprietary information that carriers obtain by virtue of providing a telecommunications service. Under Section 222(a), every telecommunications carrier has a "duty to protect the confidentiality of proprietary information of, and relating to, . . . customers." Section 222(c)(1) provides that a telecommunications carrier may only use, disclose, or permit access to customers' individually

identifiable CPNI that it has received or obtained by virtue of its provision of a telecommunications service in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived or its provision of services necessary to, or used in, the provision of such telecommunications service.

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

72. Fraudulent SIM swaps result in unauthorized disclosure of and access to customers' accounts, including individually identifiable CPNI. By successfully obtaining a fraudulent SIM swap, a bad actor can access CPNI such as incoming call information (including the date and time of the call and number from which the call is made), and gain access to a victim's account, potentially giving the bad actor access to other CPNI, like outgoing call history (including numbers called and the location, frequency, duration, and timing of such calls) and the victim's bills and the services purchased by the victim. And as described above, fraudulent SIM swaps allow bad actors to perpetrate greater fraud by giving them the means to complete text and voice authentications to access the victim's other accounts.

73. In light of the foregoing, we find that the rules we adopt today to address SIM swap fraud advance the protections against unauthorized disclosure of, and access to,

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

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

informed decisions about how they should be updated over time.

75. Our rules also further the goals of Section 222 by enabling customers to take action to prevent and address fraudulent SIM changes, and therefore help wireless providers protect against unauthorized disclosure and access to CPNI. The requirement that wireless providers immediately notify customers regarding SIM change requests provides added protection by giving customers information they can use to notify their providers that a fraudulent request has occurred at the time of the request or shortly thereafter so that the provider can take timely steps to remediate the situation. Requiring wireless providers to offer customers the option to lock their accounts so that their providers are prohibited from processing SIM changes gives security-minded customers or those who are at high risk of fraud a tool to prevent a fraudulent request from being processed in the first instance. Additionally, our new rule that wireless providers make notice of account protection mechanisms easily accessible via their websites and applications ensures that customers are aware of these tools. We also conclude that the requirements we establish to promptly resolve SIM swap and port-out fraud extend from our Section 222 authority because they will help to mitigate the unauthorized disclosure of and access to CPNI.

76. Finally, the new customer authentication requirements, with which both facilities-based providers and resellers must comply, apply to both pre-paid and postpaid services, which is consistent with Section 222(a)'s mandate that "[*e*]*very* telecommunications carrier . . . protect the confidentiality of [customer] proprietary information" and Section 222's instruction that all "customers" of those carriers benefit from such protections.

77. While Section 222 provides firm foundation for our rules to address SIM swap fraud, we also find that Section 251(e) of the Act provides additional authority for these rules. In Section 251(e)(1), Congress expressly assigned to the Commission exclusive jurisdiction over that portion of the North American Number Plan (NANP) that pertains to the United States and related telephone numbering issues. The Commission retained its "authority to set policy with

respect to all facets of numbering administration in the United States." Because our new SIM change rules prevent and address misuse of NANP numbers assigned to wireless devices, we conclude that those rules are supported by our exclusive numbering authority within Section 251(e).

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

79. We also find that the exclusive numbering authority that Congress granted this Commission under Section 251(e)(1) provides ample authority to extend the LNP requirements as set out in this *Report and Order*. Specifically, in Section 251(e)(1) of the Act, Congress expressly assigned to the Commission exclusive jurisdiction over that portion of the NANP that pertains to the United States and related telephone numbering issues. The Commission retained its "authority to set policy with respect to all facets of numbering administration in the United States." We find that the revisions to our number porting rules designed to protect the customers from port-out fraud fit comfortably within our exclusive numbering authority because the requirements we establish to prevent and promptly resolve port-out fraud are necessary to address improper use of numbering resources and ensure that customers can recover their numbers when fraudulent ports have occurred.

80. *Other Sources of Authority.* While the provisions discussed above provide sufficient authority for the entirety of the rules we adopt in this *Report and Order*, we find additional support under Sections 201 and 303. Sections 201 and 303 of the Act generally give the Commission authority for prescribing rules, but we also rely on these sources of authority as

described herein.

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

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

II. Procedural Matters

83. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA) requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant

economic impact on a substantial number of small entities." Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the potential impact of the rule and policy changes adopted in this *Report and Order* on small entities. The FRFA is set forth in Appendix B.

84. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is "non-major" under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this *Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

III. Final Regulatory Flexibility Analysis

85. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Protecting Consumers from SIM Swap and Port-Out Fraud Notice of Proposed Rulemaking* (*SIM Swap and Port-Out Fraud*) published October 15, 2021 at 86 FR 57390. The Commission sought written public comment on the proposals in the *SIM Swap and Port-Out Fraud Notice*, including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

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

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

text messages and phone calls intended for the customer.

87. The rules adopted in the *Report and Order* aim to foreclose these fraudulent practices while preserving the relative ease with which customers can obtain legitimate SIM changes and number ports. Specifically, the *Report and Order* revises the Commission's CPNI and LNP rules to require that wireless providers use secure methods of authenticating customers prior to performing SIM changes and number ports. This requirement is reinforced by other rules, including that wireless providers adopt processes for responding to failed authentication attempts, institute employee training for handling SIM swap and port-out fraud, and establish safeguards to prevent employees who receive inbound customer communications are unable to access CPNI in the course of that customer interaction until after customers have been authenticated. The *Report and Order* also adopts rules that will enable customers to act to prevent and address fraudulent SIM changes and number ports, including requiring that wireless providers notify customers regarding SIM change and port-out requests, offer customers the option to lock their accounts to block processing of SIM changes and number ports, and give advanced notice of available account protection mechanisms. Additionally, the *Report and Order* establishes requirements to minimize the harms of SIM swap and port-out fraud when it occurs, including requiring wireless providers to maintain a clear process for customers to report fraud, promptly investigate and remediate fraud, and promptly provide customers with documentation of fraud involving their accounts. Finally, to ensure wireless providers track the effectiveness of authentication measures used for SIM change requests, the *Report and Order* requires that providers keep records of SIM change requests and the authentication measures they use.

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

88. There were no comments that directly addressed the proposed rules and policies presented in the *SIM Swap and Port-Out Fraud Notice* IRFA. However two commenters

discussed the potential impact of rules on small carriers. The Competitive Carriers Association (CCA) advocated that the Commission adopt security measures that give providers flexibility to account for the constraints with which many small providers operate. The Rural Wireless Association (RWA) called for uniform standards for port-out authentication to prevent potential anticompetitive activities and increased costs for small providers in the event that larger providers hold small providers to standards that are difficult or costly to implement. The approach taken by the *Report and Order* addresses these comments by setting baseline requirements that build on existing mechanisms that many wireless providers already use to establish a uniform framework across the mobile wireless industry, while giving wireless providers the flexibility to deliver the most advanced, appropriate, and cost-effective fraud protection measures available.

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

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

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

90. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act. 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.

91. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein. 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. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.

92. 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." 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. Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

93. 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." U.S. Census Bureau data from the 2017 Census of Governments indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,931 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts with enrollment populations of less than 50,000. Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at

least 48,971 entities fall into the category of "small governmental jurisdictions."

1. Providers of Telecommunications and Other Services

94. *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. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

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

96. *Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with an SBA small

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

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

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

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

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

100. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard. 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. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services. Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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

estimates that 438 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

102. *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. The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

103. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year. Of this number, 242 firms had revenue of less than $25 million. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 65 providers that reported they were engaged in the provision of satellite telecommunications services. Of these providers, the Commission estimates that approximately

42 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

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

2. Internet Service Providers

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

employees.

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

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

108. Additionally, according to Commission data on Internet access services as of December 31, 2018, nationwide there were approximately 1,209 fixed wireless and 71 mobile wireless providers of connections over 200 kbps in at least one direction. The Commission does

not collect data on the number of employees for providers of these services, therefore, at this time we are not able to estimate the number of providers that would qualify as small under the SBA's small business size standard. However, based on data in the Commission's *2022 Communications Marketplace Report* on the small number of large mobile wireless nationwide and regional facilities-based providers, the dozens of small regional facilities-based providers and the number of wireless mobile virtual network providers in general, as well as on terrestrial fixed wireless broadband providers in general, we believe that the majority of wireless Internet access service providers can be considered small entities.

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

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

110. This *Report and Order* adopts rules that could result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance requirements for affected providers of service, including small wireless providers. Specifically, it requires that wireless providers use secure methods of authenticating customers prior to performing SIM changes and number ports, and to review and update these authentication methods as needed, but at least annually. It requires wireless providers to adopt processes for customer notification and response to failed authentication attempts, institute employee training for handling SIM swap and port-out fraud, and establish safeguards to prevent employees who receive inbound customer

communications from accessing CPNI in the course of that customer interaction until after customers have been authenticated. The *Report and Order* also adopts rules requiring that wireless providers notify customers regarding SIM change and port-out requests, offer customers the option to lock their accounts to block processing of SIM changes and number ports, and give advanced notice of available account protection mechanisms. Additionally, the *Report and Order* requires wireless providers to maintain a clear process for customers to report fraud, promptly investigate and remediate fraud, and promptly provide customers with documentation of fraud involving their accounts. Finally, the *Report and Order* requires that providers keep records of SIM change requests and the authentication measures they use.

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

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

112. The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . .including a statement of

the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."

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

data in their recordkeeping, which the *Report and Order* acknowledged would be particularly burdensome for small providers, and declining to require that providers report this data to the Commission regularly.

G. Report to Congress

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

IV. Ordering Clauses

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

116. IT IS FURTHER ORDERED that this *Report and Order* SHALL BE EFFECTIVE 30 days after publication in the Federal Register, and that compliance with the rules adopted herein shall be required six months after the effective date of the *Report and Order*, except that the amendments to Sections 52.37(c), 52.37(d), 52.37(e), 52.37(g), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8) of the Commission's rules, 47 CFR 52.37(c), 52.37(d), 52.37(e), 52.37(g), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8), which may contain new or modified information collection requirements, will not become effective until the later of i) six months after the effective date of this *Report and Order*; or ii) after the Office of Management and Budget completes review of any information collection requirements

associated with this *Report and Order* that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act. The Commission directs the Wireline Competition Bureau to announce the compliance date for §§ 52.37(c), 52.37(d), 52.37(e), 52.37(g), 64.2010(h)(2), 64.2010(h)(3), 64.2010(h)(4), 64.2010(h)(5), 64.2010(h)(6), and 64.2010(h)(8) and to amend 47 CFR 52.37 and 64.2010 accordingly.

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

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

List of Subjects

Communications, Communications common carriers, Privacy, Telecommunications, Telephone, Reporting and Recordkeeping Requirements

FEDERAL COMMUNICATIONS COMMISSION

Marlene Dortch,

Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 52 and 64 as follows:

PART 52 – NUMBERING

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

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

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

§ 52.37 Number Portability Requirements for Wireless Providers

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

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

(c)-(e) [Reserved]

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

(g) [Reserved]

(h) This section contains information-collection and/or recordkeeping requirements. Compliance with this section will not be required until this paragraph is removed or contains a compliance date.

3. Delayed indefinitely, amend § 52.37 by adding paragraphs (c), (d), (e), and (g) to read as follows:

§ 52.37 Number Portability Requirements for Wireless Providers

(c) *Customer notification of port-out requests*. Upon receiving a port-out request, and before effectuating the request, a CMRS provider shall provide immediate notification to the customer that a port-out request associated with the customer's account was made, sent in accordance with customer preferences, if indicated, and using means reasonably designed to reach the customer associated with the account and clear and concise language that provides sufficient information to effectively inform a customer that a port-out request involving the customer's number was made, except if the port-out request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. 345 and subpart II of this part, regardless of whether the line separation is technically or operationally feasible.

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

activated with instructions on how the customer can deactivate the account lock, and promptly comply with the customer's legitimate request to deactivate the account lock.

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

*****

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

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

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

(3) Promptly provide customers, upon request, with documentation of fraudulent number ports involving their accounts.

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

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

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

5. Amend § 64.2010 by adding paragraph (h) to read as follows:

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

* * * * *

(h) *Subscriber Identity Module (SIM) changes.* A provider of commercial mobile radio service (CMRS), as defined in 47 CFR 20.3, including resellers of wireless service, shall only effectuate SIM change requests in accordance with this section. For purposes of this section,

SIM means a physical or virtual card associated with a device that stores unique information that can be identified to a specific mobile network.

(1) *Customer authentication.* A CMRS provider shall use secure methods to authenticate a customer that are reasonably designed to confirm the customer's identity before executing a SIM change request, except to the extent otherwise required by 47 U.S.C. 345 (Safe Connections Act of 2022) or subpart II of this part. Authentication methods shall not rely on readily available biographical information, account information, recent payment information, or call detail information unless otherwise permitted under 47 U.S.C. 345 or subpart II of this part. A CMRS provider shall regularly, but not less than annually, review and, as necessary, update its customer authentication methods to ensure that its authentication methods continue to be secure. A CMRS provider shall establish safeguards and processes so that employees who receive inbound customer communications are unable to access CPNI in the course of that customer interaction until after the customer has been properly authenticated.

(2)-(6) [Reserved]

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

(8) [Reserved]

(9) *Compliance.* This paragraph (h) contains information-collection and/or recordkeeping requirements. Compliance with this paragraph (h) will not be required until this paragraph is removed or contains a compliance date.

6. Delayed indefinitely, amend §64.2010 by adding paragraphs (h)(2) through (6) and (h)(8) to read as follows:

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

*****

(h) ***

(2) *Response to failed authentication attempts.* A CMRS provider shall develop, maintain, and implement procedures for addressing failed authentication attempts in connection with a SIM change request that are reasonably designed to prevent unauthorized access to a customer's account, which, among other things, take into consideration the needs of survivors pursuant to 47 U.S.C. 345 and subpart II of this part.

(3) *Customer notification of SIM change requests*. Upon receiving a SIM change request, and before effectuating the request, a CMRS provider shall provide immediate notification to the customer that a SIM change request associated with the customer's account was made, sent in accordance with customer preferences, if indicated, and using means reasonably designed to reach the customer associated with the account and clear and concise language that provides sufficient information to effectively inform a customer that a SIM change request involving the customer's SIM was made, except if the SIM change request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. 345 and subpart II of this part, regardless of whether the line separation is technically or operationally feasible.

(4) *Account locks.* A CMRS provider shall offer customers, at no cost, the option to lock their accounts to prohibit the CMRS provider from processing requests to change the customer's SIM. A CMRS provider shall not fulfill a SIM change request until the customer deactivates the lock on the account, except if the SIM change request was made in connection with a legitimate line separation request pursuant to 47 U.S.C. 345 and subpart II of this part, regardless of whether the line separation is technically or operationally feasible. The process to activate and deactivate an account lock must not be unduly burdensome for customers such that it effectively inhibits customers from implementing their choice. A CMRS provider may activate a SIM change lock on a customer's account when the CMRS provider has a reasonable belief that the

customer is at high risk of fraud, but must provide the customer with clear notification that the account lock has been activated with instructions on how the customer can deactivate the account lock, and promptly comply with the customer's legitimate request to deactivate the account lock.

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

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

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

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

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

*****

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

[FR Doc. 2023-26338 Filed: 12/7/2023 8:45 am; Publication Date: 12/8/2023]