FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 22–21; FCC 23–111, FR ID 198806]

Data Breach Reporting Requirements

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) modifies the Commission's data breach notification rules to better ensure that providers of telecommunications, interconnected Voice over Internet Protocol (VoIP), and telecommunications relay services (TRS) are held accountable in their obligations to safeguard sensitive customer information, and to provide customers with the tools needed to protect themselves in the event that their data is compromised.

DATES: This rule is effective March 13, 2024, except for the amendments codified at 47 CFR 64.2011 and 64.5111, instructions 3 and 4, respectively, which are delayed indefinitely. The Commission will publish a document in the **Federal Register** announcing the effective dates for the amendments to 47 CFR 64.2011 and 64.5111.

FOR FURTHER INFORMATION CONTACT: Mason Shefa, Competition Policy Division, Wireline Competition Bureau, at (202) 418–2494, *mason.shefa@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Report and Order* in WC Docket No. 22–21; FCC 23–111, adopted on December 13, 2023 and released on December 21, 2023. The document is available for download at *https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf.* To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an email to *FCC504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (TTY).

Final Paperwork Reduction Act of 1995 Analysis

This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104–13. All such new or modified requirements will be submitted to the Office of Management and Budget (OMB) for review under section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on any new or modified information collection requirements contained in this proceeding.

Congressional Review Act

The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, OMB, 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).

Synopsis

I. Report and Order

1. In this Order, the Commission adopts several proposals from the *Data Breach Notice,* 88 FR 3953 (Jan. 23, 2023), to modernize its data breach requirements. The Commission's breach notification rule provides an important protection against improper use or disclosure of customer data, helping to ensure that carriers are held accountable and providing customers with the tools to protect themselves in the event that their data is compromised. However, in the 16 years since the Commission adopted its data breach reporting rule—designed to protect customers against the threat of ''pretexting''—data breaches have only grown in frequency and severity. As discussed below, the Commission finds that these changes will better protect consumers from improper use or disclosure of their customer information and harmonize its rules with new approaches to protecting the public already deployed by the Commission's partners in Federal and State government. To the extent that this Report and Order does not expressly address a topic that was subject to comment in the *Data Breach Notice,* that issue remains pending.

2. The Commission first expands the scope of its breach notification rules to cover not just CPNI, but all PII. The Commission next adopts its proposal to expand its definition of ''breach'' for telecommunications carriers to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or further disclosed. The Commission also adopts its proposal to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable, but no later than seven business days, after reasonable determination of a breach. The Commission next eliminates the requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. The Commission also eliminates the mandatory waiting period for carriers to notify customers, and instead requires carriers to notify customers of breaches of covered data without unreasonable delay after notification to Federal agencies, and in no case more than 30 days following reasonable determination of a breach, unless a delay is requested by law enforcement. Finally, to ensure that TRS consumers enjoy the same level of protection under its rules as consumers of telecommunications services, the Commission adopts equivalent requirements for TRS providers.

A. Defining ''*Breach*''

1. Scope of Protected Consumer Information

3. In the *Data Breach Notice,* the Commission recognized that carriers possess proprietary information of customers other than CPNI, which customers have an interest in protecting from public exposure; the notice sought comment on requiring carriers to report breaches of such information. The Commission concludes that carriers should be obligated to comply with its breach notification rule whenever such information is the subject of a breach, whether or not the information is CPNI.

4. The pervasiveness of data breaches and the frequency of breach notifications have evolved and increased since the Commission first adopted its breach notification rule in 2007. As discussed in the *Data Breach Notice,* the Commission's requirement is one of several sector-specific Federal breach notification laws in the United States. All State data breach notification requirements explicitly include categories of sensitive personal information within their scope, as do sector-specific Federal laws. The Commission believes that the unauthorized exposure of sensitive personal information that the carrier has received from the customer (*i.e.,* information ''of the customer''), or about the customer (*i.e.,* information ''relating to'' the customer), in connection with the customer relationship (*e.g.,* initiation, provision, or maintenance, of service), such as social security numbers or financial records, is reasonably likely to pose risk of customer harm. Accordingly, any unauthorized disclosure of such information warrants

notification to the customer, the Commission, and other law enforcement. Consumers expect that they will be notified of substantial breaches that endanger their privacy, and businesses that handle sensitive personal information should expect to be obligated to report such breaches.

5. The Commission requires notification of breaches that involve PII, which is a well-understood concept and thus a readily administrable way of requiring breach notifications in the case of proprietary information. The Commission rejects claims that it did not provide sufficient notice to define the scope of protected consumer information in this manner. In the *Data Breach Notice* the Commission sought comment on ''requir[ing] telecommunications carriers to report breaches of proprietary information other than CPNI under Section 222(a),'' in which case commenters were asked to address ''how broadly or narrowly [the Commission should] define that category of information.'' This provided notice that the Commission could define the scope of protected information to encompass all or any subset of the universe of proprietary information encompassed by section 222(a). And as the Commission explains below, the scope of customer information encompassed by section 222(a) is best interpreted to include PII, and the Commission defines the scope of its breach notification rules to include PII subject to the additional limitations that the Commission adopts below. The Commission therefore concludes that there was sufficient notice for the approach the Commission adopt. The definition of PII is aptly described in OMB Circular A-130, ''Managing Information as a Strategic Resource,'' as ''information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.'' CPNI is a subset of PII. As discussed below, this approach of holding carriers responsible for reporting breaches of PII is supported independently and alternatively by construing the phrase ''proprietary information of . . . customers'' in section 222(a) as covering all information defined as PII, and by recognizing that section 201(b)'s just-and-reasonable-practices obligation requires protection of PII.

6. For the purposes of its breach notification rules, the Commission further defines the scope of covered PII as (1) first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the identity of a specific individual (including, but not limited to, Social Security Number, driver's license number or State identification number, Taxpayer Identification Number, passport number, military identification number, Tribal identification card, or any other Federal or State government-issued identification card), or other unique identification number used for authentication purposes (including, but not limited to, a financial institution account number, student identification number, or medical identification number); (2) user name or email address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account (including, but not limited to, Personal Identification Numbers, private keys that are unique to an individual and are used to authenticate or sign an electronic record; unique electronic identifiers or routing codes, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or shared secrets or security tokens that are known to be used for data-based authentication); or (3) unique biometric, genetic, or medical data (including, but not limited to, fingerprints, faceprint, a retinal or iris scan, hand geometry, voiceprint analysis, or other unique biometric data generated from a measurement or analysis of human body characteristics to authenticate or ascertain an individual's identity; genetic data such as deoxyribonucleic acid data; and medical records, or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional). Moreover, dissociated data that, if linked, would constitute PII is to be considered PII if the means to link the dissociated data were accessed in connection with access to the dissociated data, and any one of the discrete data elements listed above or any combination of the discrete data elements listed above is PII if the data element or combination of data elements would enable a person to commit identity theft or fraud against the individual to whom the data element or elements pertain.

7. This approach brings the Commission's definition of covered data in line with the approaches taken at the State level, and responds to concerns raised in the record by certain parties regarding harmonization with existing breach notification regimes. In order to further harmonize its approach with analogous State law, the Commission also adopts an exception from its definition of PII for publicly available information that is lawfully made available to the general public from Federal, State, or local government records or widely distributed media. Notwithstanding these limitations, the Commission will monitor the data security landscape and will not hesitate to revisit and revise the list of data elements in a future rulemaking as necessary to ensure that carriers adequately protect sensitive customer data.

8. Without an FCC rule requiring breach notifications for the above categories of PII, there would be no requirement in Federal law that telecommunications carriers report non-CPNI breaches to their customers. CTIA's objection that doing so would ''[c]reat[e] a system of dual jurisdiction between the FCC and the FTC'' is unpersuasive. CTIA asserts that ''[c]ustomers do not expect different privacy protections for the same data depending on which entity holds the data or the kind of product or service that is being marketed'' but concedes the FTC's lack of authority in the common carrier context. By the statutory design of the Communications Act and the FTC Act, Congress assigned differing areas of responsibility to the FCC and FTC, and CTIA identifies no grounds for the Commission to ignore its responsibilities with respect to common carriers. By ensuring that the same data breach notification requirements also apply to interconnected VoIP and TRS providers, the Commission advances the interest of ensuring that consumers can have the same expectations regarding services that they view as similar. The approach the Commission adopts therefore not only reflects the practical expectations of consumers but also honors the intention of Congress. For example, as discussed in more detail below, Congress ratified the Commission's 2007 decision to extend section 222-based privacy protections for telecommunications service customers to the customers of interconnected VoIP providers. And ensuring equivalent protections for TRS subscribers advances Congress' directive to endeavor to ensure functionally equivalent service. Despite NCTA's suggestion that ''there is no other 'proprietary information' between a provider and its customer that is not CPNI but is covered by Section 222,'' the Commission has investigated several instances of breaches involving

sensitive personal information about customers held by telecommunications carriers that was not or may not have been CPNI. The Commission has also in the past concluded that names, addresses, and telephone numbers are not CPNI, even when a customer has elected not to have them disclosed publicly, and that such information therefore would not be subject to the CPNI-specific restrictions on use in section 222(c). The Commission finds that such information can be sensitive and warrants protection, including a requirement that the Commission, law enforcement, and customers be notified about breaches. Indeed, because consumers expect to be notified of substantial breaches that endanger their privacy, it better protects customers that breach notifications not turn on whether a particular breached element is or is not CPNI.

2. Inadvertent Access, Use, or Disclosure of Covered Data

9. Consistent with the *Data Breach Notice's* proposal, the Commission expands the Commission's definition of ''breach'' to include inadvertent access, use, or disclosure of covered data. Specifically, the Commission defines ''breach'' as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed covered data. While the practice of pretexting that spurred the Commission to act in 2007 necessarily involves an intent to gain access to customer information, the record before the Commission here amply demonstrates that the inadvertent exposure of customer information can result in the loss and misuse of sensitive information by scammers and phishers, and trigger a need to inform the affected individuals so that they can take appropriate steps to protect themselves and their information. The Commission agrees with the wide range of commenters that recognize that any exposure of customer data can risk harming consumers, regardless of whether the exposure was intentional. As the Accessibility Advocacy and Research Organizations (AARO) argue, ''[t]he Commission must adapt to an ever changing technological environment, which implicates all kinds of privacy concerns, and adopt measures that can effectively counter increasingly complex and evolving breaches.'' In order to address these risks, carriers not only must reasonably protect covered information as required by the Act and the Commission's rules, but also must inform affected individuals so that they can take appropriate steps to protect themselves and their information where breaches occur. In addition, notification of both intentional and unintentional breaches to the Commission and other Federal law enforcement will aid investigations and help prevent new breaches or further harm to consumers. The Commission expects that its broadening of ''breach'' to include inadvertent exposure will encourage telecommunications carriers to adopt stronger data security practices, and will help Federal agencies identify and address systemic network vulnerabilities.

10. The record supports the Commission's observation in the *Data Breach Notice* that breaches have become more prevalent and more severe in recent years. In 2021, the Identity Theft Resource Center ''estimated a record-breaking 1,862 data breaches,'' and a survey from IBM has exposed ''a recent decline in response capabilities'' due to ''informal or ad hoc'' data security plans. This rising tide of data breaches has affected the telecommunications sector as well. As the Electronic Privacy Information Center (EPIC) points out, the proprietary information of subscribers of each of the three largest carriers ''has been breached at least once within the last five years.'' Indeed, in February 2020, the Commission proposed more than $200 million in fines against AT&T, Sprint, T-Mobile, and Verizon, for apparently failing to adequately protect consumer location data. In each case, the Commission found that the carriers' apparently lacked adequate oversight over third-party location aggregators' use of their phone subscribers' location data, leading to the disclosure of their respective customers' location information, without consent, to third parties who were not authorized to receive it.

11. Given these worrying trends, the Commission agrees with EPIC that its expansion of ''breach'' to include inadvertent exposures is a necessary first step to galvanize carriers to strengthen their data security policies and oversight of customer data. In particular, broadening the breach definition will better enable the marketplace to respond to the relative strengths of particular carriers' practices and enhance the Commission's ability to identify where additional regulatory oversight might be needed. Removing the intent limitation in the Commission's breach reporting rule will reduce ambiguity regarding whether reporting a breach is necessary, and therefore decrease the risk of underreporting. Finally, the Commission's expansion of ''breach'' to include inadvertent access, use, or disclosure of customer information brings the Commission's rules in line with the overwhelming majority of State and Federal breach notification laws and regulations that lack such an intent limitation, ensuring that consumers nationwide—along with the Commission and other relevant Federal authorities—likewise receive critical breach notifications in a timely manner.

12. Notwithstanding these benefits, the Commission acknowledges concerns expressed by carriers that its expansion of the ''breach'' definition to include inadvertent disclosures, on its own, could lead to ''notice fatigue'' for consumers, deplete Commission and law enforcement resources, or increase the burden of reporting obligations. The Commission is unpersuaded by the arguments of Lincoln Network, which goes even further and contends that data breach reporting requirements would implicate the major questions doctrine. Lincoln Networks focuses solely on the alleged economic impact of the requirement to the exclusion of other considerations, and even then provides no meaningful sense of the likely magnitude of such effects—citing total estimated economic costs of breaches and asserting in a conclusory manner that ''it is reasonable to conclude that at least some of the cost per breach is assignable to notification,'' without quantifying the cost associated with such notifications, let alone any portion attributable specifically to FCC breach notification rules. The Commission thus is unpersuaded that the major questions doctrine is implicated here. In any case, the Commission explains below why these rules fall comfortably within the Commission's statutory authority. In response to these concerns, as discussed below, the Commission exempt from its expanded definition of ''breach'' a good-faith acquisition of customer data by an employee or agent of a carrier where such information is not used improperly or further disclosed. The Commission also adopts a ''harm-based notification trigger,'' such that notification of a breach to consumers is not required in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed. As discussed below, the Commission also finds that its adoption of a minimum threshold for the number of customers affected to trigger its requirement to notify the Commission and other Federal law

enforcement regarding breaches where there is no reasonable likelihood of harm will further reduce carriers' reporting burdens, and make more efficient use of agencies' resources. Although carriers' obligation to protect covered information under section 222 of the Act and the Commission's implementing rules is not limited just to scenarios where there is actual evidence of consumer harms, these common-sense limitations on the Commission's disclosure requirements are well-supported by the record and are consistent with most State and Federal data breach notification regimes. Taken together, the Commission finds that these carve-outs will mitigate any legitimate concerns expressed by commenters in the record regarding the potential for consumer notice fatigue and undue burdens on Federal agencies and carriers by triggering the requirements in situations where the Commission finds disclosures most strongly justified.

13. In the *Data Breach Notice,* the Commission also sought comment on whether it should ''expand the definition of a breach to include situations where a telecommunications carrier or a third party discovers conduct that could have reasonably led to exposure of customer CPNI, even if it has not yet determined if such exposure occurred.'' Commenters generally oppose such an expansion, arguing that it could result in over-notification to customers and to government entities, impeding carriers' and the government's investigation of actual breaches, and needlessly frightening consumers. While the Commission believes that notification of situations in which customer data are put at risk has value, no commenter in the record provides evidence in support of such an approach. The Commission nevertheless expects that in such situations, carriers will work reasonably and efficiently to confirm whether or not actual exposure has occurred. While the Commission declines at this time to amend the definition of breach to include situations where a carrier or third party has not yet determined if an exposure of covered data has occurred, the Commission also notes that it does not prohibit carriers from providing notice in such situations to their customers if, for example, they determine that doing so is appropriate under the circumstances. While the Commission has not expanded the definition of data breach to include situations where customer data is put at risk but not exposed, it notes that the threshold for reporting a breach is separate from the obligation to ''protect the confidentiality of proprietary information'' and to ''take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.'' 47 U.S.C. 222(a); 47 CFR 64.2010(a). Not only may a breach that does not meet the reporting threshold still reflect a violation of section 222 of the Act or an unreasonable practice in violation of 64.2010(a) of the rules, but a carrier can violate section 222 of the Act or section 64.2010(a) of the rules even in the absence of any breach. The Commission also will continue to monitor how such situations impact customers, and reserve the ability to expand the breach definition to cover such situations in the future, should the Commission find such an expansion is warranted.

3. Good-Faith Exception

14. The Commission excludes from the definition of ''breach'' a good-faith acquisition of covered data by an employee or agent of a carrier where such information is not used improperly or further disclosed. In the *Data Breach Notice,* the Commission used the term ''exemption'' instead of ''exception'' when asking commenters whether the Commission should exclude from the definition of ''breach'' a good-faith acquisition of covered data. For the purpose of clarity, the Commission instead uses the word ''exception'' here to describe this exclusion. While the Commission makes this exception to its definition of ''breach,'' it nevertheless expects carriers to ''take reasonable measures'' in such scenarios to protect such customer information from improper use or further disclosure, which may, for example, involve requiring that such an employee or agent destroy the data upon realizing that the data was disclosed without, or in excess of, authorization. As noted above and in the *Data Breach Notice,* the vast majority of State statutes include a similar exception from the definition of ''breach,'' and commenters overwhelmingly agree that such an exception is appropriate. As Blooston Rural Carriers argues, a good-faith exception will prevent carriers from ''unnecessarily confus[ing] and alarm[ing] consumers'' in such low-risk situations. The Commission also agrees with National Rural Electric Cooperative Association (NRECA) that, without this exception, ''more serious data breaches [will potentially] become lost in the 'noise' of multiple notifications.'' The Commission therefore finds that its good-faith exception will help avoid excessive notifications to consumers, and reduce reporting burdens on carriers. CTIA and NCTA's arguments about the Commission's allegedly overly broad definition of harm to trigger customer notifications of breaches of covered data, and their expressed concerns about excessive reporting to Federal agencies, do not account for the fact that this good-faith exception removes an entire category of breaches from the scope of reporting covered by the Commission's rules as a threshold matter. As a result, the Commission is unpersuaded by these parties' cursory claims about possible notice fatigue, consumer confusion or frustration, and interference with data breach investigations.

15. The Commission disagrees with EPIC that its adoption of a good-faith exception would ''weaken privacy and data security protections for consumers.'' In support of these claims, EPIC cites instances in which employees, ''either through bribery or inadequate training, were illegally disclosing consumer information to pretexters claiming to have authorization to access subscriber information.'' The Commission does not find that these situations justify taking a different approach; indeed, the exception the Commission adopts would not apply in the scenarios outlined by EPIC. First, the good-faith exception relieves carriers from reporting obligations only where customer information is not used improperly or further disclosed, and in EPIC's example, the information was, intentionally or not, further disclosed to a pretexter. Second, in circumstances where an employee improperly discloses consumer information due to bribery, the employee disclosing the information is, by definition, not acting in ''good faith,'' and therefore such an incident would still be considered a breach under the Commission's rules.

B. Notifying the Commission and Other Federal Law Enforcement of Data Breaches

1. Requiring Notification to the Commission

16. As proposed in the *Data Breach Notice,* the Commission requires telecommunications carriers to notify the Commission of a breach in addition to notification to the Secret Service and FBI. The Commission continues to require carriers to notify the Secret Service and the FBI because doing so enables law enforcement to investigate the breach, ''which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI.'' Moreover, law enforcement investigations into how breaches occurred would enable law

enforcement to advise the carrier and the Commission to take steps to prevent future breaches of that kind. The Commission will maintain a link to the reporting facility at *http://www.fcc.gov/eb/cpni* or a successor URL designated by the Wireline Competition Bureau (Bureau). As the Commission found when it adopted the current data breach rules, notifying law enforcement of a breach is consistent with the goal of protecting customers' personal data because it enables such agencies to investigate the breach, ''which could result in legal action against the perpetrators,'' thus ensuring that they do not continue to breach sensitive customer information. The Commission also anticipated that law enforcement investigations into how breaches occurred would enable law enforcement to advise providers and the Commission to take steps to anticipate and prevent future breaches of a similar nature. Addition of the Commission as a recipient of Federal-agency breach notifications is consistent with other Federal sector-specific laws, which require prompt notification to the relevant subject-matter agency. As large-scale security breaches resulting from lax or inadequate data security practices and employee training have become more common since the *2007 CPNI Order,* notifying the Commission of breaches will provide Commission staff with important information about data security vulnerabilities and threat patterns that Commission staff can help address and remediate. Commission notification will also shed light on carriers' ongoing compliance with the Commission's rules. Consistent with its proposal and the record in response to the *Data Breach Notice,* the Commission requires carriers to notify the Commission of a reportable breach contemporaneously with the Secret Service and FBI. As stated in the *Data Breach Notice,* requiring carriers to notify the Commission, Secret Service, and FBI at the same time will minimize burdens on carriers, eliminate confusion regarding obligations, and streamline the reporting process, allowing carriers to free up resources that can be used to address the breach and prevent further harm. Commenters support a single, contemporaneous notification to the Commission, Secret Service, and FBI.

17. The majority of commenters support including the Commission in data breach notifications. WISPA opposes contemporaneous notification to the Commission ''[i]f the Commission were to require separate notice.'' Because the Commission is not requiring separate notification to the Commission, but are merely adding the Commission as a recipient of breach notifications submitted through the preexisting central reporting facility, the Commission expects that this should allay WISPA's concern. Many of these commenters agree, however, that this new notification requirement should not create new obligations which are duplicative or inconsistent with the preexisting requirement to notify law enforcement agencies, and should instead entail one notification sent to all three. The Commission agrees with these suggestions, as the Commission sees no need for carriers to file separate or differing notifications to the Commission. As discussed below, the Commission delegates authority to the Bureau to coordinate with the Secret Service to adapt the existing central reporting facility for reporting breaches to the Commission and other Federal law enforcement agencies. Additionally, as discussed below, the Commission does not impose differing content requirements for notifications to the different agencies.

18. The Commission disagrees with commenters that oppose requiring breach notification to the Commission. For example, ITI and WISPA argue that the existing requirement to notify the Secret Service and the FBI is sufficient, and that notification to the Commission is unnecessary. WISPA also argues that notification to the Commission would hinder law enforcement investigation efforts, and attempts to distinguish the other Federal regulations that require notification to sector-specific agencies as less burdensome than the Commission notification adopted here. The Commission is unpersuaded by these arguments. First, as mentioned above, the requirement to notify the Commission of covered data breaches is necessary to ensure that Commission staff are informed of new types of security vulnerabilities that arise in today's fast-changing data security environment. Additionally, the Commission disagrees with WISPA that adding the Commission as a recipient of Federal-agency notifications would hinder law enforcement investigation efforts, given the lack of impact the addition will have on the timing, content, or format of notification to the other law enforcement agencies. Indeed, the Secret Service is supportive of the Commission receiving such notifications. Furthermore, the Commission's action here avoids adding any additional burden on filers by merely adding the Commission to the list of recipients of the same breach notifications Commission rules already require carriers to submit, and, as discussed in further detail below, further streamlines the filing process by adapting the existing reporting facility for submission. This should also address WISPA's concern that a contemporaneous, but separate, notice to the Commission would impact initial efforts to assess a breach. For these reasons, the Commission does not expect carriers of any size to experience increased regulatory burdens as a result of the Commission notification requirement. Moreover, to the extent that carriers are faced with any minimal burdens, such burdens are well justified by the value of these reports to Federal law enforcement agencies and the Commission.

2. Threshold Trigger for Federal-Agency Notification

19. The Commission requires carriers to inform Federal agencies, via the central reporting facility, of all breaches, regardless of the number of customers affected or whether there is a reasonable risk of harm to customers. For breaches that affect 500 or more customers, or for which a carrier cannot determine how many customers are affected, the Commission requires carriers to file individual, per-breach notifications as soon as practicable, but no later than seven business days, after reasonable determination of a breach. As described below, these notifications must include detailed information regarding the nature of the breach and its impact on affected customers. This same type of notification, and the seven business day timeframe for submission, will also be required in instances where the carrier has conclusively determined that a breach affects fewer than 500 customers unless the carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. As discussed below, for breaches affecting fewer than 500 customers and which do not meet the harm-based trigger, the Commission instead requires carriers to submit an annual summary of such incidents. For breaches in which a carrier can reasonably determine that a breach affecting fewer than 500 customers is not reasonably likely to harm those customers, the Commission requires the carrier to file an annual summary of such breaches via the central reporting facility, instead of a notification. To ensure that carriers may be held accountable regarding their determinations of a breach's likelihood of harm and number of affected customers, the Commission requires carriers to keep records of the bases of those determinations for two years. The

Commission also notes that carriers may voluntarily file notification of such a breach in addition to, but not in place of, this annual summary filing. In circumstances where a carrier initially determines that contemporaneous breach notification to Federal agencies is not required under these provisions, but later discovers information that would require such notice, the Commission clarifies that a carrier must report the breach to Federal agencies as soon as practicable, but no later than seven business days of their discovery of this new information. For example, if a carrier initially determines that Federal agency notification within seven business days is not required because a breach affects fewer than 500 customers and harm to customers is not reasonably likely to occur, but later discovers new information suggesting that more than 500 customers were affected, or that harm to customers has occurred, or is likely to occur, as a result of the breach, then the carrier must notify Federal agencies as soon as practicable, but no later than within seven business days of this discovery.

20. Given the Commission's expansion of the definition of ''breach'' in today's Order to include inadvertent exposure of CPNI and other types of data, allowing carriers to file information regarding smaller, less risky breaches in a summary format on an annual basis will tailor administrative burdens on carriers to reflect those scenarios where reporting is most critical. The Commission is unpersuaded by NCTA's contention that its rule for data breach reporting to Federal agencies is ''likely to tax resources and limit the regulator's ability to identify the most problematic practices and act to protect consumers'' and result in harm due to lack of harmonization. The Commission is likewise unpersuaded by CTIA's similar contention that ''the FCC is not currently equipped to 'become a repository for threat detection and monitoring' '' and that the ''flood of information threatens to distract FCC and Law Enforcement staff from real and potentially harmful security threats.'' These parties offer only generalized assertions in that regard without any evidence or analysis demonstrating concrete harms that are likely to result in practice. At the same time, NCTA and CTIA appear to neglect the potential the Commission anticipates for Federal agencies to gain useful insight into trends or particular activities that can lead to consumer harm even if, in a given instance, the reported breach happened not to involve consumer harm (whether under the standard set by Commission rules or in NCTA's and/or CTIA's own subjective judgment). The Commission's setting of a notification threshold is consistent with many State statutes that similarly do not have an intentionality requirement and require notice to State law enforcement authorities. The Commission's adoption of a 500-affected-customer threshold is also consistent with an analogous breach of health records notification required by the Federal Trade Commission (FTC).

21. The vast majority of commenters are supportive of the need for a threshold trigger generally, but are divergent regarding what the numerical threshold should be. NCTA supports a threshold of 500 affected customers for Federal-agency notifications, noting that such a threshold would ''minimize paperwork burdens on providers that wish to focus their resources on protecting customers,'' and cites a variety of State laws that use that threshold. CTIA and Verizon, however, argue that the Commission should set the threshold to be higher than 1,000 to reflect the larger customer bases of larger carriers. CTIA and Verizon do not provide additional reasoning as to why the size of the carrier's customer base is relevant in determining the threshold for Federal-agency notification. If the rationale for adopting a higher threshold for larger carriers is to reduce reporting burdens, the Commission notes that larger carriers likely have more resources than smaller carriers to respond to breach incidents. Verizon, for example, admits that it has ''a team of more than 1,000 professionals dedicated to implementing corporate-wide security controls and constantly monitoring networks to identify and respond to threats.'' Additionally, the Commission and other Federal law enforcement agencies would likely have an investigative interest in breaches affecting 500 or more customers, regardless of the percentage of the overall customer base those customers represent.

22. The Commission finds that the reporting threshold it adopts will both enable the Commission to receive more granular information regarding larger breaches to aid its investigations while also being able to study trends in breach activity through reporting of smaller breaches in annual submissions. Given that a number of States have found such a balance with a 500-affected-customer threshold, the Commission's adoption of this threshold also carries the additional benefit of ''increas[ing] harmonization with [S]tate breach notification statutes.'' The Commission therefore also rejects rural carriers' suggestion that it adopt a 5,000-affected-customer threshold.

23. Finally, as supported by the record, the Commission applies this threshold trigger only to notifications to Federal agencies, and not to customer notifications. Breaches affecting even just a few customers can pose just as much risk to those customers as could breaches with wider impact. For this reason, as discussed above, the Commission continues to require carriers to notify Federal agencies within seven business days of breaches that implicate a reasonable risk of customer harm, regardless of the number of customers affected. Doing so will permit Federal agencies to investigate smaller breaches where there is a risk of customer harm, and also allow law enforcement agencies to request customer notification delays where such notice would ''impede or compromise an ongoing or potential criminal investigation or national security,'' as specified in the Commission's rules.

3. Notification Timeframe

24. The Commission retains its existing requirement that carriers notify Federal agencies of a reportable breach as soon as practicable, but no later than seven business days, after reasonable determination of the breach. As commenters point out, in the text of the *Data Breach Notice,* the Commission occasionally used the phrase ''after discovery of a breach,'' rather than ''after reasonable determination of a breach'' when discussing the appropriate timeframe for Federal-agency notification. However, as the Proposed Rules Appendix makes clear, ''after discovery'' was intended as shorthand, rather than a proposal to substantively change the existing ''after reasonable determination of a breach'' standard. While the *Data Breach Notice* proposed eliminating the seven business day deadline, based on the record in response, the Commission finds that the existing timeframe provides greater certainty for carriers and customers affected by breaches. The Commission agrees with ACA Connects that retaining the seven business day deadline properly balances the need to give carriers ''reasonable time to prioritize remediation efforts before submitting notifications'' with the need to ensure customers receive timely notifications regarding breaches affecting their data. The Commission also agrees with NTCA that there is insufficient evidence that the current timeline ''is inadequate to accomplish the Commission's goals.'' Particularly given its historical

experience with a seven day deadline, the Commission is unpersuaded by conclusory assertions that meeting that deadline might not always be feasible. Additionally, the Commission agrees with NTCA that eliminating the seven business day deadline and only ''requiring breaches to be reported 'as soon as practicable' can be interpreted differently by different carriers or even by law enforcement and the Commission, thereby placing carriers at risk of inadvertently violating the Commission's rules if they construe 'as soon as practicable' differently than the Commission.''

25. The Commission disagrees with the arguments of other commenters that removing the seven business day deadline is necessary to afford carriers of different sizes and means the flexibility to respond to an evolving breach situation and minimize consumer harm, while also providing accurate and detailed notifications to Federal agencies. Given agencies' ability to calibrate their resources based on the volume of notifications, and the Commission's practical experience dealing with investigations at a stage where information might only be preliminary or incomplete, the Commission rejects arguments that burdens on the Commission and other law enforcement agencies justify eliminating the seven day reporting deadline. Carriers have long been subject to the existing seven business day deadline, which was adopted in 2007, and, as EPIC notes, some State jurisdictions require notification to the State attorney general within 3 days. As the Commission points out above, ACA Connects and NTCA—both associations of small-to-medium-sized carriers with presumably fewer resources than larger carriers such as Verizon—support retaining the seven business day time limit. Even assuming, *arguendo,* that the seven business day deadline is a more burdensome or inflexible timeframe for small carriers with ''limited personnel and/or resources,'' the Commission still finds that the countervailing interest in ensuring customers are notified quickly of breaches affecting them outweighs this tailored burden. For this reason, as discussed below, the Commission also removes the seven business day mandatory waiting period between Federal-agency notification and customer notification. The Commission lastly clarifies that ''reasonabl[y] determin[ing]'' a breach has occurred does not mean reaching a conclusion regarding every fact surrounding a data security incident that may constitute a breach. Rather, a carrier will be treated as having ''reasonabl[y] determin[ed]'' that a breach has occurred when the carrier has information indicating that it is more likely than not that there was a breach.

26. While the Commission sets this outer bound for Federal-agency notifications, it expects that larger carriers with significant resources and staffing will routinely be providing notification of breaches to the Commission well within the seven business day deadline, and that other carriers should strive to do so as well. Indeed, the ''as soon as practicable'' standard may require such notifications be made in *fewer* days than the seven business day deadline, and a failure to swiftly report breaches may, depending on the circumstances, be untimely and unreasonable, even if within the seven business day deadline. For example, if a carrier has made all the determinations necessary to conclude that a breach should be reported to law enforcement after only a few days, it would be inconsistent with the ''as soon as practicable'' standard for the carrier to wait until the seventh business day—merely because that is the outer limit—before providing the required notice. The Enforcement Bureau will continue to investigate carriers that have neglected to provide timely notification to Federal agencies after a breach incident pursuant to its delegated authority.

27. *Annual Reporting of Certain Small Breaches.* The Commission requires carriers to submit, via the existing central reporting facility and no later than February 1, a consolidated summary of breaches that occurred over the course of the previous calendar year which affected fewer than 500 customers, and where the carrier could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. The Commission delegates authority to the Bureau to coordinate with the Secret Service regarding any modification to the portal that may be necessary to permit the filing of this annual summary. The Commission also delegates authority to the Bureau, working in conjunction with the Public Safety and Homeland Security Bureau, and based on the record of this proceeding—or any additional notice and comment that might be warranted—to determine the content and format requirements of this filing and direct the Bureau to release a public notice announcing these requirements. The Commission instructs the Bureau to minimize the burdens on carriers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. At a minimum, the Bureau should develop requirements that are less burdensome than what is required for individual breach submissions to the reporting facility, and consider streamlined ways for filers to report this summary information. The first annual report will be due the first February 1 after the Office of Management and Budget (OMB) approves the annual reporting requirement under the Paperwork Reduction Act. The first report should cover all breaches between the effective date of the annual reporting requirement and the remainder of the calendar year.

28. The Commission disagrees with CTIA's argument that ''there is no regulatory goal served by mandating record keeping'' for incidents affecting fewer customers than the notification threshold. NCTA argues that the annual reporting requirement would ''not provide the Commission with meaningful information to serve its goals of identifying data breach patterns,'' but does not provide more detail as to why such information would not be helpful. Breaches that are limited in scope may still reveal patterns or provide evidence of security vulnerabilities at an early stage. As noted in the *Data Breach Notice* and the *2007 CPNI Order,* notification of all breaches, regardless of the number of customers affected or a carrier's determination of harm, ''could allow the Commission and Federal law enforcement to be 'better positioned than individual carriers to develop expertise about the methods and motives' '' associated with breaches. The Commission therefore finds that this annual summary of smaller breaches will continue to enable the Commission and its Federal law enforcement partners to investigate, remediate, and deter smaller breaches.

29. The Commission also disagrees with NTCA and Southern Linc who argue that ''requiring carriers to maintain records of any breaches that fall below the notification threshold 'will place an unnecessary burden on carriers. . . .' '' On the contrary, the Commission finds that any burdens associated with the annual reporting requirement are likely to be well justified by the countervailing benefits discussed above. Nor do commenters objecting to the burden of the Commission's rules as unwarranted provide a quantification of their anticipated burdens that would overcome the benefits anticipated from those rules. Moreover, this single annual report containing a summary of such

breaches will likely end up replacing numerous smaller breach notifications individually submitted via the central reporting facility throughout the year. Additionally, Commission rules already require carriers to ''maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.'' The first part of this requirement encompasses all disclosures of CPNI to third parties resulting from a data breach, and thus is broader than the small-breach reporting requirement the Commission adopts today, at least with regard to CPNI.

4. Notification Contents

30. The Commission maintains its existing requirements regarding the contents of data breach notifications to Federal law enforcement agencies, with a minor modification as noted below, and applies these same requirements to notifications to the Commission. The Commission agrees with comments submitted by WISPA arguing that ''the information currently submitted through the FBI/Secret Service reporting facility is largely sufficient and that generally the same information should be reported'' under its updated rules. The Commission also takes this opportunity to codify these categories of information in its rules to improve the ease of identifying the information that will be needed by regulated entities. Specifically, the Commission requires carriers to report, at a minimum, information relevant to the breach, including: carrier address and contact information; a description of the breach incident; the method of compromise; the date range of the incident; the approximate number of customers affected; an estimate of financial loss to the carrier and customers, if any; and the types of data breached. The Commission believes that these disclosures are sufficient to give the Commission and other Federal law enforcement agencies the information needed to determine appropriate next steps, such as, for example, conducting an investigation, determining and advising on how such a breach may be prevented in the future, and informing future rulemakings to protect consumers and businesses from harm. Carriers must update their initial breach notification report if: (1) the carrier learns that, in some material respect, the breach notification report initially submitted was incomplete or incorrect; or (2) additional information is acquired by or becomes known to the carrier after the submission of its initial breach notification report.

31. A number of carriers request changes to, or elimination of, certain fields contained in the notification. In its comments, CCA states that, while it ''does not take a position on the specific contents that should be included in all notifications to law enforcement, to the Commission, or to customers[,] . . . . [t]he detailed information currently reported to law enforcement for purposes of investigation and potential criminal charges is significantly broader than what is necessary and appropriate for the Commission's use. Indeed, over-reporting of such information outside the law enforcement context can introduce additional data-security risks and privacy concerns''. *See* CCA Comments at 7. The Commission notes that CCA does not provide further detail on ''what is necessary and appropriate'' in support of its argument or to aid its consideration. As discussed below, the Commission is unpersuaded by these arguments, and declines to alter the fields of information collected through the notification portal.

32. *Customer Billing Addresses.* ACA Connects, CTIA, and WTA request elimination of the requirement to include the billing addresses of affected customers in notifications. ACA Connects states that this reporting requirement has unclear investigative value, and its elimination would ''minimize the personal information reported to the Commission and law enforcement agencies.'' While the Commission acknowledges that Federal agencies have been directed to minimize the collection, use, storage, and disclosure of personal information to only that which is relevant and necessary to accomplish an authorized purpose, carriers are not in a position to know, in the absence of input from law enforcement agencies in this proceeding, which fields hold investigative value. Furthermore, because the portal was designed by law enforcement agencies themselves, the Commission must assume that their inclusion of this field reflects a determination that such information holds some investigative value. Finally, the Commission notes that the field is not currently marked as a required field. For this reason, the field does not present a reporting burden to carriers, but instead gives carriers an opportunity to provide Federal agencies more detail, should they wish to do so or find such detail relevant. WTA argues that ''billing names and addresses . . . are not classified as CPNI,'' and thus should be omitted from the form. The Commission's expansion of covered data to include information beyond CPNI renders this argument moot.

33. *Estimate of Financial Loss.* WTA argues that ''estimated financial loss'' is ''impossible to determine or predict with any degree of accuracy during the brief and chaotic period immediately following discovery of a data breach.'' The Commission declines to modify or remove this field. While it understands that estimating financial loss is a complex and context-specific calculation, the Commission emphasizes the critical importance of this data point in helping Federal agencies allocate their resources. Additionally, while carriers should strive to provide in their notifications as accurate a value as possible, the Commission notes that even a ballpark estimate or a range of quantities can help agencies determine an incident's priority for the purposes of opening or conducting investigations, and understand the magnitude of future risk posed by certain vulnerabilities.

34. *Other Fields.* CTIA identifies two fields which it argues are no longer necessary given the Commission's change to the reporting threshold for Federal-agency notifications, as discussed below. Specifically, CTIA requests that the Commission remove the fields regarding whether the breach ''resulted from a change of [a customer's] billing address'' or was based on ''a personal issue between two individuals.'' The Commission declines to do so. First, these fields are not marked as ''required'' on the form, and thus create no burden on reporting carriers that do not wish to complete them, while providing an opportunity for carriers to submit that information where applicable if they find it helpful or appropriate to do so. Second, under the Commission's revised rules, a breach stemming from a personal issue between two individuals or a change of a single customer's billing address may still trigger notification to Federal agencies. The reporting threshold only impacts the need to notify Federal agencies of breaches affecting fewer than 500 customers that do not implicate harm. As stated below, even small breaches may cause harm for the few customers affected by them. CTIA also requests elimination of the field that asks whether ''the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers'' before ''7 full business days have passed.'' CTIA argues that ''[r]emoving this field is consistent [with] the NPRM's proposal to eliminate the seven-business-day waiting period.'' The Commission agrees with this suggestion as its abrogation of the seven

business day waiting period rule will cause such a field to be unnecessary.

35. *Harmonizing Reporting Contents with CIRCIA.* In the *Data Breach Notice,* the Commission sought comment on whether it should require telecommunications carriers to report, at a minimum, the information required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) as part of their notifications to Federal agencies. While a few commenters support the alignment or harmonization of these data breach notifications with the requirements under CIRCIA, the Commission declines to take action in this regard at this early stage. CIRCIA directs the Cybersecurity and Infrastructure Security Agency (CISA) to publish a notice of proposed rulemaking implementing its notification provisions by March 15, 2024. The CISA must issue final rules no later than 18 months after the publication of the notice of proposed rulemaking. At the time of this Order, the CISA has not yet released the notice of proposed rulemaking. Therefore, the Commission finds it is too early to determine the precise contours of the final reporting requirements, and in the interest of preventing duplicative or inconsistent fields, and consistent with the approach advocated by ACA Connects, Blooston Rural Carriers, and CCA, the Commission will refrain from making additional changes based on CIRCIA and continue to monitor whether such changes may be required in the future.

36. The Commission does not find CTIA's comparison of its reporting trigger to that of the Critical Infrastructure Act of 2022 (CIRCIA) compelling. CIRCIA is concerned with the category of ''incidents.'' CIRCIA does not define ''breaches.'' But under Federal guidance to agencies, a breach is a specific type of incident—an incident that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition (etc.) of PII. And it would not be inconsistent for only some incidents to be reportable under CIRCIA but for all breaches to be reportable under the Commission's rules. For example, for Federal agencies, for an incident to qualify as a ''major incident'' it must be likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. But for a ''breach'' to qualify as a major incident, it can either satisfy that qualitative threshold, *or* it can involve the PII of 100,000 or more people. Thus, the individual privacy concerns implicated by a breach justify a broader reporting trigger.

37. The Commission also disagrees with CTIA's characterization of CIRCIA's incident reporting framework. CTIA argues that CIRCIA's reporting framework ''only applies—in a risk-based way—to 'covered cyber incidents,' which must be 'substantial' and do not include all incidents.' '' This argument misconstrues the statute. Section 2242(c)(2)(A) of CIRCIA sets a *minimum* on the types of ''substantial cyber incidents that constitute covered cyber incidents'' and implicitly allows the CISA to expand the definition beyond that in the course of its rulemaking. For example, one of those required minimums is to report ''cyber incident[s] that lead[ ] to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes.'' While a rulemaking implementing CIRCIA is still pending, the CISA may define ''loss of confidentiality'' to include data breaches. The Commission further notes that the two statutory exceptions to ''substantial cyber incidents that constitute covered cyber incidents'' are narrow, and likely would not prevent the CISA from adopting implementing regulations that broaden the scope of covered cyber incidents that trigger the statute's reporting obligations.

5. Other Issues

38. *Harm-based Trigger for Federal-Agency Notifications.* In the *Data Breach Notice,* the Commission sought comment on whether to forego requiring notification of a breach to customers or Federal agencies in those instances where a telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. While the Commission adopts such a harm-based notification trigger for breach notifications to customers generally, as discussed below, it declines to do so for Federal-agency notifications of breaches that meet or exceed the 500-affected-customer threshold described above. For breaches that do not meet its reporting threshold of at least 500 affected customers, the Commission do not require notification to Federal agencies via the central reporting facility in those instances where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. The Commission does not believe that the rationale for adopting a harm-based notification trigger for customer notifications applies in the Federal-agency context. Specifically, unlike customers, Federal agencies do not have the same vulnerability to notice fatigue, confusion, stress, or financial hardship that would cause the burdens they experience from additional reporting to outweigh the benefits. CTIA argues that by not extending the harm-based trigger to Federal-agency notifications, the Commission risks that notifications will ''inundate the Commission's breach reporting facility with information'' and the ''flood of information threatens to distract FCC and Law Enforcement staff from real and potentially harmful security threats.'' As an initial matter, the Commission notes that, as private entities, CTIA and its members lack any particular insight into, or expertise regarding, the administrative burdens affecting Federal agencies with respect to these rules. Contrary to CTIA's unsupported assertions, the agencies affected by these breach notification rules do not anticipate significant costs associated with the breach reporting requirements the Commission adopts today. While the Commission agrees that receiving notifications or reports of breaches that carriers have reasonably concluded do not trigger customer notification under the harm-based trigger will require the use of *some* resources by the Commission and law enforcement agencies, the Commission finds the value of enabling Federal agencies to identify patterns and insecurities and monitor all breaches of covered data outweigh the marginal costs of receiving notifications or reports for breaches that fall in this category. Additionally, as mentioned above, a report regarding a breach that does not result in harm to customers could nevertheless aid Federal agencies in identifying patterns and potential vulnerabilities and develop expertise across the industry. Commenters argue that the Commission should adopt a harm-based notification trigger for all Federal-agency notifications to avoid draining carrier resources. While commenters are correct that a general harm-based trigger would likely serve to reduce carriers' reporting burdens, so too would a reporting threshold. The Commission finds that its adoption of a reporting threshold is better tailored to reducing carriers' burdens in the Federal-agency-notification context while maintaining appropriate benefits of reporting. Commenters also argue that a harm-based notification trigger is necessary to reduce burdens on government resources. Even assuming, *arguendo,* that such burdens exist, they would likely be outweighed by the countervailing public interest in Federal

agencies receiving information concerning all breaches for investigative or trend analysis purposes. The Commission's threshold trigger ensures that Federal agencies receive breach information with the appropriate level of detail at the appropriate time given a breach's harmful impact or magnitude. the Commission's targeted application of a harm-based trigger to breaches affecting fewer than 500 customers ensures that Federal agencies are notified before customers and thereby have an opportunity to request a delay if necessary. This trigger also permits Federal agencies to investigate small breaches that are harmful sooner after the breach incident than in a carrier's annual report, as described above.

39. *Method of Notification.* In the *Data Breach Notice,* the Commission proposed to create and maintain a centralized portal for reporting breaches to the Commission and other Federal law enforcement agencies. After reviewing the record, the Commission instead requires carriers to use the existing data breach reporting facility for notifications to the Secret Service and FBI and delegate authority to the Bureau to coordinate with the Secret Service, the current administrator of the reporting facility, and the FBI, to the extent necessary, to ensure that the Commission will be notified when data breaches are reported and to implement the targeted modifications to the content of breach notifications that the Commission adopts today. The Commission's decision to require the same content and timing for notification to the Commission as for notification to the Secret Service and FBI supports the use of a single portal for notifying all three agencies. Consistent with the Secret Service's request, the Commission also delegates authority to the Bureau, working in conjunction with the Public Safety and Homeland Security Bureau and the Office of Managing Director, to collaborate with the Secret Service to explore the possibility of the Commission assuming control and responsibility for the reporting facility in the future, and to transition control of the facility to the Commission should the Bureau and Secret Service agree that such a transition is desirable.

40. Commenters widely supported the use of a single portal for all Federal-agency notifications. ACA Connects argues that using the preexisting portal for Commission notification will save government resources that would otherwise be spent developing a redundant portal. NCTA also advocates for the use of the preexisting portal, noting that the portal ''works well for service providers.'' The Commission agrees with commenters' analysis and thus requires carriers to submit their breach notifications to the Commission and other Federal law enforcement agencies through the existing portal. The Commission disagrees with John Staurulakis' suggestion that the Commission should instead require carriers to maintain a summary of inadvertent breaches for inclusion in their annual CPNI certification. The Commission finds that this approach would significantly delay notification of such breaches to Federal agencies, preventing law enforcement from acting quickly to investigate inadvertent breaches that may have widespread, harmful impact on customers.

C. Customer Notification

1. Harm-Based Notification Trigger

41. The Commission adopts a harm-based trigger for notification of breaches to customers so that they may focus their time, effort, and financial resources on the most important and potentially harmful incidents. The Commission agrees with commenters that adopting a harm-based trigger serves the public interest by protecting customers from over-notification and notice fatigue, specifically in instances where the carrier has reasonably determined that no harm is likely to occur. As the Commission recognized in the *Data Breach Notice,* it is not only distressing, but time consuming and expensive, to deal with a data breach, costing customers time, effort, and financial difficulty to change their passwords, purchase fraud alerts or credit monitoring, and freeze their credit in instances where the breach is not reasonably likely to result in any harm. Therefore the Commission finds that adopting a harm-based notification trigger, along with the expanded definition of breach, will ensure that customers are made aware of potentially harmful instances of breach, whether intentional or not, while preventing unnecessary financial and emotional difficulty in no-harm situations. The Commission agrees with those commenters that argue that the risk of notice fatigue to customers is important in light of its decision to expand the definition of breach. The Commission's adoption of the harm-based notification trigger will ensure that customer notification is focused on the incidents which are likely to cause harm, whether the incident was the result of intentional or inadvertent conduct. A harm-based trigger for notification to customers also allows carriers, particularly small and rural providers, to focus their resources on data security and mitigating any harms caused by breaches rather than generating notifications where harm was unlikely. The Commission's decision to adopt a harm-based notification trigger is also consistent with the majority of State laws, which generally do not require covered entities to notify customers of breaches when a determination is made that the breach is unlikely to result in harm.

42. While the record overwhelmingly supports the adoption of a harm-based notification trigger, some commenters worry that such a framework could result in legal ambiguity or lead to underreporting of breaches. The Commission takes several actions to mitigate these concerns. First, the Commission clarifies that where a carrier is unable to make a reasonable determination of whether or not harm to customers is likely, the obligation to notify customers remains. In making this determination, the Commission does not require carriers to consult Federal law enforcement or the Commission, as suggested by some commenters. Rather, carriers must determine using the factors outlined below whether harm to customers is likely to occur. If a provider concludes that harm to customers was unlikely and therefore customer notification was not required, but the Commission finds that conclusion to be unreasonable, the Commission will notify the provider. Stated differently, the Commission establishes a rebuttable presumption of harm and require carriers to notify customers of a breach in situations where the carrier is unable to reasonably determine that harm is reasonably unlikely to occur. ACA Connects argues that the Commission should decline to establish a rebuttable presumption of consumer harm because having to make filings in the interest of overcoming such a presumption would be burdensome for small providers. However, the Commission does not require any such filing. Rather, carriers must determine, based on the specific facts of a breach, whether consumer harm is reasonably unlikely to occur. The Commission provides further guidance to carriers on what constitutes harm to consumers below. The Commission rejects NCTA's proposal to limit the rebuttable presumption of harm to ''instances where the breach involves a risk of tangible, financial harm, identity theft or theft of service.'' NCTA's list is underinclusive in that it omits other harms that are significant. Nor does the record enable the Commission to readily draw a line that

separates the risks of some harms from others. The Commission clarifies that carriers do not need to disprove the potential for each type of harm in every instance to overcome the presumption, but must rather come to a reasonable fact-specific conclusion that, when considering all of the factors as a whole, harm is unlikely to occur. Second, as discussed above, the Commission declines to adopt a harm-based trigger for notification to Federal law enforcement agencies and the Commission for breaches affecting 500 or more customers. As such, carriers are required to provide notification for *all* incidents which meet the expanded definition of data breach and this affected-customer threshold to Federal law enforcement agencies and to the Commission. ACA Connects comments that the harm-based trigger should apply not only to customer breach notifications, but to Federal-agency notifications as well. The Commission disagrees. As ACA Connects notes, Federal agencies are not prone to notice fatigue in the same way that consumers are. Additionally, as discussed above, notifying Federal agencies of all breaches allows the Commission and law enforcement agencies to identify patterns and potential vulnerabilities and develop expertise across the industry, thereby enabling them to respond in appropriate and targeted ways. Moreover, under the rules the Commission adopts today, breaches falling below this threshold must be compiled and reported to Federal agencies annually. The Commission believes that this will serve as a backstop to any potential underreporting to customers, as the Federal agencies will have an opportunity to act even in instances where the provider may have concluded that harm to the consumer was unlikely.

43. *Evaluating Harm to Customers.* To the extent that a provider has evidence of actual harm to customers, notification is required and the harm-based analysis is conclusive. In instances where there is no definitive evidence of actual harm, as suggested in the *Data Breach Notice,* the Commission identifies a set of factors that telecommunications carriers should consider when evaluating whether harm to customers is reasonably likely. WISPA and ACA Connects support the Commission adopting a set of factors to help guide providers in determining whether harm to consumers is reasonably likely. The Commission believes that establishing a set of guidelines and recommendations strikes the right balance between preventing ambiguity, versus adopting a rigid definition which is too inflexible. The Commission believes that identifying these factors will promote consistency and further remedy concerns about ambiguity.

44. The Commission finds that ''harm'' to customers could include, but is not limited to: financial harm, physical harm, identity theft, theft of services, potential for blackmail, the disclosure of private facts, the disclosure of contact information for victims of abuse, and other similar types of dangers. Some parties raise administrability concerns about including harms such as ''disclosure of private facts'' on the theory that they are too speculative for providers. Beyond this bare assertion, these parties do not meaningfully explain what administrability problems would arise in practice. Additionally, they fail to account for the fact that providers only need make a *reasonable* determination of whether or not harm to customers is likely. Thus, even assuming *arguendo* that particular harms are challenging to evaluate in particular circumstances, a provider is not held to a standard of perfection, and any inherent challenges can be accounted for when evaluating the reasonableness of a given determination. The Commission's broad approach to the privacy harms that merit customer notice has ample legal support. First, OMB has noted that ''types of harms'' that individuals affected by a breach can experience have evolved: ''Identity theft can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and, in rare cases, risks to public safety.'' While OMB was specifically describing harms arising from an identity theft, the fact that those harms go beyond financial supports the Commission's conclusion that other types of harm should be considered when assessing the risk of harm from a breach. Second, the Commission's approach finds support from case law—*e.g.,* decisions holding that reputational harm can confer Article III standing. And third, the Commission's approach better reflects consumer expectations than a more cabined-approach to harm: Privacy harms that merit individual notice should be linked to those harms that individuals' experience, not those that carriers can most easily identify.

45. The Commission finds that this broader conception of harm is consistent with previous Commission precedent, and disagrees with commenters arguing that ''harm'' should only include the risk of identity theft or financial harm. The limited types of harm suggested by these commenters is underinclusive in that it omits other harms that are significant, particularly in the aggregate. The Commission find thats adopting such a narrow definition of harm is not only inconsistent with the Commission's longstanding approach, but also could lead to underreporting of breaches, and disregards other important and potentially costly consequences of a breach to customers. The Commission believes that a tiered approach would be unnecessarily complicated for carriers to assess the various ''levels'' of harm. Nevertheless, many of the factors that Blooston Rural Carriers suggests as relevant to their proposed analysis (*i.e.,* financial harm, encryption, risk of identity theft) are consistent with the approach that the Commission adopts. While a broader definition of harm may be more difficult for carriers to apply in certain cases, the Commission believes that carriers will be fully capable of understanding when to comply with its disclosure requirements in light of the Commission's decision to adopt a rebuttable presumption of harm.

46. When assessing the likelihood of harm to customers, carriers should consider the following factors. Consistent with the *Data Breach Notice,* the Commission finds that no single factor on its own is sufficient to make a determination regarding harm to customers.

- *The sensitivity of the information (including in totality) which was breached.* For example, the disclosure of a phone number is less likely to create harm than if the number of calls to that phone number, the duration of those calls, the name of the caller, the content of the conversations, and/or other layers of information is also disclosed. This contextual approach to gauging the sensitivity of customer information is consistent with the definition of PII the Commission adopts above with respect to its breach notification rules, which considers whether information is disclosed in combination with other information which inherently increases the risk associated with the disclosure. Additionally, harm is more likely if financial information or sensitive personal information was included in the breach. Commenters agree that a breach implicating financial information is likely harmful. Some data elements are always considered sensitive, such as bank account numbers and Social Security Numbers. Other data elements (*e.g.,* Date of Birth) become sensitive when paired with another data element (*e.g.,* name, address, or phone number). And still other data elements may be sensitive in context (*e.g.,* data identifying a subscriber in a TRS

program, because confirmed participation may be sufficient to reveal an individual's hearing- or speech-related disability). Consistent with the approach the Commission takes in this order, carriers must consider each element and all of the elements taken together, in context, to determine whether sensitive information was revealed in a breach. The data's potential for reuse should also be considered. For example, if a password is compromised, it is possible that the information could be reused to attack other accounts. Finally, if information is not able to be changed, it is more sensitive than information that is changeable. For example, a customer could change their password for an account, but the customer is unable to change their social security number, for instance. NCTA proposes an alternative approach under which the rebuttable presumption of harm only would apply ''where specific types of data are compromised.'' But the Commission's framework already factors in the sensitivity of the data as part of the overall analysis of harm. And as indicated by its guidance for evaluating harm, the Commission finds multiple considerations should be evaluated collectively to accurately gauge the likelihood of consumer harm. Thus, the Commission finds that its approach already accounts for potential differences in the risk of harm associated with specific types of data, but does so more effectively than NCTA's proposal by calling for a consideration of the broader relevant context, as well.

- *The nature and duration of the breach.* For example, if the information was widely accessible online over a long period of time, harm is more likely than if the information was only briefly accessible to a limited number of individuals. Information on a portable USB flash drive which does not require any special skill or knowledge to access is more likely to cause harm than information on a secured back-up device which is password protected. Covered data that was exposed for an extended period of time is more likely to have been accessed or used to the detriment of customers than data that was only briefly exposed.
- *Mitigations.* How quickly the carrier discovered the breach, and whether it took actions to mitigate any potential harm to the customers, is also a factor.
- *Intentionality.* In the case of an individual or entity intentionally obtaining access to covered data, such as by using the practice of pretexting, unauthorized intrusion into a physical or virtual space, theft of a device, or other similar activities, harm is more likely to occur. Conversely, an accidental breach, such as that resulting from a misdirected email, accidentally losing a device with covered data stored on it, or other similar activities, is less likely to result in harm.

47. *Encryption Safe Harbor.* As requested by a number of parties, the Commission adopts a safe harbor under which customer notification is not required where a breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed. For the purposes of this safe harbor, the Commission defines encrypted data as covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security. The Commission agrees with commenters that the risk of harm to customers is significantly reduced when the data was encrypted, provided that the carrier has evidence that the encryption key has not been compromised. While EPIC recommends that the Commission not exempt breaches solely involving encrypted data from its breach notification rules, EPIC does nonetheless acknowledge that ''a typical breach of encrypted data may present a lower risk of harm to consumers'', though ''encrypted data can nevertheless be compromised if a third party obtains access to the requisite encryption keys or is able to identify and exploit an additional security vulnerability.'' The Commission agrees. For those reasons, encrypted data is only exempted from the customer breach notification requirement where the carrier has definitive evidence that the encryption key was not compromised. Additionally, whether data was encrypted or not is irrelevant to the Federal-government breach notification requirement. As such, carriers are still required to report *all* breaches of covered data, whether that data was encrypted or not, to the Commission and law enforcement agencies. As the Commission has previously explained, data regarding breaches, even breaches with little or no risk of consumer harm, can be helpful to assist Federal agencies to determine data security vulnerabilities and threat patterns. Stated differently, encryption does not exempt an incident from the Commission's definition of breach, but rather only limits the instances where notification to a customer may be necessary. The Commission also agrees with commenters that its decision to implement a notification exception for encrypted data will incentivize and encourage the use of encryption to the benefit of the public, and further the goal of harmonization with State and other laws. Several States have established an exception for encrypted data from their breach notification requirements so long as the key has not been compromised or also breached. Additionally, in recent amendments to the Gramm-Leach-Bliley Act's Safeguards Rule, the FTC exempted encrypted data from its notification requirement. To the extent that a threat actor appears to have circumvented encryption, however, the carrier should conduct a harm-based analysis as if the data was never encrypted.

2. Customer Notification Timeframe

48. Consistent with the Commission's proposal in the *Data Breach Notice,* the Commission requires telecommunications carriers to notify customers of covered data breaches without unreasonable delay after notification to Federal agencies. The Commission finds that the current framework, which imposes a mandatory seven business day waiting period, is out-of-step with current approaches regarding the urgency of notifying victims about breaches of their personal information, and that the public interest is better served by eliminating the waiting period and thereby increasing the speed at which customers can receive the important information contained in a notice. At the same time, the Commission recognizes the importance of law enforcement's ability to investigate a breach, and understands that in certain situations, notification of a breach may interfere with a criminal investigation or national security. Therefore, consistent with the Secret Service's request, the Commission will allow law enforcement to request an initial delay of up to 30 days in those specific circumstances where one is warranted. WISPA commented that the seven business day waiting period can be ''crucial for law enforcement to effectively investigate the breach.'' The Commission agrees that law enforcement requires an opportunity to investigate a breach, but does not find that a seven business day waiting period, applied to all breaches, is necessary. Under the framework that the Commission adopts today, law enforcement may request a delay when one would be useful, but in the many circumstances where a delay is not necessary, this rule will allow carriers to more promptly notify customers,

thereby empowering them to take action to mitigate any harms.

49. The Commission finds that the ''without unreasonable delay'' standard encourages carriers to promptly notify customers of covered data breaches while offering the flexibility to be responsive to the specifics of a situation. This approach is consistent with many existing data breach notification laws that require expedited notice but refrain from requiring a specific timeframe. As suggested by commenters, the ''without unreasonable delay'' standard could take into account factors such as the provider's size, as a small carrier may have limited resources and could require additional time to investigate a CPNI data breach than a larger carrier.

50. In order to ensure that carriers notify customers quickly even in complex situations, the Commission requires customer notification no later than 30 days after reasonable determination of a breach. While in many circumstances, the ''without unreasonable delay'' standard means that the customer will be notified in less than seven business days, the Commission notes that in some circumstances, this standard may lead to a longer waiting time than the previous seven days. For that reason, the Commission adopts the 30-day back-stop in order to prevent unnecessarily long delays, even in such instances as the one described by USTelecom, where the carrier is engaged in investigations of the incident. The 30-day maximum amount of time is consistent with many existing State laws. In the *Data Breach Notice,* the Commission also considered adopting an ''outside limit'' of 45 or 60 days after discovery of a breach. However, the Commission finds that 30 days offers providers enough flexibility while recognizing the urgency of notifying customers as quickly as possible and without unnecessary delays. Some commenters request that the Commission adopt a safe-harbor for customer notification after determination or discovery of a breach. The Commission declines to adopt such a safe harbor because the Commission encourages providers to notify customers as quickly as possible in each individual instance. However, the Commission does establish a requirement that carriers notify customers no later than 30 days after reasonable determination of a breach to provide a clear outer bound to the ''without unreasonable delay'' standard.

3. Other Issues

51. *Content of Customer Breach Notification.* Consistent with its current rules, the Commission declines to adopt specific minimum categories of information required in a customer breach notification. The Commission makes clear, however, that a notification must include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. While all 50 States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information, not all of those entities impose minimum content requirements for those notices. The Commission agrees with NTCA that adding requirements with the potential to differ from other customer notice requirements imposed by States or otherwise may create unnecessary burdens on carriers, particularly small ones, as well as confusion among customers. The Commission also finds persuasive arguments by commenters that specifying the required content of customer notifications beyond the basic standard described above would prevent carriers from having enough flexibility to craft notifications that are more responsive to, and appropriate for, the specific facts of a breach, the customers, and the carrier involved. The Commission finds this argument particularly persuasive as it relates to small and rural carriers. Finally, imposing minimum requirements may delay a carrier's ability to timely notify customers, as it may take time to gather all of the necessary details and information even where it would be in the customer's best interest to receive notification more quickly albeit with less detail.

52. Instead, the Commission adopts as recommendations the following categories of information in security breach notices to customers: (1) the estimated date of the breach; (2) a description of the customer information that was used, disclosed, or accessed; (3) information on how customers, including customers with disabilities, can contact the carrier to inquire about the breach; (4) information about how to contact the Commission, FTC, and any State regulatory agencies relevant to the customer and the service; (5) if the breach creates a risk of identity theft, information about national credit reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the carrier is offering to affected customers; and (6) what other steps customers should take to mitigate their risk based on the specific categories of information exposed in the breach. Beyond the basic standard set by its rules, the Commission agrees with commenters that adopting *guidance* (rather than *requirements*) fosters the goal of ensuring that the customer has access to pertinent information about a breach while affording carriers flexibility to tailor the contents of a customer notification to the specific circumstances at hand. The Commission also agrees with some commenters that carriers may not know, with certainty, the precise date of a breach. For that reason, the Commission has modified this requirement from its original proposal by suggesting the estimated date of the breach. Breaches which involve data such as a social security number, birth certificate, taxpayer identification number, bank account number, driver's license number, and other similar types of personally identifiable information unique to each person create the highest level of risk of identity theft. While breaches involving the types of data listed here should be considered to create a risk of identity theft for customers, this is not an exclusive list and should not be considered as such. There may be other types of data not listed here that, either alone or in conjunction with other data, may potentially create a risk of identity theft for customers.

53. The Commission believes that adopting recommendations will further the goals of consistently and sufficiently notifying customers of data breaches while maintaining some flexibility for carriers to tailor each notification to the specific facts and details of the breach. While some commenters such as EPIC suggest that the Commission should adopt minimum content requirements, the Commission believes that adopting recommendations furthers the same objective of ''inform[ing] the consumer of the risks they face but also equip[ping] the consumer with options for immediate steps to reduce the downstream harms that may result'' while also maintaining the flexibility that commenters overwhelmingly noted was important for effectively and quickly notifying customers.

54. *Method of Customer Breach Notification.* The Commission declines to specify at this time the method of customer breach notification, and instead allows the carriers to assess for themselves how to best notify their customers of a data breach incident. Generally, carriers have pre-established methods of communicating with their customers about other important matters related to their service, such as outages

and scheduled repairs. These methods may differ among carriers based on their size, their unique relationship with their customers, the types of customers impacted, and other factors. Therefore, the Commission finds that maintaining flexibility in the method of customer breach notification both reduces the burden on the carriers and prevents customer confusion that could arise if carriers were required to provide disclosures in a way that differed from how customers were used to receiving important information from their carriers.

D. TRS Breach Reporting

55. In 2013, the Commission adopted privacy rules applicable to telecommunications relay services (TRS) providers, to protect the CPNI of TRS users. In doing so, the Commission found that ''for TRS to be functionally equivalent to voice telephone services, consumers with disabilities who use TRS are entitled to have the same assurances of privacy as do consumers without disabilities for voice telephone services.'' The privacy rules for TRS include a breach notification rule that is equivalent to section 64.2011 in terms of the substantive protection afforded to TRS users.

56. To maintain functional equivalency, the Commission amends section 64.5111 so that it continues to provide equivalent privacy protection for TRS users in line with its amendments to section 64.2011. Thus, in this Order the Commission applies its breach notification and reporting obligations for TRS providers to covered data, including PII and CPNI. The Commission also expands the definition of ''breach'' in section 64.5111 to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a TRS provider, and such information is not used improperly or further disclosed. The Commission also requires TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable, and in no event later than seven business days, after reasonable determination of a breach, except in cases where a breach affects fewer than 500 individuals, and a provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. As with the Commission's breach reporting rules for telecommunications carriers, where a TRS provider is unable to reasonably determine that no harm to consumers is reasonably likely to occur as a result of the breach, it must promptly notify the relevant Federal agencies regardless of the size of the breach. Any breach affecting fewer than 500 individuals where there is no reasonable likelihood of harm to customers must be reported simultaneously to the Commission, Secret Service, and FBI in a single, consolidated annual filing. The Commission further revises its rules to require TRS providers to report breaches to the Commission, Secret Service, and FBI contemporaneously via the existing centralized portal that providers already use and with which they are familiar. In terms of the content of such notifications, the Commission mandates that notifications to the Commission, Secret Service, and FBI must, at a minimum, include: TRS provider address and contact information; a description of the breach incident; a description of the customer information that was used, disclosed, or accessed; the method of compromise; the date range of the incident and approximate number of customers affected; an estimate of the financial loss to providers and customers, if any; and the types of data breached. More specifically, the Commission clarifies that, if any data, whether partial or complete, on the contents of conversations is compromised as part of a breach—such as call transcripts—the compromise must be disclosed as part of the notification to the Commission, Secret Service, and FBI.

57. Regarding breach notifications furnished to TRS users, the Commission introduces a harm-based trigger and eliminate the requirement to notify TRS users of a breach in those instances where a TRS provider can reasonably determine that no harm to TRS users is reasonably likely to occur as a result of the breach. The Commission further revises its rules to eliminate the mandatory seven business day waiting period to notify TRS users and instead require TRS providers to notify TRS users of breaches without unreasonable delay after notification to law enforcement, and in no case later than 30 days after reasonable determination of a breach, unless law enforcement requests a longer delay. The Commission also recommends minimum categories of information for inclusion in TRS user notifications. Notifications shall be provided in formats that are accessible to individuals with disabilities.

58. As with its revisions to section 64.2011, the Commission finds that these changes will best protect and inform TRS users without resulting in overreporting or excessively burdening TRS providers or Federal agencies. These changes to Commission rules will also allow the Commission and its law enforcement partners to receive the information they require in a timely manner so that they can mitigate the harm and fallout of breaches while also taking action to deter future breaches.

1. Defining ''Breach''

59. In this section, the Commission applies its breach notification and reporting obligations for TRS providers to covered data, including PII and CPNI. The Commission also takes the opportunity to emphasize that covered data under the TRS data breach notification rule includes call content given the unique concerns that arise with respect to call content in the TRS context. And, the Commission expands the definition of ''breach'' in section 64.5111 to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a TRS provider, and such information is not used improperly or further disclosed.

60. *Covered Data.* Consistent with the provisions the Commission adopts above for carriers, the Commission applies its breach notification and reporting obligations for TRS providers to covered data, including PII and CPNI. The Commission does so for the reasons discussed above with respect to its breach notification and reporting obligations for carriers. In addition, as discussed below, section 225 of the Act directs the Commission to ensure that TRS are available to enable communication in a manner that is functionally equivalent to voice telephone services. The Commission has found that applying the privacy protections of the Commission's regulations to TRS users advances the functional equivalency of TRS. In order to ensure the functional equivalency of TRS, and to ensure that TRS users enjoy the same protections as customers of telecommunications carriers and interconnected VoIP providers, the Commission applies its TRS data breach obligations to the same scope of customer information, including both PII and CPNI. The Commission also incorporates, by reference, the scope of covered PII adopted above, for the same reasons as discussed above.

61. The Commission disagrees with Hamilton Relay that the ''assurances of privacy'' that TRS users can expect ''are limited to CPNI and should not be extended to other elements of personal information, including sensitive personal information.'' In the *Data Breach Notice,* the Commission

recognized that providers possess proprietary information of customers other than CPNI, which customers have an interest in protecting from public exposure. This interest is particularly acute in the case of TRS users. TRS providers have access to the contents of customers' conversations, and, as AARO notes, any potential disclosure of TRS conversation content is a ''grave privacy concern.'' While section 225 and the Commission's TRS rules generally prohibit TRS providers from disclosing the content of any relayed conversation and from keeping records of the content of any such conversation beyond the duration of the call, that prohibition is not sufficient to protect TRS users from risks that may arise from data breaches. For instance, if a breach were to expose transcripts of TRS calls that were in progress at the time of the breach, the breaching party could obtain conversation contents between a TRS user and medical professionals, romantic partners, family members, friends, or professional colleagues, and as such may include sensitive details, such as a user's medical history, disability status, financial situation, political views, relationship status and dynamics, and religious beliefs. The disclosure of such information could lead to serious consequences, including embarrassment, ostracization from family and friends, and extortion by the breaching party or others who have gained access to the information.

62. Indeed, information about call content is not commonly available to traditional voice service providers, and thus traditional voice service customers do not face the same privacy risks in this regard as TRS users. As a result, it is particularly important in the TRS context that the Commission emphasizes the need for breach notifications with respect to call content. CPNI, PII, and the contents of calls are non-exclusive, and potentially overlapping, categories of information. Consistent with the congressional directive that the Commission's TRS rules guard against the disclosure of call content, and to promote functional equivalence between TRS and traditional voice communications services, the Commission therefore makes explicit in the text of section 64.5111 of its rules that a breach involving call content implicates those notification requirements.

63. Just as with telecommunications carriers, the Commission believes that the unauthorized exposure of sensitive personal information that the provider has received from the customer or about the customer in connection with the customer relationship (*e.g.,* initiation, provision, or maintenance, of service) is reasonably likely to pose risk of customer harm. Accordingly, any unauthorized disclosure of such information warrants notification to the customer, the Commission, and other law enforcement. Consumers expect that they will be notified of substantial breaches that endanger their privacy, and businesses that handle sensitive personal information should expect to be obligated to report such breaches.

64. The Commission further disagrees with Hamilton Relay's assertion that its privacy authority does not extend to other elements of personal information beyond CPNI, or that doing so would be inconsistent with the plain language of the Act or result in duplicative or inconsistent requirements between Commission rules and State laws. The Commission does so for the reasons discussed above, and because of the principle of functional equivalency. By ensuring that the same data breach notification requirements the Commission applies to traditional telecommunications carriers also apply to TRS providers, the Commission advances the interest of ensuring that consumers can have the same expectations regarding services that they view as similar. Thus, the approach the Commission adopts not only reflects the practical expectations of consumers but also honors the intention of Congress. For example, as discussed in more detail below, Congress ratified the Commission's 2007 decision to extend section 222-based privacy protections for telecommunications service customers to the customers of interconnected VoIP providers. And ensuring equivalent protections for TRS subscribers advances Congress' directive to endeavor to ensure functionally equivalent service.

65. EPIC concurs with this approach. The Commission notes that covered data would include PII that a TRS provider collects to register a customer in the TRS User Registration Database in order to provide services. In November 2021 and March 2022 orders revoking the operating authority of certain telecommunications carriers, the Commission further stated that all communications service providers have ''a statutory responsibility to ensure the protection of customer information, including PII and CPNI.''

66. Because TRS providers have access to proprietary information of customers other than CPNI, and customers have an interest in protecting that information from public exposure, the Commission finds that TRS providers should be obligated to comply with the Commission's breach notification rule whenever customers' personally identifiable information is the subject of a breach, whether or not the information is CPNI.

67. *Inadvertent Access, Use, or Disclosure.* The Commission expands the definition of ''breach'' in section 64.5111 to include inadvertent access, use, or disclosure of covered data, except in those cases where such information is acquired in good faith by an employee or agent of a TRS provider, and such information is not used improperly or further disclosed. Section 64.5111(e) of the Commission's rules currently defines a breach more narrowly as occurring ''when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.'' As noted above, this construction was adopted in response to the practice of pretexting. As discussed above, in the years since, numerous data breaches have shown that the inadvertent exposure—as much as intentional exposure—of customer information can and does result in the loss and misuse of sensitive information by scammers, phishers, and other bad actors, and can thus trigger a need to inform the affected consumers so that they can take appropriate action to protect themselves and their sensitive information. Whether a breach was intentional may not be readily apparent, and continuing to require disclosure of only intentional breaches could thus lead to underreporting. It is moreover critical that the Commission and law enforcement be made aware of any unintentional access, use, or disclosure of covered data so that the Commission can investigate and advise TRS providers on how best to avoid future breaches and so that the Commission is prepared and ready to investigate if and when any of the affected information is accessed by malicious actors. Requiring notification for accidental breaches will encourage TRS providers to adopt stronger data security practices and will help the Commission and law enforcement to better identify and address systemic network vulnerabilities, consistent with the Commission's analysis above.

68. The record in this proceeding confirms the need for the Commission to expand the definition of ''breach'' in section 64.5111 to include inadvertent disclosures. As AARO note in their comments, the Commission must keep pace with evolving threats to consumer privacy, and ''adopt measures that can effectively counter increasingly complex and evolving breaches.'' AARO further agrees with the Commission's assessment that an intentionality

requirement would lead to legal ambiguity and underreporting. According to AARO and EPIC, the industry will ''continue to witness breaches unless companies that operate in this area'' are required or incentivized to ''make proper investments in their 'staff and procedures to safeguard the consumer data with which they have been entrusted.' '' The Commission agrees with these commenters that expanding the definition of ''breach'' in section 64.5111 to include inadvertent access, use, or disclosure of covered data will help provide this incentive. The only two commenters who opposed expanding the Commission's definition of ''breach'' in section 64.5111 to include inadvertent disclosures of customer information were Hamilton Relay and Sorenson, and both modified their opposition to state that they only opposed such an expansion *unless* accompanied by the introduction of a harm-based trigger for data breach notification. As the Commission adopts a harm-based trigger for data breach notifications to consumers below, there is no need to address these two comments further.

69. *Good-Faith Exception.* While the Commission expands the definition of ''breach'' in section 64.5111 to include inadvertent access, use, or disclosure of covered data, consistent with its approach to the carrier data breach rule, the Commission carves out an exception for a good-faith acquisition of covered data by an employee or agent of a TRS provider where such information is not used improperly or further disclosed. No commenters opposed this amendment to the Commission's rules for TRS providers. The Commission rejected more general criticisms of such a rule above. With only a handful of exceptions, the vast majority of State statutes include a similar provision excluding from the definition of ''breach'' a good-faith acquisition of covered data by an employee or agent of a company where such information is not improperly used or disclosed further, and the Commission sees no reason not to include such an exception in the TRS rule. This good-faith exception will help reduce overreporting and, by extension, will avoid worrying consumers unnecessarily.

2. Notifying the Commission and Other Federal Law Enforcement of Data Breaches

70. In this section, the Commission requires TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable, and in no event later than seven business days, after reasonable determination of a breach, except in those instances where a breach implicates fewer than 500 individuals and a TRS provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. Where a breach affects fewer than 500 individuals and the TRS provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, the Commission requires that providers report such breaches annually to the Commission, Secret Service, and FBI in a single, consolidated annual filing. The Commission also requires TRS providers to report breaches to the Commission, Secret Service, and FBI contemporaneously via the existing centralized portal maintained by the Secret Service, and implement mandatory minimum content requirements for notifications filed with the Commission and law enforcement.

71. *Notification to the Commission and Law Enforcement.* The Commission requires TRS providers to notify the Commission, in addition to the Secret Service, and the FBI, of breaches through the central reporting facility. The Commission will maintain a link to the reporting facility at *http://www.fcc.gov/eb/cpni* or a successor URL designated by the Bureau. This requirement is consistent with other Federal sector-specific laws, including HIPAA and the Health Breach Notification Rule, which require prompt notification to the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC), respectively.

72. As the Commission found when it adopted the current data breach rules, notifying law enforcement of breaches is consistent with the goal of protecting customers' personal data because it enables such agencies to investigate the breach, ''which could result in legal action against the perpetrators,'' thus ensuring that they do not continue to breach sensitive customer information. The Commission also anticipated that law enforcement investigations into how breaches occurred would enable law enforcement to advise providers and the Commission to take steps to anticipate and prevent future breaches of a similar nature. While this reasoning remains sound, in the years since the Commission's rules were adopted it has become apparent that large-scale security breaches need not be purposeful in order to be harmful. As discussed above, breaches that occur as a result of lax or inadequate data security practices and employee training can be just as devastating as those perpetrated by malicious actors. Notification to the Commission of breaches, including inadvertent breaches, will provide Commission staff with critical information regarding data security vulnerabilities, and will help to shed light on TRS providers' ongoing compliance with the Commission's data breach rules.

73. The record in this proceeding supports requiring TRS providers to notify the Commission, the Secret Service, and the FBI of breaches. EPIC agrees that a breach impacting TRS users requires notification to the Commission in addition to the impacted user(s), and no commenter opposed amending the Commission's rules to require notification to the Commission concurrently with the Secret Service and FBI in the specific context of TRS. The Commission rejected more general criticisms of such a rule above.

74. *Reporting Threshold.* The Commission requires providers to inform Federal agencies, via the central reporting facility, of all breaches, regardless of the number of customers affected or whether there is a reasonable risk of harm to customers. For breaches that affect 500 or more customers, or for which a TRS provider cannot determine how many customers are affected, the Commission requires providers to file individual, per-breach notifications as soon as practicable, but no later than seven business days after reasonable determination of a breach. As the Commission describes below, these notifications must include detailed information regarding the nature of the breach and its impact on affected customers. This same type of notification, and the seven business day timeframe for submission, will also be required in instances where the TRS provider has conclusively determined that a breach affects fewer than 500 customers unless the provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.

75. For breaches in which a TRS provider can reasonably determine that a breach affecting fewer than 500 customers is not reasonably likely to harm those customers, the Commission requires the provider to file an annual summary of such breaches with the Commission, Secret Service, and FBI via the central reporting facility, instead of a notification. TRS providers must submit, via the existing central reporting facility and no later than February 1, a consolidated summary of breaches that occurred over the course of the previous calendar year which affected fewer than 500 customers, and where the provider

could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. To ensure that TRS providers may be held accountable regarding their determinations of a breach's likelihood of harm and number of affected customers, the Commission requires providers to keep records of the bases of those determinations for two years. The Commission also notes that TRS providers may voluntarily file notification of such a breach in addition to, but not in place of, this annual summary filing. In circumstances where a TRS provider initially determines that contemporaneous breach notification to Federal agencies is not required under these provisions, but later discovers information that would require such notice, the Commission clarifies that a TRS provider must report the breach to Federal agencies as soon as practicable, but no later than seven business days after their discovery of this new information. The Commission delegates authority to the Bureau to coordinate with the Secret Service regarding any modification to the portal that may be necessary to permit the filing of this annual summary. The Commission also delegates authority to the Bureau, working in conjunction with the Public Safety and Homeland Security Bureau and the Disability Rights Office, and based on the record of this proceeding—or any additional notice and comment that might be warranted—to determine the content and format requirements of this filing and directs the Bureau to release a public notice announcing these requirements. As above with respect to carriers, the Commission instructs the Bureau to minimize the burdens on TRS providers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. At a minimum, the Bureau should develop requirements that are less burdensome than what is required for individual breach submissions to the reporting facility, and consider streamlined ways for filers to report this summary information. The first annual report will be due the first February 1 after the Office of Management and Budget (OMB) approves the annual reporting requirement under the Paperwork Reduction Act. The first report should cover all breaches between the effective date of the annual reporting requirement and the remainder of the calendar year.

76. As the Commission determined above, this reporting threshold will enable the Commission to receive more granular information regarding larger breaches to aid its investigations while also being able to study trends in breach activity through reporting of smaller breaches in annual submissions. Such a reporting threshold is also consistent with many State statutes that require notice of breaches to State law enforcement authorities. Moreover, given the Commission's expansion of the definition of ''breach'' in today's Order to include inadvertent exposure of CPNI and other types of data, allowing TRS providers to file information regarding certain smaller breaches in a summary format on an annual basis will tailor administrative burdens on TRS providers to reflect those scenarios where reporting is most critical. At the same time, requiring TRS providers to report breaches that fall below the threshold in a single, consolidated annual filing will continue to enable the Commission and its Federal law enforcement partners to investigate, remediate, and deter smaller breaches. The Commission notes that no commenter addressed this potential amendment to its rule for TRS providers in response to the *Data Breach Notice,* and addresses more general comments in this regard in Section III.B.2, above. As above, in circumstances where a TRS provider initially determines that contemporaneous breach notification to Federal agencies is not required under these provisions, but later discovers information that would require such notice, the Commission clarifies that the TRS provider must report the breach to Federal agencies as soon as practicable, but no later than within seven business days of their discovery of this new information.

77. The Commission applies this threshold trigger only to notifications to Federal agencies, and not to customer notifications. Breaches affecting even just a few customers can pose just as much risk to those customers as could breaches with wider impact. For this reason, as discussed above, the Commission continues to require TRS providers to notify Federal agencies within seven business days of breaches that implicate a reasonable risk of customer harm, regardless of the number of customers affected. Doing so will permit Federal agencies to investigate smaller breaches where there is a risk of customer harm, and also allow law enforcement agencies to request customer notification delays where such notice would ''impede or compromise an ongoing or potential criminal investigation or national security,'' as specified in the Commission's rules.

78. *Timeframe.* The Commission retains its existing rule and require TRS providers to notify the Commission of a reportable breach contemporaneously with the Secret Service and FBI, as soon as practicable, and in no event later than seven business days, after reasonable determination of a breach. While the Commission proposed eliminating the seven business day deadline in the *Data Breach Notice,* the record received convinced the Commission that it should instead retain the more definite timeframe. The Commission agrees with AARO that the earlier TRS users are notified of breaches, the more time they will have to take actions to reduce the extent of the potential damage, and that eliminating the seven business day deadline would potentially extend the period between a breach and notification far beyond the current deadline, thus ''leaving consumers unable to remediate harms.'' The Commission finds that retaining the seven business day deadline properly balances the need to afford TRS providers sufficient time to conduct remediation efforts prior to submitting notifications with the need to ensure that customers receive timely notifications regarding breaches affecting their data. There is insufficient evidence that the current timeline is inadequate to accomplish the Commission's goals, and requiring breaches to be reported ''as soon as practicable'' without a definite timeframe could potentially be interpreted differently by different TRS providers or even by law enforcement and the Commission, thereby placing TRS providers at risk of inadvertently violating the Commission's rules should they construct ''as soon as practicable'' to mean something different than the Commission.

79. The Commission does not believe it is necessary to shorten the existing timeframe of seven business days. As Sorenson notes, businesses with any internet presence ''must routinely investigate large numbers of potential security events,'' and find that a shorter deadline would put tremendous pressure on providers to report all potential security incidents before having time to determine whether a breach is reasonably likely to have occurred. Such a result would distract providers from investigating and correcting any incident that may have occurred. As Sorenson notes, the current reporting timeline of seven business days allows providers a reasonable opportunity to investigate potential incidents and determine whether a breach is reasonably likely to have occurred.

80. The Commission disagrees with Hamilton Relay that the rigid structure

in its current rules is ''out of step'' with other data breach notification obligations and ''does not provide TRS providers with sufficient flexibility to address the different circumstances that surround data breaches.'' To begin, numerous States as well as HIPAA, the Health Breach Notification Rule, and CIRCIA impose a specific time limit on when breach notifications must be made to the State or relevant Federal agency. Furthermore, there is nothing in the record beyond Hamilton Relay's unsupported assertion to indicate that TRS providers find the current seven day business deadline to be unduly burdensome or inflexible. Indeed, Sorenson advocates in favor of retaining the current seven business day deadline. Even if the Commission were to assume the seven business day deadline to be a more burdensome or inflexible standard than a more open-ended standard, the Commission still finds that the countervailing interest in ensuring customers are notified quickly of breaches affecting them outweighs this hypothetical burden. As above, the Commission clarifies that a reasonable determination that a breach has occurred does not mean reaching a conclusion regarding every fact surrounding a data security incident that may constitute a breach. Rather, a TRS provider will be treated as having ''reasonabl[y] determin[ed]'' that a breach has occurred when the provider has information indicating that it is more likely than not that there was a breach.

81. *Content of Notification.* As currently structured, the existing central reporting facility requires TRS providers to report: information relevant to a breach, including TRS provider address and contact information; a description of the breach incident; the method of compromise; the date range of the incident and approximate number of customers affected; an estimate of the financial loss to providers and customers, if any; and the types of data breached. The record supports the imposition of minimum content requirements for breach notifications to the Commission, Secret Service, and FBI. Of the commenters who addressed this issue, only Hamilton Relay opposes minimum content requirements for TRS providers, and as their comments pertain specifically to the content of breach notifications to *customers,* the Commission addresses them below.

82. While the Commission finds that these existing content requirements are largely sufficient, it agrees with AARO that the nature of TRS and the sensitive information involved warrants more granular clarification regarding the required disclosures as part of notifications in that context. As AARO notes, TRS users face privacy risks that voice telephone service users do not face because TRS providers and their commercial partners collect particularly sensitive data about TRS users that could be accessed in a data breach. In particular, TRS providers and their partners have direct access to call audio, transcripts, and other data on the contents of TRS users' conversations. Given this, the Commission finds that providers must include a description of the customer information that was used, disclosed, or accessed as part of their notification, including whether data on the contents of conversations, such as call transcripts, are compromised as part of a breach. The Commission notes that the actual call audio or transcripts themselves *should not* be disclosed as part of the notification, as doing so would be a violation of the Commission's rules. Because of the unique nature of TRS technology, which often result in the creation of transcripts or similar artifacts, the Commission finds that clarifying these additional details of the disclosures will better protect consumers and better enable the Commission and its Federal law enforcement partners to investigate, remediate, and deter breaches.

83. *Method of Notification.* Under current Commission rules, TRS providers are required to notify the Secret Service and FBI ''through a central reporting facility'' to which the Commission maintains a link on its website. The Commission retains this requirement and revises it slightly to clarify that notifications filed through the existing central reporting facility will be transmitted to and accessible by the Disability Rights Office (DRO) of the Commission's Consumer and Governmental Affairs Bureau (CGB), in addition to the Secret Service and FBI. The Commission delegates authority to the Bureau, working in conjunction with CGB, to ensure that the central reporting facility sufficiently relays notifications to DRO. The Commission finds that retaining the existing central reporting facility, rather than creating and operating a new centralized reporting facility as contemplated in the *Data Breach Notice,* will be the simplest and most efficient approach, and will not result in the unnecessary expenditure of resources needed to build and operate a new electronic reporting facility when one already exists. It will also reduce potential provider confusion and simplify regulatory compliance by allowing providers to continue filing notifications through the existing reporting facility. The Commission notes that no commenter addressed this potential amendment to its rule governing TRS providers in response to the *Data Breach Notice,* and the Commission discusses more general comments regarding the method of disclosure to the Commission in Section III.B.5, above.

3. Customer Notification

84. In this section, the Commission introduces a harm-based trigger and eliminates the requirement to notify customers of a breach in any instance where a TRS provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. The Commission also eliminates the mandatory seven business day waiting period to notify customers and instead requires TRS providers to notify customers of breaches without unreasonable delay after notification to the Commission and law enforcement, and in no case later than 30 days after reasonable determination of the breach, unless law enforcement requests a longer delay. The Commission recommends minimum categories for information inclusion in customer notifications. The Commission declines to specify the method that notifications to customers must take, instead leaving such a determination to the discretion of TRS providers, except that such notifications must be accessible to TRS users.

85. *Harm-Based Notification Trigger.* The Commission's current TRS data breach rule requires notification to customers in every instance where a breach of their information has occurred, regardless of the risk of harm. The Commission modifies that standard and foregoes the requirement to notify customers of a breach in those instances where a TRS provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. In order to ensure the functional equivalency of TRS, and to ensure that TRS users enjoy the same protections as customers of telecommunications carriers and interconnected VoIP providers, the Commission adopts here the same definition of ''harm'' as that adopted above in the context of telecommunications carriers, for the reasons stated above.

86. In determining whether ''harm'' is likely to occur, providers should consider all the factors enumerated in the Commission's discussion above. In situations where call content—including call audio, transcripts, or other data on the contents of TRS users'

conversations—has been or has the potential to be disclosed as a result of a breach, a TRS provider must assume that harm has or is reasonably likely to occur, and the obligation to notify customers of a breach would remain. As with the rules the Commission adopts for telecommunications services above, where a TRS provider is unable to make a determination regarding harm, the obligation to notify customers of a breach would remain. For the reasons discussed above, and in order to ensure functional equivalency for TRS users, the Commission also adopts a safe harbor under which customer notification is not required where a breach solely involves encrypted data and the TRS provider has definitive evidence that the encryption key was not also accessed, used, or disclosed. To the extent that a threat actor appears to have circumvented encryption, however, the TRS provider should conduct a harm-based analysis as if the data was never encrypted.

87. The Commission finds that introducing a harm-based trigger for notifications to customers of TRS data breaches will benefit customers by avoiding confusion and ''notice fatigue'' with respect to breaches that are unlikely to cause harm. Given that it is not only emotionally distressing, but also time consuming and expensive to deal with the fallout of a data breach, the Commission believes that introducing a harm-based trigger will spare customers the time, effort, and financial strain of changing their passwords, purchasing fraud alerts or credit monitoring, and freezing their credit in the wake of any breach that is not reasonably likely to result in harm. A harm-based notification trigger also has a basis in the data breach notification frameworks employed by States, many of which do not require covered entities to notify customers of breaches when a determination has been made that the breach is unlikely to cause harm.

88. The Commission finds further that employing a harm-based notification trigger will not only benefit customers, but also assist TRS providers by allowing them to better focus their resources on improving data security and ameliorating the harms caused by data breaches rather than providing notifications to customers in instances where harm is unlikely to occur. Nor will the introduction of a harm-based trigger overburden providers by saddling them with the task of determining whether particular breaches are reasonably likely to cause harm. By making the standard for notification a rebuttable presumption of harm, providers must assume that harm is reasonably likely to occur as a result of a breach except where they can reasonably determine otherwise.

89. When determining whether a breach is reasonably likely to result in harm, TRS providers should consider the same factors laid out in the discussion above. In addition, in situations where call content—including call audio, transcripts, or other data on the contents of TRS users' conversations—has been or has the potential to be disclosed as a result of a breach, a TRS provider must assume that harm has or is reasonably likely to occur, and the obligation to notify customers of a breach would remain. TRS providers must construe ''harm'' in this context broadly. Even in those instances where no harm to customers is reasonably likely to occur, and thus the requirement to notify customers of a data breach is not triggered, TRS providers must still notify the Commission, Secret Service, and FBI of any such breach affecting 500 or more customers as soon as practicable and in any event no later than seven business days after reasonable determination of the breach via the central reporting facility. In the case of such breaches affecting fewer than 500 customers, they must be reported annually in a single, consolidated filing to the Commission, Secret Service, and FBI. While a harm-based trigger will help reduce customer notice fatigue and spare customers the time, effort, and financial strain of dealing with the fallout of a breach that is not reasonably likely to result in harm, the Commission and its law enforcement partners can still garner critical information regarding data security vulnerabilities by analyzing larger breaches, even those that are not reasonably likely to result in harm to customers.

90. The record generally supports the adoption of a harm-based trigger for TRS consumer breach notifications. AARO, however, argues that ''harm-based triggers should not be used in the context of TRS breach reporting to customers . . . because of the inherent privacy risks faced by TRS users.'' AARO goes on to argue that, because TRS involves the collection of data on the content of a user's conversation, the Commission should presume that any data breach of a TRS provider is harmful and require the disclosure of that breach to customers and law enforcement. While the Commission agrees that the Commission and law enforcement should be apprised of all breaches, it disagrees that customers must be made aware of breaches where no harm to customers is reasonably likely to result. While the Commission agrees that TRS users face heightened privacy risks because of the nature of the technology involved, such risk alone does not justify a requirement that customers receive notification of breaches in instances where a provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. TRS providers can and *must* take the heightened risks inherent to TRS users into account when determining whether harm is likely to result in the wake of a breach, and the Commission reiterates that providers must assume, in every case, that harm is reasonably likely to occur as a result of a breach *except* where they can reasonably determine otherwise. Moreover, the Commission reiterates that, in situations where call content—including call audio, transcripts, or other data on the contents of TRS users' conversations—has been or has the potential to be disclosed as a result of a breach, a TRS provider must assume that harm has or is reasonably likely to occur, and the obligation to notify customers of a breach would remain. The Commission agrees with AARO that, given the sensitive data at stake, ''it is conceivable that a TRS user would want to be aware of a data breach, even if the harm of that breach is not fully determined, so that they can take remedial measures,'' which is why the Commission imposes a rebuttable presumption of harm that requires notification in cases where the harm of a breach cannot be fully determined, or where call content has been or has the potential to be disclosed. The Commission finds that imposing a rebuttable presumption of harm, and requiring TRS providers to consider the heightened privacy risks experienced by TRS users when attempting to rebut this presumption, sufficiently addresses AARO's concerns without the need for mandatory consumer notifications that may result in notice fatigue and obligate consumers to expend time, effort, and resources dealing with the fallout of breaches that are not reasonably likely to result in harm.

91. The Commission agrees with Sorenson that, without a harm-based trigger, these rules could result in over-notification regarding non-critical security events without any corresponding benefit to consumers. The Commission also agrees with Hamilton Relay that such over-notification could very well result in notice fatigue and consumer indifference, which would perversely cause consumers to ignore or discount notifications, leading to failure to take

action even in those instances where a breach is substantially likely to result in harm, and thus eliminating the main benefit of requiring consumer notifications. The Commission therefore concludes that a harm-based trigger strikes the correct balance between keeping TRS users adequately informed, and reducing over-notification and notice fatigue while reducing the attendant burdens on TRS providers.

92. The Commission disagrees with EPIC that a harm-based trigger will lead to ''legal ambiguity and underreporting,'' or that it will delay reporting ''as it may take time to assess whether the minimum threshold for reportable harm has been met.'' By adopting a rebuttable presumption of harm and requiring consumer notification except in those instances where a provider can reasonably determine that no harm to customers is reasonably likely to occur, the Commission does not think that underreporting is a likely risk, as customers will still be made aware of breaches where protective action from the consumer is required. While the Commission does not here include a specific definition of how or under what circumstances this presumption may be rebutted—finding that such an approach would be too prescriptive—the Commission nevertheless provides guidance for evaluating customer harm, as outlined above. And, as discussed below, the rules require notification to customers without unreasonable delay after notification to law enforcement, and in no case later than 30 days after reasonable determination of a breach unless law enforcement requests a longer delay.

93. *Notifying Customers of Data Breaches Without Unreasonable Delay.* The Commission's current TRS data breach rule prohibits TRS providers from notifying customers or disclosing a breach to the public until at least seven full business days after notification to the Secret Service and FBI. The Commission eliminates this mandatory waiting period and instead requires TRS providers to notify customers of CPNI breaches without unreasonable delay after notification to law enforcement, and in no case later than 30 days after reasonable determination of a breach, unless law enforcement requests a longer delay.

94. In adopting the current rule, the Commission concluded that once customers have been notified of a breach, it becomes public knowledge, ''thereby impeding law enforcement's ability to investigate the breach, identify the perpetrators, and determine how the breach occurred.'' The Commission found that ''immediate customer notification may compromise all the benefits of requiring carriers to notify law enforcement of CPNI breaches,'' and that a short delay was thus warranted.

95. As discussed above, given the sheer volume of personal data at risk, and the proliferation of malicious schemes designed to exploit that data, the Commission finds that the need to notify victims of breaches as soon as possible has grown exponentially in the years since these rules were adopted. The rules adopted in this Order will better serve the public interest by increasing the speed at which customers may receive the important information contained in a notification, except in those circumstances when law enforcement specifically requests otherwise. The Commission finds that a requirement to notify customers of data breaches without unreasonable delay after discovery of a breach and notification to law enforcement appropriately balances legitimate law enforcement needs with customers' need to take swift action to protect their information in the wake of a breach.

96. The revised rule is consistent with many existing data breach notification laws that require expedited notice but refrain from requiring a specific timeframe. While requiring notification to customers without unreasonable delay will increase the speed at which customers receive important information related to a breach, the Commission declines to adopt a specific timeframe, and finds that such an approach would be overly prescriptive. Because each data breach is different, providers must be given sufficient latitude to address each breach separately, in the manner best befitting the nature of the breach. Even so, the Commission finds it appropriate to impose an outside limit on when customers must be notified of a breach. Requiring providers to notify customers no later than 30 days after reasonable determination of a breach, unless a longer delay is requested by law enforcement, will allow TRS providers sufficient flexibility to deal with each breach on an individual basis while simultaneously installing a backstop to ensure that customers are not made unaware of a breach indefinitely.

97. This approach is generally consistent with HIPAA, which requires notification to individuals ''without unreasonable delay and in no case later than 60 calendar days after discovery of a breach,'' as well as the Health Breach Notification Rule, which requires notification to individuals ''without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.'' Additionally, many States impose an outside limit on when customers must be notified of a breach following discovery of said breach.

98. Consistent with the Commission's current rules implementing section 222, the rule adopted here will allow law enforcement to direct a TRS provider to delay customer notification for an initial period of up to 30 days if such notification would interfere with a criminal investigation or national security. The Commission finds that in those instances where a provider reasonably decides to consult with law enforcement, a short initial delay of no longer than 30 days pending such consultation is reasonable under the ''without unreasonable delay'' standard the Commission adopts for customer notification. The Commission notes that HIPAA, the GLBA, and the Health Breach Notification Rule all allow for a delay of customer notification if law enforcement determines notification to customers would ''impede a criminal investigation or cause damage to national security,'' but only if law enforcement officials request such a delay. More specifically, both HIPAA and the Health Breach Notification Rule allow for notification delays of up to 30 days if orally requested by law enforcement. Similarly, most, if not all, States permit delays in notifying affected customers for legitimate law enforcement reasons. The Commission finds that the rule it adopts here strikes the appropriate balance between the needs of law enforcement to have sufficient time to investigate criminal activity and the needs of customers to be notified of data breaches without unreasonable delay.

99. The record supports reconfiguring the Commission's rules in this manner. As Hamilton Relay notes, TRS providers require flexibility when addressing data breaches, and a standard requiring providers to notify customers of a breach as soon as practicable will allow TRS providers sufficient time to determine the nature of the incident, ''including what consumer data may be implicated, if any. And the Commission agrees with Sorenson that imposing a rigid timeline on providers without offering sufficient time to investigate runs the risk of placing ''tremendous pressure on providers to report all potential security incidents before having time to determine whether a breach is reasonably likely to have occurred,'' and that such a result would not only overload the Commission but ''also distract providers from investigating and correcting any incident that may have occurred.'' The

Commission finds that retaining the seven business day deadline for Federal-agency notifications will allow TRS providers a reasonable opportunity to investigate potential incidents, determine whether a breach is reasonably likely to have occurred, and report it to the Commission and its law enforcement partners, if necessary, while the elimination of the mandatory seven business day waiting period and imposition of a 30-day backstop will ensure that customers receive notification of any such breach in a timely fashion.

100. The Commission disagrees with AARO that the timeframe revisions it makes will result in unwarranted delays of notifications to customers. On the contrary, the Commission finds that the pairing of an unreasonable delay standard with the elimination of the mandatory seven business day waiting period between notification of law enforcement and notification of customers is more likely to result in consumers receiving notice of a breach more quickly than they would under the Commission's current rule in many instances. By requiring TRS providers to issue consumer notifications without unreasonable delay, but in no case later than 30 days after a breach has been detected unless a longer delay is requested by law enforcement, the Commission believes that the revised rule balances the needs of law enforcement and TRS providers—to respond flexibly, with sufficient time to investigate data breaches—and customers—to take swift action in the wake of a breach.

101. *Content of Customer Breach Notification.* Consistent with the Commission's current TRS data breach rule, the Commission declines to adopt specific minimum categories of information required in a customer breach notification. The Commission makes clear, however, that a notification must include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. While all 50 States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information, of these, less than half impose minimum content requirements on the notifications that must be transmitted to affected individuals in the wake of a data breach. As noted above regarding carriers, adding requirements with the potential to differ from such a high number of State requirements may create unnecessary burdens on small TRS providers. The Commission also finds that specifying the required content of customer notifications beyond the basic standard described above would inhibit TRS providers from having the flexibility to craft notifications that are more responsive to, and appropriate for, the specific facts of a breach, the customers, and the provider involved. A stricter standard could conflict with other customer notice requirements—thus burdening providers and potentially sowing confusion among consumers—and could delay providers' ability to timely notify their customers of a breach, since it could take time to gather all of the necessary details and information even in cases where it would be in customers' best interests to receive notification more quickly, albeit with less detail.

102. Instead, the Commission adopts as recommendations the following categories of information in security breach notifications to TRS customers: (1) the date of the breach; (2) a description of the customer information that was used, disclosed, or accessed; (3) whether data on the contents of conversations, such as call transcripts, was compromised as part of the breach; (4) information on how customers can contact the provider to inquire about the breach; (5) information about how to contact the Commission, FTC, and any State regulatory agencies relevant to the customer and the service; (6) if the breach creates a risk of identity theft, information about national credit reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the provider is offering to affected customers (Breaches which involve data such as a social security number, birth certificate, taxpayer identification number, bank account number, driver's license number, and other similar types of personally identifiable information unique to each person create the highest level of risk of identity theft. While breaches involving the types of data listed here should be considered to create a risk of identity theft for customers, this is not an exclusive list and should not be considered as such. There may be other types of data not listed here that, either alone or in conjunction with other data, may potentially create a risk of identity theft for customers.); and (7) what other steps customers should take to mitigate their risk based on the specific categories of information exposed in the breach.

103. The Commission finds that adopting recommendations for minimum consistent fields of information will further the goal of assisting customers in better understanding the circumstances and nature of a breach while retaining some flexibility for TRS providers to precisely tailor each notification, depending on the specific facts and details of each breach. The Commission agrees with Hamilton Relay that the Commission should give providers the flexibility to craft breach notifications that include relevant information in an accessible format, depending on the circumstances of each breach. While the Commission acknowledges arguments by AARO and EPIC supporting the imposition of minimum content requirements for customer breach notifications, the Commission is wary of imposing specific requirements that could conflict with many State regulations, and of attempting to impose a one-size-fits-all solution for all providers and all data breaches. Rather, the Commission finds that the seven categories of information recommended in this Order appropriately balance the goal of empowering consumers to take the necessary steps to protect themselves and their information in the wake of a data breach while simultaneously enabling TRS providers to respond flexibly to data breaches as they occur, and to issue customer notifications as swiftly as possible without the need to delay as they gather all of the information needed to satisfy a rigidly prescribed set of predetermined informational categories.

104. *Method of Customer Breach Notification.* The Commission declines to specify the form that notifications to customers must take, instead leaving such a determination to the discretion of TRS providers, except to require that such notifications be provided in a format accessible to individuals with disabilities. In this proceeding, commenters were uniform in their insistence that the method of customer breach notification be left to the discretion of providers where it is not specified in State law. As CCA notes, the ''best means for reaching business customers and residential customers . . . can differ significantly, and carriers are best positioned based on their experience and contact with consumers to know customers' preferred way of receiving notifications.'' CTIA argues further that mandating the manner of customer CPNI incident notifications could ''reduc[e] carrier flexibility to provide the most up-to-date information to customers in fluid situations.'' As

Hamilton Relay points out, ''TRS providers do not have standard billing information for their customers because . . . most if not all TRS users do not pay for the service.'' Because this lack of standard billing information may complicate notifications to such users, the Commission agrees with Hamilton Relay that the Commission should grant TRS providers the discretion to take all reasonable steps necessary to provide the required information to their customers in a ''usable and readily understandable format'' whenever a breach occurs. The Commission thus declines to specify the manner that accessible notifications to customers must take, and leaves such a determination to the discretion of TRS providers where the manner of customer breach notifications is not specified by applicable State law.

105. *TRS User Registration Information.* In their comments, Sorenson notes that ''TRS customers must undergo intrusive identity and address verification that other voice telephone customers do not,'' and that data retention requirements of TRS providers put customers who rely on these critical services at heightened risk. Sorenson thus recommends that the Commission's revised rules permit TRS providers to delete sensitive customer information, such as copies of users' driver's licenses/passports and other identity or address identifying information. Convo Communications take this recommendation a step further, advocating that the Commission not just permit but *require* providers to destroy identifying records regarding TRS users after a user is successfully registered in the TRS User Registration Database (TRS URD).

106. The Commission declines to adopt these recommendations at this time. The requirements to collect and retain user registration information for registration in the TRS User Registration Database are outside the scope of this proceeding. The TRS User Registration Database is a centralized system of registration records established to protect the TRS Fund from waste, fraud, and abuse and to improve the Commission's ability to manage and oversee the TRS program. A necessary component of the administration and oversight of the TRS User Registration Database and the TRS program in general, is the ability of the Commission, the TRS User Registration Database administrator, and the TRS Fund administrator to review and audit the registration information of TRS users and the registration practices of TRS providers. Any consideration of changes to the rules concerning TRS providers retaining required registration information for TRS users must include an assessment of the impact of the ability of the Commission and relevant administrators to review the data upon which users were verified in the database. The record in this proceeding is incomplete as the Commission did not seek comment on this issue. The Commission therefore does not take action on this issue at this time.

E. Legal Authority

107. The Commission finds that sections 201(b), 222, 225, and 251(e) provide the Commission with authority to adopt the breach notification rules enumerated in this Order. The Commission concludes further that it has authority to apply these revised rules to interconnected VoIP providers. Lastly, the Commission finds that Congress' nullification of the Commission's revisions to its data breach rules in the *2016 Privacy Order* pursuant to the Congressional Review Act (CRA) does not now preclude the Commission from adopting the rules set forth in this Order.

1. Section 222

108. Section 222 of the Act provides authority for the requirements the Commission adopts and revises today. Section 222(a) imposes a duty on carriers to ''protect the confidentiality of proprietary information of, and relating to'' customers, fellow carriers, and equipment manufacturers. Section 222(c) imposes more specific requirements on carriers as to the protection and confidentiality of customer proprietary network information. Both subsections independently provide the Commission authority to adopt rules requiring telecommunications carriers and interconnected VoIP providers to address breaches of customer information, but the breadth of section 222(a) provides the additional clarity that the Commission's breach reporting rules can and must apply to all PII rather than just to CPNI.

109. The Commission has long required carriers to report data breaches as part of their duty to protect the confidentiality of customers' information. The revisions to the Commission's data breach reporting rules adopted in this Order reinforce carriers' duty to protect the confidentiality of their customers' information, including information that may not fit the statutory definition of CPNI. Data breach reporting requirements also reinforce the Commission's other rules addressing the protection of customer information by meaningfully informing customer decisions regarding whether to give, withhold, or retract their approval for carriers to use or disclose their information. Moreover, requiring carriers to notify the Commission in the event of a data breach will better enable the Commission to identify and confront systemic network vulnerabilities and help investigate and advise carriers on how best to avoid future breaches, while simultaneously assisting carriers in fulfilling their duty pursuant to section 222(a) to protect the confidentiality of their customers' information.

110. The Commission rejects Lincoln Network's argument that section 222 does not grant the Commission authority to adopt rules requiring telecommunications carriers and interconnected VoIP providers to address breaches of covered data. Section 222 explicitly imposes a duty on telecommunications carriers to ''protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers.'' To argue, as Lincoln Network does, that section 222 does not grant the Commission ''clear authority to protect the security of data'' contravenes the clear language and intent of section 222. Ever since it began implementation of the 1996 Act, the Commission has understood section 222(a) as a source of carriers' duties and as a source of Commission rulemaking authority. To the extent that the Commission has described its section 222 authority as coextensive with the definition of CPNI, the Commission disavows such an interpretation. In those proceedings, the Commission was not examining the distinction between CPNI and other sensitive personal information, and it never explicitly decided that section 222(a) does not reach other forms of personal information. In fact, the Commission in 2007 described section 222(a)'s duty as extending to ''proprietary or personal customer information,'' and more recent enforcement actions have affirmed that carriers' duty to protect customer information extends beyond CPNI. As noted below, the general interpretation of section 222 in the *TerraCom NAL* also was confirmed by the Commission in a subsequent rulemaking order. And as noted above, in November 2021 and March 2022 orders revoking the operating authority of certain telecommunications carriers, the Commission further stated that all communications service providers have ''a statutory responsibility to ensure the protection of customer information,

including PII and CPNI.'' To find that carriers have no duty to protect the confidentiality of non-CPNI PII would be inconsistent with the plain language of section 222(a)'s use of the term ''proprietary information of, and relating to, . . . customers'' and is not the best interpretation of that provision. Instead, consistent with those recent Commission actions, the Commission finds that the phrase ''information of, and relating to, . . . customers'' in section 222(a) is naturally—and indeed best—interpreted to have the same definition as PII, subject to the additional limitation that the information be ''proprietary'' to the carrier—*i.e.,* obtained in connection with establishing or maintaining a communications service. NCTA asserts that ''most PII . . . is not 'proprietary information,'' but does not justify why the Commission should adopt an understanding of that term different than the one here. Finally, given the larger context discussed below, to the extent that an obligation to take reasonable measures to protect all PII were not derived directly from section 222(a), that would be because Congress understood it already to be based in section 201(b)'s prohibition on unjust or unreasonable practices.

111. Some commenters contend that section 222(a) simply sets out high-level principles the substantive details of which are specified elsewhere. The Commission rejects NCTA's claim that ''legislative history supports an interpretation of Section 222 that does not impose an affirmative obligation under Section 222(a), which shows that Congress deliberately chose not to use 'personally identifiable information' in Section 222.'' NCTA cites a statement from the conference report that '' 'the new section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI.''' But as even commenters opposed to the Commissin's interpretation of section 222(a) recognize, section 222 applies to more than just CPNI, undercutting any understanding of that statement as reflecting the full scope and contours of section 222. NCTA also cites a House Report discussing earlier statutory language considered by the House, which would have specified a different scope of covered information. But that alternative definition also was part of a statutory provision that different in many other ways from section 222 as ultimately adopted, *see* July 24, 1995 House Rep., at 22–23, and section 222 as enacted ultimately was based on the Senate version. In sum, the Commission sees nothing in the legislative history that would persuade it to depart from what it sees as the best interpretation of section 222(a) based on the statutory text. But even beyond the foregoing analysis, that interpretation of section 222(a) is at odds with the fact that section 222(a) lists ''equipment manufacturers'' among the classes of entities owed confidentiality protections as part of a carrier's ''general'' duty. Given that section 222 never otherwise mentions confidentiality protections owed to those entities, this reinforces the Commission's view that section 222(a) is best read as imposing enforceable obligations on telecommunications carriers separate and apart from the requirements of section 222(b) and (c). Admittedly, as CTIA points out, *see* CTIA Comments at 12, section 273(d)(2) separately prohibits ''[a]ny entity which establishes standards for telecommunications equipment or customer premises equipment, or generic network requirements for such equipment, or certifies telecommunications equipment or customer premises equipment . . . from releasing or otherwise using any proprietary information, designated as such by its owner, in its possession as a result of such activity, for any purpose other than purposes authorized in writing by the owner of such information.'' But CTIA fails to demonstrate that the entities that are the focus of section 222(a)—*i.e.,* telecommunications carriers—are fully subsumed by (or even substantially overlap with) the entities that are the focus of section 273(d)(2)—*e.g.,* entities that establish equipment standards or requirements or certify such equipment. The significant mismatch between sections 222(a) and 273(d)(2) thus gives the Commission no reason to question its understanding of section 222(a). Nor does section 222(a) otherwise include textual indicia at odds with the Commission's understanding. Section 222(a) employs regulatory terminology in imparting a general ''duty'' on telecommunications carriers. Section 222(a)'s heading of ''In General'' also is fully compatible with the Commission's understanding of that provision as imposing a general duty—in contrast to alternative headings such as ''Purpose'' or ''Preamble'' that would indicate that the ''duty'' announced by such a provision is merely precatory or a ''statement of purpose'' with no legal force of its own.

112. Contrary to some commenters' claims, the Commission's interpretation of section 222(a) also otherwise is compatible with the remainder of section 222. The Commission reads section 222(a) as imposing a broad duty that can and must be read in harmony with the more specific mandates set forth elsewhere in the statute. This understanding of section 222(a) also accords with the fact that the Commission generally has relied on a ''reasonableness'' standard when evaluating carriers' protection of information under section 222. Provisions such as sections 222(b) and (c) directly impose specific requirements on telecommunications carriers to address concerns that were particularly pressing at the time of section 222's enactment, which continue to control over the more general duty in section 222(a) to the extent of any overlap. The Commission's interpretation of section 222(a) thus preserves the role of each of these provisions within the section 222 framework. And given the more detailed statutory specification of carriers' requirements regarding CPNI in section 222, it is understandable the Congress made a point of establishing express exceptions from those requirements in section 222(d). Part of interpreting section 222(a) in harmony with section 222 as a whole includes interpreting it in harmony with section 222(d). Thus, the Commission does not interpret the grounds for disclosure authorized by section 222(d) as violating carriers' obligation to protect the confidentiality of proprietary information imposed by section 222(a). The Commission's analysis is the same regarding other provisions of section 222, such as the subscriber information disclosure requirements in section 222(e) and (g). Thus, the Commission does not interpret section 222(a) to impose obligations inconsistent with those disclosure requirements, either. Because the Commission reads section 222(a) in harmony with the remainder of section 222 there is no incompatibility in its approach. And the mere omission of section 222(a) from provisions like section 222(d), (e), and (g) would have been an oblique and indirect way of dictating an interpretation of section 222(a) that runs counter to its plain meaning: a reasonable person would not interpret ''a duty to protect the confidentiality'' of customer information as prohibiting its use for billing, for example, as is permitted by section 222(d)(1).

113. Lincoln Network attempts to draw a distinction between security and confidentiality that is unavailing. Lincoln Network itself appears to recognize that something that could be characterized as a ''security'' breach can

result in loss of confidentiality for data or information. Thus, even assuming *arguendo* that breaches of security and breaches of confidentiality are not coextensive, that would matter only if the Commission were attempting to act beyond the scope of section 222's statutory grant of authority with respect to confidentiality—which is not the case here. Based on relevant textual indicia, the Commission concludes that ''confidentiality'' within the meaning of section 222 encompasses impermissible access to, use of, and/or disclosure of covered information. Section 222(a) establishes carriers' ''duty to protect the confidentiality of proprietary information . . . .'' Section 222(b), in turn, is entitled ''[c]onfidentiality of carrier information,'' and limits carriers' ''use'' of proprietary information. Section 222(c) is entitled ''[c]onfidentiality of customer proprietary network information'' and limits how carriers ''use, disclose, or permit access to'' individually identifiable CPNI. ''Although section headings cannot limit the plain meaning of a statutory text, 'they supply cues' as to what Congress intended.'' Against that backdrop the Commission rejects Lincoln Network's attempts to rely on isolated examples of terminology uses from recent industry reports or the like. The Commission's data breach reporting requirements focus on ''breaches,'' which occur when ''a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data.'' The ''covered data'' is defined in terms of the statutory categories of proprietary information and customer proprietary network information, and the focus on access, use, and disclosure of those data fits comfortably within the Commission's section 222 authority.

2. Section 201(b)

114. Section 201(b) of the Act requires practices of common carriers to be just and reasonable and declares any unjust or unlawful practices to be unlawful. The Commission concluded in the *TerraCom NAL* that section 201(b) was violated when carriers failed to notify customers whose personal information had been breached by the carriers' inadequate data-security policies. The *TerraCom NAL* explicitly put carriers ''on notice that in the future [the Commission] fully intend[s] to assess forfeitures for such violations'' under section 201(b). As NCTA points out, the Commission did not propose a forfeiture under section 201(b), NCTA Reply at 10–11, but that was because it was the first time the Commission had declared a carrier's practices related to its failure to notify consumers of a data breach to be a violation of section 201(b). The Commission made explicit that, in the future, such violations would be penalized under section 201(b). The Commission now makes that clear again here. The Commission therefore concludes that its authority to prohibit unjust and unreasonable practices and to ''prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of'' the Act pursuant to section 201(b) provides independent authority for the Commission to consider PII as protected consumer information and to require carriers to notify customers, law enforcement, and the Commission about breaches as discussed throughout this Report and Order.

115. CTIA provides no explanation for its conclusory assertion that carriers' data privacy and security practices are not practices ''in connection with'' communications services. The Commission is no more persuaded by arguments that take a different tack and contend that the carrier actions at issue in this proceeding are not ''charges,'' ''practices,'' ''classifications,'' or ''regulations'' within the meaning of section 201(b). This argument relies on the theory that the Supreme Court has held ''that activity is not covered by Section 201(b) unless it '*resembles* activity that . . . transportation and communications agencies have long regulated.' '' But in that decision, the Supreme Court did not so hold; it merely considered that factor in support of its threshold determination that the activity at issue there ''easily fits within the language of the statutory phrase'' as understood ''in ordinary English.'' The Commission sees no reason why a carrier's privacy and data breach notification practices with respect to customer PII that it has by virtue of its service relationship with them would not easily fit within the ordinary understanding of that statutory phrase, as well. Independently, the Commission also observes that the Commission has, in fact, historically regulated carriers' privacy practices under its section 201(b) authority. Certainly any information collected from a customer or prospective customer related to establishing or maintaining the provision of a communications service would qualify. As discussed above, it is well established that carriers have come into possession of, and sometimes suffered breaches of, sensitive personal information that may not be CPNI. Nor does the canon of statutory construction about specific provisions governing general ones apply here. Section 222, adopted as part of the Telecommunications Act of 1996 (1996 Act), was not intended to narrow carriers' privacy duties or the Commission's authority to oversee carriers' privacy practices. The Commission rejects contrary arguments premised on the fact that section 222 does not itself include a savings clause expressly preserving the Commission's authority under section 201, in contrast to section 251 of the Act. The 1996 Act made clear that ''the amendments made by this Act shall not be construed to modify, impair, or supersede Federal, State, or local law unless expressly so provided in such Act or amendments.'' Nothing in section 222 expressly modifies, impairs, or supersedes the Commission's authority under section 201(b) to act to ensure that carriers' practices are just and reasonable. While it is not entirely clear why Congress felt the need for an additional savings clause in section 251(i), it might simply have done so ''to be doubly sure,'' *Barton* v. *Barr,* 140 S. Ct. 1442, 1453 (2020), particularly given the responsibilities assigned to the States in the implementation of sections 251 and 252 of the Act. Nor is the Commission persuaded by contrary claims based on high-level statements in legislative history about the balancing various interests underlying various legislative alternatives that eventually led to section 222 of the Act. *See, e.g.,* CTIA Dec. 6, 2023 *Ex Parte* at 5–6. Such high-level statements in legislative history do not persuade the Commission to depart from what it sees as the best interpretation of the statutory text. Nor is it even clear that the relevant balancing of interests in the cited legislative history necessarily is relevant to the particular exercise of section 201(b) authority at issue here. *See, e.g.,* H.R. Rep. No. 103–559, at 60 (June 24, 1994) (discussing the ''careful balance of competing, often conflicting, considerations'' of consumers' need ''to be sure that information about them that carriers can collect is not misused'' with consumers' expectation that ''the carrier's employee will have available all relevant information about their service,'' which ''argues for looser restrictions on internal use of customer information''). The Commission regulated carriers' privacy practices under its general Title II authority even before enactment of the 1996 Act, and the 1996 Act codified the privacy duty and enacted specific restrictions for the new competitive environment that the Act was intended to promote. In the course of rejecting a request that carriers be compelled to share customer

information with certain other carriers to protect against discrimination against competitors under sections 201(b) and 202(a) of the Act, the Commission stated that ''the specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a).'' Understood in context, that simply stands for the proposition that where consumer privacy issues addressed specifically in section 222 are implicated, the requirements of section 222 are controlling over more general protections in section 201(b) and 202(a) that are unrelated to privacy—such as advancing competitive neutrality. The Commission similarly rejects attempts to rely on statements about section 222 that the Commission made in analogous statutory contexts where it rejected pro-competition requirements under statutory provisions like sections 272 or 274 in light of the privacy requirements of section 222. More generally, to the extent that the Commission has made statements that its section 222 authority supersedes its authority under section 201(b), the Commission disavows such an interpretation for the reasons stated in this section. Independently, with particular respect to data breach notification requirements, the Commission does not find either section 201(b) or section 222 to be a more specific provision. And even assuming *arguendo* that section 222 were controlling within its self-described scope, the Commission's rules are fully consistent with that authority as well. As the Commission stated in 1998, ''Congress . . . enacted section 222 to prevent consumer privacy protections from being inadvertently swept away along with the prior limits on competition.'' For the reasons discussed throughout this Report and Order, notification to customers, law enforcement, and the Commission are essential to the Commission's oversight of carriers' privacy practices.

116. The structure of the Communications Act and its relationship with the Federal Trade Commission Act also demonstrate that this Commission has authority to make rules governing common carriers' protection of PII. The FTC has broad statutory authority to protect against ''unfair or deceptive'' acts or practices, but that authority is limited by carving out several exceptions for categories of entities subject to oversight by other regulatory agencies, one of which is common carriers subject to the Communications Act. The clear intent is that the expert agencies in those areas will act based on the authorities provided by those agencies' statutes. It is implausible that Congress would have exempted common carriers from any obligation to protect their customers' private information that is not CPNI. Insofar as some parties contend that section 222 establishes a comprehensive scheme of privacy regulation for carriers to the exclusion of section 201(b), yet also contest the Commission's interpretation of section 222(a), they effectively ask the Commission to accept that the supposedly comprehensive privacy scheme that Congress enacted intentionally left the non-CPNI PII of carriers' customers unprotected by Federal law. As discussed, the Commission not only finds that view contrary to the statutory text, but find it implausible more generally.

3. Interconnected VoIP

117. The Commission finds that section 222 and the Commission's ancillary jurisdiction grant the Commission authority to apply the rules it adopts here to interconnected VoIP providers. Interconnected VoIP providers have been explicitly subject to the Commission's data breach rules since 2007, when the Commission first adopted the data breach notification rule. In the *2007 CPNI Order,* the Commission recognized that if interconnected VoIP services were telecommunications services, they self-evidently would be covered by section 222 and the Commission's implementing rules. Although the Commission has not broadly addressed the statutory classification of interconnected VoIP as a general matter, it has consistently recognized that a provider may offer VoIP on a Title II basis if it voluntarily ''holds itself out as a telecommunications carrier and complies with appropriate Federal and State requirements.'' But because the Commission generally had not classified interconnected VoIP, the Commission also exercised its Title I ancillary jurisdiction to extend its CPNI rules to interconnected VoIP services, finding that ''interconnected VoIP services fall within the subject matter jurisdiction granted to [the Commission] in the Act,'' and that ''imposing CPNI obligations is reasonably ancillary to the effective performance of the Commission's various responsibilities.''

118. The Commission proceeds under the same alternative bases here, and concludes that legal and factual bases for the findings relied on in the *2007 CPNI Order* have only grown more persuasive since then. The Commission observed at the time that ''interconnected VoIP service 'is increasingly used to replace analog voice service.' '' This trend has continued. Interconnected VoIP now accounts for a far larger share of the residential fixed voice services market than legacy switched access services, and ''fixed switched access continues to decline while interconnected VoIP services continue to increase.'' Therefore, as the Commission found in 2007, today's consumers should reasonably expect ''that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VoIP provider, given that these services, from the perspective of a customer making an ordinary telephone call, are virtually indistinguishable.'' The Commission likewise thinks interconnected VoIP subscribers should reasonably expect their other information to also be protected and treated confidentially consistent with the other protections that apply under section 222. Furthermore, extending section 222's protections to interconnected VoIP service customers remains ''necessary to protect the privacy of wireline or wireless customers that place calls to or receive calls from interconnected VoIP customers.'' Indeed, following the *2007 CPNI Order,* Congress ratified the Commission's decision to apply section 222's requirements to interconnected VoIP services, adding language to section 222 that applied provisions of section 222 to users of ''IP-enabled voice service.'' These revisions to section 222 would not make sense if the privacy-related duties of subsections (a) and (c) did not apply to interconnected VoIP providers. The Commission notes that no commenter chose to address this issue in the course of this proceeding.

119. In the case of interconnected VoIP providers that have obtained direct access to telephone numbers, the Commission concludes that section 251(e) also gives the Commission authority to condition that access on those providers' compliance with privacy requirements equivalent to those that apply to telecommunications carriers. The Commission previously exercised its authority under section 251(e) to ensure, for example, that an interconnected VoIP provider receiving direct access to numbers ''possesses the financial, managerial, and technical expertise to provide reliable service.'' Ensuring that interconnected VoIP providers remain on the same regulatory footing as telecommunications carriers with respect to customer privacy—as was the case when direct access to numbers for interconnected VoIP providers began—will ensure a level

competitive playing field and ensure that consumers' expectations are met regarding the privacy of their information when using the telephone network.

4. Legal Authority To Adopt Rules for TRS

120. The Commission finds that it has separate and independent authority under sections 225 and 222 to amend its data breach rule for TRS to ensure that TRS users receive privacy protections equivalent to those enjoyed by users of telecommunications and VoIP services. Section 225 of the Act directs the Commission to ensure that TRS are available to enable communication in a manner that is functionally equivalent to voice telephone services. In the *2013 VRS Reform Order,* the Commission found that applying the privacy protections of the Commission's regulations to TRS users advances the functional equivalency of TRS. The Commission concluded further that the specific mandate of section 225 to establish ''functional requirements, guidelines, and operations procedures for TRS'' authorizes the Commission to make the privacy protections included in the Commission's data breach regulations applicable to TRS users.

121. The Commission also found that extending its privacy—including data breach—regulations to TRS users was ancillary to its responsibilities under section 222 of the Act to telecommunications service subscribers that place calls to or receive calls from TRS users, because TRS call records include call detail information concerning all calling and called parties. The Commission moreover determined that applying data breach requirements to point-to-point video services provided by VRS providers (such point-to-point services, while provided in association with VRS, are not themselves a form of TRS) is ancillary to its responsibilities under sections 222 and 225, including the need to protect information that VRS providers had by virtue of being a given customer's registered VRS provider—even in the context of point-to-point video service—and to guard against the risk to consumers who are likely to expect the same privacy protections when dealing with VRS providers, whether they are using VRS or point-to-point video services.

122. The Commission concludes that, for the same reasons cited in the *2013 VRS Reform Order,* these sources of authority for establishing the current data breach rule for TRS now authorize the Commission to amend this rule to ensure that TRS users continue to receive privacy protections equivalent to those enjoyed by users of telecommunications and VoIP services. The record in this proceeding supports this conclusion. As AARO states, the Commission has ''ample legal authority'' to amend its data breach rule for TRS under sections 222 and 225.

5. Impact of the Congressional Disapproval of the *2016 Privacy Order*

123. In 2016, the Commission attempted to revise its breach notification rules as part of a larger proceeding addressing privacy requirements for broadband internet service providers (ISPs). In 2015, the Commission classified broadband internet access service as a telecommunications service subject to Title II of the Act, a decision that the D.C. Circuit upheld in *U.S. Telecom Ass'n* v. *FCC,* 825 F.3d 674 (D.C. Cir. 2016). As a result of classifying broadband internet access service as a telecommunications service, such services were subject to sections 201 and 222 of the Act. The rules the Commission adopted in the *2016 Privacy Order* applied to telecommunications carriers and interconnected VoIP providers in addition to ISPs, which had been classified as providers of telecommunications services in 2015. In 2017, however, Congress nullified those 2016 revisions to the Commission's privacy rules under the CRA. Pursuant to the language of the Resolution of Disapproval, the *2016 Privacy Order* was rendered ''of no force or effect.'' That resolution conformed to the procedure set out in the CRA, which requires agencies to submit most rules to Congress before they can take effect and provides a mechanism for Congress to disapprove of such rules. Pursuant to the operation of the CRA, the *2016 Privacy Order* ''may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule.''

124. In analyzing the impact of the Resolution of Disapproval of the *2016 Privacy Order,* the Commission first explains its understanding of the CRA's prohibition on reissuance. The Commission also shows that, in any event, the revisions made here to the breach notification rule are different in substantial ways from those that were included in the *2016 Privacy Order.*

125. First, the Commission concludes that the CRA is best interpreted as prohibiting the Commission from reissuing the *2016 Privacy Order* in whole, or in substantially the same form, or from adopting another item that is substantially the same as the *2016 Privacy Order.* It does not prohibit the Commission from revising its breach notification rules in ways that are similar to, or even the same as, some of the revisions that were adopted in the *2016 Privacy Order,* unless the revisions adopted are the same, in substance, as the *2016 Privacy Order* as a whole. To be clear, although the CRA would permit the Commission to adopt a breach notification rule that is the same as the breach notification rule that was adopted by the *2016 Privacy Order,* the rule that the Commission adopts here has substantial differences. The Commission rejects arguments that there was insufficient notice for the Commission to adopt this interpretation of the effect of the CRA resolution of disapproval. In pertinent part, notice under the APA requires ''reference to the legal authority under which the rule is proposed'' and ''either the terms or substance of the proposed rule or a description of the subjects and issues involved.'' The *Data Breach Notice* described the proposal to adopt expanded data breach notification requirements pursuant to its statutory authority under sections 222, 225, and other possible sources of authority. In the course of this request for comment, the Commission sought specific comment regarding ''the effect and scope of the Congressional disapproval of the *2016 Privacy Order.*'' This satisfies the requirements of the APA. Even beyond that, however, the Commission's interpretation flows from ordinary tools of statutory interpretation, first and foremost by focusing on the relevant statutory text and context. Contrary to the suggestion of some, the Commission finds nothing ''novel'' about this interpretive approach, providing additional grounds to conclude that the notice and comment requirements of the APA were satisfied here.

126. Congress's Resolution of Disapproval, by its terms, disapproved ''the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 FR 87274 (December 2, 2016)).'' This referred to the *2016 Privacy Order* in its entirety, which was summarized in the cited **Federal Register** document. The statutory term ''rule,'' as used in the CRA, refers to ''the whole or a part of an agency statement of general or particular applicability and future effect

designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency.'' Thus, ''rule'' can and does refer to an entire decision that adopts rules. In implementing Congress's resolution of disapproval, the Commission treated the *2016 Privacy Order* as a single rule. In a ministerial order, the Commission ''simply recogniz[ed] the effect of the resolution of disapproval'' should be that ''the *2016 Privacy Order* 'shall be treated as though [it] had never taken effect.' '' As a result, all of the changes that the *2016 Privacy Order* made to the Commission rules codified in the Code of Federal Regulations were reversed, with the result that all of the Commission rules in part 64, subpart U, were restored to how they read prior to their amendment by the *2016 Privacy Order.* The term ''rule'' can also refer to parts of such a decision, or to various requirements as adopted or amended by such a decision. In the context of the CRA's bar on reissuance, the Commission must consider which rule is specified by that bar. The reissuance bar, 5 U.S.C. 801(b)(2), provides that ''a new rule that is substantially the same as such a rule may not be issued''—where ''such a rule'' refers to the rule specified in the joint resolution of disapproval as described in section 802. As shown above, the joint resolution referred to the entirety of the *2016 Privacy Order.* Therefore, the Commission concludes that the ''rule'' to which the reissuance bar applies is the entire *2016 Privacy Order* with all of the rule revisions adopted therein.

127. The Commission concludes that it would be erroneous to construe the resolution of disapproval as applying to anything other than all of the rule revisions, as a whole, adopted as part of the *2016 Privacy Order.* That resolution had the effect of nullifying each and every provision of the *2016 Privacy Order*—each of those parts being rules under the APA—but not ''the rule'' specified in the resolution of disapproval. By its terms, the CRA does not prohibit the adoption of a rule that is merely substantially similar to a limited portion of the disapproved rule or one that is the same as individual pieces of the disapproved rule. The Commission rejects arguments that because the CRA borrows from the APA's definition of ''rule'' as referring to the whole or a part of certain agency statements of general applicability and future effect, an agency cannot adopt a rule substantially similar to any part of an agency rulemaking decision that does not take effect due to a resolution of disapproval under the CRA. The key issue is not the definition of ''rule'' in the abstract, but the wording of 5 U.S.C. 801(b)(2) (along with the wording of the resolution of disapproval itself). And 5 U.S.C. 801(b)(2) is worded in singular terms—referring to ''*A rule* that does not take effect (or does not continue) under paragraph (1) . . . '' as opposed to saying ''*Any rule* that does not take effect (or does not continue) under paragraph (1) . . . '' or ''*Rules* that do not take effect (or do not continue) under paragraph (1) . . . .'' So even if there might be multiple APA rules that do not take effect as a result of a resolution of disapproval, the CRA's focus is on a singular ''rule'' that does not take effect. Since the whole *2016 Privacy Order* was the subject of the resolution of disapproval, and the whole *2016 Privacy Order* did not take effect as a result, the Commission concludes that the whole *2016 Privacy Order* is the relevant ''rule'' for purposes of 5 U.S.C. 801(b)(2). And although some commenters claim that the Commission's approach to interpreting the CRA could lead to uncertainty about what is subject to 5 U.S.C. 801(b)(2), they do not identify any actual ambiguity as the Commission's approach is applied here—instead, they seemingly just dislike the outcome. Nor is the Commission persuaded that Congress lacks the tools to address any concerns about the scope of a resolution of disapproval if any were to arise. For example, the record does not reveal why Congress could not specify the ''relating to'' criterion in the resolution of disapproval language required by 5 U.S.C. 802(a) in more granular or detailed ways. Independently, Congress also always remains free to enact laws outside the CRA process that reject agency rules with as much detail and precision as they wish should ambiguity concerns become a practical problem.

128. To prohibit an agency from making any of the individual decisions made in an entire disapproved rulemaking action would not only be contrary to the text of the resolution of disapproval, interpreted consistently with the CRA, but also would be contrary to the apparent intent of the CRA. When Congress adopted the CRA, it recognized that it would be necessary for agencies to interpret the scope of the bar on reissuance in the future. According to a floor statement that its authors intended to be authoritative,

> [t]he authors [of the CRA] intend the debate on any resolution of disapproval to focus on the law that authorized the rule and make the congressional intent clear regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval. It will be the agency's responsibility in the first instance when promulgating the rule to determine the range of discretion afforded under the original law and whether the law authorizes the agency to issue a substantially different rule. Then, the agency must give effect to the resolution of disapproval.

129. Accordingly, the Commission observes that, in the floor debate on the resolution of disapproval in 2017, supporters of the resolution did not mention the breach notification provision apart from a brief reference. Senators who spoke in favor of the resolution cited the *2016 Privacy Order*'s treatment of broadband providers and the information they hold as different from providers of other services on the internet. The debate gives no reason to believe that the breach notification rule motivated those members of Congress who supported the resolution. Although the Commission's conclusion that the whole *2016 Privacy Order* is the relevant ''rule'' for purposes of 5 U.S.C. 801(b)(2) is fully justified even without considering the legislative history of the resolution of disapproval, the Commission rejects arguments that it is inappropriate to also look at that history and contentions that the Commission is misinterpreting that history. In addition to legislative history of the CRA that indicates that the legislative history of each resolution of disapproval should be relevant, out of an abundance of caution given the lack of an authoritative determination specifying the details of how to evaluate whether a rule is substantially the same under 5 U.S.C. 801(b)(2), the Commission considers whether there are indicia from the legislative history of the resolution of disapproval here to inform that analysis. For instance, if the legislative history indicated that the resolution of disapproval of the *2016 Privacy Order* somehow hinged entirely or significantly on concern about some or all of the 2016 data breach reporting requirements, the Commission then could consider whether and how to account for that in the 5 U.S.C. 801(b)(2) analysis notwithstanding the fact that there is little practical overlap between this order and the entirety of the *2016 Privacy Order.* Although data breach notification issues occasionally appear to have been raised by opponents of the resolution of disapproval, high-level statements by supporters of the resolution about ''FCC overreach'' or the like do not, without more, persuade the Commission that the 2016 data breach notification requirements played a

significant role in motivating the resolution of disapproval. Thus, the Commission sees nothing in the legislative history of the resolution of disapproval that would cause the Commission to question its conclusion that its action here does not adopt substantially the same rule for CRA purposes.

130. As EPIC notes in its comments, Congressional disapproval of the *2016 Privacy Order* under the CRA was largely predicated on claims that the Order would create duplicative privacy authority with the Federal Trade Commission as relates to broadband internet service providers. A review of the Congressional record from 2017 reveals that this indeed appears to have been the animating justification for Congressional disapproval of the *2016 Privacy Order.* Whatever the merits of such an argument, the Commission finds that it does not now preclude the Commission from adopting the rules set forth in this Order. As EPIC notes, the rules the Commission adopts here are not privacy measures directed at broadband internet service providers, but rather, data security measures directed at providers of telecommunications, interconnected VoIP services, and TRS, and which build upon rules that have existed since 2007. Thus, the primary animating justification behind Congressional disapproval of the *2016 Privacy Order* is irrelevant to the present case.

131. In addition, the revisions that the Commission makes here to the breach notification rule are different in substantial ways from those that Congress disapproved in 2017. The *2016 Privacy Order* was focused in large part on adopting privacy rules for broadband internet access service, and also made a number of changes to the Commission's privacy rules more generally that, among other things, required carriers to disclose their privacy practices, revised the framework for customer choice regarding carriers' access, use, and disclosure of the customers' information, and imposed data security requirements in addition to data breach notification requirements. When the *2016 Privacy Order* is viewed as a whole, it is clear that there is at most a small conceptual overlap between the adoption of data breach notification requirements at issue here and the many actions taken in that *Order* of which data breach notification requirements represented only a small fraction.

132. Independently, even assuming *arguendo* that the CRA were interpreted to require an evaluation on a more granular basis here, the Commission is not persuaded that the requirements it adopts here are substantially the same as analogous requirements in the *2016 Privacy Order.* For example, the customer notification requirement the Commission adopts here is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 data breach notification rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches that the Commission adopts here. With respect to the Federal agency notification requirements, as compared to the 2016 rules, the rules the Commission adopts here in that regard provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight. Consequently, even assuming *arguendo* that one were to conduct the 5 U.S.C. 801(b)(2) evaluation on a more granular basis, the Commission is not persuaded that the data breach notification requirements the Commission adopts here would be substantially the same as breach notification requirements adopted in the *2016 Privacy Order.* Even assuming one were to conduct the 5 U.S.C. 801(b)(2) evaluation at a more granular basis, the Commission is not persuaded that the breach notification rule from the *2016 Privacy Order* is the right level of granularity, nor that the evaluation of whether rules are substantially the same should be conducted based on high-level policy similarities, as some commenters contend. For example, the customer notification requirement is itself a ''rule'' within the meaning of the APA, as is the Federal agency notification requirement. Ultimately, however viewed, the Commission is persuaded that the rules it adopts here are not substantially the same as a disapproved rule for purposes of the CRA.

133. Nor is the Commission adopting something substantially the same as the *2016 Privacy Order* as a whole through the aggregate effect of individual Commission actions. For one, the theory that classification of broadband internet access service as a telecommunications service will automatically subject those services to the Commission's privacy rules, including the data breach notification requirements adopted here, is belied by multiple considerations: (1) the Commission has simply sought comment on those classification issues in its *Open internet Notice* and has not yet acted in that regard; (2) the *2015 Open internet Order* shows that the Commission is willing and able to decline to apply rules that might be triggered by a classification decision, having done so there, for example, by forbearing from all rules implementing section 222 pending consideration in a subsequent proceeding; and (3) the *Open internet Notice* sought comment on following the same approach to privacy that the Commission took in the *2015 Open internet Order* and specifically noted the resolution of disapproval of the *2016 Privacy Order* as a relevant consideration bearing on how it proceeds there. The Commission's analysis also is not materially altered by arguments that the Commission otherwise has adopted ''data security, customer authentication, employee training, and other requirements.'' In addition to being unpersuaded that such requirements substantially ''mirror provisions of the 2016 order,'' the Commission independently is not persuaded that the aggregation of such requirements and the data breach notification requirements adopted here lead to such a significant overlap with the *2016 Privacy Order* as to render the Commission's collective actions substantially the same as the *2016 Privacy Order* as a whole. For example, in the recent *SIM Swap Order,* the Commission adopted certain privacy requirements focused on wireless carriers' practices in the specific context of account transfers (or ''swaps'') from a device associated with one subscriber identity module (SIM) to a device associated with a different SIM on in connection with a wireless number being ported out. That is a vastly different focus than the *2016 Privacy Order,* which focused on the general privacy practices of all carriers. Thus, even assuming *arguendo* some high-level conceptual similarities, the operation and practical effect is significantly different than even arguably analogous requirements that were part of the *2016 Privacy Order.* As discussed above, the primary focus of the *2016 Privacy Order* was privacy rules for broadband internet access service, along with a number of changes to the Commission's privacy rules more generally that, among other things, required carriers to disclose their privacy practices, and revised the framework for customer choice regarding carriers' access, use, and disclosure of the customers' information. Given the other significant issues central to that decision, even assuming *arguendo* that there were some conceptual overlap between the

issues addressed in the *2016 Privacy Order* and data security, customer authentication, and employee training requirements recently adopted by the Commission—and even considered in conjunction with the data breach notification rules the Commission adopts here—the Commission is not persuaded that the Commission has adopted substantially the same rule as the *2016 Privacy Order.* Separately, insofar as the Commission considers the legislative history of the 2017 resolution of disapproval, data security, customer authentication, and employee training requirements likewise received only isolated mention, and then primarily with respect to broadband internet access service. Consequently, that legislative history does not reveal that the resolution of disapproval hinged entirely or significantly on concerns about such issues, even considered collectively. Thus, whether viewed alone or in the aggregate, the Commission is not persuaded that it has adopted substantially the same rule as the *2016 Privacy Order* as a whole. And the Commission notes, of course, that Congressional disapproval of a particular rule implementing a statute does not nullify an agency's general authority under that statute.

II. Effective Dates

134. The revised recordkeeping and reporting requirements adopted in this Report and Order, including the revisions to 47 CFR 64.2011 and 64.5111 set forth in Appendix A, are subject to approval by the Office of Management and Budget (OMB). Unless and until such time as OMB approves these new or modified requirements, the current, unmodified versions of 47 CFR 64.2011 and 64.5111 shall continue to apply.

135. The Commission directs the Wireline Competition Bureau to announce OMB approval and effective dates for the modified rules contained within this Order by subsequent public notice. Pursuant to this process, the Commission anticipates that carriers of all sizes will have ample time to come into compliance with these requirements, and therefore rejects CCA's request for a 12-month implementation timeline.

III. Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Data Breach Reporting Requirements* (*Data* Breach *Notice*), released in January 2023. The Commission sought written public comment on the proposals in the *Data Breach Notice,* including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

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

2. The *Report and Order* takes several important steps aimed at updating the Commission's rules regarding data breach notifications, both to Federal agencies and to customers, to better protect consumers from the dangers associated with data security breaches of customer information and to ensure that the Commission's rules keep pace with modern challenges.

3. First, the Commission expands the scope of the data breach notification rules to cover various categories of personally identifiable information (PII) that carriers hold with respect to their customers. Second, the Commission expands the definition of ''breach'' for telecommunications carriers to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or futher disclosed. Third, the Commission requires carriers to notify the Commission, in addition to the United States Secret Service (Secret Service) and Federal Bureau of Investigation (FBI), as soon as practicable, and in no event later than seven business days after reasonable determination of a breach. Fourth, the Commission eliminates the requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where a breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed. Fifth, the Commission eliminates the mandatory waiting period for carriers to notify customers, and instead requires carriers to notify customers of breaches of covered data without unreasonable delay after notification to Federal agencies, and in no case more than 30 days following reasonable determination of a breach, unless a delay is requested by law enforcement. Sixth, and finally, to ensure that telecommunications relay service (TRS) customers enjoy the same level of protections as customers of telecommunications carriers, the Commission adopts equivalent requirements for TRS providers. By adopting these requirements the Commission increases the the protection of consumers from improper use and/or disclosure of their information consistent with approaches to protect the public adopted by the Commission's Federal and State government partners.

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

4. There were no comments raised that specifically addressed the proposed rules and policies presented in the IRFA. Nonetheless, the Commission considered the general comments received about the potential impact of the rules proposed in the IRFA on small entities and took steps where appropriate and feasible, as discussed below, to reduce the compliance burden and the economic impact of the rules adopted in the *Report and Order* on small entities.

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

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

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

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein. 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.

7. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* The Commission's actions, over time, may affect small entities that are not easily categorized at present. The Commission therefore describes, 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 32.5 million businesses.

8. Next, the type of small entity described as a ''small organization'' is generally ''any not-for-profit enterprise which is independently owned and operated and is not dominant in its field.'' 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.

9. Finally, the small entity described as a ''small governmental jurisdiction'' is defined generally as ''governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand.'' 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, the Commission estimates that at least 48,971 entities fall into the category of ''small governmental jurisdictions.''

1. Wireline Carriers

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

11. 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.

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

13. *Incumbent Local Exchange Carriers* (*Incumbent LECs*). Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers 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.

14. *Competitive 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 several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with a 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.

15. *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 a 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.

16. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended, contains a size standard for a ''small cable operator,'' which is ''a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000.'' For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 498,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator. Based on industry data, only six cable system operators have more than 498,000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. The Commission notes however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore, the Commission is unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

17. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers is the closest industry with a 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 90 providers that reported they were engaged in the provision of other toll services. Of these providers, the Commission estimates that 87 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.

2. Wireless Carriers

18. *Wireless Telecommunications Carriers (except Satellite*). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. 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.

19. *Satellite Telecommunications.* This industry comprises firms ''primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications.'' 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.

3. Resellers

20. *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 a 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.

21. *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 a 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.

22. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications Resellers is the closest industry with a 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 62 providers that reported they were engaged in the provision of prepaid card services. Of these providers, the Commission estimates that 61 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.

4. Other Entities

23. *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.

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

24. In the *Report and Order,* the Commission expanded the scope of the Commission's breach notification rules to cover various categories of customer PII held by telecommunications carriers. The Commission also adopted a requirement that all telecommunications carriers notify the Commission, in addition to the Secret Service and the FBI, as soon as practicable, and in no event later than seven business days after reasonable determination of a breach of covered data. The Commission exempted from this notification requirement breaches that affect fewer than 500 customers and for which the carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. Instead, the Commission required carriers to sign and file with the Commission and other law enforcement an annual summary regarding all such breaches occurring in the previous calendar year. Carriers must also notify affected customers of breaches, with the exception of instances where a carrier can reasonably determine that no harm to such customers is reasonably likely to occur as a result of the breach. Additionally, the Commission applied similar rules to TRS providers.

25. The Commission's review of the record included comments about unique burdens for small businesses that may be impacted by the notification requirements adopted in the *Report and Order.* Accordingly, the Commission considered, and adopted provisions to mitigate, some of those concerns. For example, the Commission decided to utilize the existing reporting portal, which small and other carriers and TRS providers are already accustomed to using to notify the Commission along with the Secret Service and FBI of breaches rather than creating a centralized reporting facility operated by the Commission to report breaches to the Commission and these agencies as proposed in the *Data Breach Notice.* As such, the Commission anticipates that the requirement to notify it of data breaches will have de minimis cost implications because small and other carriers and TRS providers are already obligated to notify the Secret Service and FBI of such breaches, and will use the existing portal to do so. The Commission delegated authority to the Wireline Competition Bureau to coordinate with the Secret Service, the current administrator of the reporting facility, and the FBI, to the extent necessary, to ensure that the Commission will be notified when data breaches are reported, thereby ensuring that no additional burden would be imposed on small and other carriers and TRS providers. The Commission also adopted a threshold trigger that permits carriers and TRS providers to forgo notifying Federal agencies of breaches that are limited in scope and unlikely to pose harm to customers, instead requiring small and other carriers and TRS providers to maintain the information, and file an annual summary of such breaches. Additionally, with the support of several small carriers, the Commission adopted a harm-based notification trigger for reporting breaches to customers, which allows small and rural providers to focus their resources on data security and mitigation measures rather than generating notifications where harm to the consumer is unlikely.

26. In the *Report and Order* the Commission also adopted a ''without unreasonable delay, but no later than 30 days after reasonable determination of the breach'' timeframe for notifying customers of covered data breaches. Consistent with the comments in support of small carriers interests, the Commission recognizes that this reporting standard can take into account factors such as the provider's size, as a small carrier may have limited resources and could require additional time to investigate a data breach than a large carrier. The Commission notes that many State laws similarly require breach notifications which are in line with the requirements that the Commission adopts today. Therefore, although the Commission cannot quantify the compliance costs, it does not expect the adopted rules to impose any significant cost burdens for small entities, or require these entities to hire professionals to meet their compliance obligations.

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

27. 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.''

28. The Commission took steps and considered alternatives in this proceeding that may reduce the impact of the adopted rule changes on small entities. For example, the Commission's expansion of the definition of ''breach'' included consideration of whether to include situations where a telecommunications carrier, or a third party discovers conduct that could have reasonably led to exposure of customer CPNI, even if it has not yet determined if such exposure occurred. Small and other commenters generally opposed such an expansion, and the Commission ultimately declined to expand ''breach'' to include these situations. Conversely, although some commenters on behalf of small entities opposed requiring breach notification to the Commission, the Commission was not persuaded by their arguments. The Commission disagreed that the existing requirement to notify the Secret Service and the FBI is sufficient and that adding the Commission to the list of recipients of the same breach notifications Commission rules already require carriers to submit would impose any additional burden on carriers. Several actions the Commission takes in the *Report and Order* will avoid imposing additional burdens on small and other carriers who have to file breach notifications with the Commission.

29. As an initial matter the Commission considered, and included a good-faith exception that excluded from the definition of ''breach'' a good-faith acquisition of covered data by an employee or agent of a carrier where such information is not used improperly or further disclosed. The Commission believes this exception will help avoid excessive notifications to consumers, and reduce reporting burdens on small and other carriers. Furthermore, in the *Data Breach Notice,* the Commission proposed to create a new portal for reporting breaches to the Commission. However, in the *Report and Order* the Commission decided instead to make use of the existing portal which small and other carriers and TRS providers are already accustomed to using for data breach reporting requirements to Federal law enforcement agencies. The Commission's decision to continue using a portal that small and other carriers and providers are already familiar and comfortable working with reduces the administrative burdens on small entities of learning a new mechanism and creating new reporting processes. Additionally, the contents of the notification to the Commission are the same fields that carriers and providers already report to the Secret Service and the FBI. The Commission agreed with commenters on behalf of small entities that the breach notification information small and other carriers and providers are required to submit to the FBI and Secret Service is largely sufficient, and the Commission should generally require reporting of the same information. As such, the impact of also reporting the breach to the Commission should be de minimis on small carriers and providers. The Commission considered adopting a lower reporting threshold for the affected-customer notification of no-harm-risk breaches to the Federal agencies but ultimately decided to adopt a 500-customer threshold because that is consistent with many other State laws, and would therefore promote consistency and efficiency in compliance. A lower threshold could impose higher burdens on small and other carriers and providers, so the Commission declined to adopt such a rule. Likewise for consistency and efficiency, the Commission similarly declined to adopt a threshold of 5000 affected customers to trigger notification to Federal agencies. The Commission also considered ways to reduce the burden of the annual reporting requirement for breaches affecting fewer than 500 individuals and where the carrier or TRS provider could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. In determining the content and format requirements of the annual report, the Commission instructed the Bureau to minimize the burdens on carriers and TRS providers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. At a minimum, the Commission directed the Bureau to develop requirements that are less burdensome than what is required for individual breach submissions to the reporting facility, and to consider streamlined ways for filers to report this summary information.

30. The Commission also considered adopting minimum requirements for the contents of customer notifications for telecommunications carriers and TRS providers. However, the Commission declined to impose such minimum requirements on carriers and TRS providers because doing so may create unnecessary burdens on carriers and TRS providers, particularly small ones. Specifically, the Commission considered but declined to adopt minimum reporting requirements harmonizing content requirements for carriers with the information required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) as part of their notifications to Federal agencies. In the absence of final rules, and a potential for imposing duplicative or inconsistent fields, by declining to adopt such a requirement the Commission minimizes the economic impact for small entities. Relatedly, the Commission declined to adopt a specific method of notification for customers, instead deciding that carriers and TRS providers have pre-established methods of reaching their customers, each carrier or TRS provider is in the best position to know how best to reach their customers, and imposing a specific method would add unnecessary burdens to the industry. The Commission also considered requiring notification to all customers whenever a breach occurred. Such a requirement would lead to increased obligations to notify customers of every instance which qualified as a ''breach''

under the expanded definition and scope of the rules described in the *Report and Order.* However, by adopting the harm-based trigger, the Commission limits the applicability of the customer-notification obligations to breaches which are likely to cause harm to customers, thereby reducing burdens on small and other telecommunications carriers and TRS providers. In addition, the Commission also adopted a safe harbor under which customer notification is not required where a breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed, further reducing burdens on small and other carriers from the Commission's customer notification requirements.

31. The Commission's actions and the considerations discussed above lead the Commission to believe that the new requirements adopted in the *Report and Order* are minimally burdensome, and small carriers and TRS providers should not have any increased regulatory burdens, or significant compliance issues with including these new breach notification requirements in their existing processes. Nevertheless, the importance of the breach notification requirements adopted in the *Report and Order* to safeguard the public against improper use or disclosure of their customer data, to hold telecommunications carriers and TRS providers accountable, and to ensure customers are provided with the necessary resources to protect themselves in the event their data through their association with a telecommunications carrier or TRS provider is compromised, outweighs any minimal burdens that telecommunications carriers and TRS providers may experience in providing information to the Commission, and Federal law enforcement agencies.

G. Report to Congress

32. The Commission will send a copy of the *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 *Report and Order,* including this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Report and Order* (or summaries thereof) will also be published in the **Federal Register**.

IV. Procedural Matters

33. *Final Regulatory Flexibility Analysis.* Pursuant to the Regulatory Flexibility Act of 1980 (RFA), as amended, the Commission's Final Regulatory Flexibility Analysis is set forth in Appendix B. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this Report and Order, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

34. *Paperwork Reduction Act.* This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104–13. All such new or modified requirements will be submitted to OMB for review under section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on any new or modified information collection requirements contained in this proceeding. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, *see* 47 U.S.C. 3506(c)(4), the Commission previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

35. In this Report and Order, the Commission has assessed the effects of (1) expanding the scope of the data breach notification rules to cover specific categories of PII that carriers hold with respect to their customers; (2) expanding the definition of ''breach'' to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or further disclosed; (3) requiring carriers to notify the Commission, in addition to Secret Service and FBI, as soon as practicable, and in no event later than seven business days after reasonable determination of a breach; (4) eliminating the requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involved encrypted data and the carrier had definitive evidence that the encryption key was not also accessed, used, or disclosed; and (5) applying similar rules to TRS providers, and the Commission finds that the impact on small businesses with fewer than 25 employees will be minimal. While the Commission expanded the scope of the data breach notification rules, the Commission also adopted a good-faith exception from the definition of breach which limits the reportable instances. Additionally, the Commission decided to utilize the existing reporting portal, which small carriers and TRS providers are already accustomed to using, for Federal agency breach notifications rather than creating a new centralized portal. The Commission delegated authority to the Wireline Competition Bureau to coordinate with the Secret Service, the current administrator of the reporting facility, and the FBI, to the extent necessary, to ensure that the Commission will be notified when data breaches are reported, thereby ensuring that no additional burden would be imposed on small and other carriers and TRS providers from separate reporting requirements. The Commission also exempted from the Federal agency reporting requirement breaches that affect fewer than 500 customers and for which the carrier reasonably determines that no harm to customers is reasonably likely to occur, and instead require carriers to file with Federal agencies an annual summary regarding all such breaches occurring in the previous calendar year. This annual reporting requirement is intended to minimize the burden of reporting such breaches to Federal law enforcement and the Commission. In determining the content and format requirements of the annual report, the Commission instructed the Bureau to minimize the burdens on carriers and TRS providers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. Additionally, with the support of several small carriers, the Commission adopted a harm-based notification trigger for reporting breaches to customers, which allows small providers to focus their resources on data security and mitigation measures rather than generating notifications where harm to the consumer is unlikely.

36. *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).

37. *OPEN Government Data Act.* The OPEN Government Data Act, requires agencies to make ''public data assets'' available under an open license and as ''open Government data assets,'' *i.e.,* in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and

based on an open standard that is maintained by a standards organization. This requirement is to be implemented ''in accordance with guidance by the Director'' of the OMB. The term ''public data asset'' means ''a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)].'' A ''data asset'' is ''a collection of data elements or data sets that may be grouped together,'' and ''data'' is ''recorded information, regardless of form or the media on which the data is recorded.'' The Commission delegates authority, including the authority to adopt rules, to the Wireline Competition Bureau, in consultation with the agency's Chief Data Officer and after seeking public comment to the extent it deems appropriate, to determine whether to make publicly available any data assets maintained or created by the Commission pursuant to the rules adopted herein, and if so, to determine when and to what extent such information should be made publicly available. In doing so, the Bureau shall take into account the extent to which such data assets should not be made publicly available because they are not subject to disclosure under the FOIA.

38. *People with Disabilities.* To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice).

39. *Contact Person.* For further information, please contact Mason Shefa, Competition Policy Division, Wireline Competition Bureau, at (202) 418–2494 or *mason.shefa@fcc.gov.*

V. Ordering Clauses

40. Accordingly, *it is ordered* that, pursuant to sections 1, 2, 4(i), 4(j), 201, 202, 222, 225, 251, 303(b), 303(r), 332, and 705 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(j), 201, 202, 222, 225, 251, 303(b), 303(r), 332, 605, this Report and Order *is adopted.*

41. *It is further ordered* that part 64 of the Commission's rules *is amended* as set forth in Appendix A of the *Report and Order.*

42. *It is further ordered* that this Report and Order *shall be* effective thirty (30) days after publication of the text or a summary thereof in the **Federal Register**, except that the amendments to 47 CFR 64.2011 and 64.5111, which contain new or modified information collection requirements that require approval by the Office of Management and Budget under the Paperwork Reduction Act, will not be effective until the Office of Management and Budget completes any required review under the Paperwork Reduction Act. The Commission directs the Wireline Competition Bureau to publish a notice in the **Federal Register** announcing completion of such review and the relevant effective date. It is the Commission's intention in adopting the foregoing Report and Order that, if any provision of the Report and Order or the rules, or the application thereof to any person or circumstance, is held to be unlawful, the remaining portions of such Report and Order and the rules not deemed unlawful, and the application of such Report and Order and the rules to other person or circumstances, shall remain in effect to the fullest extent permitted by law.

43. *It is further ordered* that the Commission's Office of the Secretary, Reference Information Center, *shall send* a copy of this Report and Order to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A).

44. *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.

List of Subjects in 47 CFR Part 64

Carrier equipment, Communications common carriers, Reporting and recordkeeping requirements, Telecommunications, Telephone.

Federal Communications Commission.

Marlene Dortch,

Secretary.

Final Rules

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

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

■ 1. 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), 255, 262, 276, 403(b)(2)(B), (c), 616, 620, 716, 1401–1473, unless otherwise noted; Pub. L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

■ 2. Effective March 13, 2024, the heading for subpart U is revised to read as follows:

Subpart U—Privacy of Customer Information

■ 3. Delayed indefinitely, amend § 64.2011 by revising the section heading and paragraphs (a) through (e) to read as follows:

§ 64.2011 Notification of security breaches.

(a) *Commission and Federal Law Enforcement Notification.* Except as provided in paragraph (a)(3) of this section, as soon as practicable, but no later than seven business days, after reasonable determination of a breach, a telecommunications carrier shall electronically notify the Commission, the United States Secret Service (Secret Service), and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility on its website.

(1) A telecommunications carrier shall, at a minimum, include in its notification to the Commission, Secret Service, and FBI:

(i) The carrier's address and contact information;

(ii) A description of the breach incident;

(iii) The method of compromise;

(iv) The date range of the incident;

(v) The approximate number of customers affected;

(vi) An estimate of financial loss to the carrier and customers, if any; and

(vii) The types of data breached.

(2) If the Commission, or a law enforcement or national security agency, notifies the carrier that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security.

(3) A telecommunications carrier is exempt from the requirement to provide notification to the Commission and law enforcement pursuant to paragraph (a) of this section of a breach that affects fewer than 500 customers and the

carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. In circumstances where a carrier initially determined that it qualified for an exemption under this paragraph (a)(3), but later discovers information such that this exemption no longer applies, the carrier must report the breach to Federal agencies as soon as practicable, but no later than within seven business days of this discovery, as required in this paragraph (a).

(b) *Customer notification.* Except as provided in paragraph (a)(2) of this section, a telecommunications carrier shall notify affected customers of a breach of covered data without unreasonable delay after notification to the Commission and law enforcement pursuant to paragraph (a) of this section, and no later than 30 days after reasonable determination of a breach. This notification shall include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. Notwithstanding the foregoing, customer notification shall not be required where a carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed.

(c) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Commission, Secret Service, and the FBI pursuant to paragraph (a) of this section, and notifications made to customers pursuant to paragraph (b) of this section. The record shall include, if available, dates of discovery and notification, a detailed description of the covered data that was the subject of the breach, the circumstances of the breach, and the bases of any determinations regarding the number of affected customers or likelihood of harm as a result of the breach. Carriers shall retain the record for a minimum of 2 years.

(d) *Annual Reporting of Certain Small Breaches.* A telecommunications carrier shall have an officer, as an agent of the carrier, sign and file with the Commission, Secret Service, and FBI, a summary of all breaches occurring in the previous calendar year affecting fewer than 500 individuals and where the carrier could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. This filing shall be made annually, on or before February 1 of each year, through the central reporting facility, for data pertaining to the previous calendar year.

(e) *Definitions.* (1) As used in this section, a ''breach'' occurs when a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data. A ''breach'' shall not include a good-faith acquisition of covered data by an employee or agent of a telecommunications carrier where such information is not used improperly or further disclosed.

(2) As used in this section, ''covered data'' includes both a customer's CPNI, as defined by § 64.2003, and personally identifiable information.

(3) As used in this section, ''encrypted data'' means covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

(4) As used in this section, ''encryption key'' means the confidential key or process designed to render encrypted data useable, readable, or decipherable.

(5) Except as provided in paragraph (e)(6) of this section, as used in this section, ''personally identifiable information'' means:

(i) An individual's first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the identity of a specific individual, or other unique identification number used for authentication purposes;

(ii) An individual's username or email address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account; or

(iii) Unique biometric, genetic, or medical data.

(iv) Notwithstanding the above:

(A) Dissociated data that, if linked, would constitute personally identifiable information is to be considered personally identifiable if the means to link the dissociated data were accessed in connection with access to the dissociated data; and

(B) Any one of the discrete data elements listed in paragraphs (e)(5)(i) through (iii) of this section, or any combination of the discrete data elements listed above is personally identifiable information if the data element or combination of data elements would enable a person to commit identity theft or fraud against the individual to whom the data element or elements pertain.

(6) As used in this section, ''personally identifiable information'' does not include information about an individual that is lawfully made available to the general public from Federal, State, or local government records or widely distributed media.

* * * * *

■ 4. Delayed indefinitely, amend § 64.5111 by revising the section heading and paragraphs (a) through (e) to read as follows:

§ 64.5111 Notification of security breaches.

(a) *Commission and Federal law enforcement notification.* Except as provided in paragraph (a)(3) of this section, as soon as practicable, but not later than seven business days, after reasonable determination of a breach, a TRS provider shall electronically notify the Disability Rights Office of the Federal Communications Commission's (Commission) Consumer and Governmental Affairs Bureau, the United States Secret Service (Secret Service), and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility on its website.

(1) A TRS provider shall, at a minimum, include in its notification to the Commission, Secret Service, and FBI:

(i) The TRS provider's address and contact information;

(ii) A description of the breach incident;

(iii) A description of the customer information that was used, disclosed, or accessed;

(iv) The method of compromise;

(v) The date range of the incident;

(vi) The approximate number of customers affected;

(vii) An estimate of financial loss to the provider and customers, if any; and

(viii) The types of data breached.

(2) If the Commission, or a law enforcement or national security agency notifies the TRS provider that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the TRS provider not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the TRS provider when it appears that public disclosure or notice to affected customers will no longer

impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the TRS provider, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by TRS providers.

(3) A TRS provider is exempt from the requirement to provide notification to the Commission and law enforcement pursuant to paragraph (a) of this section of a breach that affects fewer than 500 customers and the carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. In circumstances where a carrier initially determined that it qualified for an exemption under this paragraph (a)(3), but later discovers information such that this exemption no longer applies, the carrier must report the breach to Federal agencies as soon as practicable, but not later than within seven business days of this discovery, as required in this paragraph (a).

(b) *Customer Notification.* Except as provided in paragraph (a)(2) of this section, a TRS provider shall notify affected customers of breaches of covered data without unreasonable delay after notification to the Commission and law enforcement as described in paragraph (a) of this section, and no later than 30 days after reasonable determination of a breach. This notification shall include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. Notwithstanding the foregoing, customer notification shall not be required where a TRS provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the provider has definitive evidence that the encryption key was not also accessed, used, or disclosed.

(c) *Recordkeeping.* A TRS provider shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Commission, Secret Service, and the FBI pursuant to paragraph (a) of this section, and notifications made to customers pursuant to paragraph (b) of this section. The record shall include, if available, the dates of discovery and notification, a detailed description of the covered data that was the subject of the breach, the circumstances of the breach, and the bases of any determinations regarding the number of affected customers or likelihood of harm as a result of the breach. TRS providers shall retain the record for a minimum of 2 years.

(d) *Annual reporting of certain small breaches.* A TRS provider shall have an officer, as an agent of the provider, sign and file with the Commission, Secret Service, and FBI, a summary of all breaches occurring in the previous calendar year affecting fewer than 500 individuals and where the provider could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. This filing shall be made annually, on or before February 1 of each year, through the central reporting facility, for data pertaining to the previous calendar year.

(e) *Definitions.* (1) As used in this section, a ''breach'' occurs when a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data. A ''breach'' shall not include a good-faith acquisition of covered data by an employee or agent of a TRS provider where such information is not used improperly or further disclosed.

(2) As used in this section, ''covered data'' includes:

(i) A customer's CPNI, as defined by section 64.5103;

(ii) Personally identifiable information, as defined by section 64.2011(e)(5); and

(iii) The content of any relayed conversation within the meaning of § 64.604(a)(2)(i).

(3) As used in this section, ''encrypted data'' means covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

(4) As used in this section, ''encryption key'' means the confidential key or process designed to render encrypted data useable, readable, or decipherable.

* * * * *

[FR Doc. 2024–01667 Filed 2–9–24; 8:45 am]

BILLING CODE 6712–01–P