epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

Request for Comment on Standards for Safeguarding Customer Information

86 Fed. Reg. 70,062

February 7, 2022

By notice published on December 9, 2021, the Federal Trade Commission ("FTC" or "Commission") has requested comment on a proposed supplemental rulemaking to further amend the Standards for Safeguarding Customer Information ("Safeguards Rule").[1] The FTC's proposed amendment would "require financial institutions to report to the Commission any security event where the financial institutions have determined misuse of customer information has occurred or is reasonably likely and at least 1,000 consumers have been affected or reasonably may be affected."[2]

The Electronic Privacy Information Center ("EPIC") submits these comments in support of the proposed amendment and to share additional recommendations and expertise with the Commission. EPIC is a public interest research center in Washington, D.C. established in 1994 to focus on public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in data protection and has played a leading role in developing the authority of the FTC to address emerging privacy and

[1] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,062 (Dec. 9, 2021), https://www.federalregister.gov/documents/2021/12/09/2021-25064/standards-for-safeguarding-customer-information.
[2] *Id.*

cybersecurity issues and to safeguard the privacy rights of consumers.[3] EPIC routinely files comments in response to proposed FTC rules and consent orders as well as complaints concerning business practices that violate privacy rights.[4] EPIC previously filed comments in response to the FTC's proposed (and now final) amended Standards for Safeguarding Customer Information,[5] and EPIC recently called on the Commission to increase enforcement under the Safeguards Rule.[6]

EPIC urges the Commission to adopt the proposed amendment requiring security event reporting to the Commission. This safeguard will further incentivize the use of strong data security measures by financial institutions, bring additional accountability and transparency to the handling of security events, and enhance the data security and privacy of all consumers. In response to the questions posed by the Commission in its supplemental notice of proposed rulemaking, EPIC offers the following additional recommendations: (1) the Commission should require that the four proposed elements be included in all security event notices but should also demand a more comprehensive

---

[3] *See, e.g.*, Consumer Reports & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities* (June 2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.

[4] *See, e.g.*, Comments of EPIC, *In re Matter of Support King, LLC (SpyFone.com)* (Oct. 8, 2021), https://archive.epic.org/apa/comments/In-re-SpyFone-Order-EPIC-comment-100821.pdf; Comments of EPIC et al., *In re Zoom Video Communications, Inc.* (Dec. 14, 2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; Complaint of EPIC, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf; Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Petition of EPIC, *In re Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce* (Feb. 3, 2020), https://epic.org/privacy/ftc/ai/epic-ai-rulemaking-petition/; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *In re Unrollme, Inc.,* FTC File No. 172-3139 (Sept. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (Sept. 3, 2019), https://epic.org/apa/comments/EPIC-FTC-CambridgeAnalytica-Sept2019.pdf; Complaint of EPIC, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf.

[5] EPIC, Comments on Standards for Safeguarding Customer Information (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf.

[6] EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy*, *supra* note 2, at 18–19.

account of the security event; (2) the Commission should require notification for any security event implicating the personal information of 1,000 or more customers and should not provide a carve out for encrypted data; (3) the Commission should look to state notification deadlines to inform the timing of security event reports; (4) the Commission should not allow an institution to withhold notice of a security event from the Commission but could delay public dissemination of that notice where there is a compelling law enforcement basis to do so; (5) the Commission should publish notification information by default, only delaying publication where there is a compelling law enforcement basis to do so or where the vulnerability causing the incident remains exploitable; (6) a stand-alone reporting requirement is appropriate because it will pose only a *de minimis* burden on most covered institutions; (7) the Commission should impose a requirement on covered entities to notify the Commission of security events; and (8) the Commission should impose a requirement on covered entities to notify affected consumers of security events implicating their personal information.

I. EPIC endorses the Commission's proposed elements for security event notices but urges the Commission to require more detail.

EPIC supports the proposed list of elements to be contained in any notice to the Commission and suggests more specific language for two elements. Affected financial institutions should be required to report the name and contact information of the reporting financial institution (element 1) and the date or date range of the security event if possible (element 3). EPIC suggests that financial institutions should also be required to provide a *comprehensive* description of the types of information involved in the security event (element 2) and a *comprehensive* description of the security event (element 4). It is critical that financial institutions provide a sufficiently detailed account of each security event to enable the FTC and affected consumers to assess whether and how personal information is at risk.

II. The Commission should require notification for any security event implicating the personal information of 1,000 or more customers and should not provide a carve out for encrypted data.

Any security event implicating the personal information of the threshold number of consumers—1,000 or more—should be reported to the Commission regardless of the financial institution's view on whether such information is likely to be misused. Tying the reporting requirement to a "likelihood" standard risks converting what should be a routine report into a more resource-intensive filing that is understood as an 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 evade the reporting requirement.[7] A "likelihood" standard is also highly malleable; every financial institution 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 financial institutions to report each security event that implicates the personal information of a threshold number of consumers set by the FTC.

For the same reasons, EPIC recommends that the Commission not provide a carve out for security events solely involving encrypted data. 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 financial institutions to determine on a case-by-case basis how likely it is that encrypted data will be misused, institutions should be required to treat breaches of encrypted data like any other security event and submit a report to the Commission if personal information from more than 1,000 customers is implicated.

[7] *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.").

III. The Commission should look to state notification deadlines to inform the timing of security event reports.

The Commission seeks input on the timing of security event reporting to the Commission. 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 just three days.[8] Most states also require that direct 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.[9]

IV. The Commission should not allow an institution to withhold notice of a security event from the Commission but could delay public dissemination of that notice where there is a compelling law enforcement basis to do so.

The Commission seeks comment on preventing or delaying notification to the FTC if notice would affect an ongoing law enforcement investigation. EPIC notes that the Commission has extensive experience collaborating with other enforcement agencies and maintaining the confidentiality of sensitive information. A financial institution or law enforcement agency should be permitted to show cause to the Commission as to why public dissemination of a security event notice should be delayed, but a law enforcement investigation of a security event should not be a basis to withhold notice from the Commission itself.

V. The Commission should publish notification information by default, only delaying publication where there is a compelling law enforcement basis to do so or where the vulnerability causing the incident remains exploitable. Incident data should still be included in aggregate reporting, even if it has not yet been published.

The Commission seeks input as to what circumstances would merit preventing or delaying publication of security event information or granting a financial institution's request for confidential

[8] *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.

[9] *See* Chelsea Saniuk-Heinig, *State Data Breach Notification Chart* (Mar. 2021), https://iapp.org/resources/article/state-data-breach-notification-chart/.

treatment of the required information. As the Commission notes, because it is not seeking confidential or proprietary information, there is no reason to implement any mechanism for requests for confidential treatment.[10] Security event information shared with the Commission should be reported to the public by default. However, if the vulnerability leading to the incident has not been fully resolved, the Commission should consider delaying publication until the vulnerability has been addressed. Additionally, as noted above, if a financial institution or law enforcement agency demonstrates that publication could interfere with an active investigation, that may also be a basis for delaying publication. Even where the Commission has determined that a delay in informing consumers about a security event would be justified, the Commission should incorporate the data from these events into any aggregate or statistical reporting the Commission provides to the public regarding security incidents, redacting details where necessary.

VI. A stand-alone reporting requirement is appropriate because it will pose only a *de minimis* burden on most covered institutions.

The Commission should implement a stand-alone reporting requirement regardless of whether a financial institution is required to provide notice of security events under another provision of federal or state law. Tethering the Commission's reporting requirement to other federal or state statutes, rules, and regulations would unduly limit the amended Safeguards Rule and undermine the FTC's mandate to protect consumers. The Commission's ability to understand and inform the public about the nature and frequency of security events would be limited by a patchwork of rules beyond the Commission's control, leading to an incomplete and inconsistent portrait of U.S. cybersecurity incidents involving personal data. The Commission has a unique charge to protect U.S. consumers, and other security event reporting rules may not be drafted with this same purpose in mind. Where, as here, the Commission finds that a reporting requirement would be beneficial to

[10] *See* Standards for Safeguarding Customer Information, *supra* note 1.

consumers, the Commission should not rely on other provisions of law to dictate the scope of that reporting.

Further, the stand-alone reporting requirement would in most cases impose a *de minimis* burden on financial institutions. If a security event is covered under the reporting requirements of another state or federal statute, rule, or regulation, then an institution need only to provide substantially the same notice to the Commission. At most, an institution would need to reformat material or provide additional details about the security event, but this would represent a modest administrative burden. In cases where a financial institution is not required already to report a security event under a similar notification rule, the proposed rule will offer a valuable safeguard for consumers potentially harmed by the security event. Thus, even if the Safeguards Rule would represent the only reporting mandate for a given security event, the Commission should still require the institution to notify the FTC and make the incident known to the public.

VII. The Commission should impose a requirement on covered entities to notify the Commission of security events.

For the reasons set forth above, the Commission should impose a requirement on covered entities to notify the FTC of security events. Doing so will further encourage the use of strong data security measures by financial institutions, bring additional accountability and transparency to the handling of security events, and enhance the data security and privacy of all consumers.

VIII. The Commission should impose a requirement on covered entities to notify affected consumers of security events implicating their personal information.

EPIC urges the Commission to require that covered entities provide timely notice to consumers of any breach or other security event implicating their customer information, subject only to the narrow bases for withholding information discussed *supra* in Parts IV and V. Public notice of security events is an essential feature of an effective data protection and cybersecurity framework. Ensuring that institutions directly notify consumers of security incidents involving their personal

information—especially in cases where those institutions are not already subject to a consumer notice requirement—is essential for consumers to understand, mitigate, and seek redress for the resulting risks to their privacy. Accordingly, the FTC should require notice of security events to affected consumers in all cases where notice to the Commission is required.

IX. Conclusion.

The Commission should adopt the proposed amendment to the Safeguards Rule consistent with the recommendations above. EPIC applauds the Commission for its continued attention to the security of consumers' personal information and thanks the Commission for considering EPIC's recommendations.

Sincerely,

/s/ John Davisson
EPIC Director of Litigation
& Senior Counsel

/s/ Sara Geoghegan
EPIC Law Fellow

/s/ Chris Frascella
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)