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

In the Matter of	)	
	)	
Data Breach Reporting Requirements	)	WC Docket No. 22-21

NOTICE OF PROPOSED RULEMAKING

Adopted: December 28, 2022 **Released: January 6, 2023**

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

By the Commission:

TABLE OF CONTENTS

I. INTRODUCTION

1. The Commission first adopted a rule in 2007 requiring telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers to notify customers and federal law enforcement of breaches of customer proprietary network information (CPNI) in the carriers' possession.[1] In the almost decade and a half since that time, data breaches nationwide have increased in both frequency and severity in all industries.[2] In the telecommunications industry, the public has suffered an

[1] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*); 47 CFR § 64.2011.

[2] Identity Theft Resource Center, *Identity Theft Resource Center to Share Latest Data Breach Analysis With U.S. Senate Commerce Committee; Number of Data Breaches in 2021 Surpasses All of 2020* (Oct. 6, 2021), https://www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/; *see also* IAPP, *U.S. State Data Breach Lists*, https://iapp.org/resources/article/u-s-state-data-breach-lists/ (last visited Jan. 4, 2023) (compilation of the numerous states agency-maintained databases listing breaches reported in their states).

increasing number of security breaches of customer information in recent years.[3] Federal and state data breach laws covering other areas have evolved since 2007.[4] Those developments combined with our specific experience suggest opportunities for improvement in our own breach notification rule. The time is ripe. Today, we begin the process to update and strengthen our data breach rule to provide greater protections to the public.

II. BACKGROUND

2. *Privacy of Telecommunications Customer Information.* Section 222 of the Communications Act of 1934, as amended (the Act), requires telecommunications carriers to protect the privacy and security of information about their customers to which they have access as a result of their unique position as network operators.[5] Section 222(a) requires carriers to protect the confidentiality of proprietary information of and relating to their customers.[6] Section 222(c)(1) provides that a carrier may only use, disclose, or permit access to CPNI that it has received by virtue of its provision of a telecommunications service: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[7] The Act defines CPNI as "(A)

[3] *See, e.g.*, *AT&T Services, Inc.*, Order, 30 FCC Rcd 2808 (2015) (reaching $25 million settlement of investigation into three breaches); Selena Larson, *Verizon data of 6 million users leaked online*, CNN Business (July 12, 2017), https://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html; T-Mobile, *Notice of Data Breach: Keeping you safe from cybersecurity threats* (Sep. 7, 2021), https://www.t-mobile.com/brand/data-breach-2021 (providing notice that in August 2021 T-Mobile discovered a breach that occurred in July 2021); CNET, *T-Mobile hack: Here's what we know about the massive data breach* (Aug. 28, 2021), https://www.cnet.com/tech/t-mobile-hack-heres-what-we-know-about-the-massive-data-breach/; Lorenzo Franceschi-Bicchierai, Company that Routes Billions of Text Messages Quietly Says It Was Hacked, Motherboard Tech by Vice (Oct. 4, 2021), https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked (last visited Jan. 4, 2023) (reporting that Syniverse, a telecommunications infrastructure provider for mobile service, disclosed that its databases has been breached on several occasions since 2016, impacting potentially millions of cellphone users worldwide); *see also TerraCom, Inc. and YourTel America, Inc.; Apparent Liability for Forfeiture*, File No.: EB-TCD-13-00009175, NAL/Acct. No.: 201432170015, Notice of Apparent Liability For Forfeiture, 29 FCC Rcd 13325 (2014) (*TerraCom NAL*) (proposing to find that two companies failed to protect customer information and proposing forfeiture of $10 million).

[4] *See, e.g.*, American Recovery and Reinvestment Act, Pub. L No. 111-5, 123 Stat. 258, §§ 13400-13402 (2009); Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. Law 111-203, 124 Stat. 1376, §1093 (2010); Cal. Civ. Code §§ 1798.82 (amended 2020); Del. Code § 12B-102 (amended 2017); Wash. Rev. Code § 19.252.01 (amended 2019).

[5] 47 U.S.C. § 222. *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket Nos. 96-115, et al., Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14419-20, paras. 12-14 (1999) (*1999 CPNI Reconsideration Order*) (denying petitions for reconsideration and forbearance seeking different treatment for wireless providers under the Commission's CPNI rules, concluding that "there is nothing in the statute or its legislative history to indicate that Congress intended the CPNI requirements in section 222 should not apply to wireless carriers").

[6] 47 U.S.C. § 222(a).

[7] 47 U.S.C. § 222(c)(1). Section 222(b) provides that a carrier that receives or obtains proprietary information from other carriers in order to provide a telecommunications service may only use such information for that purpose and may not use that information for its own marketing efforts. 47 U.S.C. § 222(b). Section 222(d) delineates certain exceptions to the general principle of confidentiality, including permitting a carrier to use, disclose, or permit access to CPNI obtained from its customers to protect telecommunications services users "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services. 47 U.S.C. § 222(d). Subsequent to the adoption of section 222(c)(1), Congress added section 222(f). Section 222(f) provides that for purposes of section 222(c)(1), without

(continued….)

information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[8] The Commission has explained that CPNI includes (but is not limited to) information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; the location of a mobile device when it is in active mode (i.e., able to signal its location to nearby network facilities); and any services purchased by the consumer, such as call waiting.[9]

3. The Commission first promulgated rules implementing section 222 in 1998.[10] In addition to adopting restrictions on the use and disclosure of CPNI, the Commission adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.[11] In 2007, the Commission amended its CPNI rules to, among other things, require carriers[12] to notify law enforcement and customers of security breaches involving CPNI.[13] The Commission defined "breach" for this purpose as one that occurs "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[14] The Commission's rules require a telecommunications carrier to notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (Secret Service) and the Federal Bureau of Investigation (FBI).[15] The rules permit a telecommunications

(Continued from previous page)
the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location information concerning the user of a commercial mobile service or (2) automatic crash notification information of any person other than for use in the operation of an automatic crash notification system. 47 U.S.C. § 222(f).

[8] 47 U.S.C. § 222(h)(1).

[9] *2007 CPNI Order*, 22 FCC Rcd at 6930, para. 5; *see also AT&T, Inc.*, File No.: EB-TCD-18-00027704, Notice of Apparently Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1757, paras. 33-35 (2020) (finding that customer location information is CPNI under the Act); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609 (2013) (*2013 CPNI Declaratory Ruling*) (concluding that information collected by a customer's device at the carrier's direction may be CPNI); *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14487, paras. 146-47 (adopting the conclusions of the Common Carrier Bureau that names, addresses, and telephone numbers are not CPNI).

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

[11] *See id.* at 8195, para. 193.

[12] In this Notice of Proposed Rulemaking, we refer to telecommunications carriers and interconnected VoIP providers collectively as "telecommunications carriers" or "carriers," consistent with our existing Part 64, Subpart U rules. In doing so, we do not address the regulatory classification of interconnected VoIP service or interconnected VoIP service providers. *See* 47 CFR § 64.2003(o) (defining *telecommunications carrier* or *carrier* for purposes of Subpart U to include an entity that provides interconnected VoIP service as that term is defined in 47 CFR § 9.3).

[13] *2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32.

[14] 47 CFR § 64.2011(e).

[15] 47 CFR § 64.2011(b). Additionally, the Commission's rules require carriers to maintain a record of any discovered breaches, notifications to the Secret Service and the FBI regarding those breaches, as well as the Secret Service and the FBI response to the notifications for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the Secret Service and the (continued….)

carrier to notify the customer and/or disclose the breach publicly after seven business days following notification to the Secret Service and the FBI, if the Secret Service and the FBI have not requested that the telecommunications carrier continue to postpone disclosure.[16] Under the rules, a telecommunications carrier may immediately notify a customer or disclose the breach publicly only after consultation with the relevant investigative agency and only if the carrier believes that there is an extraordinarily urgent need to notify a customer or class of customers in order to avoid immediate and irreparable harm.[17] The Commission declined to specify the precise content of the notice that must be provided to customers in the event of a breach of CPNI, saying that it was leaving telecommunications carriers discretion to tailor the language and method of notification to the circumstances.[18]

4. In 2016, the Commission acted to revise its breach notification rule as part of a larger proceeding addressing privacy requirements for broadband internet access service providers (ISPs).[19] In 2017, however, Congress nullified those 2016 revisions to the Commission's CPNI rules under the Congressional Review Act.[20]

5. In 2013, as part of a larger proceeding addressing the video relay service (VRS) and telecommunications relay (TRS) programs, the Commission adopted rules to protect the privacy of

(Continued from previous page)
FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach. *See* 47 CFR § 64.2011(d).

[16] If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, the law enforcement agency may direct the carrier not to disclose the breach for an initial 30-day period. This 30-day period may be extended by the law enforcement agency as reasonably necessary in the judgment of the agency. The law enforcement agency shall provide in writing to the carrier its initial direction to the carrier and any subsequent direction. 47 CFR § 64.2011(b)(3).

[17] *See* 47 CFR § 64.2011(b)(2) (requiring a telecommunications carrier to indicate its desire to notify its customer or class of customers immediately in the notice that it provides to the Secret Service and FBI).

[18] *2007 CPNI Order*, 22 FCC Rcd at 6945, para. 32.

[19] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911, 14019-33, paras. 261-291 (2016) (*2016 Privacy Order*). 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 *United States Telecom Ass'n v. FCC*. *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5733, paras. 306 (2015), *aff'd*, *United States 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 section 222 of the Act. The rules the Commission adopted in the *2016 Privacy Order* applied to carriers and interconnected VoIP providers in addition to ISPs. *See 2016 Privacy Order*, 31 FCC Rcd at 13925, para. 39, 14033-34, para. 293. In 2017, the Commission reversed the 2015 classification decision so that Title II obligations, including section 222, no longer apply to ISPs. *Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017) (subsequent history omitted).

[20] *See* Joint Resolution, Pub. L. No. 115-22 (2017) ("*Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,* That Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have no force or effect."); 5 U.S.C. § 801(f) ("Any rule that takes effect and later is made of no force or effect by enactment of a joint resolution under section 802 shall be treated as though such rule had never taken effect."); *id.* § 801(b)(1) ("A rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval . . . of the rule."); *see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services; Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, WC Docket No. 16-106, CC Docket No. 96-115, Order, 32 FCC Rcd 5442 (2017).

customer information relating to all relay services authorized under section 225 of the Act.[21] In that proceeding, the Commission adopted a data breach reporting rule applicable to TRS modeled off of the CPNI data breach reporting rule applicable to telecommunications services.[22]

6. *Data Breach Notification Laws and Regulations.* As the Commission has previously explained, its data breach rule is "not intend[ed] to supersede any statute, regulation, order, or interpretation in any state, except to the extent that such statute regulation, order, or interpretation is inconsistent with the provisions" of the rule, and then only to the extent of the inconsistency.[23] In 2007, the Commission explicitly rejected requests to preempt all state CPNI obligations, finding instead that states should also be allowed to create rules for protecting CPNI.[24]

7. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring covered entities to notify individuals of data breaches.[25] Our breach notification requirement is one of several sector-specific breach notification laws in the United States. The Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Federal Trade Commission (FTC)-enforced Health Breach Notification Rule all have customer notification requirements for breaches of individual data.[26] In addition to sector-specific breach notification rules, the FTC has brought actions under section 5(a) of the FTC Act raising allegations that companies acted unfairly by failing to protect consumer data, resulting in security breaches.[27] The FTC has also published extensive guidance for businesses in the event of a security breach of customer information, setting forth recommendations for appropriate best practices after a data breach has

---

[21] *Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket Nos. 10-51, 03-123, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 8618, 8680, para. 155 (2013) (*2013 VRS Reform Order*); 47 CFR § 64.5111.

[22] *2013 VRS Reform Order*, 28 FCC Rcd at 8684, para 165.

[23] *2007 CPNI Order*, 22 FCC Rcd at 6945, para. 31; 47 CFR 64.2011(f).

[24] *2007 CPNI Order*, 22 FCC Rcd at 6957-58, para. 60 (recognizing that many states have laws relating to the safeguarding of personal information such as CPNI, and to the extent those laws do not create a conflict with federal requirements, carriers are able to comply with both federal and state law).

[25] *See* National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (with links to notification laws of each state, district, and territory).

[26] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (HIPAA); Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (GLBA); 16 CFR § 318.3.

[27] *See, e.g.*, *FTC v. Wyndham Worldwide Corporation*, 799 F.3d 236 (3rd Cir. 2015) (upholding the FTC's assertion that cybersecurity practices can, as a general matter, form the basis of an unfair practice under section 45(a) of the FTC Act); *see also, e.g.*, *Skymed International Inc.*, FTC Docket No. C-4732, Complaint, at https://www.ftc.gov/system/files/documents/cases/c-4732_skymed_final_complaint.pdf (2021) (alleging that the company failed to provide reasonable security for the personal information it collected which resulted in exposure of personal information in a cloud database that could be located and accessed by anyone on the internet, and contained approximately 130,000 membership records with consumers' personal information stored in plain text, including information populated in certain fields for names, dates of birth, gender, home addresses, email addresses, phone numbers, membership information and account numbers, and health information); *InfoTrax Systems L.C.*, FTC Docket No. C-4696, Complaint, at https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_complaint_clean.pdf (2020) (alleging that the company failed to put in place reasonable security safeguards, which allowed hackers to access the personal information of more than a million consumers); *LightYear Dealer Technologies, LLC*, FTC Docket No. C-4687, Complaint, https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_final_complaint.pdf (2019) (alleging that the auto dealer software provider failed to take reasonable steps to secure consumers' data, leading to a breach that exposed the personal information of millions of consumers).

occurred.[28]

8. *Recent Developments.* The Commission adopted the data breach rule, like the rest of the privacy safeguards adopted in the *2007 CPNI Order*, to address the problem of "pretexting," the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.[29] In the almost 15 years since, it has become clear that breaches of customer information in many contexts extend far beyond pretexting in general or the specific type of pretexting addressed at that time and are increasing in scale and evolving in methodology. For example in 2015, AT&T reached a settlement with the Commission to resolve an investigation into three data breaches at call centers in Mexico, Columbia, and the Philippines perpetrated by insiders who sold customer information to criminals that resulted in the compromise of the personal information of almost 52,000 customers.[30] In 2017, Verizon confirmed the leak of the personal data of six million customers, caused by a misconfigured security configuration on a cloud server.[31] And in 2021, T-Mobile disclosed that the personal information of over 50 million customers was stolen by hackers.[32] Verizon also recently disclosed a breach of its subsidiary Visible.[33] And Syniverse, which provides interconnection services to wireless carriers, disclosed that that an unknown "individual or organization gained unauthorized access to databases within its network on several occasions," potentially compromising the security of text messages of millions of wireless customers in a series of breaches spanning years.[34] These examples demonstrate the increasing severity and diversifying methods of security breaches involving customer information, which can have lasting detrimental impacts on customers whose information has been breached.[35]

9. To help protect consumers from the ever-growing harms of breaches of personal information across sectors, Congress and the states have taken action. For example, in 2009, Congress enacted laws that created breach notification requirements for businesses that maintain health care information, resulting in HIPAA's breach notification rules and the FTC's Health Breach Notification

---

[28] FTC, Data Breach Response: A Guide for Business at 6 (2021), https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf; (FTC Data Breach Guidance).

[29] *2007 CPNI Order*, 22 FCC Rcd at 6928, paras. 1-2 & n.1.

[30] *AT&T Services, Inc.*, Order, 30 FCC Rcd 2808 (2015).

[31] *See* Selena Larson, *Verizon data of 6 million users leaked online*, CNN Business (July 12, 2017), https://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html (last visited Jan. 4, 2023).

[32] T-Mobile, *Notice of Data Breach: Keeping you safe from cybersecurity threats* (Sep. 7, 2021), https://www.t-mobile.com/brand/data-breach-2021 (providing notice that in August 2021 T-Mobile discovered a breach that occurred in July 2021); CNET, *T-Mobile hack: Here's what we know about the massive data breach* (Aug. 28, 2021), https://www.cnet.com/tech/t-mobile-hack-heres-what-we-know-about-the-massive-data-breach/.

[33] Scott Ikeda, Attack on Verizon Visible Confirmed To Be a Credential Stuffing Campaign; Hacked Accounts Charged for Thousands of Dollars in Purchases, CPO Magazine (Oct. 21, 2021), https://www.cpomagazine.com/cyber-security/attack-on-verizon-visible-confirmed-to-be-a-credential-stuffing-campaign-hacked-accounts-charged-for-thousands-of-dollars-in-purchases/ (reporting that Visible recently experienced an attack that saw customer accounts taken over and orders placed using stored payment information).

[34] *See* Lorenzo Franceschi-Bicchierai, Company that Routes Billions of Text Messages Quietly Says It Was Hacked, Motherboard Tech by Vice (Oct. 4, 2021), https://www.vice.com/en/article/z3xpm8/company-that-routes-billions-of-text-messages-quietly-says-it-was-hacked (last visited Jan. 4, 2023).

[35] *See, e.g.*, RAND Corporation, Consumer Attitudes Toward Data Breach Notifications at xii (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf (finding that 68% of data breach victims reported an estimated financial loss, with a median loss of $500); Identity Theft Resource Center, 2021 Identity Crimes Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces at 16-20 (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (finding that 32% of identity theft victims reported identity-related financial problems, among other consequences).

Rule.[36] In 2010, Congress passed laws imposing breach notification requirements on financial institutions through amendments to GLBA.[37] At the state level, California has been an active leader in consumer privacy laws,[38] most recently in 2019 with the California Consumer Protection Act (CCPA)[39] and the passage of the California Privacy Rights Act (CPRA) in 2020.[40] Elsewhere, in 2021, Virginia and Colorado became the second and third states respectively to enact comprehensive consumer privacy laws,[41] while every state and territory now has some form of breach notification requirements.[42] Both California's and Virginia's recent privacy laws drew inspiration from the 2016 passage of the European Union's General Data Protection Regulation (GDPR) which created one of the world's most comprehensive privacy regimes.[43]

III. DISCUSSION

10. To better protect telecommunications customers and ensure that our rules keep pace with today's challenges, we propose a number of updates to our rule addressing telecommunications carriers' breach notification duties. We seek to ensure that affected customers, the Commission, and other federal law enforcement agencies receive the information they need in a timely manner so they can mitigate and prevent harm due to the breach and take action to deter future breaches.[44] To identify best practices and to minimize burdens, we look to other federal and state breach laws as potential models for our rules.

11. We propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the

---

[36] American Recovery and Reinvestment Act, Pub. L. No. 111-5, 123 Stat. 258 §§ 13400-13402 (2009). *See also*, Department of Health and Human Services, Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740, 42767 (Aug. 24, 2009) (implementing the HIPAA breach notification rule); Federal Trade Commission, Health Breach Notification Rules, 74 Fed. Reg. 42962 (Aug. 25, 2009) (implementing the Health Breach Notification Rule).

[37] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. Law 111-203, 124 Stat. 1376, §1093 (2010).

[38] *See* Gerald D. Peake, *Data Security and Privacy Law*, §7.11 (2021) (describing California's evolving privacy laws).

[39] Cal. Civ. Code §§ 1798.100.199; *see* State of California Department of Justice, *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa (last visited Jan. 4, 2023).

[40] *See*, IAPP, *The California Privacy Rights Act*, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/ (last visited Jan. 4, 2023).

[41] Sarah Rippy, *Virginia Passes the Consumer Data Protection Act* (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/; GibsonDunn, *The Colorado Privacy Act: Enactment of Comprehensive U.S. State Consumer Privacy Laws Continues* (July 9, 2021), https://www.gibsondunn.com/the-colorado-privacy-act-enactment-of-comprehensive-u-s-state-consumer-privacy-laws-continues/.

[42] National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (with links to notification laws of each state, district, and territory).

[43] Jennifer Bryant, *3 Years in, GDPR Highlights Privacy in Global Landscape* (May 25, 2021), https://iapp.org/news/a/three-years-in-gdpr-highlights-privacy-in-global-landscape. *See* Council Directive 2016/679, art. 34, 2016 O.J. (L 119) 1-88 (EC) (text of GDPR).

[44] *See 2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27 ("Notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI [because] [l]aw enforcement can investigate the breach, which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI . . . [and] this should enable law enforcement to advise industry, the Commission, and perhaps Congress regarding additional measures that might prevent future breaches.").

mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless requested by law enforcement. We also seek comment on whether we should adopt minimum requirements for the content of customer breach notices. We also evaluate and seek comment on the impact of the Congressional disapproval of the *2016 Privacy Order* on the Commission's legal authority to issue the rules proposed herein for telecommunications carriers. Finally, we propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

A. Defining "Breach"

12. *Inadvertent Disclosures*. We propose to expand the Commission's definition of "breach" to include inadvertent access, use, or disclosures of customer information and seek comment on our proposal. Our current rule, adopted in response to the practice of pretexting,[45] defines a "breach" as "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[46] While the practice of pretexting necessarily involves an intent to gain access to customer information, the intervening years since the adoption of our existing rule have demonstrated 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.[47] Further, whether or not a breach was intentional may not always be immediately apparent, which may lead to legal ambiguity and under-reporting. We also believe that it is important that the Commission and law enforcement be made aware of any accidental access, use, or disclosures so that we can (1) investigate and advise carriers on how best to avoid future breaches, and (2) stand ready to investigate if and when any of the affected information falls prey to malicious actors.[48] We anticipate that requiring notification for accidental breaches will encourage telecommunications carriers to adopt stronger data security practices and will help us identify and confront systemic network vulnerabilities. Do commenters agree with the foregoing analysis? Are

[45] *See supra* para. **Error! Reference source not found.**.

[46] 47 CFR § 64.2011(e).

[47] *Cf., e.g.*, Shawn Snow, *Major data breach at Marine Forces Reserve impacts thousands*, Marine Corps Times (Feb. 28, 2018), https://www.marinecorpstimes.com/news/your-marine-corps/2018/02/28/major-data-breach-at-marine-forces-reserve-impacts-thousands/ (describing the accidental disclosure of highly sensitive data of more than 21,000 service members, including truncated Social Security numbers, electronic funds transfer and bank routing numbers, truncated credit card information, mailing and residential addresses, and emergency contact information, caused by the transmission of an unencrypted email with an attachment to the wrong distribution list); Jan Murphy, *Data breach put 360,000 Pa. teachers, education department staffers' personal information at risk*, PennLive (Mar. 23, 2018), https://www.pennlive.com/politics/2018/03/data_breach_put_360000_pa_teac.html (reporting that human error led to the accidental exposure of highly sensitive information of approximately 360,000 current and retired teachers in Pennsylvania, including users' Social Security numbers); *see also, e.g.*, Australian Associated Press, *Melbourne student health records posted online in 'appalling' privacy breach: Health and medication data posted in error on Strathmore secondary college intranet*, The Guardian (Aug. 21, 2018), https://www.theguardian.com/australia-news/2018/aug/22/melbourne-student-health-records-posted-online-in-appalling-privacy-breach (reporting that in August 2018, the personal records of 300 students at Strathmore secondary college in Melbourne, Australia were accidentally published to the school's intranet service, resulting in the inadvertent disclosure of data relating to medical and mental health conditions, medications, and learning and behavioral difficulties for hundreds of high school students); Volodymyr "Bob" Diachenko, Head of Security Research at Comparitech, *Veeam inadvertently exposed marketing database with hundreds of millions of records*, Linkedin (Sept. 11, 2018), https://www.linkedin.com/pulse/veeam-inadvertently-exposed-marketing-info-hundreds-its-bob-diachenko/ (reporting on an exposed database that had been accidentally made available on the Internet by Veeam, a company that develops backup, disaster recovery, and intelligent data management software for virtual, physical, and multi-cloud infrastructures, which contained more than 200 gigabytes of customer records, including names, several hundred million email addresses, and IP addresses).

[48] *See 2007 CPNI Order*, 22 FCC Rcd at 6944, para. 27.

there other policy factors the Commission should consider in determining whether to require disclosure for unintentional breaches? What are the benefits and burdens associated with this proposal? We note that state data breach laws overwhelmingly do not include an intent limitation,[49] and we seek comment on how state and other federal data breach laws should influence the policy we adopt.

13. We seek comment on the impact of requiring reporting of accidental breaches on the number of reported breaches. Do commenters foresee a significant increase in the number of reported breaches? If so, how would our proposal affect reporting costs for telecommunications carriers and is that burden outweighed by the benefits to customers, who may need to take actions to protect their personal and financial information whether or not the breach was intentional? Would removing the intentionality limit potentially risk over-notification of data breaches to customers? What would the impacts of over-notification be? Would the potential benefits outweigh any potential harm? To help us assess the burden to both carriers and consumers from requiring reporting of accidental breaches, we invite commenters to provide estimates on the total number of breaches they have detected over the past few years, as well as the number of people affected by those breaches, and the severity of the compromised CPNI.

14. We propose to revise our definition to define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI. We seek comment on this proposal and other possible definitions. Should we retain the intent limitation in certain contexts? If so, what contexts and why? With only a few exceptions, the vast majority of state statutes include a provision exempting from the definition of breach a good-faith acquisition of covered data by an employee or agent of the company where such information is not used improperly or further disclosed.[50]

---

[49] *See, e.g.*, Ala. Code § 8-38-2(1); Alaska Stat. § 45.48.090; Ariz. Rev. Stat. § 18-551(1)(a); Ark. Code § 4-110-103(1)(A); Cal. Civ. Code § 1798.29(f); Colo. Rev. Stat. § 6-1-716(1)(a); Conn. Gen. Stat. § 36a-701b(a); Del. Code tit. 6 § 12B-101(1)(a); D.C. Code § 28-3851(1); Fla. Stat. § 501.171(1)(a); Ga. Code § 10-1-911(1); 9 GCA § 48.20(a); Haw. Rev. Stat. § 487N-1; 815 ILCS § 530-5; Ind. Code § 4-1-11-2(a); Iowa Code § 715C.1(1); Kan. Stat. § 50-7a01(h); KRS § 365.732(1)(a); KRS § 61.931(9)(a); La. Rev. Stat. § 51.3073(2); Me. Rev. Stat. tit. 10 § 1347(1); Md. Code Com. Law § 14-3504(a)(1); Md. State Govt. Code § 10-1305(a)(1); Mass. Gen. Laws § 93H-1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61 Subd. 1(d); Miss. Code § 75-24-29(2)(a); Mo. Rev. Stat. § 407.1500 1. (1); Mont. Code § 2-6-1501(1); Mont. Code § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. § 603A.020; N.H. Rev. Stat. § 359-C:19(V); N.J. Stat. § 56:8-161; N.M. Stat. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-AA(c); N.C. Gen. Stat § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code § 1347.12(A)(2)(a); Ohio Rev. Code § 1349.19(A)(1)(a); Ohio Rev. Code § 1354.01(C); Okla. Stat. § 74-3113.1(D)(1); Okla. Stat. § 24-162(1); Oregon Rev. Stat. § 646A.602(1); 73 Pa. Stat. § 2302; 10 L.P.R.A. § 4051(c); R.I. Gen. Laws § 11-49.3-3(a)(1); S.C. Code § 39-1-90(D)(1); S.D. Cod. Laws § 20-40-19(1); Tenn. Code § 47-18-2107(a)(1)(A); Tex. Bus. & Com. Code § 521.053(a); Utah Code § 13-44-102(1)(a); 9 V.S.A. § 2430(13)(A); Va. Code § 18.2-186.6(A); V.I. Code tit. 14, § 2208(d); Wash. Rev. Code § 19.255.005(1); W.V. Code § 46A-2A-101(1); Wis. Stat. § 134.98(2)(a)-(b); Wyo. Stat. § 40-12-501(a)(i).

[50] *See, e.g.*, Ala. Code § 8-38-2(1); Alaska Stat. § 45.48.050; Ariz. Rev. Stat. § 18-551(1)(b); Ark. Code § 4-110-103(1)(B); Cal. Civ. Code § 1798.29(f); Colo. Rev. Stat. § 6-1-716(1)(a); Del. Code tit. 6 § 12B-101(1)(a); D.C. Code § 28-3851(1); Fla. Stat. § 501.171(1)(a); Ga. Code § 10-1-911(1); 9 GCA § 48.20(a); Haw. Rev. Stat. § 487N-1; Idaho Stat. § 28-51-104(2); 815 ILCS § 530-5; Ind. Code § 4-1-11-2(b)(1); Iowa Code § 715C.1(1); Kan. Stat. § 50-7a01(h); KRS § 365.732(1)(a); KRS § 61.931(9)(b); La. Rev. Stat. § 51.3073(2); Me. Rev. Stat. tit. 10 § 1347(1); Md. Code Com. Law § 14-3504(a)(2); Md. State Govt. Code § 10-1305(a)(2); Mass. Gen. Laws § 93H-1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61 Subd. 1(d); Mo. Rev. Stat. § 407.1500 1. (1); Mont. Code § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. § 603A.020; N.H. Rev. Stat. § 359-C:19(V); N.J. Stat. § 56:8-161; N.M. Stat. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-AA(c); N.C. Gen. Stat § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code § 1347.12(A)(2)(b)(i); Ohio Rev. Code § 1349.19(A)(1)(b)(i); Ohio Rev. Code § 1354.01(C)(1); Okla. Stat. § 74-3113.1(D)(1); Okla. Stat. § 24-162(1); Oregon Rev. Stat. § 646A.602(1); 73 Pa. Stat. § 2302; R.I. Gen. Laws § 11-49.3-3(a)(1); S.C. Code § 39-1-90(D)(1); S.D. Cod. Laws § 20-40-19(1); Tenn. Code § 47-18-2107(a)(1)(B); Tex. Bus. & Com. Code § 521.053(a); Utah Code § 13-44-102(1)(b); 9 V.S.A. § 2430(13)(B); Va. Code § 18.2-186.6(A); V.I. Code tit. 14, § 2208(d); Wash. Rev. Code § 19.255.005(1); W.V. Code § 46A-2A-101(1); Wis. Stat. § 134.98(2)(cm)(2); Wyo. Stat. § 40-12-501(a)(i).

Should we include such an exemption in our definition of "breach" or is such a provision unnecessary or otherwise inadvisable? Is our proposed rule sufficient to capture all instances in which persons, either purposefully or inadvertently, gain access to, use, or disclose CPNI? If not, how should we revise our proposed rule to ensure that it does? We also seek comment on whether we 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.[51]

15. *Harm-Based Notification Trigger.* We seek comment on whether to forego requiring notification to customers or law enforcement of a breach 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. Our current rule requires no showing of harm, instead requiring that notification be furnished in every instance where a breach of a carrier's customers' CPNI has occurred, where such breach is defined as any instance when "a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[52]

16. We seek comment on the benefits and drawbacks of adopting a "harm-based" notification trigger. How would it impact consumers? Would it benefit consumers by avoiding confusion and "notice fatigue" with respect to breaches that are unlikely to cause harm? Recognizing that it is not only distressing, but time consuming and expensive, to deal with the fallout of a data breach, we seek comment on whether a harm-based notification trigger could save consumers the time, effort, and financial difficulty of changing their passwords, purchasing fraud alerts or credit monitoring, and freezing their credit in the wake of a breach that is not reasonably likely to result in harm. Alternatively, does a harm-based notification trigger risk that consumers would be unaware of important information regarding their CPNI? We note that a harm-based trigger has a basis in data breach notification frameworks employed by states, which generally do not require covered entities to notify customers of breaches when a determination is made that the breach is unlikely to cause harm.[53] How should state and other data breach laws influence our analysis?

17. We also seek comment on the potential impacts of adopting a harm-based trigger on telecommunications carriers. Would a harm-based trigger allow carriers to better focus their resources on data security and ameliorating the harms caused by data breaches? Or to the contrary, would a harm-

[51] For example, in 2017 Verizon notified the public that an employee of one of its vendors had put information in cloud storage with settings that could have allowed it to be exposed to the public even though it did not result in "a loss or theft of Verizon or Verizon customer information" because the issue was remedied before any public exposure occurred. Verizon, *Verizon responds to report: Confirms no loss or theft of customer information* (July 12, 2017), https://www.verizon.com/about/news/verizon-responds-report-confirms-no-loss-or-theft-customer-information.

[52] 47 CFR § 64.2011(e); *see also* 47 CFR § 64.2011(a), (c).

[53] *See, e.g.*, Alaska Stat. § 45.48.010(c); Arizona Stat. §44-7501(G); Conn. Gen. Stat. § 36a-701b(b)(1) (exempting entities from disclosing breaches when an investigation determines that no harm is likely); Ark. Code § 4-110-105(d) (stating that notice is not required if there is no reasonable likelihood of harm); Fla. Stat. § 501.171(6)(b) (holding that no notice is required if it is reasonably determined that breach has not and will not likely result in identity theft or any other financial harm); Iowa Code § 715C.2(6) (stating that no notice is required if no reasonable likelihood of financial harm has resulted or will result from the breach); Or. Rev. Stat. § 646A.602(1)(a) (stating that no notice is required if no reasonable likelihood of harm has resulted or will result from the breach); N.J. Stat. Ann. § 56:8-163(a) (stating that notice is not required if it is determined that misuse of the information is not reasonably possible); Vt. Stat. Ann. tit. 09 § 2435(d)(1); Md. Com. Law Code Ann. § 14-3504(c); *see also Preparing for and Responding to a Breach of Personally Identifiable Information*, Office of Management and Budget, M-17-12, Memorandum for Heads of Executive Departments and Agencies at 29 (Jan. 3, 2017) (OMB M-17-12) (granting federal agencies discretion on whether to notify individuals potentially affected by a breach when the assessed risk of harm is low, and advising agencies to "balance the need for transparency with concerns about over-notifying individuals").

based trigger require carriers to unnecessarily expend resources determining whether particular breaches are reasonably likely to cause harm instead of more efficiently providing notice?

18. If we adopt a harm-based trigger, how should telecommunications carriers and the Commission determine the likelihood of misuse or harm? Should we identify a standard or set of factors that telecommunications carriers must consider to evaluate whether no harm to customers is reasonably likely?[54] If so, what factors should carriers consider in making their evaluation? We preliminarily believe that no single factor on its own (*e.g.*, basic encryption) is sufficient to make a determination regarding harm to customers. Do commenters agree? Do carriers have sufficient expertise and experience to determine whether a breach is likely to result in harm? Should we establish a rebuttable presumption of consumer harm unless and until a carrier demonstrates that no harm to consumers is reasonably likely to occur as a result of a breach?[55]

19. We seek comment on whether we should clarify the definition of "misuse" or "harm."[56] For example, should we construe "harm" broadly to encompass not only financial, but also physical and emotional harm, including reputational damage, personal embarrassment, and loss of control over the exposure of intimate personal details? Should we require telecommunications carriers to consider whether other information about the customers that may be available combined with CPNI could result in harm when determining whether notification is required? Should any harm-based trigger apply even where the data breached is encrypted? What are the potential enforcement and compliance implications associated with this approach? Should breaches without such "harm" be reported to the Commission even if not reported to customers? Should we require the carrier to consult with federal law enforcement and/or the Commission prior to determining that there is no reasonable likelihood of harm or misuse?[57] We seek comment on whether there are other triggers we should consider for which notice would be unnecessary, such as the number of affected consumers or the length of time exposure occurred. Are there other factors that we should consider before requiring breach notifications? Should we adopt a harm-based trigger only if we require notices of unintentional breaches, or should we evaluate the two issues independently? We also seek comment on the current notification practices in the industry. How do carriers currently make decisions regarding whether to notify customers and law enforcement of a breach?

20. We seek comment on whether any harm-based notification trigger should apply to both

[54] *See, e.g.*, OMB M-17-12 at 20-27 (setting forth a list of factors that agencies should consider when assessing the risk of harm to potentially affected individuals resulting from a breach); 45 CFR § 164.402(2) (setting forth a list of four factors that covered entities must consider when determining whether an acquisition, access, use, or disclosure of protected health information demonstrates a sufficiently high probability of harm so as to constitute a breach and trigger the notification requirements under HIPAA).

[55] *See* 45 CFR § 164.402(2) (establishing a rebuttable presumption of a "breach" that triggers the notification requirements under HIPAA except where covered entities demonstrate that there is a low probability that the protected health information in question has been compromised based on a risk assessment of four listed factors, including "(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who sued the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated").

[56] *See Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011) (agreeing that the term "'harm' is a broad concept that encompasses financial, physical, and emotional harm"); *see also Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leader, Inc.*, File No.: EB-TCD-15-00020488, NAL/Acct. No.: 201732170006, Notice of Apparent Liability For Forfeiture, 32 FCC Rcd 5418, 5423-25, paras. 16-21 (2017); *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, File No.: EB-TCD-16-00023195, NAL/Acct. No.: 201732170007, Forfeiture Order, 33 FCC Rcd 9204, 9218-20, paras. 39-42 (2018).

[57] *See, e.g.*, Conn. Gen. Stat. § 36a-701b(b)(1); Fla. Stat. §501.171(4)(c).

notifications to customers and notifications to law enforcement. While there are legitimate reasons to consider eliminating notifications to customers in those instances where a breach is not reasonably likely to result in harm—including reducing confusion, stress, financial hardship, and notice fatigue—can the same be said of notifications to law enforcement? Are there compelling reasons for carriers to continue notifying law enforcement of data breaches even where such breaches are not reasonably likely to result in consumer harm? Do the benefits of notifying law enforcement of all breaches, regardless of whether the breach is likely to result in harm, outweigh the attendant costs to carriers of providing such notice?

21. We propose that if we adopt a harm-based trigger, where a carrier is unable to make a determination regarding harm or is uncertain whether harm is likely to occur, the obligation to notify would remain. We seek comment on this proposal.

22. We also recognize that telecommunications carriers possess proprietary information other than CPNI that customers have an interest in protecting from public exposure, such as Social Security Numbers and financial records. We seek comment on the Commission's authority to establish breach-reporting obligations for this type of information under Section 222, to the extent that this information is obtained by a telecommunications carrier in its activity as a common carrier.[58] We also seek comment on the role of the Commission in protecting such information in light of the existing role of other agencies, including the FTC and Cybersecurity and Infrastructure Security Agency (CISA).[59] If we were to require telecommunications carriers to report breaches of proprietary information other than CPNI under Section 222(a), how broadly or narrowly should we define that category of information? If we were to extend our data breach rule to cover such information, how could we minimize duplicative reporting obligations from the FTC and CISA?

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

23. *Commission Notification*. We propose to require telecommunications carriers to notify the Commission of breaches, in addition to the Secret Service and FBI, as soon as practicable, and seek comment on our proposal. Our proposal is consistent with other federal sector-specific laws, which require prompt notification to the relevant subject-matter agency. For example, both HIPAA and the Health Breach Notification Rule require notice to the department of Health and Human Services (HHS) and the FTC respectively.[60] We seek comment on the benefits and costs of requiring notification to the Commission in addition to notifying the Secret Service and the FBI, as our existing rules require.[61]

24. As discussed above, the Commission adopted its existing data breach rule to address concerns regarding pretexting practices.[62] The Commission found that notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI because it 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."[63] Moreover, the Commission anticipated that 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.[64] However, as we have seen in the

[58] 15 U.S.C. § 45(a) (prohibiting unfair or deceptive acts or practices in or affecting commerce, but exempting "common carriers subject to the Acts to regulate commerce"), 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto").

[59] *See infra* para. 26 (discussing CISA duplication).

[60] 45 CFR § 164.408 ("A covered entity shall, following the discovery of a breach . . . notify the Secretary); 16 CFR § 318.3(a)(2).

[61] 47 CFR § 64.2011(b)(2).

[62] *See supra* para. **Error! Reference source not found.**.

[63] *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27.

[64] *See id*.

years since our data breach rule was initially adopted, not all breaches of customer data are the result of criminal pretexting, which was Commission's sole focus in 2007. Large-scale security breaches can also be the result of lax or inadequate data security practices and employee training. Thus, we tentatively conclude that notification of breaches will provide Commission staff important information about data security vulnerabilities that Commission staff can help address and remediate. We anticipate that breach notification to the Commission will also shed light on carriers' ongoing compliance with our rules. We seek comment on these tentative conclusions. How much of an incremental burden is associated with notifying the Commission of data breaches as compared to the existing data breach notification requirement for the Secret Service and FBI? Are there any other government entities to which we should require data breach reporting, such as the FTC? What would be the benefits and burdens of doing so?

25. *Method of Notification*. We propose that the Commission create and maintain a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies, and we seek comment on our proposal. Our current breach notification rule requires that telecommunications carriers notify the FBI and Secret Service "through a central reporting facility" to which the Commission maintains a link on its website.[65] We believe that the creation and operation by the Commission of a centralized reporting facility for reporting of breaches to the Commission, Secret Service, and FBI will streamline the notification process and improve federal coordination. Do commenters agree? Are there alternative mechanisms for breach reporting to the Commission and other federal law enforcement that we should consider instead, such as leveraging the existing central reporting facility? Are there existing notification resources that we can leverage? For example, could we leverage the CISA Incident Reporting System[66] to minimize burdens on carriers?

26. We seek comment on how we can minimize data breach reporting burdens for telecommunications carriers. The recently-passed Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires covered entities to notify CISA of cyber security incidents and establishes an interagency Cyber Incident Reporting Council intended to streamline interagency cyber incident reporting.[67] When implemented, CIRCIA will require covered entities to report cybersecurity incidents to CISA, except where covered entities "by law, regulation, or contract" are already required to report "substantially similar information to another Federal agency within a substantially similar timeframe,"[68] in which case the other agency will report the incident to CISA.[69] To the extent that a breach of CPNI is a result of a cyber incident, we seek comment on whether there are any modifications to our proposed rules that would minimize potential duplicate reporting of such breaches.

27. *Contents.* We seek comment on applying our existing requirements regarding the contents of the data breach notification to federal law enforcement agencies to breaches reported to the Commission. Generally, the central reporting facility requires carriers to report information relevant to the breach, including carrier contact information; a description of the breach incident; the method of

[65] 47 CFR § 64.2011(b). *See* Federal Communications Commission, CPNI Breach Reporting Facility, https://www.fcc.gov/general/cpni-breach-reporting-facility (last visited Jan. 4, 2023).

[66] Cybersecurity & Infrastructure Security Agency, *CISA Incident Reporting System*, https://us-cert.cisa.gov/forms/report (last visited Jan. 4, 2023). The CISA Incident Reporting System allows Federal Government departments and agencies, and other entities, to report breaches of federal government information and information systems. *See* CISA, *US-CERT Federal Incident Notification Guidelines*, https://us-cert.cisa.gov/incident-notification-guidelines (last visited Jan. 4, 2023).

[67] Cyber Incident Reporting for Critical Infrastructure Act of 2022, sec. 2242(a)(1)(A), adopted as part of Consolidated Appropriations Act, 2022, Division Y, sec. 103, Pub. L. No. 117-103. CIRCIA's requirements will not go into effect until after CISA completes a rulemaking implementing the Act.

[68] CIRCIA, sec. 2242(a)(5)(B).

[69] Consolidated Appropriations Act, 2022, Division Y, sec. 104(a)(5), Pub. L. No. 117-103. The federal agency must establish an interagency sharing agreement and mechanism with CISA for this exception.

compromise; the date range of the incident, approximate number of customers affected; an estimate of financial loss to the carriers and customers, if any; types of data breached; and the addresses of affected customers. We believe 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 the rule we propose here. Do commenters agree? Are there any additional or alternative categories of information that should be included in these disclosures? For example, should we require telecommunications carriers to report, at a minimum, the information required under CIRCIA with the aim of minimizing potentially duplicate reporting requirements?[70] Should we curtail or streamline any of the existing content requirements? For example, should we eliminate the requirement that carriers report the addresses of affected individuals to law enforcement and the Commission, to minimize the personal information reported to the Commission and law enforcement?

28. *Timeframe.* We seek comment on the appropriate timeframe for notifying the Commission and other federal law enforcement of a breach. Our current rule requires telecommunications carriers to notify the Secret Service and the FBI of all breaches of CPNI no later than seven business days after reasonable determination of the breach.[71] We propose to require carriers to notify the Commission of a reportable breach contemporaneously with notification to other law enforcement agencies as soon as practicable after discovery of a breach. We believe that 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. We seek comment on our proposal. Is "as soon as practicable after discovery of a breach" an appropriate timeframe for notifying law enforcement after reasonable determination of a CPNI breach? Or, should we maintain the current "no later than seven business days" standard? Is there an alternative timeframe we should adopt for reporting CPNI breaches to the Commission and other federal law enforcement such as 24 hours or 72 hours as has been proposed in other contexts,[72] or should we consider adopting a graduated timeframe?[73] We also seek comment on whether we should clarify when a carrier should be treated as having "reasonably determined" that a breach has occurred. Should a carrier be held to have "reasonably determined" a breach has occurred when it has information indicating that it is more likely than not that there was a breach? Should we publish guidance on what constitutes a reasonable determination? Should we adopt a more definite standard?

29. *Threshold Trigger.* We seek comment on whether it is appropriate to set a threshold for the number of customers affected to require a breach report to the Commission, Secret Service, and/or FBI. We observe that breaches affecting smaller numbers of customers may not necessitate the same law enforcement attention as larger breaches because they may be less likely to reflect coordinated attacks on CPNI. Under our current rule, telecommunications carriers must notify federal law enforcement of *all*

[70] *See* CIRCIA, sec. 2242(b)(4) (requiring, at a minimum, a description of the covered cyber incident; a description of the vulnerabilities exploited and security defense that were in place, as well as the techniques used to perpetrate the covered incident; any identifying information related to those reasonably believed to be responsible for the incident; the categories of information reasonably believed to have been accessed or acquired by unauthorized persons; and contact information of the covered entity impacted).

[71] 47 CFR § 64.2011(a)-(b).

[72] CIRCIA requires covered entities to notify CISA no later than 72 hours after the entity "reasonably believes" that a covered cybersecurity incident has occurred, and to report ransomware payments within 24 hours. *See* CIRCIA, sec. 2242(a)(1)(A); 2242(a)(2). The GDPR requires notification of a personal data breach to the relevant government authority within 72 hours of discovery of the breach. Council Directive 2016/679, art. 33, 2016 O.J. (L 119) 1 (EC).

[73] *See, e.g.*, Executive Order 14028 (mandating updates to the Federal Acquisition Regulation that will require, among other things, federal contractors to report cyber incidents "based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection").

reportable breaches, regardless of the number of customers affected. Setting a threshold for the number of customers affected for breach reporting to the Secret Service and FBI could reduce the administrative burdens on carriers and law enforcement agencies from excessive reporting, and is consistent with many state statutes requiring notice to state law enforcement authorities, which require law enforcement notification of large breaches.

30. At the same time, establishing a threshold may limit our and our federal partners' abilities to remediate, investigate, and deter smaller breaches. Further, as the Commission has previously found, notification of all breaches 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 CPNI breaches."[74] Is this still the case, given the development of data breach law and practices since 2007? Should we adopt a threshold for reporting to federal law enforcement? If so, should the threshold be the same for the Commission as for federal law enforcement? If not, how should the threshold differ? What would be an appropriate threshold for reporting? Most states that adopt a threshold for reporting to law enforcement or government agencies require reporting at 250,[75] 500,[76] or 1000[77] individuals affected. What reporting threshold would meet the needs of law enforcement and provide adequate safeguards? What are the benefits and drawbacks of setting a threshold, particularly for small carriers? If we adopt a threshold trigger, should we require carriers to maintain a record of smaller breaches that fall below the threshold and report such small breaches to the Commission in a report at the end of the year?[78] What are the benefits and drawbacks to such an approach? Rather than a numerical threshold, should we instead consider requiring carriers to report only intentional breaches to law enforcement, but to report all breaches, whether intentional or inadvertent, to the Commission?

C. Customer Notification

31. *Notifying Customers of Data Breaches without Unreasonable Delay.* We propose to require telecommunications carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach and notification to law enforcement, unless law enforcement requests a delay. We seek comment on our proposal. Our existing data breach rule prohibits telecommunications carriers from notifying customers or disclosing the breach to the public until at least seven full business days after

[74] *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27.

[75] *See, e.g.*, N.D. Cent. Code § 51-30-02 (requiring entities to report data breaches affecting 250 residents or more to the state Attorney General); Or. Rev. Stat. § 646A.604(1)(b) (same); S.D. Codified Laws § 20-40-20 (same).

[76] *See, e.g.*, Cal. Civ. Code § 1798.82(f) (requiring entities to report data breaches affecting 500 residents or more to the state Attorney General); Colo. Rev. Stat. § 6-1-716 (requiring entities to report data breaches affecting 500 residents or more to the state Attorney General); Del. Code tit. 6, § 12B-102(d) (same); Fla. Stat. § 501.171(3)(a) (same); R.I. Gen. Laws § 11-49.3-4(a)(2) (requiring entities to report data breaches affecting 500 residents or more to the state Attorney General and major credit reporting agencies); *see also* 45 CFR § 164.408 (requiring notification to the Secretary of Health and Human Services for breaches of unsecured protected health information involving 500 or more individuals).

[77] *See, e.g.*, Ala. Admin. Code § 8-38-6(a) (requiring entities to report data breaches affecting 1000 residents or more to the state Attorney General); Ariz. Rev. Stat. Ann. § 18-552 (requiring entities to report data breaches affecting 1000 residents or more to the state Attorney General and three largest nationwide consumer reporting agencies); Haw. Rev. Stat. § 487N-2 (requiring entities to report data breaches affecting 1000 residents or more to the state Office of Consumer Protection); N.M. Code § 57-12C-10 (requiring entities to report data breaches affecting 1000 residents or more to the state Attorney General and major consumer reporting agencies); Colo. Rev. Stat. § 6-1-716 (requiring entities to report data breaches affected 1000 residents or more to the credit reporting agencies).

[78] *See, e.g.*, 45 CFR § 164.408(c) (requiring covered entities to maintain a log of breaches affecting less than 500 individuals and provide the log to Department of Health and Human Services not later than 60 days after the end of each calendar year).

notification to the Secret Service and FBI.[79] In cases where a carrier believes that there is an extraordinarily urgent need to notify affected customers in order to avoid immediate and irreparable harm, our rules permit carriers to notify affected customers after consultation with relevant investigating agencies.[80] In adopting the existing rule, the Commission concluded that once customers have been notified, a breach may become public knowledge, "thereby impeding law enforcement's ability to investigate the breach, identify the perpetrators, and determine how the breach occurred."[81] In short, the Commission found, "immediate customer notification may compromise all the benefits of requiring carriers to notify law enforcement of CPNI breaches," and therefore a short delay was warranted.[82]

32. We tentatively conclude that this existing approach is out-of-step with current approaches regarding the urgency of notifying victims about breaches of their personal information. We tentatively conclude that our proposal better serves the public interest than our current rule because it increases the speed at which customers may receive the important information contained in a notice, except in those specific circumstances when law enforcement officials specifically request otherwise.[83] We seek comment on our tentative conclusion. What are the benefits and drawbacks to such an approach? Is there any reason to maintain our current absolute bar to customer notification for a set period? Does our proposal to eliminate the seven business-day waiting period before notifying customers appropriately balance legitimate law enforcement needs with the customers' need to take action to timely protect their information after a breach? We seek comment on whether a "without unreasonable delay" notification requirement would allow carriers enough time to determine the scope and impact of a breach. Would prompt customer notification compromise a carrier's ability to discover the source of the breach, mitigate the loss of data, and ensure further data is not compromised?

33. Our proposed requirement is consistent with many existing data breach notification laws that require expedited notice but refrain from requiring a specific timeframe. For example, the GLBA requires customer notification "as soon as possible" after a determination that customer information has been misused.[84] California law requires notification "be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."[85] Similarly, many state data breach statutes impose an "expeditiously as practicable" or "without unreasonable delay" standard instead of a set time limit for reporting.[86] In addition, FTC guidance on addressing data breaches explains that "if you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused."[87] How should state and other federal law influence the approach we adopt?

---

[79] 47 CFR § 64.2011(b)(1).

[80] 47 CFR § 64.2011(b)(2).

[81] *2007 CPNI Order*, 22 FCC Rcd at 6943-44, para. 28.

[82] *Id*. at 6944, para. 28.

[83] *Cf., e.g.*, R.I. Gen. Laws § 11-49.3-4(a)(2) (requiring notification to state Attorney General and major credit reporting agencies if more than 500 residents are affected by a breach, specifying that such notice should be made *without* delaying notice to affected residents, and permitting law enforcement to delay notification if necessary for investigation).

[84] 12 CFR pt. 364, Appx. B, Supp. A § III(A)(1) (interpreting GLBA § 501(b)).

[85] Cal. Civ. Code § 1798.29(a).

[86] *See, e.g.*, Va. Code Ann. § 18.2-186.6(B) ("without unreasonable delay"); D.C. Code § 28-3852(a) ("in the most expedient time possible and without unreasonable delay"); Wyo. Stat. Ann. § 40-12-502(a) ("notice shall be made in the most expedient time possible and without unreasonable delay").

[87] FTC, Data Breach Response: A Guide for Business at 6 (2021), https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf (FTC Data Breach Guide).

34. We seek comment on whether requiring notice to customers "without unreasonable delay" after discovery of a breach provides sufficient guidance as to the required timeframe to notify customers. Should we adopt a different approach, such as a fixed number of days for notification, and if so what should we adopt? If we were to adopt a "without unreasonable delay" standard, we seek comment on whether we should provide guidance on a specific time period that would be considered "reasonable" for notification. For example, HIPAA requires notification to individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[88] The Health Breach Notification Rule also requires notification to individuals "without unreasonable delay and in no case later than 60 days after the discovery of a breach of security."[89] Most states that impose an outside limit on when consumers must be notified of a breach require notification to affected consumers no later than 30,[90] 45,[91] or 60[92] days after discovery of a breach. What are the benefits and drawbacks to setting a definite time limit on notification while requiring notification without unreasonable delay?

35. We also seek comment on whether the same notification deadline should be applied to all carriers. Are there unique concerns or compliance barriers for small carriers that make prompt response unfeasible, such as resource availability or reliance on third-party cybersecurity services for breach detection? Should we adopt different notification requirements for small carriers? If so, what threshold should we establish for small carriers? Should we consider establishing any other exceptions to this proposed requirement? We also seek comment on whether we should take into consideration the scope of the breach, e.g., how many customers are affected, the type of information breach, in determining the appropriate timeframe for customer breach reporting.

36. We seek comment on how best to coordinate the timing of customer notification and federal law enforcement notification. Our current rule, providing for consecutive rather than simultaneous notification of federal law enforcement and customers, was adopted at the request of federal law enforcement.[93] Is such an approach still necessary? Are there circumstances where it would be acceptable for carriers to notify customers and law enforcement simultaneously in certain instances? Given that nearly all, if not all, state data breach statutes subject the timing of customer notification to legitimate law enforcement needs,[94] we seek comment on whether it is necessary to provide any further guidance to help coordinate the timing of notice to customers with notice to the Commission and other federal law enforcement.

37. In addition, consistent with our current rules implementing section 222, our proposed rules would allow a federal agency to direct a carrier 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.[95] In

---

[88] 45 CFR § 164.404(b). For breaches involving more than 500 individuals, HIPAA also requires notification of "prominent media outlets serving the state or jurisdiction" without unreasonable delay and no later than 60 days. 45 CFR § 164.406. For breaches involving more than 500 individuals HIPAA also requires notification to the Secretary of Health and Human Services (HSS). 45 CFR § 164.408.

[89] 16 CFR § 318.4(a).

[90] *See, e.g.*, Colo. Rev. Stat. § 6-1-716; Fla. Stat. § Fla. Stat. § 501.171(3)(a); Wash. Rev. Code § 19.255.010(8).

[91] *See, e.g.*, Ala. Code § 8-38-5(a); Ariz. Rev. Stat. Ann. § 18-552(B); Md. Code Ann. § 14-3504(b)(3); N.M. Stat. Ann. § 57-12C-6(A); Ohio Rev. Code Ann. § 1349.19(B)(2); Or. Rev. Stat. § 646A.604(3)(a); R.I. Gen. Laws § 11-49.3-4(a)(2); Tenn. Code § 47-18-2107(b); Vt. Stat. Ann. Tit. 9, § 2435(b)(1).

[92] *See, e.g.*, Del. Code Ann. Tit. 6, § 12B-102(c); S.D. Codified Laws § 20-40-20.

[93] *See 2007 CPNI Order*, 22 FCC Rcd at 6943-44, paras. 26-29.

[94] *See, e.g.*, Ala. Code § 8-38-5(c); Ariz. Rev. Stat. Ann. § 18-552(D); Cal. Civ. Code § 1798.29(c); Colo. Rev. Stat. § 6-1-716(2)(c); D.C. Code § 28-3852(d); Fla. Stat. § 501.171(4)(b); Haw. Rev. Stat. § 487N-2; Md. Code Ann. § 14-3504(d); Ohio Rev. Code Ann § 1349.19(d); Miss. Code § 75-24-29(5); Mont. Code § 2-6-1503(3); Utah Code § 13-44-102(4); Wash. Rev. Code § 19.255.010(3).

circumstances when a carrier reasonably decides to consult with law enforcement, a short delay pending such consultation would likely be reasonable for purposes of a "without unreasonable delay" standard for customer notification. We seek comment on this proposal. We observe that HIPAA, the GLBA, and the Health Breach Notification Rules 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.[96] Both HIPAA and the Health Breach Notification Rule allow notification delays of up to 30 days if requested by law enforcement.[97] Similarly, GLBA allows that "customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for a delay."[98] Likewise, most, if not all, states permit delays in notifying affected consumers for legitimate law enforcement needs.[99] We tentatively conclude that our proposal strikes an appropriate balance between the needs of law enforcement to have time to investigate criminal activity and the needs of customers to be notified of data breaches. Do commenters agree? We also observe that these other regimes appear to allow non-federal law enforcement to request a delay, whereas the Commission's rule currently allows only federal agencies to so request.[100] Should our rule also allow carriers to delay notification upon request of non-federal law enforcement?

38. *Contents of Customer Breach Notification*. We seek comment on whether we should require customer breach notifications to include specific minimum categories of information. Our current rules specify when and to whom breach notifications must be made, but do not address the content of such notifications.[101] In adopting the current breach notification rules, the Commission declined to specify the precise content of the notice that must be provided to customers in the event of a security breach of CPNI, "leav[ing] carriers the discretion to tailor the language and method of notification to the circumstances."[102] Nearly 15 years later, we now seek comment on whether it is appropriate to require a minimum amount of information to ensure that such data breach notifications contain actionable information that is useful to the consumer. We seek comment on the benefits to customers and carriers of requiring carriers to include minimum categories of information in customer data breach notices. Will having minimum consistent fields of information assist consumers in understanding the circumstances and nature of the breach and streamline notice practices for carriers? What are the drawbacks to doing so? Are there any legal barriers to adopting a rule that prescribes the minimum categories of information in these breach notices?

39. To so identify possible categories of information to require, we look to numerous state

(Continued from previous page)

[95] *See* 47 CFR § 64.2011(b)(3).

[96] *See* 16 CFR § 318.4(c); 12 CFR part 364, Appx. B, Supp. A; 45 CFR § 164.412.

[97] 45 CFR § 164.412; 16 CFR § 318.4(c).

[98] 12 CFR part 364, Appx. B, Supp. A § III(A)(1).

[99] *See, e.g.*, Cal. Civ. Code § 1798.82(c) ("The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation."); Alaska Stat. Ann. § 45.48.020 ("An information collector may delay disclosing the breach . . . if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation."); Ariz. Rev. Stat. Ann. § 18-552(D) ("The notifications required by subsection B of this section may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation"); Conn. Gen. Stat. Ann. § 36a-701b(d) ("Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed.").

[100] *See* 47 CFR § 64.2011(b)(3); *2007 CPNI Order*, 22 FCC Rcd at 6944, para. 29 & n.96.

[101] *See* 47 CFR § 64.2011.

[102] *2007 CPNI Order*, 22 FCC Rcd at 6945, para. 32.

data breach statutes as well as existing federal guidance regarding data breach notices. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information.[103] Of these, many impose minimum content requirements on the notifications that must be transmitted to affected individuals in the wake of a data breach,[104] including: the name and contact information for the entity reporting the breach;[105] the date, estimated date, or estimated date range of the breach;[106] a description of the breach incident;[107] a description of the personally identifiable information that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed;[108] any actions the entity is taking to remedy the situation and/or protect affected individuals;[109] a brief list of steps that affected consumers can take to protect themselves and their information, such as contacting credit bureaus to ask that fraud alerts or credit freezes be placed on their credit reports;[110] and contact information for the FTC and any federal agency that assists consumers with matters of identity theft.[111] Similarly, both the HIPAA Breach Notification Rule and guidance issued by the Federal Deposit Insurance Corporation (FDIC) in response to the GLBA impose minimum content requirements on data breach notifications.[112] In its Data

[103] *See Security Breach Notification Laws*, National Conference of State Legislatures (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[104] *See, e.g.*, Ala. Code § 8-38-5(d); Ariz. Rev. Stat. § 18-552(E); Cal. Civ. Code § 1798.82(d)(2); Colo. Rev. Stat. § 6-1-716(2)(a.2); 815 ILCS § 530/10(a)(1); Md. Code Com. Law § 14-3504(g), Md. State Govt. Code § 10-1305(g); Mass. Gen. Laws § 93H-1 Sec. 3(b); Mich. Comp. Laws § 445.72(6)(c)-(g); N.Y. Gen. Bus. Law § 899-AA(7); Oregon Rev. Stat. § 646A.604(5); 9 V.S.A. § 2435(b)(5); Wash. Rev. Code §§ 19.225.010(6)(b), 42.56.590(6)(b).

[105] *See* Ala. Code § 8-38-5(d); Cal. Civ. Code § 1798.82(d)(2); Colo. Rev. Stat. § 6-1-716(2)(a.2); Md. Code Com. Law § 14-3504(g), Md. State Govt. Code § 10-1305(g); N.Y. Gen. Bus. Law § 899-AA(7); Oregon Rev. Stat. § 646A.604(5); Wash. Rev. Code §§ 19.225.010(6)(b), 42.56.590(6)(b); 45 CFR § 164.404(c)(1).

[106] *See* Ala. Code § 8-38-5(d); Ariz. Rev. Stat. § 18-552(E); Cal. Civ. Code § 1798.82(d)(2); Colo. Rev. Stat. § 6-1-716(2)(a.2); Oregon Rev. Stat. § 646A.604(5); 9 V.S.A. § 2435(b)(5); Wash. Rev. Code §§ 19.225.010(6)(b), 42.56.590(6)(b); 45 CFR § 164.404(c)(1).

[107] *See* Cal. Civ. Code § 1798.82(d)(2); Mich. Comp. Laws § 445.72(6)(c)-(g); Oregon Rev. Stat. § 646A.604(5); 9 V.S.A. § 2435(b)(5).

[108] *See* Ala. Code § 8-38-5(d); Ariz. Rev. Stat. § 18-552(E); Cal. Civ. Code § 1798.82(d)(2); Colo. Rev. Stat. § 6-1-716(2)(a.2); Md. Code Com. Law § 14-3504(g), Md. State Govt. Code § 10-1305(g); Mich. Comp. Laws § 445.72(6)(c)-(g); N.Y. Gen. Bus. Law § 899-AA(7); Oregon Rev. Stat. § 646A.604(5); 9 V.S.A. § 2435(b)(5); Wash. Rev. Code §§ 19.225.010(6)(b), 42.56.590(6)(b).

[109] *See* Ala. Code § 8-38-5(d); 9 V.S.A. § 2435(b)(5); Mich. Comp. Laws § 445.72(6)(c)-(g); *see also* Cal. Civ. Code § 1798.82(d)(3)(A) (making the requirement optional).

[110] *See* Ala. Code § 8-38-5(d); 45 CFR § 164.404(c)(1); *see also* Cal. Civ. Code § 1798.82(d)(3)(B) (making the requirement optional); Mich. Comp. Laws § 445.72(6)(c)-(g); Ariz. Rev. Stat. § 18-552(E); Cal. Civ. Code § 1798.82(d)(2); Colo. Rev. Stat. § 6-1-716(2)(a.2); 815 ILCS § 530/10(a)(1); Md. Code Com. Law § 14-3504(g), Md. State Govt. Code § 10-1305(g); Oregon Rev. Stat. § 646A.604(5); Wash. Rev. Code §§ 19.225.010(6)(b), 42.56.590(6)(b); Mass. Gen. Laws § 93H-1 Sec. 3(b).

[111] *See* Ariz. Rev. Stat. § 18-552(E); Colo. Rev. Stat. § 6-1-716(2)(a.2); 815 ILCS § 530/10(a)(1); Md. Code Com. Law § 14-3504(g), Md. State Govt. Code § 10-1305(g); N.Y. Gen. Bus. Law § 899-AA(7); *see also* 9 V.S.A. § 2435(b)(5).

[112] *See* 45 CFR § 164.404(c)(1); *Data Security & Customer Notification Requirements for Banks*, American Bankers Association, https://www.aba.com/banking-topics/technology/data-security/data-security-customer-notification (last visited Jan. 4, 2023); *Final Guidance on Response Programs: Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, Federal Deposit Insurance Corporation, Michael J. Zamorski, Director, Division of Supervision and Consumer Protection, Financial Institution Letters, FIL-27-2005 (Apr. 1, 2005), https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html (*GLBA Customer Notice Guidance*).

Breach Response Guide, the FTC advises companies on specific information that should be included in their breach notices to individuals, including describing what the company knows about the breach (how it happened, what information was taken, how the thieves have used the information (if known), what actions the company has taken to remedy the situation, what actions the company is taking to protect individuals, how to reach the relevant contact in the organization); the steps individuals can take, given the type of information exposed, and provide relevant contact information; current information about how to recover from identity theft; information about the law enforcement agency working on the case, if the law enforcement agency agrees that would help; encouraging people who discover that their information has been misused to report it to the FTC; and describing how the company will contact consumers in the future to help victims avoid phishing scams.[113]

40. We seek comment on adapting these models to telecommunications carriers and requiring carriers to include, at a minimum, the following information in security breach notices to customers: (1) the 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. Are the identified categories the correct information to be included in data breach notices? Should we consider requiring any additional or alternative categories of information that carriers must include in customer breach notices? For example, would it be helpful to include a statement of whether the notification was delayed due to reporting requirements to law enforcement or a law enforcement investigation, and if so, the length of the delay to help explain to customers the time lapse between discovery of the breach and customer notification?[114] Should we require notifications to include a list of the law enforcement and government entities that have been notified of the breach? Should we require carriers to include a brief description of how the carrier will contact consumers in the future regarding the breach to help consumers avoid phishing scams related to breaches? What are best practices for providing consumers with actionable information in a breach notification? We seek comment on what minimum required information appropriately balances empowering consumers to take the necessary steps to protect themselves and their information in the wake of a data breach and appropriately limiting burdens on telecommunications carriers. We also seek comment on whether adopting or adapting a set of existing notification contents requirements will help to create a measure of consistency across breach notifications and will benefit both consumers and carriers, particularly smaller carriers, by streamlining the manner and content of their response in the event of a data breach.

41. *Method of Customer Breach Notification*. We observe that many state regulations specify the form that notifications to customers may take, whether by physical mail, email, or telephone.[115] We seek comment on whether we should adopt a similar requirement and, if so, on what form notifications to consumers should take. Is there a method or methods of notification that would make the most sense or be most beneficial to consumers? What are the benefits and burdens of imposing such a requirement?

---

[113] *See Data Breach Response: A Guide For Business*, Federal Trade Commission (Feb. 2021), https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

[114] *See* Cal. Civ. Code § 1798.82(d)(2).

[115] *See, e.g.*, Ala. Code § 8-38-5(d) (specifying that notice to affected individuals shall be "given in writing, sent to the mailing address of the individual . . . or by email notice"); Haw. Rev. Stat. § 487N-2(e) (allowing notice to be provided via physical mailing, email, or telephone); Mass. Gen. Laws § 93H-1(a); Oregon Rev. Stat. § 646A.604(4); Wash. Rev. Code § 19.255.010(4).

D. TRS Breach Reporting

42. In 2013, the Commission adopted CPNI rules applicable to all forms of Telecommunications Relay Services (TRS), as well as to point-to-point video calls handled over the video relay services (VRS) network.[116] 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."[117] The CPNI rules for TRS include a breach notification rule that is equivalent to section 64.2011 in terms of the substantive protection provided to TRS users.[118] To maintain functional equivalency for TRS users, we propose to amend section 64.5111 so that it continues to provide equivalent privacy protection for TRS users. The amendments we propose for section 64.5111 are thus essentially the same as those proposed for users of telecommunications and interconnected VoIP services. That is, we propose: (1) to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information; (2) to require TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach; and (3) to eliminate the mandatory waiting period to notify customers, instead requiring TRS providers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. Further, we seek comment on the following additional issues, raised above regarding section 64.2011, as they relate to TRS providers: (1) whether to adopt a harm-based trigger for breach notifications; (2) whether we should adopt minimum requirements for the content of customer breach notices; and (3) whether our rules should address breaches of sensitive personal information.

43. We seek comment on each of these proposals and their costs and benefits. Should updated data breach requirements for TRS providers be identical to those we adopt for providers of telecommunications and interconnected VoIP services, or are there circumstances unique to TRS providers that warrant differences in their obligations regarding data breaches? Are any additional notification requirements necessary to ensure TRS users receive functionally equivalent privacy protection? If we adopt the proposed requirement that service providers notify the Commission of breaches via a centralized portal, is there any need to retain the current requirement that TRS providers submit a copy of any breach notification to the Disability Rights Office of the Consumer and Governmental Affairs Bureau?[119] Finally, would TRS providers incur costs or other compliance burdens under the proposed amendments that are disproportionately greater than those incurred by providers of telecommunications and interconnected VoIP services, and if so, would the extent of such costs or burdens justify the application of different breach notification requirements to TRS?

44. *Legal Authority*. 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.[120] In 2013, the Commission found that applying the privacy protections of the Commission's

---

[116] *Structure and Practices of the Video Relay Service Program*; *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket Nos. 10-51 and 03-123, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 8618, 8680-87, para. 155-172 (2013) (*2013 VRS Reform Order*); 47 CFR §§ 64.5101-64.5111 (TRS CPNI rules). This includes the breach notification rule. *See* 47 CFR § 64.5111.

[117] *2013 VRS Reform Order*, 28 FCC Rcd at 8683, para. 164

[118] The texts of the two provisions are virtually identical, except for the substitution of the term "TRS provider" for "telecommunications carrier" in section 64.5111. *Compare* 47 CFR § 64.2011 *with* 47 CFR § 64.5111. The only substantive difference is that under the TRS rule, after a TRS provider notifies law enforcement of a breach, it "shall file a copy of the notification with the Disability Rights Office of the Consumer and Governmental Affairs Bureau at the same time as when the TRS provider notifies the customers." 47 CFR § 64.5111(a).

[119] *See* 47 CFR § 64.5111(a).

[120] 47 U.S.C. § 225(a)(3), (b)(1).

CPNI regulations to TRS users advances the functional equivalency of TRS.[121] 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 of the Commission's CPNI regulations applicable to TRS users.[122] In addition, the Commission found that extending the CPNI regulations to TRS users is 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.[123] Finally, the Commission determined that applying CPNI requirements to point-to-point video services provided by VRS providers[124] is ancillary to its responsibilities under sections 222 and 225.[125]

45. We tentatively conclude that, for the same reasons cited in the *2013 VRS Reform Order*, these sources of authority for establishing the current CPNI rules for TRS authorize the Commission to amend those rules to ensure that TRS users receive privacy protections equivalent to those proposed for users of telecommunications and VoIP services. We seek comment on this tentative conclusion.

E. Legal Authority

46. *Section 222.* We believe that section 222 provides authority to adopt the breach notification rules for which we seek comment in this *Notice*.[126] We also tentatively conclude that we have authority to apply the rules proposed in this *Notice* to interconnected VoIP providers. We seek comment on these tentative conclusions.

47. Section 222 of the Act governs telecommunications carriers in their use, disclosure, and protection of proprietary information that they obtain in the course of providing telecommunications services. 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.[127] Section 222(c) imposes more specific requirements on carriers as to the protection and confidentiality of CPNI.[128] We tentatively conclude that both subsections provide us authority to adopt rules requiring telecommunications carriers and interconnected VoIP providers to address breaches of CPNI.

48. The Commission has long required carriers to report data breaches as part of their duty to protect the confidentiality of customers' information.[129] We believe that the proposed revisions to the Commission's data breach reporting rule reinforce carriers' duty to protect the confidentiality of their customers' information. Data breach reporting requirements also reinforce our other rules addressing the protection of CPNI.[130] For example, data breach notifications can meaningfully inform customer decisions regarding whether to give, withhold, or retract their approval to use or disclose their information. Similarly, we believe that 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

---

[121] *2013 VRS Reform Order*, 26 FCC Rcd at 8685-86, para. 170.

[122] *Id.* at para. 170 & n.430, citing 47 U.S.C. § 225(d)(1)(A).

[123] *2013 VRS Reform Order*, 26 FCC Rcd at 8685-86, para. 170.

[124] Such point-to-point services, while provided in association with VRS, are not themselves a form of TRS.

[125] *2013 VRS Reform Order*, 26 FCC Rcd at 8686-87, para.171.

[126] We discuss legal authority for non-CPNI sensitive personal information above at *supra* para. 22 and for TRS breach reporting above at *supra* para. 43.

[127] 47 U.S.C. § 222(a).

[128] *See* 47 U.S.C. § 222(c).

[129] *See 2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32.

[130] *See* 47 CFR §§ 64.2001-2010.

help investigate and advise carriers on how best to avoid future breaches, also helping carriers to fulfill their duty under section 222(a) to protect the confidentiality of their customers' information. We seek comment on this analysis.

49. *Interconnected VoIP*. We believe that we have authority under section 222 and our ancillary jurisdiction to apply the rules we propose today to interconnected VoIP providers. In 2007, the Commission exercised ancillary jurisdiction to extend its Part 64 CPNI rules to interconnected VoIP services.[131] Since then, interconnected VoIP providers have operated under these rules. Interconnected VoIP services remain within the Commission's subject matter jurisdiction and we believe that the application of customer privacy requirements to these services is "reasonably ancillary to the effective performance" of our statutory responsibility under section 222.[132] As the Commission explained in 2007, "American consumers [can reasonably] expect that their telephone calls are private irrespective of whether the call is made using the service of a wireline carrier, a wireless carrier, or an interconnected VoIP provider."[133] Now, as then, extending section 222's protections to interconnected VoIP service customers is also "necessary to protect the privacy of wireline or wireless customers that place calls to or receive calls from interconnected VoIP providers."[134] In addition, in 2008, Congress ratified the Commission's decision to apply section 222's requirements to interconnected VoIP services by adding language to section 222 that expressly covers "IP-enabled voice service,"[135] defined expressly to incorporate the Commission's definition of "interconnected VoIP service."[136] The 2008 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. We seek comment on this analysis.

50. We seek comment on whether there are other bases of authority on which we can rely to adopt the rules we propose and seek comment on today.

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

51. As noted above, in 2016, the Commission acted to revise its breach notification rule as part of a larger proceeding addressing privacy requirements for broadband internet access service providers (ISPs).[137] 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

---

[131] *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59; *see also* 47 CFR § 64.2003(o) (defining "telecommunications carrier or carrier" for purposes of the CPNI rules to include interconnected VoIP providers).

[132] *See 2007 CPNI Order*, 22 FCC Rcd at 6955, para. 55; *see also United States v. Southwestern Cable*, 392 U.S. 157, 177-78 (1968) (setting forth the two-part "ancillary jurisdiction" test); *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010) (holding that ancillary jurisdiction must be "necessary to further its regulation of activities over which [the Commission] does have express statutory authority").

[133] *2007 CPNI Order*, 22 FCC Rcd at 6956, para. 56.

[134] *Id*. at 6956, para. 57.

[135] *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283 (2008) (NET 911 Act); *see also* 47 U.S.C. § 222(d)(4), (f)(1), (g).

[136] 47 U.S.C. § 222(d)(4), (f)(1), (g) (applying provisions of section 222 to "IP-enabled voice service"); § 615b(8) (defining "IP-enabled voice service" as having "the meaning given the term 'interconnected VoIP service' by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)").

[137] *2016 Privacy Order*, 31 FCC Rcd at 14019-33, paras. 261-291. 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 *United States Telecom Ass'n v. FCC*. *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5733, paras. 306 (2015), *aff'd*, *United States 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 section 222 of the Act.

classified as providers of telecommunications services in 2015.[138] In 2017, however, Congress nullified those 2016 revisions to the Commission's CPNI rules under the Congressional Review Act.[139]

52. As a threshold matter, we seek comment on the effect of the Congressional disapproval of the *2016 Privacy Order* under the Congressional Review Act.[140] While we seek comment on a range of proposals in this item, we clarify that, in light of the Congressional resolution of disapproval, we are not seeking comment on "reissu[ing] . . . in substantially the same form," or on issuing "a new rule that is substantially the same as," the rule disapproved by Congress.[141] More generally, though, we seek comment here on the effect and scope of the Congressional disapproval of the *2016 Privacy Order* for purposes of adopting rules that apply to telecommunications carriers.

G. Digital Equity Considerations

53. The Commission, as part of its continuing effort to advance digital equity for all,[142] including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality, invites comment on any equity-related considerations[143] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility.

---

[138] *See 2016 Privacy Order*, 31 FCC Rcd at 13925, para. 39, 14033-34, para. 293. In 2017, the Commission reversed the 2015 classification decision so that Title II obligations, including section 222, no longer apply to ISPs. *Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017), *aff'd in part and remanded in part*, *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019), *on remand*, Order on Remand, 35 FCC Rcd 12328 (2020), *ptns. for recon. pending*.

[139] *See* Joint Resolution, Pub. L. No. 115-22 (2017) ("*Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,* That Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have no force or effect."); 5 U.S.C. § 801(f) ("Any rule that takes effect and later is made of no force or effect by enactment of a joint resolution under section 802 shall be treated as though such rule had never taken effect."); *id.* § 801(b)(1) ("A rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval . . . of the rule."); *see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services; Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, WC Docket No. 16-106, CC Docket No. 96-115, Order, 32 FCC Rcd 5442 (2017).

[140] *See 2016 Privacy Order*, 31 FCC Rcd at 14019-33, paras. 261-293.

[141] *See* 5 U.S.C. § 801(b)(2) ("A rule that does not take effect (or does not continue) [due to a joint resolution of disapproval] 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.").

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

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

IV. PROCEDURAL MATTERS

54. *Initial Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this Notice. The IRFA is set forth in Appendix B. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the Notice indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this Notice, including the IRFA, to the Chief Counsel for Advocacy of the SBA.[144]

55. *Paperwork Reduction Act*. The Notice contains proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

56. *Ex Parte Presentations—Permit-But-Disclose.* The proceeding this Notice initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[145] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with section 1.1206(b) of the Commission's rules. In proceedings governed by section 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.[146]

57. *Comment Filing Procedures*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: https://www.fcc.gov/ecfs/.

[144] *See* 5 U.S.C. § 603(a).

[145] 47 CFR §§ 1.1200 *et seq.*

[146] 47 CFR § 1.49(f).

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.

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

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE
- Washington, DC 20554.

- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020).

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

59. *Additional Information*. For further information about this *Notice*, contact Melissa Kirkel, Deputy Chief, Competition Policy Division, Wireline Competition Bureau, at melissa.kirkel@fcc.gov, (202) 418-7958.

V. ORDERING CLAUSES

60. Accordingly, IT IS ORDERED that, pursuant to sections 1, 2, 4(i), 4(j), 201, 202, 222, 225, 303(b), 303(r), 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 201, 202, 222, 225, 303(b), 303(r), 332, this Notice of Proposed Rulemaking IS ADOPTED.

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

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Proposed Rules

The Federal Communications Commission proposes to amend part 64 of Title 47 of the Code of Federal Regulations 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.

Subpart U – Customer Proprietary Network Information

2. Amend § 64.2011 by revising paragraphs (a) through (e) to read as follows:

§ 64.2011 Notification of customer proprietary network information security breaches.

(a) A telecommunications carrier shall notify affected customers, the Federal Communications Commission (Commission), and other federal law enforcement of a breach of its customers' CPNI as provided in this section.

(b)(1) As soon as practicable after reasonable determination of a breach, a telecommunications carrier shall electronically notify the Commission, the United States Secret Service (USSS), and the Federal Bureau of Investigation (FBI) through a central reporting facility maintained by the Commission and made available on its website.

(2) If 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.

(c) *Customer Notification.* A telecommunications carrier shall notify affected customers of covered breaches of CPNI without unreasonable delay after discovery of the breach after notification to the Commission and law enforcement as described in paragraph (b) of this section.

(d) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Federal Communications Commission, USSS, and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(e) *Definitions.* As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI.

* * * * *

3. Amend § 64.5111 by revising paragraphs (a) through (e) to read as follows:

§ 64.5111 Notification of customer proprietary network information security breaches.

(a) A TRS provider shall notify affected customers, the Federal Communications Commission (Commission), and other federal law enforcement of a breach of its customers' CPNI as provided in this section.

(b)(1) As soon as practicable after reasonable determination of a breach, a TRS provider shall electronically notify the Commission, the United States Secret Service (USSS), and the Federal Bureau of Investigation (FBI) through a central reporting facility maintained by the Commission and made available on its website.

(2) If 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 provider .

(c) *Customer Notification.* A TRS provider shall notify affected customers of covered breaches of CPNI without unreasonable delay after discovery of the breach after notification to the Commission and law enforcement as described in paragraph (b) of this section.

(d) *Recordkeeping.* All TRS provider shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Federal Communications Commission, USSS, and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. TRS providers shall retain the record for a minimum of 2 years.

(e) *Definitions.* As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI.

* * * * *

APPENDIX B

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities by the policies and rules proposed in this Notice of Proposed Rulemaking (Notice). The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided on the first page of the Notice. The Commission will send a copy of the Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the Notice and IRFA (or summaries thereof) will be published in the Federal Register.[3]

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

2. The Commission first adopted a rule in 2007 requiring telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers to notify customers and federal law enforcement of breaches of customer proprietary network information (CPNI) in the carriers' possession.[4] In the almost decade and a half since that time, data breaches nationwide have increased in both frequency and severity in all industries. In the telecommunications industry, the public has suffered an increasing number of security breaches of customer information in recent years. Federal and state data breach laws covering other areas have evolved since 2007. Those developments combined with our specific experience suggest opportunities for improvement in our own breach notification rule. Today, we begin the process to update and strengthen our data breach rule to provide greater protections to the public.

3. The Commission adopted the data breach rule, like the rest of the privacy safeguards adopted in the *2007 CPNI Order*, to address the problem of "pretexting," the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.[5] In the almost 15 years since, it has become clear that breaches of customer information in many contexts extend far beyond pretexting in general or the specific type of pretexting addressed at that time and are increasing in scale and evolving in methodology. The increasing severity and diversifying methods of security breaches involving customer information can have lasting detrimental impacts on customers whose information has been breached.

4. To better protect telecommunications customers and ensure that our rules keep pace with today's challenges, we propose a number of updates to our rule addressing telecommunications carriers' breach notification duties. We seek to ensure that affected customers, the Commission, and other federal law enforcement agencies receive the information they need in a timely manner so they can mitigate and prevent harm due to the breach and take action to deter future breaches. To identify best practices and to minimize burdens, we look to other federal and state breach laws as potential models for our rules.

5. In this *Notice*, we propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for

---

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

[2] *See* 5 U.S.C. § 603(a).

[3] *See* 5 U.S.C. § 603(a).

[4] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*); 47 CFR § 64.2011.

[5] *2007 CPNI Order*, 22 FCC Rcd at 6928, paras. 1-2 & n.1.

breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. We also seek comment on whether we should adopt minimum requirements for the content of customer breach notices, and we seek comment on whether our rules should address breaches of other types of sensitive personal information beyond CPNI. Finally, we propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

B. Legal Basis

6. The legal basis for any action that may be taken pursuant to this Notice is contained in sections 1, 4(i), 4(j), 201, 202, 222, 225, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 202, 222, 225, 303(r), 332.

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

7. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and by the rule revisions on which the Notice seeks comment, if adopted.[6] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[7] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[8] 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.[9]

8. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[10] 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.[11] These types of small businesses represent 99.9 percent of all businesses in the United States, which translates to 32.5 million businesses.[12]

9. 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."[13] The

[6] *See* 5 U.S.C. § 603(b)(3).

[7] *See* 5 U.S.C. § 601(6).

[8] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[9] *See* 15 U.S.C. § 632.

[10] *See* 5 U.S.C. § 601(3)-(6).

[11] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf (Nov 2021).

[12] *Id*.

[13] 5 U.S.C. § 601(4).

Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[14] Nationwide, for tax year 2018, there were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[15]

10. 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."[16] U.S. Census Bureau data from the 2017 Census of Governments[17] indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[18] Of this number there were 36,931 general purpose governments (county,[19] municipal and town or township[20]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[21] with enrollment

[14] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* IRS, *Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), Who May File Form 990-N to Satisfy Their Annual Reporting Requirement*, https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard (last visited Aug. 2, 2021). We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[15] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for Region 1-Northeast Area (76,886), Region 2-Mid-Atlantic and Great Lakes Areas (221,121), and Region 3-Gulf Coast and Pacific Coast Areas (273,702) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[16] 5 U.S.C. § 601(5).

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

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

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

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

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

populations of less than 50,000.[22] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[23]

1. Wireline Carriers

11. *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.[24] 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.[25] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[26] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[27]

12. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[28] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[29] Of this number, 2,964 firms operated with fewer than 250 employees.[30] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services.[31] Of these providers, the Commission estimates that 4,737

---

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

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

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

[25] *Id.*

[26] *Id.*

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

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

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

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

[31] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

providers have 1,500 or fewer employees.[32] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. *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[33] is the closest industry with an SBA small business size standard.[34] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[35] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[36] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[37] Of this number, 2,964 firms operated with fewer than 250 employees.[38] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were fixed local exchange service providers.[39] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[40] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

14. *Incumbent LECs*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. Wired Telecommunications Carriers[41] is the closest industry with an SBA small business size standard.[42] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[43] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[44] Of this number, 2,964 firms operated with fewer than 250 employees.[45] Additionally, based

---

[32] *Id.*

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

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

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

[36] *Id.*

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

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

[39] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[40] *Id.*

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

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

[43] *Id.*

[44] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311,

(continued….)

on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers.[46] Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees.[47] 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.

15. *Competitive Local Exchange Carriers (Competitive LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers.[48] Wired Telecommunications Carriers[49] 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.[50] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[51] Of this number, 2,964 firms operated with fewer than 250 employees.[52] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers.[53] Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees.[54] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

16. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[55] is the closest industry with a SBA small business size standard.[56] The SBA small business size

(Continued from previous page)
https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

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

[46] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[47] *Id.*

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

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

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

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

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

[53] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/pubId.lic/attachments/DOC-379181A1.pdf.

[54] *Id.*

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

standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[57] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[58] Of this number, 2,964 firms operated with fewer than 250 employees.[59] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 providers have 1,500 or fewer employees.[60] 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.

17. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended (the Act), also contains a size standard for small cable system operators, 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."[61] For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice.[62] Based on industry data, only six cable system operators have more than 677,000 subscribers.[63] Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note 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.[64] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable

(Continued from previous page)

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

[57] *Id.*

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

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

[60] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[61] 47 U.S.C. § 543(m)(2).

[62] *FCC Announces New Subscriber Count for the Definition of Small Cable Operator*, Public Notice, 16 FCC Rcd 2225 (CSB 2001) (*2001 Subscriber Count PN*). In this Public Notice, the Commission determined that there were approximately 67.7 million cable subscribers in the United States at that time using the most reliable source publicly available. *Id*. We recognize that the number of cable subscribers changed since then and that the Commission has recently estimated the number of cable subscribers to traditional and telco cable operators to be approximately 58.1 million. *See Communications Marketplace Report*, GN Docket No. 20-60, 2020 Communications Marketplace Report, 36 FCC Rcd 2945, 3049, para. 156 (2020) (*2020 Communications Marketplace Report*). However, because the Commission has not issued a public notice subsequent to the *2001 Subscriber Count PN,* the Commission still relies on the subscriber count threshold established by the *2001 Subscriber Count PN* for purposes of this rule. *See* 47 CFR § 76.901(e)(1).

[63] S&P Global Market Intelligence, S&P Capital IQ Pro, *Top Cable MSOs 12/21Q (*last visited May 26, 2022); S&P Global Market Intelligence, Multichannel Video Subscriptions, Top 10 (April 2022).

[64] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules. *See* 47 CFR § 76.910(b).

operators under the definition in the Communications Act.

18. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a size standard 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[65] is the closest industry with a SBA small business size standard.[66] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[67] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[68] Of this number, 2,964 firms operated with fewer than 250 employees.[69] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services.[70] Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees.[71] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

2. Wireless Carriers

19. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[72] 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.[73] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[74] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[75] Of that number, 2,837 firms employed fewer than 250 employees.[76] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report,

---

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

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

[67] *Id.*

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

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

[70] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[71] *Id.*

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

[73] *Id.*

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

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

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

as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[77] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[78] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

20. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[79] 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.[80] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[81] Of this number, 242 firms had revenue of less than $25 million.[82] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[83] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[84] Consequently, using the SBA's small business size standard, a little more than of these providers can be considered small entities.

3. Resellers

21. *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.[85] 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.[86] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[87] Mobile virtual network operators (MVNOs) are

---

[77] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[78] *Id.*

[79] US Census Bureau, *2017 NAICS Definitions, "517410 Satellite Telecommunications";* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017.

[80] *See* 13 CFR § 121.201, NAICS Code 517410.

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

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

[83] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[84] *Id.*

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

[86] *Id.*

[87] *Id*.

included in this industry.[88] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[89] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[90] Of that number, 1,375 firms operated with fewer than 250 employees.[91] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services.[92] Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees.[93] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

22. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[94] 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.[95] Mobile virtual network operators (MVNOs) are included in this industry.[96] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[97] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[98] Of that number, 1,375 firms operated with fewer than 250 employees.[99] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services.[100] Of these providers, the Commission estimates that

---

[88] *Id*.

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

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

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

[92] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[93] *Id.*

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

[95] *Id.*

[96] *Id*.

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

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

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

[100] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/pubId.lic/attachments/DOC-379181A1.pdf.

495 providers have 1,500 or fewer employees.[101] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

23. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business definition specifically for prepaid calling card providers. Telecommunications Resellers[102] 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.[103] Mobile virtual network operators (MVNOs) are included in this industry.[104] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[105] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[106] Of that number, 1,375 firms operated with fewer than 250 employees.[107] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services.[108] Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees.[109] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

4. Other Entities

24. *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.[110] 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.[111] 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.[112] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million

[101] *Id.*

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

[103] *Id.*

[104] *Id*.

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

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

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

[108] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[109] *Id.*

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

[111] *Id.*

[112] *Id*.

or less as small.[113] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[114] Of those firms, 1,039 had revenue of less than $25 million.[115] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

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

25. In this *Notice*, we propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. We also seek comment on whether we should adopt minimum requirements for the content of customer breach notices, and we seek comment on whether our rules should address breaches of other types of sensitive personal information beyond CPNI. Finally, we propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

26. Should the Commission decide to modify existing rules or adopt new rules to strengthen our data breach reporting rule, such action could potentially result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance requirements for affected providers of service. We seek comment on the effect of any proposals on small entities. Entities, especially small businesses, are encouraged to quantify the costs and benefits of any reporting, recordkeeping, or compliance requirement that may be established in this proceeding.

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

27. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rules for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities. [116]

28. The *Notice* seeks comment on the particular impacts that the proposed rules may have on small entities. Specifically, the *Notice* seeks comment on whether there are unique concerns or compliance barriers for small carriers that make notice to customers without unreasonable delay unfeasible;[117] if there should be different notification requirements for small carriers;[118] if streamlining

---

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

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

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

[116] 5 U.S.C. § 603(c)(1)-(4).

[117] *See supra* at para. 35.

notice requirements will benefit small providers;[119] if a centralized reporting portal would reduce compliance barriers for small providers;[120] and if a threshold trigger would benefit small providers.[121]

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

29. None.

(Continued from previous page)

[118] *Id.*

[119] *See supra* at para. 40.

[120] *See supra* at para. 25.

[121] *See supra* at para. 30.

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Data Breach Reporting Requirements*, WC Docket No. 22-21, Notice of Proposed Rulemaking (January 5, 2023).

Our mobile phones are in our palms, pockets, and purses. We rarely go anywhere without them. There is good reason for this—the convenience and safety of being able to reach out anytime and virtually anywhere is powerful. But this always-on connectivity means that our carriers have access to a treasure trove of data about who we are, where we have traveled, and who we have talked to.

It is vitally important that this deeply personal data does not fall into the wrong hands. That is why the Federal Communications Commission has long had rules that require carriers to protect the privacy and security of data, under Section 222 of the Communications Act. But the rules this agency has on the books that require carriers to notify consumers and law enforcement of data breaches under Section 222 are more than 15 years old.

That is why we kick off a proceeding to modernize our data breach rules here. We propose to eliminate the outdated seven business day mandatory waiting period before notifying customers, require the reporting of inadvertent but harmful data breaches, and ensure that the agency is notified of major data breaches. We also seek comment on how our breach reporting obligations can work alongside those forthcoming from the Cybersecurity and Infrastructure Security Agency under the Cyber Incident Reporting for Critical Infrastructure Act. I look forward to the record that develops—and updating our policies under the law.