PUBLIC SUBMISSION

Comment Submitted by The Clearing House Association, L.L.C.

Posted by the **Federal Trade Commission** on Feb 7, 2022

View More Comments 21 (/document/FTC-2021-0071-0001/comment)

View Related Comments 21 (/docket/FTC-2021-0071/comments)

Share

Comment

See attached file(s)

Attachments 1

The Clearing House_FTC Comment Letter_2_7_22

Download (https://downloads.regulations.gov/FTC-2021-0071-0011/attachment_1.pdf)

Comment ID

FTC-2021-0071-0011

Tracking Number

kzc-xpns-qdfh

Comment Details | **Submitter Info**

Received Date

Feb 7, 2022

The Clearing House

February 7, 2022

Submitted electronically through https://www.regulations.gov

David Lincicum, Katherine McCarron & Robin Wetherill
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B)
Washington, D.C. 20580

Re: Safeguards Rule, 16 CFR part 314, Project No. P145407

Dear Mr. Lincicum, and Mses. McCarron and Wetherill,

The Clearing House Association, L.L.C. ("The Clearing House")[1] appreciates this opportunity to comment on the Federal Trade Commission's request for public comment on its proposal to further amend the Standards for Safeguarding Customer Information (the "Safeguards Rule") to require Federal-Trade-Commission-regulated financial institutions to report to the Federal Trade Commission ("FTC") any security event where the financial institution has determined that misuse of customer information has occurred or is reasonably likely, and at least 1,000 consumers have been affected or may reasonably be affected.[2]

The Clearing House commends the FTC for its work improving and strengthening the Safeguards Rule,[3] and for proposing to provide data security event reporting requirements for FTC-regulated institutions.[4] These institutions, including many financial technology companies ("fintechs"), often engage in activities that are similar to the activities undertaken by banks subject to oversight by the federal prudential regulators. Since The Clearing House's August 2019 comment letter to the FTC on the FTC's 2019 Safeguards Rule Notice of Proposed

[1] The Clearing House Association, L.L.C., the country's oldest banking trade association, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the U.S., clearing and settling more than $2 trillion each day. *See* The Clearing House's web page at www.theclearinghouse.org.
[2] "Standards for Safeguarding Customer Information," 86 Fed. Reg. 70,062 (Dec. 9, 2021).
[3] Including the immediate proposal and the FTC's final rule, contained in "Standards for Safeguarding Customer Information," 86 Fed. Reg. 70,272 (Dec. 9, 2021).
[4] 86 Fed. Reg. 70,062 (Dec. 9, 2021).

Rulemaking,[5] the fintech industry has continued its rapid growth.[6] According to one estimate, fintechs made up one quarter of the fastest growing brands in 2021, with annual fintech funding for the first three quarters of 2021 estimated at $44.3 billion, nearly double full-year-2020 funding.[7] And according to the consulting firm McKinsey & Company, "one in two consumers [in the U.S.] now use a fintech solution, primarily peer-to-peer payment solutions and non-bank money transfers."[8] As a result, non-bank payment providers and data aggregators today hold and use vast amounts of consumer financial data.

Along with the rapid growth of fintech companies have come data security risks and lapses. For example, as recently as this past July, fintech data aggregator Dave confirmed that a data breach had exposed the personal information of as many as 7.5 million banking users.[9] And in August of 2021, data aggregation firm Plaid settled a multi-million-dollar class action lawsuit claiming that the fintech firm had shared consumers' personal banking data with third party firms, including other fintech companies, without consent.[10] Given the risks posed by the growth of these companies and their holding and use of vast amounts of consumer financial data, it is vital that consumer financial data be properly handled and safeguarded to ensure the security of the information, the safety and soundness of payments and financial systems, and consumer confidence in these systems. As such, it is essential fintechs engaged in functionally similar banking- and payments-related activities as banks should be subject to functionally similar requirements, including data breach notification requirements.

While the FTC's proposed security event reporting requirements represent a significant improvement to the overall Safeguards Rule, and The Clearing House has encouraged the FTC to

[5] Letter from The Clearing House Association, L.L.C. to David Lincicum and Allison M. Frank, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (Aug. 2, 2019) (available at: https://www.theclearinghouse.org/advocacy/articles/2019/08/tch-comments-response-ftc-nprm-08-02-2019).

[6] *See* Tracy Mayor, "Fintech, explained," MIT Sloan School of Management (Feb. 4, 2021) (available at: https://mitsloan.mit.edu/ideas-made-to-matter/fintech-explained) (citing research finding that "[g]lobally, financial technology is projected to reach a market value of $305 billion by 2025"). *See also* Congressional Research Service, "Fintech: Overview of Innovative Financial Technology and Select Policy Issues," research report (April 28, 2020) (highlighting growth of different types of fintech companies and policy issues raised by such growth).

[7] *See* Charlotte Principato, "Fintechs Dominated Morning Consult's 2021 Fastest Growing Brands List: Here's What That Means for the Industry" (Dec. 2, 2021) (available at: https://morningconsult.com/2021/12/01/fastest-growing-brands-fintech-2022/) (noting that as of Q3 2021, fintech funding has exceeded $44.3 billion, "nearly double the amount received in all of 2020," and that one quarter of the fastest growing brands are fintechs).

[8] Asif et al., "Financial Services Unchained: The ongoing rise of open financial data," McKinsey & Company article (July 11, 2021) (available at: https://www.mckinsey.com/industries/financial-services/our-insights/financial-services-unchained-the-ongoing-rise-of-open-financial-data).

[9] *See* "FinTech Dave Reports Data Breach Involving 7.5M Users" PYMNTS article (July 27, 2020) (available at: https://www.pymnts.com/news/security-and-risk/2020/fintech-dave-data-breach-hackers/); *and* Phil Muncaster, "US Digital Bank Dave Admits Customer Data Breach," Infosecurity Group (July 27, 2020) (available at: https://www.infosecurity-magazine.com/news/us-bank-dave-admits-customer-data/).

[10] *See* Penny Crosman, "Plaid settles class-action lawsuit for $58 million," American Banker (Aug. 6, 2021) (available at: https://www.americanbanker.com/news/plaid-settles-class-action-lawsuit-for-58-million); *and* Sara Merken, "Fintech firm Plaid agrees to $58 mln deal to end privacy case," Reuters (Aug. 6, 2021) (available at: https://www.reuters.com/legal/litigation/fintech-firm-plaid-agrees-58-mln-deal-end-privacy-case-2021-08-06/).

adopt requirements such as these,[11] The Clearing House remains concerned about differences that exist between the standards to which traditional financial institutions regulated by the prudential regulators are subject and those that the FTC has proposed in the supplemental notice of proposed rulemaking ("SNPRM") on the security event reporting requirements. In order to further enhance the proposed security event reporting component of the SNPRM/Safeguards Rule, and to ensure that the security event reporting component applies functionally similar requirements to FTC-regulated financial institutions as apply to banks today, The Clearing House makes the following recommendations:

- The FTC should proceed with supplementing the Safeguards Rule with standalone security event reporting requirements.
- Security event reporting requirements under the Safeguards Rule would benefit from alignment with requirements applicable to federally-supervised banks. In particular:
    - The threshold for event reporting and event reporting requirements should be aligned with the notification requirements contained in "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" adopted by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation; and
    - The notification timeframe for qualifying security events should be expressed in a matter of hours and days, similar to guidance adopted by federal financial regulators, and the timeframe provided in the recently-adopted "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" final rule. A uniform reporting timeframe would ensure a common standard applies to businesses engaged in functionally similar activities, and would ensure the FTC is updated in a timely fashion, consistent with other federal financial regulators.
    - The FTC should further supplement the Safeguards Rule to require the reporting of material disruption or degradation, or reasonable likelihood of material disruption or degradation, of an FTC-regulated financial institution's abilities, business lines, or operations, or similar such disruptions at FTC-regulated financial institutions' service providers, similar to the requirements of the "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" final rule.

[11] *See* Letter from The Clearing House Association, L.L.C. to David Lincicum and Allison M. Frank, footnote 5, *and* Letter from The Clearing House Association, L.L.C. to David Lincicum and Katherine McCarron, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (Nov. 21, 2016) (available at: https://www.theclearinghouse.org/advocacy/articles/2016/11/11072016_comments_response_ftc_notice_safeguards_rule).

I. The Proposed Security Event Reporting Requirements Can Be Further Strengthened by Aligning the Requirements with Requirements Promulgated by Other Federal Financial Regulators

The FTC's proposed security event reporting requirements represent a significant and much-needed improvement to the overall Safeguards Rule. The Clearing House remains concerned, however, about key differences that exist between the standards to which traditional financial institutions regulated by the prudential regulators are subject and those that the FTC has proposed in the SNPRM. In particular, key differences exist in the threshold for event reporting, and in the timeframe for the reporting of an event. The Clearing House believes the proposal to amend the Safeguards Rule to require FTC-regulated financial institutions to report certain security events to the FTC would benefit from alignment with requirements promulgated by other federal financial regulators as detailed below.

a. Event Reporting Requirements and the Threshold for Event Reporting Should be Aligned with the Notification Requirements Contained in the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" Adopted by Federal Financial Regulators

Under the FTC's proposal, a notice filing is triggered by the "discovery" of a "security event" ("misuse of the information of 1,000 or more consumers [that] has occurred or is reasonable likely to occur").[12] The Clearing House appreciates the FTC's efforts to be judicious in the notices that it requires to be filed by defining "security event" as it has, but respectfully recommends that the FTC's reporting requirements be refined to align with the Office of the Comptroller of the Currency's ("OCC"), Board of Governors of the Federal Reserve System's ("Board"), and Federal Deposit Insurance Corporation's ("FDIC") (collectively the "Agencies") "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" ("Interagency Guidance")[13] because the FTC's proposed

[12] 86 Fed. Reg. 70,064 & 70,067. The Clearing House also notes that in the SNPR the FTC alternates between using the term "customer" and the term "consumer," and uses the phrase "consumer information" in defining the term "security event," but that the Gramm-Leach-Bliley Act defines "customer information," not "consumer information," and addresses "customer information" in relevant parts. Similarly, the Interagency Guidance use the term "customer information," not "consumer information." (*Compare, e.g.*, 86 Fed. Reg. 70,063, detailing inquiries by the FTC leading up to the SNPR that looked at "harm to customers" and the effects on customers of data security events, *with* pp. 70,062 & 70,064 noting that "at least 1,000 *consumers* [must] have been affected or reasonable may be affected" to constitute a security event. *But see* Gramm-Leach-Bliley Act, Pub. Law 106-102 (Nov. 12, 1999) (available at: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf), at Sec. 521, providing for privacy protection for "customer information" in financial institutions, and section 527(2), defining "customer information of a financial institution" as "any information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer" (the law does not define "consumer information"); *and* 70 Fed. Reg. 15,736 *et seq.*, using "customer information," not "consumer information.")

[13] "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," 70 Fed. Reg. 15,736 (March 29, 2005). *See also* "Interagency Guidelines Establishing Information Security Standards," available, for example, at: https://www.fdic.gov/regulations/laws/rules/2000-8660.html *and* https://www federalreserve.gov/supervisionreg/interagencyguidelines htm.

reporting requirement subjects FTC-regulated financial institutions to a fundamentally different standard than financial institutions regulated by other federal regulators. Additionally, the FTC's threshold for notice filing fails to capture incidents of unauthorized access to sensitive consumer information involving misuse of consumer information that has occurred, or is reasonably possible, if 1,000 or more consumers are not impacted, leaving many consumers without the benefit of important notifications, and potentially subject to harm or inconvenience, if the scope of a data security event does not rise to the designated level.[14]

In contrast to the FTC's proposal, the Interagency Guidance provides for a banking organization to notify its primary federal regulator "as soon as possible when the institution *becomes aware* of an incident involving unauthorized access to or use of *sensitive customer information*" (defined as "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account" as well as "any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number).[15] The Interagency Guidance also provides for a banking organization to notify customers "when warranted," stating, more fully, that "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused"; and that "[i]f the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible."[16] The Interagency Guidance further notes that "[i]f a financial institution, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible," but that there may be situations where "the institution determines that a group of files has been accessed improperly," and that all customers in a particular group should be notified if the "circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible."[17]

The Clearing House respectfully recommends the FTC refine its notification threshold so as to adopt a threshold similar to that which has been adopted by the OCC, Board, and FDIC. Specifically, the FTC should, similar to the standard set by the OCC, Board, and FDIC, require notices of security events to be filed as soon as possible when an FTC-regulated financial institution becomes aware of an incident involving unauthorized access to or use of sensitive customer/consumer information. In imposing such a requirement, the FTC should not apply a

[14] *See supra* note 12 regarding the use of the term "consumer," as opposed to "customer." For purposes of these comments, The Clearing House has generally substituted the term "customer" for "consumer" because relevant sections of the Gramm-Leach-Bliley Act refer to "customer information," and the Interagency Guidance uses the term "customer information."
[15] 70 Fed. Reg. 15,752 (italics added for emphasis).
[16] *Id.*
[17] *Id.*

1,000-or-more-customer/consumer threshold as doing so diminishes the protective effects of the rule, and leaves myriad consumers out of receiving important notifications that might help them avoid becoming subject to harm or inconvenience.

Adopting a notification trigger similar to the notification requirements of the Interagency Guidance would align the FTC's notification requirements with those of other federal financial regulators and would ensure a uniform standard applies to businesses engaged in functionally similar activities. Such a standard would also ensure that institutions are focused on reporting events involving unauthorized access to or use of sensitive customer information, rather than engaging in the additional determination of whether misuse of customer information constitutes a "security event," at a time when it is critical that resources be dedicated to effectively responding to the incident.

b. Timeframe for the Reporting of a Qualifying "Security Event"

Under the proposed rule, required "security event" notifications must be submitted to the FTC "as soon as possible" and "no later than 30 days after discovery of an event."[18] The Interagency Guidance similarly requires notifications to be submitted "as soon as possible," after concluding that misuse of customers' information has occurred or is reasonably possible, but, in contrast to the proposed rule, the Interagency Guidance generally contemplates a notification timeframe of hours and days, rather than a month.[19] The Interagency Guidance notes that "[a]s the scope and timing of a financial institution's investigation is dictated by the facts and circumstances of a particular case, the Agencies have not designated *a specific number of hours or days* by which financial institutions should provide notice to customers."[20] The recently-adopted "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" final rule ("CSI Rule") similarly incorporates an hours-and-days timeframe – requiring notification "no later than 36 hours after the banking organization determines that a notification incident has occurred."[21] The Clearing House appreciates the FTC's efforts to provide institutions it supervises with a "reasonable" time period in which to report security events, but notes that a month is an eternity in the wake of a data breach. The Clearing House respectfully recommends that the FTC align its notice period with that provided by the OCC, Board, and FDIC in the Interagency Guidance. Adoption of a uniform reporting timeframe would ensure a common standard applies to businesses engaged in functionally

[18] 86 Fed. Reg. 70,067.
[19] 70 Fed. Reg. 15,750 & 15,752.
[20] *Id*. at 15,744 (italics added for emphasis).
[21] *See* "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 Fed. Reg. 66,442-66,444 (Nov. 23, 2021) (to be codified at 12 C.F.R. 53; 12 C.F.R. 225, 12 C.F.R. 304) (effective date April 1, 2022) (noting that "36 hours is [an] appropriate timeframe, given the simplicity of the notification requirement and the severity of incidents captured by the definition of 'notification incident'," and a rule that combines a 36-hour reporting period with a "notification incident" threshold does not expect organization to "typically be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident," but to take a reasonable amount of time to determine that a "notification incident" has occurred).

similar activities, and would ensure the FTC is updated in a timely fashion consistent with other federal financial regulators.

c. The FTC Should Further Amend The Safeguards Rule to Require the Reporting of Material Disruption or Degradation, or Reasonable Likelihood of Material Disruption or Degradation, of an FTC-Regulated Financial Institution's Abilities, Business Lines, or Operations, and Similar Such Disruptions at FTC-Regulated Financial Institutions' Service Providers

In addition to harmonizing the proposed security event reporting requirements with the requirements of the Interagency Guidance, the FTC should further supplement the Safeguards Rule to require FTC-regulated financial institutions to notify the FTC of material disruptions or degradations of those organizations' abilities, business lines, or operations, similar to the reporting requirements provided in the recently-adopted "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" final rule ("CSI Rule").[22] Doing so would align FTC-regulated financial institutions' reporting requirements with the requirements applicable to financial institutions regulated by other federal regulators, and would help ensure that the FTC's notice filing requirements do not fail to capture significant events that are likely to materially disrupt or degrade organizations' abilities, business lines, or operations.

In contrast to the FTC's proposal, the CSI Rule requires a banking organization to notify its primary federal regulator of a "computer-security incident," which is defined as an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores or transmits."[23] Further, to be reportable, the computer security incident must rise to the level of a "notification incident" – a "computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, including associated services, functions

[22] *See* "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 Fed. Reg. 66,424 & 66,442-66,444 (Nov. 23, 2021) (to be codified at 12 C.F.R. 53; 12 C.F.R. 225, 12 C.F.R. 304) (effective date April 1, 2022) (requiring a banking organization to notify its primary federal regulator of a "computer-security incident" (defined as an "occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores or transmits") that rises to the level of a "notification incident" (a "computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States")).

[23] *Id.* at 66,442.

and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States," or a service provider of the banking organization experiences material disruption or degradation that has occurred or is likely to occur for four or more hours.[24]

The Clearing House respectfully recommends the FTC further refine its security event reporting requirements to adopt a reporting requirement similar to that which has been adopted by the OCC, Board, and FDIC in the CSI Rule. Specifically, the FTC should, in addition to the requirements noted in section I(a) above, require notices of security events to be filed when such an event constitutes a material disruption or degradation, or the reasonable likelihood of material disruption or degradation, of an FTC-regulated financial institution's abilities, business lines, or operations, or, when an FTC-regulated financial institution receives a notification from one of its service providers that the service provider has experienced a material disruption or degradation, or a notice that a material disruption or degradation at a service provider is likely to occur for four or more hours. Adopting additional notification requirements that are similar to the "notification incident" reporting requirement of the CSI Rule would align the FTC's overall notification obligations with those of other federal financial regulators and would ensure a uniform standard applies to businesses engaged in functionally similar activities.

II. Responses to Specific Questions Posed in the SNPRM

The FTC requests comment on a number of specific questions, including whether the Safeguards Rule should contain a reporting requirement for security events, whether such a requirement should be a standalone requirement, whether the notice threshold is the appropriate one, whether the timeframe for reporting is appropriate, whether law enforcement investigations should interact with the notice-filing process to prevent or delay notice filing, and whether notices should be made public. The Clearing House provides the following comments:

A standalone notice requirement should be a part of the Safeguards Rule. While a growing number of states are amending their data breach notification laws to include usernames and passwords and/or security questions and answers in their definitions of personal information (either generally or when the credentials permit access to a financial account), a substantial portion of states do not include this data element. Therefore, without a specific breach notice requirement in the FTC Safeguards Rule, FTC-regulated institutions may be required to notify some consumers only in some states if a breach results in a compromise of consumer banking credentials. The FTC's immediate proposal helps solve this problem and represents an important improvement to the overall Safeguards Rule as it helps ensure that institutions engaged in functionally equivalent activities as banks are subject to a reporting requirement that is not tied to state data breach notification laws that cover different types of information, are triggered in different circumstances, and generally remain a patchwork. Further, the FTC's notice-filing

[24] *Id*.

requirement should be a standalone requirement, analogous to requirements for notifications to be sent to prudential bank regulators, for example under the Interagency Guidance.

The notice threshold should be aligned to the threshold required by other federal financial regulators. The Clearing House remains concerned about differences that exist between the standards to which traditional financial institutions regulated by the prudential regulators are subject and those that the FTC has proposed in the SNPRM on the security event reporting requirements. In order to ensure that the security event reporting component applies functionally similar requirements to FTC-regulated financial institutions as apply to banks today, the FTC should require notices of security events to be filed as soon as possible when an FTC-regulated financial institution becomes aware of an incident involving unauthorized access to or use of sensitive customer/consumer information. In requiring such notices, the FTC should not impose a 1,000-or-more-customer/consumer threshold as doing so excludes myriad consumers from receiving important notifications – notifications that might help consumers avoid harm or inconvenience. Additionally, the FTC should consider further supplementing the Safeguards Rules through the enactment of a requirement for FTC-regulated financial institutions to notify the FTC of material disruptions or degradations of those organizations' abilities, business lines, or operations, similar to the reporting requirements provided in the recently-adopted CSI Rule. A clear and consistent standard for entities engaged in banking- and payments-related activities to report unauthorized access to or use of sensitive customer/consumer information, and to report material disruptions or degradations of abilities, business lines, or operations, helps not only ensure uniformity but helps preserve consumer confidence in important infrastructure.

The timeframe for event reporting should be aligned to the timeframe provided by other federal financial regulators. The current proposal of a maximum of 30 days after discovery of a security event is a significantly longer period than the "hours or days" contemplated in the Interagency Guidance, and the 36 hours provided under the CSI Rule.[25] A month can constitute an eternity in a fast-paced, post-breach environment. The Clearing House respectfully recommends that the FTC align its notice timeframe with that provided by the OCC, Board, and FDIC in the Interagency Guidance.

Noninterference with valid law enforcement investigations is essential and helps to protect the safety of the financial system. The ability of law enforcement to conduct unimpeded investigations is imperative to the safety of financial systems, can help reduce illicit use of banking and payments systems, and can aid national security interests. The Clearing House supports the valid exercise of law enforcement functions, and observes that federally-regulated banks are obligated to report certain data and data security incidents to law enforcement today.[26]

---

[25] *See supra* notes 20 and 21.

[26] *See, for example*, 70 Fed. Reg. 15,740 (requiring financial institutions to "immediately notify law enforcement in situations involving Federal criminal violations requiring immediate attention"); Federal Deposit Insurance Corporation, "Interagency Guidelines Establishing Information Security Standards" (available at: https://www.fdic.gov/regulations/laws/rules/2000-8660.html) (requiring response programs to include "appropriate reports to … law enforcement agencies," and the notification of law enforcement agencies in connection with suspicious activity report regulations); *and* Board of Governors of the Federal Reserve System, "Interagency

The Interagency Guidance provides for modifications to the notice process, notice contents, and notice delivery when law enforcement is or should be involved.[27] For example, the Interagency Guidance notes that "it is appropriate to delay customer notice if such notice will jeopardize a law enforcement investigation," and provides for delay of a notice if "an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay."[28] Similar to the Interagency Guidance, the FTC's security-event reporting requirement for FTC-regulated financial institutions should permit delay of consumer/customer notice if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. Such a provision balances the need of customers to obtain important information in a timely fashion with the needs of law enforcement.

Public access to certain important security-event-related information helps the public take action to protect themselves. The Clearing House observes that public access to certain important security-event-related information can help the public take action to protect themselves. For example, a consumer that becomes aware of the exposure of her username and password held by a data aggregator would be able to take action to change similar or the same information used at other financial service providers. The Clearing House respectfully recommends that, similar to the Interagency Guidance, the FTC require direct notice be provided to consumers in certain instances, such as when an organization becomes aware of an incident of unauthorized access to sensitive customer/consumer information.[29] The beneficial value of providing the public with actionable information must, however, be weighed against risks to consumer privacy, information confidentiality, of potentially aiding perpetrators of cyberattacks, and of potentially causing consumer confusion or alarm, as well as the need to contain and control security risks.

III. Conclusion

Ensuring that businesses, including fintechs, engaged in functionally similar banking- and payments-related activities as banks are subject to functionally similar requirements is

---

Guidelines Establishing Information Security Standards" (available at: https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm) (requiring incident response programs to include notification of law enforcement where appropriate).

[27] 70 Fed. Reg. 15,737, 15,739-15,740 & 15,744 (noting modifications to the standards for law enforcement, and requiring financial institutions to "immediately notify enforcement in situations involving Federal criminal violations requiring immediate attention").

[28] *Id.*

[29] The Interagency Guidance provides for a banking organization to notify customers "when warranted." For example, under the Interagency Guidance, "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused," and "[i]f the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." (70 Fed. Reg. 15,752.)

imperative to the safety and soundness of financial systems and to preserving public confidence in these systems. The FTC's work improving and strengthening the Safeguards Rule, and proposal to provide data security event reporting requirements for FTC-regulated institutions, are important steps in the right direction, particularly in light of the massive amounts of consumer financial data held and used by FTC-regulated institutions such as fintechs. Nevertheless, addressing key differences between the standards to which traditional financial institutions regulated by the prudential regulators are subject and those proposed in the SNPRM would strengthen the proposed security event reporting component of the SNPRM/Safeguards Rule and would ensure that the security event reporting component applies functionally similar requirements to FTC-regulated financial institutions as apply to banks today. In particular, the key differences that exist in the threshold for event reporting/what constitutes a reportable "security event" under the SNPRM, and in the timeframe for the reporting of an event under the SNPRM, should be aligned and harmonized with requirements promulgated by other federal financial regulators.

We appreciate the important work that the FTC is doing to enhance the Safeguard's Rule, as well as this opportunity to comment on the proposed security event reporting requirements for FTC-regulated institutions. We hope that the FTC will take the points made above into consideration. In updating the Safeguards Rule, and promulgating data security event notification requirements, the FTC has an important opportunity to take action in an area of increased risk both to consumers and to the safety and soundness of the financial system. If you have any questions, please contact the undersigned by phone at (646) 709-3026 or by email at Philip.Keitel@theclearinghouse.org.

Respectfully submitted,

/S/

Philip Keitel
Associate General Counsel & Vice President
The Clearing House Association L.L.C.