Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS ON NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC)

Submitted February 22, 2023

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Summary

The Commission's Notice of Proposed Rulemaking regarding data breach reporting requirements is an important recognition of the increasingly severe and frequent harms suffered by consumers as a result of inadequate data security practices that fail to safeguard an increasingly vulnerable network. We applaud the Commission for its attention to this issue and encourage the FCC to continue to take a leadership role in advancing the security of America's telecommunications networks.

In particular, we urge the Commission to prioritize: tools to help protect consumers from the downstream harms that can result from breaches such as identity theft and account compromise, enhanced data security standards that require carriers to do more to prevent breaches from happening in the first place, and processes that empower Commission staff to support multi-agency efforts to respond nimbly to new attack patterns and shore up network vulnerabilities. We believe this includes the Commission's proposals to expand the definition of breach, to extend its data security protections to non-CPNI data, and to require remediation measures in notifications, but would be ill-served by filtering breach notifications through a threshold harm requirement.

Table of Contents

Comments

I. Introduction

The **Electronic Privacy Information Center (EPIC)** files these comments to applaud the Federal Communications Commission ("Commission" or "FCC") for its attention to the increasingly severe and largely avoidable harms of data breaches on phone subscribers, and to urge the Commission to adopt rules that prioritize: equipping consumers to mitigate downstream harms resulting from data breaches, informing the Commission's staff of possible network vulnerabilities, and implementing a higher standard for what constitutes basic data security practices to prevent consumer data from breached in the first place.

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has long defended the rights of consumers and has played a leading role in developing the Commission's authority to address emerging privacy and cybersecurity issues.[1] EPIC routinely urges the Commission to adopt and improve rules that protect consumers from exploitative data practices.[2]

[1] *See, e.g.*, *In re* Implementation of the Telecommunications Act of 1996, Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, CC Docket. No. 96-115, RM-11277 (Aug. 30, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513325075.

[2] *See, e.g.*, *In re* Empowering Broadband Consumers Through Transparency, Comments on FNPRM by Center for Democracy & Technology, Electronic Privacy Information Center, and Ranking Digital Rights, CG Docket No. 22-2 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/102161424008021; *In re* Location-Based Routing for Wireless 911 Calls, Comments of EPIC, PS Docket No. 18-64 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009; *In re* Rates for Inmate Calling Services, Comment Letter by EPIC, WC Docket No. 12-375 (Dec. 15, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/121545964412).

The Commission asks several questions that address what constitutes a reportable event (e.g. questions concerning inadvertent breach,[3] likelihood of harm,[4] non-CPNI breach-reporting requirements,[5] and minimum threshold of affected customers[6]). We support the Commission's proposals to expand the definition of breach, to extend its data security protections to non-CPNI data, and to require information about remediation measures in notifications. We urge the Commission to avoid incorporating any harm requirement (including exemptions for encrypted data) and urge the Commission to reiterate that its data security protections apply to program applicants not merely to active subscribers. We also offer commentary on the timetable and content of notifications, both to consumers and to the Commission. Finally, we offer a simple explanation for why Congressional disapproval of the Commission's *2016 Privacy Order* should not be an obstacle to this rulemaking.

II. The Commission Should Expand the Definition of Breach to Reflect Modern Reality.

EPIC supports the Commission's proposal to expand the definition of breach to cover instances of unauthorized access or misuse beyond pretexting, including inadvertent or accidental disclosures.[7] EPIC applauds and wholly agrees with the Commission's analysis that breaches have become more prevalent, that scammers and phishers have become more prevalent, that affected consumers must be informed of privacy risks in order to better protect themselves and their personal data, and that requiring determinations of intentionality (like harm, see below)

[3] *See* Fed. Commc'ns Comm'n, *In re* Data Breach Reporting Requirements, Notice of Proposed Rulemaking in WC Docket No. 22-21, 88 Fed. Reg. 3953, 3954 at ¶ 3 (Jan. 23, 2023), https://www.federalregister.gov/d/2023-00824/p-22 [hereinafter "NPRM"].
[4] *See* NPRM at 3955 ¶ 8, https://www.federalregister.gov/d/2023-00824/p-27.
[5] *See id.* at ¶ 13, https://www.federalregister.gov/d/2023-00824/p-32.
[6] *See id.* at 3956-57 ¶ 20, https://www.federalregister.gov/d/2023-00824/p-39.
[7] *See id.* at 3954 ¶ 3, https://www.federalregister.gov/documents/2023/01/23/2023-00824/data-breach-reporting-requirements#p-22.

can result in legal ambiguity and underreporting. EPIC also applauds and agrees with the Commission's analysis that requirements to notify accidental breaches will encourage carriers to adopt stronger data security practices and help the Commission to identify and address systemic network vulnerabilities.[8] EPIC also supports the Commission's proposal to protection non-CPNI proprietary information[9] (discussed further in Section III below).

In its most recent annual report, the Identity Theft Resource Center estimated a record-breaking 1,862 data breaches occurred in 2021.[10] A survey by IBM attributes a recent decline in response capabilities to the fact that approximately only one quarter of organizations with response plans (itself only 77% of organizations) apply them across the enterprise and that one quarter of organizations with plans admitted that their plans were informal or ad hoc.[11] One cybersecurity certification company identified numerous deficiencies resulting from inadequate staffing, including patching vulnerabilities in a timely fashion, engaging in ongoing risk assessment and management, and training employees.[12] Companies must be required to invest in staff and procedures to safeguard the consumer data with which they have been entrusted, or multiple widescale breaches will continue to occur every year. The proprietary information of

[8] *See id.*
[9] *See id.* at ¶ 13, https://www.federalregister.gov/d/2023-00824/p-32.
[10] *See Record Number of Data Breaches in 2021*, IAPP Daily Dashboard (Jan. 25, 2022), https://iapp.org/news/a/record-number-of-data-breaches-in-2021/ (citing to ITRC report which estimated "1,862 breaches last year, up 68% from the year prior, and exceeded 2017's previous record of 1,506").
[11] *See* IBM Security, *Cyber Resilient Organization Study* at 8 (2020), https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.
[12] *See* (ISC)^2, *Cybersecurity Workforce Study* 2022 at 10 (2022), https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx. The Commission notes much of this itself in its NPRM. *See, e.g.*, NPRM at 3956 ¶ 15 https://www.federalregister.gov/d/2023-00824/p-34 ("Large-scale security breaches can also be the result of lax or inadequate data security practices and employee training.").

subscribers of each of the three largest carriers, for example, has been breached at least once within the last five years.[13]

Downstream consumer harms resulting from data breaches can include identity theft and other forms of account compromise. The Federal Trade Commission (FTC) reported in 2020 and in 2021 that credit card fraud and government documents or benefits fraud individually accounted for more than 27% of identity theft reports nationwide.[14] In 2021, the Department of Justice found that 68% of victims of identity theft suffered $1 or more in direct financial losses with their most recent incident of identity theft,[15] and estimated that this fraud cost the U.S. economy more than $15 billion.[16] For example, in late 2020, websites used to generate auto insurance quotes were exploited to obtain personal data later used to submit fraudulent claims for pandemic and unemployment benefits.[17] Breached proprietary information could be used to similar ends.

---

[13] *See*, *e.g.*, Lily Hay Newman, *T-Mobile's $150 Million Security Plan Isn't Cutting It*, Wired (Jan. 20, 2023), https://www.wired.com/story/tmobile-data-breach-again/; Brian Krebs, *It Might Be Our Data, But It's Not Our Breach*, KrebsOnSecurity (Aug. 11, 2022), https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/; Sergiu Gatlan, *Verizon notifies prepaid customers their accounts were breached*, Bleeping Computer (Oct. 18, 2022), https://www.bleepingcomputer.com/news/security/verizon-notifies-prepaid-customers-their-accounts-were-breached/.

[14] *See* FTC, *Consumer Sentinel Network: Data Book* 2020 at 9 (2021), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf (dividing number of reports by theft type by total identity theft reports).

[15] *See* Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft*, 2018 at 9 (Apr. 2020), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

[16] *See id.* at 1 ($15.1 billion in total financial losses due to identity theft where the victim lost $1 or more). This was also true in the DOJ's two prior reports. *See* Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft*, 2016 at 1 (Jan. 2019), https://bjs.ojp.gov/content/pub/pdf/vit16.pdf ($17.5 billion); Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft*, 2014 at 7 (Sept. 2015), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf ($15.4 billion).

[17] *See* Industry Letter Re: Cyber Fraud Alert, N.Y. State Dep't of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

The impacts of identity theft can be far-reaching, discovered only after downstream harms have occurred (e.g., through a collections notice for a bill the consumer never incurred nor knew of before receiving the notice), and difficult to remedy after the fact. A Government Accountability Office report indicated that past victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[18] Yet these harms do not appear on the victim's bank statement or credit report, and can be nearly impossible to control where a Social Security Number (SSN) is used, by virtue of the role the SSN plays as a government and private-sector identifier.[19] To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.[20]

Although it is difficult to remedy the harms of identity theft after the fact, preventing the underlying breach is neither difficult nor expensive. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable,[21] and more recently the Internet Society has estimated 95 percent of breaches could have been prevented.[22] The FTC has often noted that reasonable security measures are a relatively low cost.[23] Renowned security

---

[18] U.S. Gov't Accountability Off., GAO-14-34, Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent at 11 (2013), http://www.gao.gov/assets/660/659572.pdf.
[19] *See* Br. of Amicus Curiae EPIC, *Storm v. Paytime, Inc.*, No. 15-3690 (3d Cir. Apr. 18, 2016) at 14, https://epic.org/documents/storm-v-paytime-inc/.
[20] *See id.* at 13.
[21] *See* 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016), https://www.us-cert.gov/ncas/alerts/TA15-119A. The California Attorney General's Office similarly concluded that many of the hundreds of breaches it studied could have been prevented, or detected and corrected more rapidly, by implementation of its recommended data security controls. *See* Kamala D. Harris, Attorney General, *California Data Breach Report* at 32 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[22] *See* Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* at 3 (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.
[23] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter; Complaint, *In re SkyMed International, Inc.,* FTC File No. 1923140 at ¶ 23 (Jan. 26, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-

technologist and fellow at Harvard Kennedy School Bruce Schneier recently observed in the New York Times:

> In all of these cases, the victimized organizations could have very likely protected our data better, but the reality is that the market does not reward healthy security. Often customers aren't even able to abandon companies with poor security practices, as many of them build "digital moats" to lock their users in. Customers don't abandon companies with poor security practices. Hits to the stock prices quickly recover. It's a classic market failure of a powerful few taking advantage of the many, and that failure is one that only representation through regulation can fix.[24]

Two professors at Antonin Scalia Law School have similarly argued, in a recent Michigan Technology Law Review article, that a strict liability regime would correct for the current failure of firms to internalize the cost and benefits of their data security decisions.[25] They further argue that the firm has incentives to take socially optimal security precautions—which will in turn lead to socially optimal data collection decisions—if a firm internalizes the harm,[26] and moreover that strict liability would facilitate cyber insurance calibrated to an optimal standard of care.[27]

This strongly suggests that the cost and harm to consumers and to the American economy (due to fraud facilitated by identity theft) that result from data breaches would be better

---

matter; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 at ¶ 11 (Dec. 30, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc; Complaint, *In re LightYear Dealer Technologies, LLC*, FTC File No. 1723051 at ¶ 22 (Sept. 6, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter; Complaint, *FTC v. Equifax, Inc.*, No. 1:2019-cv-03297 at ¶¶ 23(A)(iv), 24 (N.D. Ga. Jul. 22, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc; Complaint, *FTC v. Ruby Life Inc. d/b/a AshleyMadison.com*, No. 1:16-cv-02438 at ¶¶ 23(A)(iv), 24 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc.

[24] Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, The New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html.

[25] *See* James C. Cooper & Bruce H. Kobayashi, *Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem*, 28 Mich. Tech. L. Rev. 257, 263–64 (2022), https://repository.law.umich.edu/mtlr/vol28/iss2/3.

[26] *See id.* at 287.

[27] *See id.* at 295.

internalized as preventative data security costs incurred by the carriers (and their partners and vendors), which are best positioned to prevent the harm from occurring in the first place.

III. The Commission Should Articulate its Broad Data Security Authority.

EPIC supports the Commission's proposal to protect consumers from improper disclosure of non-CPNI data that is nonetheless still personal data and encourages the Commission to consider how legal authorities in addition to Section 222 can support this important goal. For example, the Commission has used Section 201(b) to enforce violations of basic data security practices and failure to notify consumers of a breach.[28] In a 2014 Notice of Apparently Liability (NAL), the Commission also stated explicitly that CPNI is a subset of proprietary information (PI) the unlawful disclosure of which is a violation of 201(b),[29] as well as noting that "proprietary information" encompasses "all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or reasons of personal privacy."[30] Notably, the order stated: "carriers are now on notice that in the future we fully intend to assess forfeitures for such violations."[31]

The Commission could also consider other context-specific authorities for protecting consumers from data breaches, for example Title III for breaches of wireless consumer data or Section 706 for breaches of broadband consumer data.

---

[28] *See, e.g.*, *In re* TerraCom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175, at ¶ 12 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1.pdf (provider failed to "employ reasonable data security practices to protect consumers' [Proprietary Information] PI" in violation of 201(b)) [hereinafter "2014 NAL"].

[29] *See id.* at ¶ 32 (citing to Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 FCC Rcd 6927 at 6946); *see also* id. at ¶¶ 14-16.

[30] *Id.* at ¶¶ 14-15.

[31] *Id.* at ¶ 53 (referring to failures related to data security and notice to consumers in connection with a security breach).

EPIC also notes that the Commission has brought enforcement actions in the past which indicate that the mere existence of an "unacceptable risk of identity theft and other serious consumer harms" may be sufficient to constitute a violation of the Communications Act, independently of whether any breach actually occurred.[32]

IV. The Commission Should Require Actionable Remediation Information in Breach Notifications.

We support and applaud the Commission's proposal to include remediation measures in the breach notification, addressing how customers, including customers with disabilities, can contact the carrier to inquire about the breach; how to contact the Commission or any other regulatory agency relevant to the customer and service; how to guard against identity theft (including credit monitoring, credit reporting, and/or credit freezes); and other steps customers should take to mitigate their risk based on the specific information exposed in the breach.[33] In this way, the breach notification not only informs the consumer of the risks they face but also equips the consumer with options for immediate steps to reduce the downstream harms that may result.

V. The Commission Should Not Delay Breach Notifications and Expose Consumers to Unnecessary Risk by Implementing a Harm Trigger.

EPIC urges the Commission to avoid incorporating any harm requirement as a trigger in its breach notification regime. As with requiring determinations of intentionality (see above), establishing harm a threshold issue can result in legal ambiguity and underreporting. Additionally, it can result in delayed reporting as it may take time to assess whether the minimum threshold for reportable harm has been met. It is simpler, faster, and more consistent

[32] *See id.* at ¶ 1; *id.* at ¶¶ 33-34 (noting that "the Companies' data security practices created an unacceptable risk of unauthorized access" separate and apart from the breach of "approximately 128,066 proprietary records").
[33] *See* NPRM at 3958-59 ¶ 31, https://www.federalregister.gov/d/2023-00824/p-50.

and transparent to require covered entities to report any unauthorized disclosure or misuse of consumer information without filtering by harm (or even worse, by likelihood of harm).

For similar reasons, EPIC recommends that the Commission not exempt breaches solely involving encrypted data.[34] Whether breached data is encrypted is only relevant within a harm-based framework, and even within that framework only of limited relevance. Although a typical breach of encrypted data may present a lower risk of harm to consumers, encrypted data can nevertheless be compromised if a third party obtains access to the requisite encryption keys or is able to identify and exploit an additional security vulnerability. Rather than leaving it to covered entities to determine on a case-by-case basis how likely it is that encrypted data will be misused, they should be required to treat breaches of encrypted data like any other security event and submit a breach report to the Commission and to consumers. We further note that in 2014 the Commission stated that "given the state of the technology" "the lack of encryption clearly evidences the unjust and unreasonable nature of the Companies' data security practices", giving rise to a violation of 201(b). The Commission clarified that deploying encryption alone would not necessarily satisfy a carrier's duty under 222(a) nor render a carrier's practices just and reasonable under 201(b).[35]

EPIC does not take a position on the minimum threshold of affected customers at this time but reiterates that the Commission should not incorporate a harm trigger. Such a rule would convert what should be a routine report into a more resource-intensive filing that could be understood as implicit admission of liability by the reporting institution. This, in turn, may lead institutions to play down the likelihood of data misuse resulting from security events in order to

[34] *See* NPRM at 3955, ¶ 10, https://www.federalregister.gov/d/2023-00824/p-29.
[35] *See* 2014 NAL at ¶ 32.

evade the reporting requirement.[36] Moreover, any standard based on "likelihood" of harm is also highly malleable; every covered entity may use different risk calculations and legal analysis to determine whether such a threshold is met. To promote uniformity and clarity, the Commission should require covered entities to report each security event that implicates the personal information of a threshold number of consumers set by the Commission.

VI. The Commission Should Reiterate its Protections for Applicant Data.

EPIC urges the Commission to reiterate that its data security protections for consumers also apply to applicants seeking to become consumers—for example, Lifeline applicants.[37] This concern is particularly relevant as the Commission is considering expanding access for survivors of domestic violence to its Lifeline and Affordability Connectivity Programs.[38]

VII. The Commission Should Require Basic Content and a Timeframe for Breach Reports.

The Commission asks what information should be included in a breach report to consumers.[39] We support the Commission's proposal to require the date of the breach (or the date range, where appropriate), as well as the name and contact information of the breached entity. We also support the Commission's proposal to require a detailed description of the types of

[36] The Center for Information Technology Policy at Princeton University made a similar point to the Federal Trade Commission in the context of the FTC's Safeguards Rule NPRM, which addressed breach notifications for financial institutions. *See* Ctr. for Info. Tech. Pol'y, Comments on Standards for Safeguarding Customer Information 7 (Aug. 2, 2019), https://downloads.regulations.gov/FTC-2019-0019-0054/attachment_1.pdf ("Basing the reporting threshold on the likelihood of consumer harm could disincentivize receiving timely and comprehensive reports as that could require making a more involved legal judgment.").

[37] *See* 2014 NAL at ¶ 6 (breach of Lifeline applicant data), ¶¶ 21-23 (protections apply immediately, not after consumer becomes actual subscriber), ¶ 28 (222(a) includes applicants, not merely customers).

[38] *See In re* Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program, Notice of Proposed Rulemaking in WC Docket Nos. 22-238, 11-42, 21-450 (Feb. 17, 2023), https://www.fcc.gov/document/fcc-looks-help-domestic-violence-survivors-access-connectivity-0.

[39] *See* NPRM at 3958-59, ¶¶ 29-31, https://www.federalregister.gov/documents/2023/01/23/2023-00824/data-breach-reporting-requirements#p-48.

information involved in the breach, information about how the breached entity will contact consumers to avoid phishing scams related to the breach, and remediation measures (as discussed above).

The Commission also asks what information should be included in a breach report to the Commission.[40] We support the Commission's approach of using breach notifications it receives to "provide Commission staff important information about data security vulnerabilities that Commission staff can help address and remediate,"[41] not unlike the Information Sharing and Analysis Organizations within the Cybersecurity & Infrastructure Security Agency.[42] Many entities concerned with industry-level cybersecurity publish risk alerts based on breach notifications they receive from the private sector to prevent known attack methodologies from impacting additional businesses.[43] To this end, we support covered entities sharing a detailed description of the breach to the Commission.

The Commission asks about the timeframe for notifications.[44] EPIC does not take a position on a specific deadline but notes that in several states, entities are required to report incidents to the attorney general within three days.[45] Most states also require that direct

---

[40] *See id.* at 3956 ¶ 15, https://www.federalregister.gov/d/2023-00824/p-34.
[41] *Id.*
[42] *See* United States Cybersecurity & Infrastructure Security Agency, Information Sharing and Analysis Organizations (ISAOs), https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos.
[43] *See, e.g.*, *Private Industry Notification, Cyber Criminals Targeting Healthcare Payment Processors, Costing Victims Millions in Losses*, PIN 20220914-001, FBI Cyber Division (Sept. 14, 2022), https://www.americanbar.org/content/dam/aba/administrative/cybersecurity-legal-task-force/fbi-alert-220914-2.pdf; Industry Letter Re: Cyber Fraud Alert, *supra* note 17.
[44] *See* NPRM at 3956 ¶ 19, https://www.federalregister.gov/d/2023-00824/p-38 (notification to the Commission); *id.* at 3957 ¶ 22, https://www.federalregister.gov/d/2023-00824/p-41 (notification to consumers).
[45] *See* Nat'l Conf. of State Legis., *2021 Security Breach Legislation* (Jan. 12, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/2021-security-breach-legislation.aspx; Spirion, New U.S. Data Protection Laws Enforceable in 2020 (2020), https://www.spirion.com/wp-content/uploads/2020/04/SPIRION-Datasheet-US-State-Data-Protection-Laws-2019-WEB.pdf.

notification to affected individuals be sent as expeditiously as possible and without undue delay, even where a state's outer limit is 30, 45, or 60 days.[46] Although EPIC recognizes a breached entity's need to address the underlying vulnerability(ies) that led to a breach, we urge the Commission to prioritize equipping consumers to protect themselves against downstream harms resulting from a breach.

VIII. The Congressional Review Act Does Not Preclude the Commission from Improving Data Security Practices.

The Commission seeks comment on the scope of Congressional disapproval of its *2016 Privacy Order*.[47] Congressional disapproval of the *2016 Privacy Order* under the Congressional Review Act (CRA) was largely in response to the creation of duplicative privacy authority to the Federal Trade Commission's as relates to broadband internet service providers.[48] Here, the Commission is seeking to address data security rules to protect users of telecommunications and interconnected VoIP providers, building upon rules that have existed since 2007.[49] While data security and privacy are related, and while some companies offer both telecom and broadband services, there is daylight between what the Commission is proposing in this rulemaking and what falls within the scope of Congress' disapproval of the *2016 Privacy Order*. We would further note that changes in underlying circumstances or in the agency's cost-benefit analysis,

[46] *See* Chelsea Saniuk-Heinig, *State Data Breach Notification Chart* (Mar. 2021), https://iapp.org/resources/article/state-data-breach-notification-chart/.
[47] *See* NPRM at 3960 ¶ 44, https://www.federalregister.gov/d/2023-00824/p-63.
[48] *See, e.g.*, Comments of RWA, WC Docket No. 21-341, at 9 (filed Nov. 15, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/1115194054299 (citing to Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission, 163 Cong. Rec. H2489, H2489 (2017) (statement of Rep. Blackburn)).
[49] *See* NPRM at 3961 ¶ 2, https://www.federalregister.gov/d/2023-00824/p-68.

among other considerations, would be relevant to a determination as to whether a new rule is "substantially the same" as a disapproved one.[50]

IX. Conclusion

We applaud the Commission's attention to the increasingly severe and largely avoidable impacts of data breaches on phone subscribers and appreciate the opportunity to respond to the Commission's NPRM on data breach requirements, to better protect consumers from breaches and downstream harms as well as to strengthen the overall security of America's networks.

Respectfully submitted, this the 22nd day of February 2023, by:

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
frascella@epic.org

[50] *See, e.g.*, Comments of RWA *supra* note 48 at 7-11 (noting recent DOL rule disapproved under CRA later resubmitted with broader scope and unchallenged by Congress, and arguing prevalence of data breaches has become endemic problem within telecom industry within recent years).