June 5, 2023

Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (File No. S7-05-23, RIN 3235-AN26); 88 Fed. Reg. 20616 (Mar. 15, 2023)

Dear Ms. Countryman:

Better Markets[1] appreciates the opportunity to comment on the above-captioned Proposed Rule ("Proposal" or "Release")[2] intended to bolster protections for customer information by amending Regulation S-P. The Proposal is an appropriate and necessary step to help prevent, and mitigate the harm from, data breaches. Once final, it will improve the way firms respond to breaches, enhance the required notice to affected customers, expand the entities subject to the regulation's requirements, and broaden the types of information covered by a final rule.

While these reforms may seem technical or mundane, they are in fact exceedingly important, as data breaches are on the rise in frequency and magnitude and they impose huge costs on investors, customers, and companies tasked with safeguarding sensitive customer information. These reforms are also timely, since the threat from data breaches will inevitably grow as finance becomes increasingly virtual through the rise of fintech platforms, which rely principally if not entirely on databases and electronic communications. Ultimately, protecting customer and investor data is essential to ensuring confidence in the integrity and safety of the financial markets.

For these reasons, we support the Proposal, although as detailed below, we urge the Commission to strengthen it in some important respects. Specifically, the Commission should require customer notification for any incident of unauthorized access to or use of sensitive

[1] Better Markets is a non-profit, non-partisan, and independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support the financial reform of Wall Street, and make our financial system work for all Americans again. Better Markets works with allies—including many in finance—to promote pro-market, pro-business, and pro-growth policies that help build a stronger, safer financial system that protects and promotes Americans' jobs, savings, retirements, and more.

[2] 88 Fed. Reg. 20,616 (Mar. 15, 2023).

customer information, should shorten the period for notifying customers, and should require notification to the Commission at the same time and in the same form as the notice to customers.

Regulation S-P currently requires brokers, dealers, investment companies, and registered investment advisers to adopt written policies and procedures to ensure that administrative, technical, and physical safeguards are in place to protect customer records and information ("the safeguards rule"). Regulation S-P also currently requires brokers, dealers, investment companies, and registered investment advisers, as well as transfer agents registered with the Commission, to properly dispose of consumer report information ("the disposal rule").

The Proposal amending Regulation S-P has four components. It would add a requirement to the safeguards rule that covered institutions have incident response programs to address unauthorized access to or use of customer information, including procedures for providing timely notification to affected individuals; it would extend both the safeguards rule and the disposal rule to all transfer agents registered with the Commission or other appropriate regulatory agency; it would more closely align the information protected under the safeguards rule and the disposal rule by applying the protection of both rules to "customer information," a newly-defined term; and it would broaden the group of customers whose information is protected under both rules by applying the safeguards rule and the disposal rule to both nonpublic personal information that a covered institution collects about its own customers and to nonpublic personal information that it receives from a third-party financial institution about that institution's customers.

All four components of the Proposal are necessary to reduce the risk of harm to customers as a result of the unauthorized access to or use of their personal information. For example, the requirement that covered institutions provide timely notification to affected individuals would enable those individuals to take measures to protect themselves from the harms that could result from unauthorized access to or use of their information. As the Commission finalizes the Proposal, it should resist pressure to dilute its provisions. The Commission should also enhance some of those provisions. Specifically, the Commission should require customer notification for any incident of unauthorized access to or use of sensitive customer information regardless of the risk of use in a manner that would result in substantial harm or inconvenience; it should shorten the period for customer notification to 14 days to ensure timely notification; and it should require notification to the Commission at the same time and in the same form as the notice to customers.

BACKGROUND

In 2022, 1,774 organizational data compromises impacted over 392 million individual victims globally. The cost of these data breaches continues to rise by more than 20% year-over-year, amounting to 4-6% of the global gross domestic product. Despite these effects, 66% of public disclosures in the United States in 2022 did not include information on impacted victims.[3]

[3] Anna Sarnek, *Data breaches are increasing at a rapid speed. Here's what can be done*, World Economic Forum (Mar. 21, 2023), https://www.weforum.org/agenda/2023/03/data-breaches-are-increasing-at-a-rapid-

The lack of information in public notices about impacted victims is part of a troubling trend. In its 2022 Data Breach Report, the Identity Theft Resource Center noted that prior to 2021, data breach notices generally included information that could help individuals and businesses determine the relative risks of any given breach and the steps needed to protect against similar attacks. However, beginning in the fourth quarter of 2021 and accelerating throughout 2022, the trend reversed with less information being included in public notices. In 2019, 72% of public notices included details about the breaches and their victims. That number decreased to 60% in 2020 and 58% in 2021 before failing drastically to 34% in 2022.[4] The lack of actionable information in breach notices prevents consumers from effectively judging the risks they face of identity misuse and taking the appropriate actions to protect themselves.[5]

In addition to public notices about data breaches that do not include information about impacted victims, the United States also trails the European Union in overall reporting of data breaches. In the EU, there were 356 breach notices issued each day in 2021, the last year for which data is available. In the United States, there were an average of only seven breach notices issued each business day in 2022. The result is that individuals remain unable to protect themselves against the harmful effects of data compromises, and those effects are fueling an epidemic of identity fraud committed with stolen or compromised information.[6]

Below are just a few examples of significant data breaches in 2022 alone:

- Samsung was breached twice in 2022—once in March and once in August. During the first breach, the attackers obtained 200 gigabytes of confidential data, including source code related to Galaxy devices. During the second breach, the attackers obtained customers' personal information, such as names, contact information, demographic data, dates of birth, and product registration information.[7]

- Uber also suffered two breaches in 2022. The first breach resulted from an employee providing access to a hacker. The hacker obtained access to the systems where Uber stored sensitive customer and financial data.[8] Uber suffered the second

---

speed-here-s-what-to-do-about-it; IDENTITY THEFT RESOURCE CENTER, 2022 DATA BREACH REPORT 6 (Jan. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf.

4 IDENTITY THEFT RESOURCE CENTER, 2022 DATA BREACH REPORT, supra note 3, at 2, 8.

5 IDENTITY THEFT RESOURCE CENTER, 2021 DATA BREACH REPORT 15 (January 2023), https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf.

6 IDENTITY THEFT RESOURCE CENTER, 2022 DATA BREACH REPORT, supra note 3, at 3.

7 Sourabh Jain, *From Twitter, Samsung to Rockstar Games, here are the top data breaches of 2022*, Business Insider (Dec. 19, 2022), https://www.businessinsider.in/tech/news/here-are-the-top-data-breaches-of-2022/articleshow/96340624.cms.

8 *After a serious breach, Uber says its services are operational again*, NPR (Sept. 16, 2022), https://www.npr.org/2022/09/16/1123578408/uber-data-breach-hack.

breach as a result of an attack on a third-party vendor. That attack exposed the names, email addresses, and locations of over 77,000 employees.[9]

- T-Mobile suffered a breach that allowed a malicious intruder to gain access to the personal information of 37 million customers, including addresses, phone numbers, and dates of birth. That incident followed another major breach in August 2021 that involved social security numbers and driver's license numbers and that affected nearly 80 million U.S. residents. The 2021 data breach triggered a class action lawsuit by customers of T-Mobile that the company settled for $350 million.[10]

- Twitter suffered a breach that affected 5.4 million users. The breach resulted in the exposure of the users' phone numbers and email addresses. The hacker offered to sell the data of the users, which included companies and celebrities, for $30,000.[11]

- American Airlines suffered a breach that allowed an unauthorized actor to gain access to the personal information of customers and employees through a phishing campaign. The unauthorized actor accessed customers' personal information such as addresses, phone numbers, driver's license numbers, and passport numbers.[12]

- The Red Cross suffered a breach that allowed attackers to gain access to the data of over 515,000 "highly vulnerable" people. The database included information on people separated from their families due to conflict, migration, and disaster. The data breach included people's names, locations, and contact information.[13]

The financial industry is not immune or insulated from the risk of a data breach. For example, in 2021, ransomware operators manipulated a Robinhood customer service representative into giving a criminal access to the investment platform's customer support system. The data breach impacted over 7 million account holders and revealed their names and email addresses.[14] In 2019, a hacker exploited a vulnerability in Capital One's firewall and obtained the data of over 100 million people. The hacker stole 140,000 Social Security numbers, 80,000 bank

---

9 Katrina Manson, *Uber Conducting Probe After Vendor Hit With Cyberattack*, Bloomberg (Dec. 12, 2022), https://www.bloomberg.com/news/articles/2022-12-13/uber-says-its-investigating-after-vendor-hit-with-cyberattack?sref=mQvUqJZj#xj4y7vzkg.

10 *T-Mobile says breach exposed personal data of 37 million customers*, NPR (Jan. 20, 2023), https://www.npr.org/2023/01/20/1150215382/t-mobile-data-37-million-customers-stolen.

11 *Twitter hacker touting the data of over 5.4 million users, including celebrities and companies, for $30,000*, Yahoo! (July 26, 2022), https://www.yahoo.com/video/twitter-hacker-touting-data-over-124242963.html.

12 *American Airlines says data breach affected some customers, employees*, Reuters (Sept. 20, 2022), https://www.reuters.com/business/aerospace-defense/american-airlines-says-data-breach-affected-small-number-customers-employees-2022-09-20/.

13 Jain, supra note 7.

14 IDENTITY THEFT RESOURCE CENTER, 2021 DATA BREACH REPORT, supra note 5, at 20; *see also* Matt Egan, *Robinhood discloses breach that exposed information of millions of customers*, CNN (Nov. 8, 2021), https://www.cnn.com/2021/11/08/tech/robinhood-data-breach/index.html.

account numbers, and tens of millions of credit card applications. Capital One said that the breach would cost it over $150 million.[15] And in 2014, a cyberattack at JPMorgan Chase compromised the accounts of 76 million households and seven million small businesses. The attackers accessed the names, addresses, phone numbers, and email addresses of JPMorgan account holders.[16]

The COVID-19 pandemic and the resulting changes in the modern workplace have only elevated businesses' risk of a data breach.[17] Research shows that 91% of data security professionals saw negative risk implications from remote and hybrid work.[18] And in 2021, the average cost of a data breach was highest, at $5.54 million, for companies with 81% to 100% of remote employees.[19] The cost of a data breach was also $1 million more on average when remote work was a factor in the breach than when remote work was not a factor in the breach.[20]

As these statistics indicate, data breaches exact a huge toll on their corporate victims as well as the customers and investors whose sensitive information is hacked. While the magnitude of dollar losses is difficult to estimate, it is clear that companies must expend significant resources to prevent breaches, detect breaches that do occur, contain the damage from breaches, prevent future breaches, and in some cases make customers whole. Indeed, one study found that the average cost of a data breach in 2022 was $4.35 million, which was 2.6% greater than the average cost in 2021 and 12.7% greater than the average cost in 2020.[21] Customers in turn suffer untold harms, both financial and psychological, as many become victims of identity theft.

The theft of information about financial accounts poses an especially grave threat of harm, as hackers gain access to uniquely valuable information about individuals who are ripe targets for identity theft. As a result, financial market participants must be increasingly vigilant to guard against breaches that compromise sensitive customer information. The Proposal, once finalized, will help ensure that stronger protections to safeguard that information are in place.

OVERVIEW OF THE PROPOSAL

The Commission has proposed amendments to Regulation S-P to require that brokers, dealers, investment companies, registered investment advisers, and transfer agents ("covered

---

15 Emily Flitter and Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. Times (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

16 Jessica Silver-Greenberg, et al., *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. Times (Oct. 2, 2014), https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.

17 Benjamin Laker, *Remote Working Increases Likelihood of Data Breaches Says Research*, Forbes (Jan. 10, 2023), https://www.forbes.com/sites/benjaminlaker/2023/01/10/remote-working-increases-likelihood-of-data-breaches-says-research/?sh=1eb2cdfad3a9.

18 Hugo Guzman, *Remote Work Leading to Big Data-Loss Problems*, Law.com (Mar. 7, 2023), https://www.law.com/corpcounsel/2023/03/07/remote-work-leading-to-big-data-loss-problems/.

19 *Cost of a Data Breach*, ProxyRack (Dec. 2, 2022), https://www.proxyrack.com/blog/cost-of-a-data-breach/.

20 IBM, COST OF A DATA BREACH REPORT 6 (2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.

21 *Id.* at 5.

institutions") have incident response programs to address unauthorized access to or use of customer information, including notification to affected individuals, and to otherwise enhance the protection of customers' personal information. The Proposal has four main components:

- First, the Proposal would amend the safeguards rule to require that covered institutions develop, implement, and maintain written policies and procedures establishing an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.
  - A response program must include procedures to assess the nature and scope of any incident and to take appropriate steps to contain and control the incident to prevent further unauthorized access or use, including notifying individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, unless the covered institution determines after a reasonable investigation that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

  - A covered institution required to provide notice to affected individuals would be required to do so as soon as practicable, but not later than 30 days, after the institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.

  - A covered institution required to provide notice to affected individuals would be required to do so in a clear and conspicuous and reasonably understandable manner and in a manner reasonably designed to ensure that the customer receives actual notice of the unauthorized access or use.

- Second, the Proposal would extend both the safeguards rule, which currently does not apply to any transfer agents, and the disposal rule, which currently applies to transfer agents registered with the Commission only, to apply to any transfer agent registered with the Commission or another appropriate regulatory agency.

- Third, the Proposal would amend the safeguards rule, which currently applies to "customer records and information," and the disposal rule, which currently applies to "consumer report information," by applying the protection of both rules to "customer information," which the Proposal broadly defines to encompass any record containing "nonpublic personal information" as defined in Regulation S-P about a "customer of a financial institution," whether in paper, electronic, or other form.[22]

[22] The Proposal would include a separate definition of "customer information" for transfer agents. It would define "customer information" with respect to transfer agents as any record containing nonpublic personal

- Fourth, the Proposal would amend the safeguards rule and the disposal rule to apply to both nonpublic personal information that a covered institution collects about its own customers and to nonpublic personal information that it receives from a third-party financial institution about that institution's customers.[23]

COMMENTS

I. The Commission should adopt the proposed requirement that covered institutions notify affected individuals of the unauthorized access to or use of their sensitive customer information, but it should strengthen that measure in several ways.

A. The Commission should require that covered institutions notify affected individuals of any incident of unauthorized access to or use of sensitive customer information regardless of the risk of harm or inconvenience.

The American people deserve to know when their data has been compromised. Otherwise, they may be victimized twice: once when a breach that exposes their information occurs, and again when bad actors use the information to steal their identity, drain their back accounts, or run up their credit cards. Indeed, data breaches may cause significant harm and therefore must be addressed by the individuals whose information is exposed in an appropriate and timely manner.[24] But companies will not always disclose data breaches to affected individuals voluntarily. They may be concerned about the damage to their reputation and their bottom line from disclosing a breach. As a result, companies generally must be required to promptly disclose any significant data breaches so that affected individuals are informed and can protect themselves.[25]

The Proposal correctly notes that currently no Commission rules require broker-dealers, investment companies, or registered investment advisers to have policies and procedures for responding to data breach incidents or to notify customers of those breaches.[26] This regulatory gap poses unnecessary risks to the customers of these institutions. The Proposal would better protect these customers from the unauthorized access to or use of their personal information because, as the Commission notes, advanced planning would be part of any reasonably designed

---

information identified with any natural person, who is a securityholder of an issuer for which the transfer agent acts or has acted as transfer agent, that is handled or maintained by the transfer agent or on its behalf.

23 Regulation S-P defines "financial institution" generally to mean any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities.

24 Mark Verstraete and Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 817-18 (2021) (citing Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. Times (Sept. 9, 2017), https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html%20[https://perma.cc/D55C-F6ZN and EU General Data Protection Regulation ("GDPR) Recital 85, https://gdpr.eu/recital-85-notification-obligation-of-breaches-to-the-supervisory-authority/).

25 Dennis Kelleher, *Worse than nothing's been done since the massive Equifax hack*, The Hill (Feb. 25, 2019), https://thehill.com/opinion/cybersecurity/431335-a-year-after-the-equifax-hack-nothings-changed/; GDPR Recital 86.

26 Release at 20,620.

incident response program and its prompt implementation following a breach (including notification to affected individuals) would help limit potential harmful effects.[27]

Breach notification requirements empower individuals to proactively limit the negative effects of a breach. They can rely on credit monitoring services that provide alerts about potential uses of their information, they can lock or freeze their credit reports to prevent their information from being used to open fraudulent accounts, and they can cancel their credit cards or close other affected accounts. With respect to data breaches at financial institutions specifically, they can open new bank or investment accounts and monitor their financial accounts vigilantly.[28]

In light of the benefits of notification, the Commission should require customer notification for any incident of unauthorized access to or use of sensitive customer information regardless of the risk of use in a manner that would result in substantial harm or inconvenience. That way customers can determine for themselves whether they believe there is risk of substantial harm or inconvenience that should prompt action on their part. Otherwise, the very institutions responsible for a breach would be in the position of determining whether customers should be notified due to a risk of substantial harm or inconvenience. Any risk that requiring notice regardless of the risk of substantial harm or inconvenience would lead to a volume of notices that would inure affected individuals to the notices and result in their not taking proactive action is outweighed by the risk that individuals will not be notified at all and will not have the opportunity to decide for themselves whether to take action. Customers should always be notified when their sensitive information is accessed or used without authorization.[29] This approach also reduces the risk that firms will use the proposed test as an excuse to refrain from making disclosures they would prefer to avoid.[30]

Covered institutions should still be required to conduct an investigation to determine whether sensitive customer information has been, or is reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. But a determination that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience should not lead to the covered institution being able to withhold notice to the affected individuals. Rather, that determination should be provided in the notice to the affected individuals so that the affected individuals can use that information as they decide for

---

27 *Id*.

28 Verstraete and Zarsky, supra note 24, at 818.

29 *Id.* at 819 (stating that in order to achieve mitigation of a data breach "notification recipients must include the affected individuals directly, in order to ensure that those impacted by the breach will take action to remedy potential harms," and cautioning that a regime that "requires notification only when the breach results in a 'high risk' . . . leav[es] data subjects out of the loop").

30 Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 939 (2007) ("A finding of misuse [to require disclosure] requires a determination beyond acquisition, namely that the breached information will be used in fraudulent activities. The raised threshold permits additional discretion to the breached entity; this broader delegation, coupled with the existence of the disclosure disincentive, might bias the business's investigation of a data leak and lead to a facile conclusion that misuse of information was unlikely and consumer notification was not required.").

themselves whether to take action and to help the affected individuals differentiate between the various notices that they receive of unauthorized access or use.

Finally, the Commission should not narrow the definition of sensitive customer information.[31] A broad definition of the information that, if exposed, triggers a notification requirement best protects customers by ensuring that they can take the necessary steps to minimize their exposure risks.[32] A broad definition of the information that triggers a notification requirement also serves the objective of formulating and improving security standards.[33]

B. The Commission should adopt the part of the Proposal that requires notification to affected individuals as soon as practicable, but it should shorten the maximum amount of time to provide the notification from 30 to 14 days after the covered institution becomes aware of the incident.

The Proposal requires that covered institutions provide the required notices as soon as practicable, but not later than 30 days, after the covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to occur.[34] The requirement that covered institutions provide notice as soon as practicable is designed to expeditiously notify individuals whose information is compromised so that these individuals may take timely action to protect themselves from identity theft or other harm. The requirement that covered institutions provide the notice no more than 30 days after becoming aware of the incident is designed to balance the need for covered institutions to perform their assessments, take remedial measures, conduct any investigation, and prepare the notices with the need to promote timely notifications.[35]

---

31 The Proposal defines "sensitive customer information" as "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information."

32 Verstraete and Zarsky, supra note 24, at 819.

33 *Id*. at 861.

34 If the Commission chooses not to help customers minimize the potential harm from a breach by shortening the maximum amount of time for providing notice, it should at the least resist pressure to lengthen the time period. Thirty days is more than an ample amount of time for covered institutions to provide the required notification. *See* Gregory S. Gaglione, Jr., Comment, *The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America*, 67 BUFF. L. REV. 1133, 1207 (2019) (stating that "an analysis of the current state data breach notification laws shows that requiring notification within thirty days of a breach to affected consumers would . . . give an organization ample time to conduct a full investigation" while "ensur[ing] that consumers are notified of a breach in a timely manner so they can take the proper steps to mitigate any losses and protect their personal information from further exposure"); Stephen Jones, Comment, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH L. REV. 783, 809-10 (2018) ("The required time of notification should be no longer than thirty days after a data breach occurs. The thirty-day period will provide businesses with ample time to assess a possible breach, determine the scope of the information compromised, and compile lists of consumers that must be notified.").

35 Release at 20,632.

The Commission should adopt the requirement that covered institutions provide notification as soon as practicable, but it should shorten the maximum amount of time for providing notice to 14 days. The failure to timely notify an individual of a breach of their data can cause real, concrete harm.[36] And empirical findings demonstrate the benefits of rapid detection of identity theft.[37] The longer an instance of identity theft goes undetected, the greater the damage that usually follows.[38] As a result, the Commission should provide covered institutions with at most 14 days to notify affected individuals so that those individuals may take timely action to protect themselves.

Unlike many state laws governing data breach notifications, the Proposal does not allow for a delay in notification if there is an ongoing law enforcement investigation,[39] and the Commission should not allow for such a delay in the final rule. A law enforcement delay heightens the lag in customer detection of identity theft.[40] Accordingly, a delay for law enforcement activity may cause harm to the customer whose personal information has been exposed.[41] A delay for law enforcement activity is also unnecessary in this context. There is no reason that notification to affected individuals specifically would impede a law enforcement investigation of the breach.

C. The Commission should adopt the part of the Proposal that requires covered institutions to provide basic information to affected individuals in their notices in a clear and conspicuous and reasonably understandable manner.

The Proposal requires that covered institutions provide notices to affected individuals in a clear and conspicuous manner and by means reasonably designed to ensure that the customer receives actual notice. The notices must be reasonably understandable and designed to call attention to the nature and significance of the information required to be provided. The information required to be provided includes a description of the incident, the type of sensitive customer information that was accessed or used without authorization, and the measures taken to protect the sensitive customer information from further unauthorized access or use. The Proposal would also require covered institutions to include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident. The Proposal would require further that covered institutions include a recommendation that the customer review account statements and report suspicious activity; explain what a fraud alert is, how an individual may place a fraud alert in credit reports, and how a credit report may be obtained free of charge; and include information regarding Federal Trade Commission (FTC) and usa.gov guidance on

---

36 Taryn Elliott, Comment, *Standing a Chance: Does Spokeo Preclude Claims Alleging the Violation of Certain State Data Breach Laws*, 49 SETON HALL L. REV. 233, 253 (2018).

37 Schwartz and Janger, supra note 30, at 939 (citing SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 8 (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf).

38 *Id.* (citing SYNOVATE, supra note 37, at 8).

39 Release at 20,633.

40 Schwartz and Janger, supra note 30, at 968.

41 *Id*. at 943.

steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidences of identity theft to the FTC, and the FTC's website address.[42]

The Commission should adopt these provisions as proposed. As a general proposition, we know that the value of any required disclosure depends largely on the extent to which it conveys clear, comprehensible, and usable information. That is especially true in the context of breach notifications, where the stakes may be high and prompt action may be necessary. The Proposal addresses these concerns. It avoids some common problems with the content of many data breach notifications, such as confusing language, a lack of details, and insufficient attention to the practical steps customers should take in response.[43] Indeed, one study showed that 61% of consumers had problems understanding a data breach notification and 72% said the notification "'did not increase their understanding about the data breach.'"[44]

As a result, data breach notices should identify the source of the breach, the protective measures customers should take to avoid identity theft, and the ways in which customers may monitor their accounts.[45] The Proposal requires covered institutions to provide this information in their notices. Organizations should also endeavor to get the full attention of affected individuals, such as by using a clearly headed letter of notification.[46] Again, the Proposal requires covered institutions to provide notification in a clear and conspicuous manner. The Proposal should be adopted as proposed without any dilution of the requirements governing the content or manner of notification.

II. The Commission should, as proposed, extend the safeguards rule and disposal rule to all transfer agents, to all customer information as defined in the Proposal, and to information that a covered institution both collects about its own customers and receives from a third-party financial institution about that institution's customers.

A. Transfer agents should be subject to the safeguards rule and the disposal rule.

The Proposal would extend the *safeguards rule* to transfer agents, who are currently not subject to the rule. As a result, transfer agents would be required to develop, implement, and maintain written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information. They would also be required to develop, implement, and maintain an incident response program, including customer notifications, for unauthorized access to or use of customer information. The Proposal would also extend the

42 Release at 20,634.

43 *See* Schwartz and Janger, supra note 30, at 952-53 (noting that notifications sometimes focus more on damage control for the breached entity than on convincing customers to take appropriate steps).

44 Samson Yoseph Esayas, *Breach Notification Requirements under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 317, 343 (2014) (quoting PONEMON INSTITUTE, 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION 4-5, 10 (June 2012), http:// www.experian.com/assets/databreach/brochures/ponemon-notification-study-2012.pdf).

45 Schwartz and Janger, supra note 30, at 963.

46 Esayas, supra note 44, at 344.

disposal rule to all transfer agents, including those transfer agents that are registered with another appropriate regulatory agency other than the Commission, whereas it currently applies only to transfer agents registered with the Commission. As a result, all transfer agents would be required to take measures to properly dispose of customer information.[47]

Extending the protections of the safeguards rule and the disposal rule to all transfer agents would benefit the public and protect investors. Transfer agents perform a vital if largely unknown or unappreciated role in the securities markets: they track, record, and maintain the official record of ownership of each issuer's securities; cancel old certificates, issue new ones, and perform other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of securities; facilitate communications between issuers and securityholders; and make dividend, principal, interest, and other distributions to securityholders.[48] As the Commission recognizes, transfer agents therefore have information related to securityholders that may include names, addresses, phone numbers, email addresses, employers, employment history, bank account information, credit card information, transaction histories, and securities holdings. The systems transfer agents maintain are subject to the same risks of a breach as other covered institutions, and therefore the individuals whose customer information transfer agents maintain are subject to the same risks as customers of other covered institutions.[49] And yet despite the sensitive information transfer agents possess and the risks of a breach to the systems they maintain, no transfer agents are currently subject to the safeguards rule, and only transfer agents registered with the Commission are subject to the disposal rule. These regulatory gaps have no justification, and the Proposal would appropriately close them and reduce the concomitant risks to investors and the public.

The Proposal also has the benefit of equalizing the standards governing transfer agents. Many transfer agents must comply with the requirements of financial regulators other than the Commission such as the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation ("Banking Agencies").[50] The Banking Agencies' Incident Response Guidance applies to these transfer agents and requires them to develop an incident response program for breaches of sensitive customer information.[51] Therefore, currently, *bank* transfer agents must comply with requirements for safeguarding nonpublic personal information whereas *non-bank* transfer agents need not do so. The Proposal eliminates this asymmetry by ensuring that all transfer agents have the appropriate procedures in place to safeguard the nonpublic personal information of securityholders. This will promote not only investor protection but also regulatory parity and fair competition among firms.[52]

---

47 Release at 20,638-20,639.

48 *Transfer Agent Regulations*, Exchange Act Release No. 76743, 2015 WL 9311555 (Dec. 22, 2015).

49 Release at 20,638.

50 *Id.* at 20,619 n.37, 20,640.

51 *Id.* at 20,658.

52 *See* ComputerShare, Regulation S-P: Privacy of Consumer Financial Information Safeguarding Personal Information (May 12, 2008) (supporting efforts to require that all transfer agents be subject to the same information security and privacy requirements), https://www.sec.gov/comments/s7-06-08/s70608-45.pdf.

B. As proposed, the protections of both the safeguards rule and the disposal rule should apply to customer information as that term is defined in the Proposal.

The Proposal would amend the safeguards rule and the disposal rule so that they both apply to "customer information." Currently, the safeguards rule applies to "customer records and information," a term which Regulation S-P does not define. The disposal rule applies to "consumer report information," which Regulation S-P defines as a record in any form about an individual that is a consumer report or is derived from a consumer report. The Proposal would replace the term "customer records and information" in the safeguards rule with "customer information," and would add "customer information" to the coverage of the disposal rule. The Proposal would define "customer information" as any record containing "nonpublic personal information," as defined in Regulation S-P, about a "customer of a financial institution," whether in paper, electronic, or other form that is handled or maintained by the covered institution or on its behalf.[53]

The Commission should adopt these amendments as proposed. The amendments expand and clarify the type of personal information that is subject to the safeguards rule and the disposal rule. They apply both rules to records containing nonpublic personal information about a customer, and Regulation S-P contains an extensive definition of nonpublic personal information, which includes personally identifiable financial information.[54] The Commission should not narrow the definition of "customer information" in the final rule. The broad definition of "customer information" ensures that covered institutions must take the necessary steps to safeguard and properly dispose of personally identifiable financial information about their customers.

In addition to better specifying the information subject to the safeguards rule and the disposal rule, the amendments also align the information subject to both rules. As the Commission recognizes, aligning the information subject to both rules better protects personal financial information from unauthorized disclosure. As the Commission recognizes further, applying both rules to the same set of information could reduce any burdens associated with the application of the safeguards rule and the disposal rule to two different sets of information.[55]

C. As proposed, the protections of the safeguards rule and the disposal rule should apply to both nonpublic personal information that a covered institution collects about its own customers and nonpublic personal information that it receives from a third-party financial institution about that institution's customers.

The Proposal would amend the safeguards rule and the disposal rule so that they both apply to nonpublic personal information that a covered institution collects about its own customers

---

53 Release at 20,636. As noted above, the Proposal defines "customer information" differently for transfer agents since transfer agents do not generally have individuals as clients. *See id.* at n.163; supra note 22.

54 17 C.F.R. § 248.3(t).

55 Release at 20,636.

and nonpublic personal information that it receives from a third-party financial institution about that institution's customers. As the Commission recognizes, applying the safeguards rule and the disposal rule to nonpublic personal information that a covered institution receives from other financial institutions should ensure that customer information safeguards are not neglected when a third-party financial institution shares that information with a covered institution.[56] The amendments clarify that a covered institution retains responsibility for safeguarding customers' nonpublic personal information regardless of whether the information originates with it or not.[57]

III. The Commission should adopt the proposed amendments to Regulation S-P regardless of the fact that covered institutions would also be required to comply with other rules in other Commission proposals to address cybersecurity risks.

In addition to the Proposal, the Commission has also proposed amendments to Regulation SCI ("the Regulation SCI Proposal") as well as new rules addressing cybersecurity specifically ("the Exchange Act Cybersecurity Proposal" and "the Investment Management Cybersecurity Proposal"). Regulation SCI requires certain market participants to have policies and procedures in place to help ensure the robustness and resiliency of their systems that support certain market functions ("SCI systems"), and the Regulation SCI Proposal would extend Regulation SCI to additional market participants and update its requirements. The Exchange Act Cybersecurity Proposal and the Investment Management Cybersecurity Proposal would require that certain market participants have policies and procedures to address cybersecurity risks specifically.

The Commission should amend Regulation S-P regardless of the fact that some of the rules under the Regulation SCI Proposal, the Exchange Act Cybersecurity Proposal, and the Investment Management Cybersecurity Proposal would apply to covered institutions subject to the Proposal. The Proposal addresses the risks to customers of the unauthorized disclosure of their nonpublic personal information specifically, and those risks are not adequately addressed by the other cybersecurity-related proposals. The Proposal also points out that covered institutions would be able to adopt some policies and procedures that would satisfy its obligations under both the Proposal and the other cybersecurity-related proposals, thus allowing for efficient compliance.

Moreover, any increased costs from compliance with both the Proposal and the other cybersecurity-related proposals would be offset by the savings to covered institutions from the prompt detection and notification of a data breach. Studies have shown that businesses with an incident response team that tested its incident response plan saw an average of $2.66 million lower breach costs—or a cost savings of 58%—compared to organizations without an incident response

---

56 *Id*.

57 Brad Carr, et al., *Liability and Consumer Protection in Open Banking*, INST. INT'L FIN. 5 (2018) (arguing that when data is shared all market participants must apply the most robust security to customers' data and should be "directly and explicitly" responsible for failures in their own security), https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf.

team and that did not test their incident response plan.[58] Studies have also shown that organizations that contain a data breach in less than 30 days—and, as discussed above, the Proposal requires covered institutions to notify affected individuals within 30 days—may save over $1,000,000 versus organizations that take more than 30 days to contain a breach.[59]

As a result, the Commission should require that covered institutions have incident response programs to address unauthorized access to or use of customer information even if they would also be required to have policies and procedures that address cybersecurity risks under the Regulation SCI Proposal or the other cybersecurity-related proposals. As the Commission recognizes, the incident response program policies and procedures requirements under the Proposal are specifically tailored to address unauthorized access to or use of customer information and therefore serve a different purpose than the other proposals. For example, the Proposal requires that covered institutions protect customer information not stored on SCI systems and focuses on individuals affected by a data breach in a way that the other cybersecurity-related proposals do not.[60]

The Commission should also require that covered institutions provide notification to individuals affected by a breach of customer information even if those institutions would also be required to disclose cybersecurity-related incidents under the Regulation SCI Proposal or the other cybersecurity-related proposals. The Proposal requires the disclosure of different information than that required under the other proposals. The Proposal also requires that disclosures be made to different persons than under the other proposals. Although a single incident may trigger reporting requirements under all of the proposals, the other proposals do not encompass the notification required under the Proposal. Accordingly, the Commission should adopt the Proposal's notification requirements regardless of the disclosures mandated under the other proposals.

Finally, the Commission should strengthen the Proposal in another important respect by requiring that covered institutions provide notice to the Commission when covered institutions are required to provide notice to affected individuals under the Proposal. The other cybersecurity-related proposals require disclosures to the Commission. These disclosures ensure that the Commission is aware of significant cybersecurity incidents involving market participants. Covered institutions should be required to provide the same notice to the Commission as it would provide to affected individuals under the Proposal and should do so at the same time as it provides the notice to the individuals. This procedure for notification to the Commission would impose minimal additional burdens on covered institutions while ensuring that the Commission is aware of incidents of unauthorized access to or use of customer information.

---

58 IBM, supra note 20, at 7.

59 David Tersteeg, Note and Comment, *Legislative and Regulatory Obligations on Corporate Attorneys: Production Data in the World of Sarbanes-Oxley and General Data Protection*, 39 N. ILL. U. L. REV. 456, 479 (2019) (citing IBM, 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 4 (July 2018)).

60 *See* Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKLEY TECH. L.J. 449, 465 (2019) (noting that "data-breach notification law is but one solution to a broader cybersecurity law problem).

CONCLUSION

We hope these comments are helpful as the Commission finalizes the Proposal.

Sincerely,

Stephen W. Hall
Legal Director and Securities Specialist

Better Markets, Inc.
2000 Pennsylvania Avenue, NW
Suite 4008
Washington, DC 20006
(202) 618-6464

shall@bettermarkets.org
http://www.bettermarkets.org