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

June 5, 2023

Ms. Vanessa Countryman
Secretary, Securities and Exchange Commission
By email: rule-comments@sec.gov

Re: S7-05-23, S7-06-23, Request for Comment on Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Cybersecurity Risk Management Rule, 88 FR 20616, 88 FR 20212

Secretary Countryman:

The Electronic Privacy Information Center (EPIC) hereby submits comments in response to the U.S. Securities and Exchange Commission (SEC or "Commission") April 5, 2023 Notice of Proposed Rulemaking[1] on a proposed cybersecurity risk management rule (Cybersecurity Audit NPRM) and the Commission's April 6, 2023 Notice of Proposed Rulemaking on proposed changes to Regulation S-P (Reg. S-P NPRM).[2] Data breaches, and the resulting harms they cause to consumers, are one of the most significant and omnipresent threats that individuals face. We commend the SEC for taking action to raise the bar for mitigation, notification, and oversight of breaches, and we offer these comments to suggest ways in which the rules could provide stronger and clearer incentives for SEC regulated entities to implement more robust data security practices.

The Commission's proposed changes to Reg. S-P would establish incident response requirements and a minimum data breach reporting requirement for all broker dealers, investment

[1] Cybersecurity Risk Management Rule, S7-06-23, 88 Fed. Reg. 20,212 (Apr. 5, 2022), https://www.federalregister.gov/documents/2023/04/05/2023-05767/cybersecurity-risk-management-rule-for-broker-dealers-clearing-agencies-major-security-based-swap [hereinafter "Cybersecurity Audit NPRM"].
[2] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, S7-05-23, 88 Fed. Reg. 20,616 (Apr. 6, 2022), https://www.federalregister.gov/documents/2023/04/06/2023-05774/regulation-s-p-privacy-of-consumer-financial-information-and-safeguarding-customer-information [hereinafter "Reg. S-P NPRM"].

companies, investment advisors, and transfer agents and would broaden the scope of information covered by the data security rules. These are important changes that would be a significant step in the right direction towards a stronger and more comprehensive national data breach regime. However, we believe that the Commission should further amend the rules to ensure that the incident response programs and data breach notifications carried out under Reg. S-P give consumers the information they need to understand and take any necessary action in response to a breach. The costs associated with the incident response programs and more robust notification regime serve an important forcing function for entities that might otherwise not adequately invest in safeguards on the front end. And those incentives, in conjunction with aggressive Commission enforcement of the safeguards rule itself and routine independent audits carried out under the proposed rules in the Cybersecurity Audit NPRM, are necessary to raise data security standards across the industry.

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 supporting regulatory authority to address emerging privacy and cybersecurity threats.[3] EPIC routinely urges regulators to adopt and improve rules that protect consumers from exploitative and harmful data practices.[4] We offer these comments in support of the Commission's efforts to raise the bar for data security and work to improve industry cybersecurity standards and practices. We also

[3] *See, e.g.*, Generating Harms: Generative AI's Impact & Paths Forward (May 2023), https://epic.org/documents/generating-harms-generative-ais-impact-paths-forward/; How the FTC Can Mandate Data Minimization Through a Section 5 Rulemaking (Jan. 2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/; What the FTC Could Be Doing (But Isn't) To Protect Privacy (June 2021), https://epic.org/documents/epic-ftc-unused-authorities-report-june2021-2/.

[4] *See, e.g.*, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; *In re* Data Breach Reporting Requirements, Comments of EPIC, WC Docket. No. 22-21 (Feb. 22, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527.

believe that the SEC must ensure that these rules are enforced and that regulated entities face financial penalty whenever they fail to safeguard the personal data that they collect.

Data Breaches Pose a Substantial Threat to Consumers and to Businesses

The Commission has requested that commentors speak to the quantitative and qualitative considerations that inform their economic analysis of the proposed regulations. One of the most important considerations for this rule is the scope of the harm and risk that consumers and businesses face every day because of insecure data practices. Nearly half of US consumers have been affected by data breaches where a company holding their personal data was hacked, compared to a global average of just 33% of consumers.[5] The costs of these breaches are staggering, and the Commission's proposals to establish minimum standards for incident response and breach notification can help with mitigation.

Ultimately the best way for a company to avoid the potential costs associated with the proposed rules is to adequately invest in data protection on the front end. Although it can be difficult to remedy the harms of identity theft after the fact, preventing the underlying breach is in many cases neither difficult nor expensive. The Department of Homeland Security has estimated that 85 percent of data breaches were preventable,[6] and more recently the Internet Society has estimated 95 percent of breaches could have been prevented.[7] The FTC has often noted that reasonable security measures are a relatively low cost.[8]

---

[5] *See* Prof. Carsten Maple, 2022 Consumer Digital Trust Index: Exploring Consumer Trust in a Digital World 9 (2022), available at https://cpl.thalesgroup.com/resources/encryption/consumer-digital-trust-index-report.

[6] *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.

[7] *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.

[8] *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),

Consumers bear the costs of inadequate data security practices, and breaches that fuel identity theft impose an especially heavy burden. 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."[9] 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.[10] To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.[11]

A company has better visibility than its consumers do into the threats to the privacy and security of consumer data entrusted to that company's custody; and the company's interests are not directly aligned with those of its consumers. That is why the Commission's role in enforcing the safeguards rule is an essential part of improving data security practices. If companies choose to collect data but fail to adequately protect data, they should face penalties and repercussions.

---

https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-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.

[9] 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.

[10] *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/.

[11] *See id.* at 13.

The new proposed Reg. S-P rules address the circumstances where a breach has already happened and seek to improve the ways that companies can work to mitigate the harm they have caused and to inform consumers about what has happened, what to expect, and what more can be done to prevent further harm. These rules should be crafted in a way that maximizes the useful information that consumers receive to ensure that they are able to understand what has happened and what they can and should do next. All too often companies either seek to skirt notification requirements altogether or provide vague or confusing notifications that leave the consumer in the dark. And this information asymmetry "prevents individual customers whose information has been compromised from taking timely actions."[12]

The Commission itself has observed that companies do not adequately invest in data security protection due in part to the existing information asymmetry between breached companies and impacted consumers:

> First, the information asymmetry prevents individual customers whose information has been compromised from taking timely actions (*e.g.,* increased monitoring of account activity, or placing blocks on credit reports) necessary to mitigate the consequences of such compromises. Second, the information asymmetry can lead covered institutions to generally devote too little effort (*i.e.,* "underspend") toward safeguarding customer information, thereby increasing the probability of information being compromised in the first place.[13]

Risk of reputational harm from mandated notifications can be a powerful motivator, and stronger notification requirements can effectively incentivize covered entities to improve their data security practices to avoid having to distribute breach notifications.[14] The Federal Communications Commission (FCC) similarly "anticipate[s] that requiring notification for accidental breaches will

[12] See Reg. S-P NPRM at III(B), https://www.federalregister.gov/d/2023-05774/p-690.
[13] See id.
[14] See id. at III(A), https://www.federalregister.gov/d/2023-05774/p-670 ("These benefits would result from covered institutions allocating additional resources towards information safeguards and cybersecurity to comply with the proposed new requirements and/or to avoid reputational harm resulting from the mandated notifications").

encourage telecommunications carriers to adopt stronger data security practices and will help us identify and confront systemic network vulnerabilities."[15]

The Commission's proposal to broaden the scope of entities and data subject to the safeguards, notification, and disposal rules to include data received from other institutions,[16] or entrusted to a third-party service provider,[17] is an important and laudable change. The Commission is attempting to raise the standard for data security, in response to an evolving threat environment;[18] it would be counterproductive to this goal for the Commission to permit some data to go unprotected merely because it came from a different source. Additionally, third-party service providers are specifically a favored attack vector and so the Commission's attention to this risk is well-directed.[19]

---

[15] See Fed. Commc'ns Comm'n, Data Breach Reporting Requirements, Proposed Rule, FCC 22-102, 88 FR 3953 ¶ 3 (Jan. 23, 2023), available at https://www.federalregister.gov/d/2023-00824/p-22 [hereinafter "FCC Breach Reporting NPRM"].

[16] See Reg. S-P NPRM at I, https://www.federalregister.gov/d/2023-05774/p-100 ("Applying the safeguards rule and the disposal rule to customer information that a covered institution receives from other financial institutions would better protect individuals by ensuring customer information safeguards are not lost when a third-party financial institution shares that information with a covered institution.")

[17] See id. at III(C)(3)(E), https://www.federalregister.gov/d/2023-05774/p-802 ("These contracting requirements on a covered institution would affect a third party service provider that "receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to [the] covered institution." ")

[18] See id. at I, https://www.federalregister.gov/d/2023-05774/p-80 ("Although many firms have improved their programs for safeguarding customer records and information in light of these observations, nonetheless we are concerned that some firms may not maintain plans for addressing incidents of unauthorized access to or use of data. We also are concerned the incident response programs that firms have implemented may be insufficient to respond to evolving threats or may not include well-designed plans for customer notification./We therefore preliminarily believe specifically requiring a reasonably designed incident response program, including policies and procedures for assessment, control and containment, and customer notification, could help reduce or mitigate the potential for harm to individuals whose sensitive information is exposed or compromised in a data breach.") (internal citations omitted)

[19] See, e.g., Kevin McCoy, Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers, USA Today (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/) ("For example, in 2013, attackers were reportedly able to use stolen credentials obtained from a third-party service provider to access a customer service database maintained by national retailer Target Corporation, resulting in the theft of information relating to 41 million customer payment card accounts."). Supply chain security literature suggests that third parties are often a preferred attack vector. See, e.g., ABA Cybersecurity Legal Task Force, Vendor Contracting Project: Cybersecurity Checklist Second Edition 1 (2021), https://www.potteranderson.com/media/publication/941_Vendor%20Contracting%20Project%20-%20Cybersecurity%20Checklist.pdf; Target Hackers Broke in Via HVAC Company, Krebs on Security (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

Reporting a Breach Equips Consumers to Protect Themselves from Downstream Harms

EPIC supports the Commission's efforts to establish a uniform minimum standard for breach notifications. However, the proposed definitions of "sensitive customer information" and "substantial harm or inconvenience" create an unnecessary circularity problem with the notification trigger in § 248.30(b)(3)(iii) and (b)(4). We recommend that the Commission instead impose a two-tiered notification requirement, where breaches that pose a reasonable risk of substantial harm or inconvenience are sent directly to customers, along with a description of the risks posed, and other breaches that do not pose a reasonable risk are announced transparently in an easily accessible format. The goal of these notifications should be to provide clear and transparent information about what data was impacted and what risks the breach reasonably poses to consumers.

Inconsistencies in data breach notifications can impact consumer mitigation response as well as consumer trust. Breach notifications should be timely, communicate the likelihood of harm to the affected consumer clearly, and present the consumer with options for immediate steps to reduce any downstream harms that may occur as a result of the incident (e.g. identity theft, account compromise).[20] And companies should be required to provide consumers with a general assessment of the risk posed by the breach. Timeliness is key because any delay will impact consumers ability to take steps to protect themselves from identity theft, account compromise, and other downstream impacts resulting from the initial harm of the unauthorized access. A breach notification regime is fundamentally deficient if it does not empower consumers with the information and tools necessary to take action to protect themselves, or at least to understand what risks they may face as a result of

[20] The FCC has proposed this as a required element of breach reporting to consumers. See FCC Breach Reporting NPRM at 3958-59 ¶ 31, https://www.federalregister.gov/d/2023-00824/p-50 ("(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").

the breach. It should not be incumbent on the consumer to know what harms may result from the breach; the communication from the breached entity should be clear.

Included in this last point of downstream harms, the Commission should require notifications to alert consumers as to what future communications from the company will look like, what email address they will come from, etc., as a proactive measure of protecting consumers from phishing attempts in which the fraudster poses as the breached company contacting their customers in the wake of a data breach, a recommendation the FCC has observed from Federal Trade Commission guidance.[21] This will reduce the likelihood of consumers falling victim to these types of scams.

EPIC strongly agrees with the Commission that a Federal minimum standard for customer (consumer) notification should:

> help affected customers understand how to respond to a data breach to protect themselves from potential harm that could result…. [and] protect individuals in an environment of enhanced risk… regardless of whether that data breach occurs at a broker-dealer, investment company, registered investment adviser, or transfer agent.[22]

However, EPIC disagrees with the Commission's proposal that notification is only necessary where a breach of sensitive customer information is likely to result in a substantial harm or inconvenience. The Commission notes that:

> [w]e do not believe that notification would be appropriate if unauthorized access to customer information is not reasonably likely to cause a harm risk because a customer is unlikely to need to take protective measures. Moreover, the large volume of notices that individuals might receive in the event of unauthorized access to such customer information could erode their efficacy.[23]

[21] See id. at ¶ 30 ("In its Data Breach Response Guide, the FTC advises companies on specific information that should be included in their breach notices to individuals, including…describing how the company will contact consumers in the future to help victims avoid phishing scams"); id at para 31 ("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?")
[22] See Reg. S-P NPRM at I, https://www.federalregister.gov/d/2023-05774/p-87.
[23] See, e.g. id. at II(4)(B) https://www.federalregister.gov/d/2023-05774/p-267.

Harms suffered by consumers as a result of data breaches can take many forms, not all of them financial.[24]

Companies experiencing cyber incidents should be trusted to communicate clearly the likelihood of harm to the impacted consumer, but a consumer should not be denied the opportunity to respond to a cyber incident when their data has been accessed without authorization.[25] Failing to notify the consumer of a cyber incident, due to a company's self-interested determination of whether the consumer was harmed, denies the consumer that opportunity to respond as the consumer feels they must. A more robust notification requirement would also help to re-balance the information asymmetry observed by the Commission.

In order to ensure that the full range of impacts on consumers are clearly considered and delineated, the Commission should amend the definition of "substantial harm or inconvenience" to read as follows:

> *Substantial harm or inconvenience* means personal injury—including theft, fraud, harassment, physical harm, psychological harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit or government benefits, or the misuse of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise misuse the individual's account—or financial loss, or expenditure of effort or loss of time that is more than trivial.

[24] See, e.g., *In re* Data Breach Reporting Requirements, Reply Comments of Just Futures Law, WC Docket. No. 22-21 (Mar. 23, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10325231325541 at 9 ("harms include physical, emotional, and reputational harms, many of which may fall disproportionately on historically disadvantaged communities"); id. at 10 ("potential abuses are likely to negatively and disproportionately affect people in disadvantaged and marginalized communities who often lack the necessary resources to assert their rights"); Danielle K. Citron & Daniel J. Solove, Privacy Harms, 102 B.U. L. Rev. 793 (2022), available at: https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

[25] See, e.g., *In re* Data Breach Reporting Requirements, Reply Comments of EPIC, et al., WC Docket. No. 22-21 at 18 n 66 (Mar. 23, 2023), https://www.fcc.gov/ecfs/document/1032465071814/1 ("For example, we believe a breach of encrypted data should still be reported, and that the burden should be on the provider to communicate clearly to consumers about the urgency of the risk of any given breach (rather than to communicate less frequently out of fear that urgent notifications will go unheeded if more notifications are sent).").

This revised definition would make clear that there are a range of "personal injuries" that can be caused by exposure of personal data, and that these must all be considered by a company when they are conducting their incident response and notice plan.

Additionally, EPIC responds to statements from the comments of the North American Securities Administrators Association (NASAA) on notification.[26] EPIC agrees that businesses have a natural tendency to want to avoid making disclosures that could incur liability or lose customers, and that consequently customers may not be notified of data security failures that could threaten their investments if the Commission implements a "reasonably likely" standard for harm determinations.[27] EPIC also agrees that securities firms should not have to determine whether personal or financial harms require notice,[28] although EPIC does not agree that it is appropriate to make a harm determination in other circumstances (e.g. NASAA's proposed cost of time and personal labor).[29] EPIC agrees with NASAA's observation that unintended acts that result in cybersecurity incidents should not be excluded from the Commission's rule,[30] and notes that the FCC recently proposed expanding its breach notification rules to cover inadvertent exposure and not merely intentional, unauthorized disclosure.[31]

---

[26] Comments of the North American Securities Administrators Association (NASAA), (May 22, 2023), https://www.sec.gov/comments/s7-05-23/s70523-192320-382862.pdf.

[27] Id. at 4. EPIC has offered similar observations to the FTC and the FCC. See, e.g., https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527 at 9-10 ("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.") (citing to 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.").).; https://www.regulations.gov/comment/FTC-2021-0071-0019 (citing to same 2019 Ctr. for Info. Tech. Pol'y comment).

[28] NASAA at 6.

[29] See also note 24 supra.

[30] NASAA at 12.

[31] FCC Breach Reporting NPRM, https://www.federalregister.gov/documents/2023/01/23/2023-00824/data-breach-reporting-requirements#p-22 ("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.

Annual Cybersecurity Audits Can Help to Identify Deficient Practices and Shore Up Vulnerabilities Before a Breach Occurs

We applaud the Commission's proposal to implement annual cybersecurity audits. Consumers rely on the entities that collect their personal data to take the necessary steps to protect that data. These entities are in control of how much personal data they collect, how long they retain it, how (and whether) they dispose of it, and what safeguards they implement to prevent unauthorized access throughout the data lifecycle. There are cost-effective and well-established methods for reducing the likelihood of breaches and for mitigating the harm of unauthorized access when it does occur. Poor data security practices increase the likelihood and severity of breaches, which in turn increase the risk of identity theft and other downstream harms to consumers. As the Commission notes, these downstream harms can also include "business disruptions that are not only costly to the Market Entity but also the other market participants that rely on Market Entity's services."[32]

Cybersecurity audits can identify deficient practices and help companies to shore up vulnerabilities before a breach occurs, mitigating the damage or perhaps preventing it entirely. However, it is important to note that it remains the company's responsibility to maintain best practices in between annual audits.[33] If the audit process amounts to a standalone annual exercise in compliance, it is unlikely to meaningfully improve data security year-round.

We thank the Commission for the opportunity to comment on these important issues.

Our current rule, adopted in response to the practice of pretexting, defines a "breach" as "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." ").

[32] See Cybersecurity Audit NPRM, Introduction, https://www.federalregister.gov/d/2023-05767/p-190.

[33] In the context of credit card payments and data security, for example, Verizon consistently reports that 44% or more of organizations fail to maintain PCI-DSS compliance in between annual compliance validations (most recently more than 56% failed to maintain compliance). *See* Verizon, *2022 Payment Security Report* 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf.

Respectfully submitted, June 5, 2023.

Chris Frascella
Law Fellow
frascella@epic.org
Electronic Privacy Information Center (EPIC)
1519 New Hampshire Avenue NW
Washington, D.C. 20036

Alan Butler
Executive Director
EPIC