PUBLIC SUBMISSION

# Comment Submitted by CTIA

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

Comments of CTIA re FTC Safeguards Rule Supplemental NPRM

Download (https://downloads.regulations.gov/FTC-2021-0071-0020/attachment_1.pdf)

**Comment ID**

FTC-2021-0071-0020

**Tracking Number**

kzd-86jp-ogz7

**Comment Details** **Submitter Info**

**Received Date**

Feb 7, 2022

*Your Voice in Federal Decision Making*

**Before the**
**FEDERAL TRADE COMMISSION**
**Washington, D.C. 20580**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Standards for Safeguarding Customer Information | ) | Docket No. FTC-2021-0071 |
| | ) | |
| | ) | |
| Safeguards Rule, 16 CFR Part 314, Project No. P145407 | ) | |
| | ) | |

# COMMENTS OF CTIA


Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

**CTIA**
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org


February 7, 2022

## TABLE OF CONTENTS

## I. INTRODUCTION

CTIA[1] is pleased to submit comments in response to the Federal Trade Commission's ("FTC" or "Commission") Supplemental Notice of Proposed Rulemaking ("Supplemental NPRM") proposing to further amend the Standards for Safeguarding Customer Information ("Safeguards Rule") to require that covered financial institutions report to the FTC certain security events.[2] Specifically, the Supplemental NPRM proposes to "require financial institutions that experience a security event in which the misuse of customer information has occurred or is reasonably likely, and at least 1,000 consumers have been affected or reasonably may be affected, to provide notice of the security event to the Commission."[3] Further, the Supplemental NPRM proposes that the FTC would create a public database of information it receives from such reports,[4] and asks additional questions, including "[w]hether notification to consumers, as well as to the Commission, should be required."[5]

CTIA and its members are leaders in the areas of privacy and security. CTIA's Cybersecurity Working Group ("CSWG") brings together all sectors of wireless communications—including service providers, manufacturers, and wireless data, internet, and

[1] CTIA – The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Federal Trade Commission, Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,062 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25064.pdf ("Supplemental NPRM").

[3] *Id*. at 70,064. A financial institution's report to the FTC would include "(1) [t]he name and contact information of the reporting financial institution; (2) a description of the types of information involved in the security event; (3) if the information is possible to determine, the date or date range of the security event; and (4) a general description of the security event." *Id*.

[4] *Id*.

[5] *Id*.

applications companies—to facilitate innovation and cooperation in response to evolving security threats. Through the CSWG, CTIA and its members actively engage in security policy discussions at the federal level and regularly collaborate with federal partners, including the National Institute of Standards and Technology, the Federal Communications Commission, and the Department of Homeland Security, as well as the White House. CTIA's Privacy Working Group similarly brings together wireless industry stakeholders to engage on various data privacy issues.

While the wireless sector agrees safeguarding customer information is critical, the current proposal in the Supplemental NPRM will not further that goal, and it will only add unnecessary cost and complexity to an already fragmented reporting and notification landscape. Accordingly, CTIA respectfully requests that the FTC not establish a reporting requirement or standard for financial institutions under the Safeguards Rule. As detailed below, financial institutions already have detailed new security requirements under the revised Safeguards Rule,[6] and are also already subject to extensive state incident reporting requirements that cover the waterfront of reporting obligations. The FTC's proposal for another notification requirement—particularly one that would use different standards from existing frameworks—would only add to the burden on covered companies, while not yielding marginal benefits for the FTC or for consumers.

In the alternative, if the FTC moves forward with a reporting requirement under the Safeguards Rule, it should establish a simple requirement under which a financial institution would notify the FTC if (1) it experiences a breach involving customer information related to the provision of financial products or services, consistent with the purpose of the Gramm-Leach-

[6] Federal Trade Commission, Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,272 (Dec. 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25736.pdf ("Final Safeguards Rule").

Bliley Act ("GLBA")[7]; *and* (2) it otherwise has reported such a security breach to a governmental or regulatory authority or has notified 1,000 or more consumers of such a security breach, in either case pursuant to an independent legal requirement. While CTIA does not believe this approach is necessary, given the other options for the FTC to achieve its goals without an additional reporting requirement, this would be preferable to a new, stand-alone reporting requirement for financial institutions under the FTC's Safeguards Rule. However, should the FTC choose to implement a stand-alone requirement, it should significantly narrow its proposal to focus on security breaches that are likely to cause actual harm to consumers. Otherwise, an overbroad requirement would result in the FTC simply being inundated with notifications of low-risk events, making it more challenging to identify actual Safeguards Rule violations.

Additionally, as discussed in greater detail below, the FTC should not create a public database of incidents, which could allow hackers to re-victimize both companies and consumers using published information, with no clear benefit, nor should the FTC extend its proposal to include consumer notifications, as consumers already receive direct notifications of relevant breaches under existing laws.

## II. THE FTC SHOULD NOT IMPOSE A SECURITY EVENT REPORTING REQUIREMENT UNDER THE SAFEGUARDS RULE, AS DOING SO WOULD DO LITTLE TO ADVANCE THE SECURITY OF CUSTOMER INFORMATION AND WOULD IMPOSE ADDITIONAL BURDENS.

### A. The Proposed Reporting Requirement Will Not Yield Additional Benefits Beyond Existing Safeguards Rule Security Requirements and State Law Breach Notification Requirements.

The FTC's proposal would not improve the data security of covered financial institutions.

[7] Gramm-Leach-Bliley Act, Pub. L. No. 106–102.

Last year, the FTC revised its Safeguards Rule to impose additional requirements on covered financial institutions.[8] The FTC does not need to couple these already extensive mandates with a reporting requirement, which will not meaningfully improve security; instead, given the existing requirements under state law, it will just add administrative burdens to both the government and businesses after an incident.

Financial institutions are already subject to a patchwork of state data breach notification requirements, under which they are obligated to notify consumers—and in many cases state regulators—about security breaches.[9] All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted state-level breach notification laws.[10] Further, Congress is actively considering incident reporting requirements for critical infrastructure, including financial institutions.[11] Adding yet another layer of reporting obligations on organizations that are victims of cybersecurity attacks and are working to contain the threat and assess and mitigate the damage is unnecessary and overly burdensome. Indeed, the current patchwork of state laws already creates an inefficient and confusing approach, which is why CTIA supports a single federal data breach notification standard where there is a reasonable risk that the breach has resulted in, or will result in, actual harms to consumers. Having a single national framework will reduce confusion for consumers and burdens on businesses. In the

[8] *See* Final Safeguards Rule. This includes a requirement that financial institutions develop an incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in its control. *Id*. at 70,308 (outlining the incident reporting requirement to be effective under Revised.16 C.F.R. § 314.4(h)).

[9] *See* National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 17, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ("NCSL Security Breach Notification Laws").

[10] *Id*.

[11] *See, e.g.*, Cyber Incident Reporting Act, S. 2875, 117th Cong. (2021); Cyber Incident Reporting for Critical Infrastructure Act, H.R. 5440, 117th Cong. (2021).

absence of a single, federal framework to achieve uniformity in breach reporting obligations, additional requirements on top of the existing patchwork will do little to advance the goal of safeguarding consumer data.

Adding to the complexities and burdens associated with the FTC's proposed reporting requirement is the fact that the FTC's proposal could be read to include incidents that do not pose a risk of consumer harm, which is inconsistent with most existing state breach notification laws. Such an expansive reporting trigger would be confusing, would inundate the FTC with reports, and would likely inhibit the FTC's ability to focus on the most serious incidents. For example, state laws generally require notice of breach based on a clearly defined incident, such as unauthorized acquisition[12] of sensitive personal information, but the FTC's proposed reporting requirement would be triggered by a "misuse" standard that could be construed more broadly.[13] Moreover, the FTC's proposal would cover "customer information,"[14] which can be read broadly to include a wide range of information that is otherwise public, if collected in the course of a financial transaction under certain circumstances,[15] whereas state laws generally only cover a defined set of sensitive, nonpublic personal information that is much more likely to result in consumer harm if exposed, such a first and last name in combination with a Social Security number, driver's license number, or financial account information.[16] Accordingly, it is simply not the case that, as the Supplemental NPRM states,"[t]o the extent state law already requires notification to consumers or state regulators, . . . there is little additional burden in providing

[12] *E.g.*, Cal. Civ. Code § 1798.82(a); 815 Ill. Comp. Stat. 530/5; Tex. Bus. & Com. Code § 521.053(a).

[13] Supplemental NPRM at 70,064.

[14] *Id*.

[15] *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314.2.

[16] *See, e.g.*, Cal. Civ. Code § 1798.82(h); Fla. Stat. § 501.171(1)(g)(1); N.Y. Gen. Bus. Law § 899-aa(1)(b); Tex. Bus. & Com. Code §§ 521.001(a)(2); Va. Code § 18.2-186.6(A).

notice to the Commission as well."[17] The FTC's proposal is inconsistent with existing state data breach notification standards, creating additional burdens for covered financial institutions without providing meaningful security benefits.

### B. The FTC Can Achieve Its Stated Goals Through Existing Channels Without Imposing a Broad Requirement.

The FTC's primary stated goal for the proposed reporting requirement is to help its enforcement of the Safeguards Rule: the Supplemental NPRM states that "[t]he proposed reporting requirement would ensure the Commission is aware of security events that could suggest a financial institution's security program does not comply with the Rule's requirements, thus facilitating Commission enforcement of the Rule."[18] This is a different goal from incident reporting requirements in other contexts; for example, cybersecurity incident reporting can be useful for government entities with operational expertise to mitigate attacks or collaborate with industry to combat cyber-criminals. Given the FTC's specific goal, the FTC and financial institutions are better served by the FTC gathering information through existing channels that it already uses in the course of its data security enforcement.

For purposes of enforcement, information about financial institution breaches is already reported and available under existing state breach notification laws, and the FTC can access such information in more efficient ways than the broad new proposed approach. There is no evidence that the FTC is not alerted to significant data breaches given existing breach notification statutes. Aside from notices that must be given to individual consumers under state law, many data breaches are publicized in news reporting and often by impacted organizations, and state AGs

[17] Supplemental NPRM at 70,064.

[18] *Id*. at 70,066.

publicize breaches in many cases as well.[19] To the extent that the FTC determines these information channels are not adequate for the FTC to enforce the Safeguards Rule, the FTC already has other options to obtain information. For example, the FTC already works with state AGs and other regulators, especially on consumer complaint reporting, so the FTC can draw on existing channels to access available and relevant information. The FTC also can use its existing investigation tools to seek additional information about a breach that has been made public. Indeed, the agency has used these tools for years, and is highly active in data security and identity theft enforcement, having brought 80 data security cases from 2002-2020 under its Section 5 authority and investigating even more cases than those that proceeded to an enforcement action.[20]

Moreover, as proposed, the FTC's broad reporting requirement is not likely to aid in the agency's Safeguards Rule enforcement efforts. As discussed below, the overly broad definitions proposed in the Supplemental NPRM would likely result in a flood of reports, which are unlikely to be helpful in identifying actual material deficiencies in companies' information security plans. Indeed, an overly broad reporting requirement may hurt the FTC's ability to investigate the most serious financial institution security events, as such a broad requirement will result in a high volume of reports—including reports of minor events—which will divert FTC staff resources away from being able to focus on serious trends or breaches. The proposed reporting requirement is an overly burdensome mechanism for the FTC to facilitate Safeguards Rule

[19] *E.g.*, Delaware Department of Justice, *Data Security Breaches*, https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification/ (last visited Jan. 17, 2022) ("Delaware Data Security Breaches"); Maryland Attorney General, *Maryland Information Security Breach Notices*, https://www marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx (last visited Jan. 17, 2022) ("Maryland Information Security Breach Notices").

[20] Federal Trade Commission, FTC Report to Congress on Privacy and Security: A Report to Congress at 3 (Sept. 13, 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

enforcement, and the agency can rely on existing channels that are more appropriately tailored for the FTC to achieve its goals.

Regarding the FTC's other justification for its proposed rule—"[t]o . . . assist consumers by providing information as to the security of their personal information in the hands of various financial institutions"[21]—consumers already receive direct notification about breaches that are likely to cause harm to them under existing state breach notification laws, making the FTC's proposed rule unnecessary, and only likely to cause confusion to the extent that additional customer notification is involved.[22] Additionally, as discussed further below in Part III.C, the FTC's proposal to publicize breach information in a centralized database will not improve upon these existing consumer notification frameworks and may work against those goals by creating additional security and re-victimization risks.

The FTC's proposal is not simply duplicative of existing reporting requirements, as the FTC implies.[23] If the proposal were simply duplicative, then it is conceivable that this additional reporting requirement to the FTC would impose little burden. But instead, the proposal would add onerous new requirements on covered financial institutions without adding marginal benefits for the FTC, which can already obtain the most relevant information, or for consumers, who are already recipients of direct notices from financial institutions and other organizations in the event of a breach. Accordingly, CTIA recommends that the FTC not establish a reporting requirement or standard under the Safeguards Rule.

[21] Supplemental NPRM at 70,066.

[22] *See* NCSL Security Breach Notification Laws.

[23] *See* Supplemental NPRM at 70,064 ("To the extent state law already requires notification to consumers or state regulators, moreover, there is little additional burden in providing notice to the Commission as well.").

## III. IN THE ALTERNATIVE, ANY REPORTING REQUIREMENT SHOULD BE NARROWLY TAILORED SO THE FTC CAN ACCESS INFORMATION ABOUT FINANCIAL INSTITUTION BREACHES WITHOUT ADDING TO THE ALREADY COMPLEX PATCHWORK OF NOTIFICATION LAWS.

As detailed below, if the FTC moves forward with a security event reporting requirement, it should establish a simple notification requirement under which a financial institution must notify the Commission if (1) it experiences a breach involving customer information related to the provision of financial products or services, consistent with the purpose of the GLBA; *and* (2) it otherwise has reported such a security breach to a governmental or regulatory authority or has notified 1,000 or more consumers of such a security breach, in either case pursuant to an independent legal requirement. This approach would save financial institution and FTC resources, while allowing the FTC to achieve its stated goals. In the alternative, if the FTC moves forward with a stand-alone reporting requirement, then it should refine its current proposal in specific ways discussed below. Finally, regardless of how the FTC proceeds, it should not create a public database to centralize financial institution breach information, as doing so could create security risks, and it should not establish a separate consumer reporting requirement, as consumers already receive direct notification of breaches and adding more would risk consumer confusion and notice fatigue.

### A. The FTC Could Require Financial Institutions to Notify the Commission of Covered Breaches When They Report Under Independent Legal Requirements.

The Supplemental NPRM asks "[w]hether, instead of implementing a stand-alone reporting requirement, the Commission should only require notification to the Commission whenever a financial institution is required to provide notice of a security event or similar to a

governmental entity under another state or Federal statute, rule, or regulation."[24] The answer to this question is "yes." Specifically, the FTC could establish a much more tailored reporting trigger, under which covered financial institutions would be required to provide a simple notice to the FTC if: (1) they experience a breach involving customer information related to the provision of financial products or services, consistent with the purpose of the GLBA; *and* (2) they otherwise have reported such a security breach to a governmental or regulatory authority or have notified 1,000 or more consumers of such a security breach, in either case pursuant to an independent legal requirement.

Establishing a reporting requirement with these triggers would allow the FTC to achieve its stated goal of facilitating enforcement of the Safeguards Rule, in a manner that is significantly less burdensome than the FTC's current proposal. A new, stand-alone FTC reporting rule would add to an already complex legal patchwork of laws, forcing financial institutions to expend resources to navigate additional requirements and customize reports on the same security event to multiple agencies. On the other hand, tying an FTC reporting obligation to an independent legal reporting requirement would allow financial institutions to streamline compliance efforts and focus resources on protecting customer information and remediating incidents and threats.

### B. If the FTC Establishes a Stand-Alone Reporting Requirement for Financial Institutions, It Should Be Significantly Refined.

If the FTC decides to adopt its own stand-alone reporting requirement, then it should adjust the proposal significantly to: (1) target reporting of incidents likely to cause harm to consumers, which will reduce the potential for overreporting and better assist the agency and consumers in targeting significant breaches, and (2) ensure adequate time to investigate and

[24] *Id*.

mitigate security events and provide a reasonable reporting timeline beginning when a financial institution has confirmed that a breach has occurred as opposed to when it initially discovers an event.

1. *The FTC's Proposed Reporting Requirement Is Too Broad.*

The FTC's current proposal potentially applies broadly to a wide range of information security issues, regardless of whether they result in actual breaches that are likely to cause consumer harm. This lack of focus is not helpful for either the FTC or consumers, in addition to burdening businesses, because it will likely lead to a deluge of reports out of an abundance of caution on the part of financial institutions. If the FTC chooses to impose a reporting requirement, it should follow the lead of other government entities and focus on breaches where there is a reasonable risk of consumer harm.

*First,* as proposed, the FTC's new reporting requirement would apply broadly to security events involving *all* "customer information," which is a capacious term that could encompass information that is not sensitive, such as name and street address.[25] Reporting requirements should be reserved for *sensitive* information, the unauthorized acquisition of which may result in actual harm to consumers, including the risk of financial harm. Accordingly, for the purposes of a reporting requirement, FTC rules should apply to a narrower set of data, similar to the types of sensitive data protected under many state laws, such as Social Security numbers, driver's license numbers, and financial account information.

*Second*, the reporting requirement as proposed is tied partially to the definition of "security event," which is also far too broad for a reporting requirement.[26] "Security event" is

[25] *Id.*; *see* Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.2(d), 314.2(l).

[26] *See* Supplemental NPRM at 70,067.

defined as "an event resulting in unauthorized access to, or *disruption or misuse of*, an information system, information stored on such information system, or customer information held in physical form."[27] However, not all "disruption or misuse" of customer information stored on information systems would result in a risk of harm, especially to the extent that the requirement would apply to *all* customer information, broadly defined to include information that is held by the financial institution but that is not sensitive. Further, tying a reporting requirement to such a broad term would be overly burdensome and would result in a flood of unnecessary and unhelpful reports, again distracting from the pursuit of investigations involving actual consumer harm.[28] Therefore, instead of relying on the current definition of a "security event," any reporting regime under the GLBA should have a high and clear trigger, based on a confirmed financial institution breach where there is a reasonable risk that the breach has resulted in, or will result in, actual consumer harms.

*Third*, the FTC's proposal should include reasonable reporting limitations, such as those in state data breach notification laws, that also bear on risk of harm. Specifically:

- The FTC asks "whether events involving encrypted information should be included in the requirement."[29] Indeed data that is encrypted or otherwise masked should be excluded from the reporting requirement, as states have done.[30] This data is less likely to be misused in a way that harms consumers.
- Any reporting requirement should include an exception for good faith acquisition of covered data, even if unauthorized, as provided under several state laws, for similar reasons.[31]

[27] Final Safeguards Rule at 70,307 (emphasis added).

[28] While CTIA acknowledges that under the proposal, reporting would only be required of security events if "misuse of customer information has occurred or is reasonably likely to occur and . . . at least 1,000 consumers have been affected or reasonably may be affected," as described below, these standards for assessing risk of harm are not sufficient to only target those breaches that will reasonably result in harm to consumers.

[29] Supplemental NPRM at 70,063.

[30] *E.g.*, Cal. Civ. Code § 1798.82(a); Colo. Rev. Stat. § 6-1-716(1)(a); Fla. Stat. § 501.171(1)(g)(2); N.Y. Gen. Bus. Law § 899-aa(2)(a); Wash. Rev. Code § 19.255.010(1). The FTC asks: "[s]hould there be a carve-out for security events solely involving encrypted data?" Supplemental NPRM at 70,064.

[31] *E.g.*, Cal. Civ. Code § 1798.82(g); S.D. Codified Laws § 22-40-19(1); Tex. Bus. & Com. Code §§ 521.053(a).

- Critically, regardless of whether the trigger is a "security event," any stand-alone FTC reporting requirement should include an adequate "risk of harm analysis." The proposed rule indicates that the new reporting requirement would not be triggered unless "misuse of customer information has occurred or is reasonably likely to occur and at least 1,000 consumers have been affected or reasonably may be affected."[32] This standard, however, is not equivalent to the more targeted risk of harm analysis found in many state laws.[33] Reporting should only be required when a breach is reasonably likely to cause *actual harm* to a financial institution's customer, such as identity theft or other financial harm, not merely if "*misuse* of customer information has occurred or is reasonably likely to occur" or when "consumers have been *affected* or reasonably may be affected," as the latter standards could be interpreted incredibly broadly.[34] This is especially true under the current proposal, given that "security event" includes system disruptions that could arguably affect consumers, but ultimately do not lead to potential harm.[35]

The FTC's overly broad reporting standard, if adopted, would result in overreporting with no benefit for consumers, and would ultimately harm rather than aid the FTC's security efforts. Instead of being able to focus on breaches that are likely to result in consumer harm, the FTC would be inundated with reports of "events" that do not rise to the level of information security breaches and that are unlikely to harm consumers. This would burden staff and divert FTC resources by burying significant trends and serious incidents due to over-reporting minor or non-

[32] Supplemental NPRM at 70,064.

[33] *See, e.g.*, Ariz. Rev. Stat. § 18-552(J) ("A person is not required to make the notification required by subsection B of this section if the person, an independent third-party forensic auditor or a law enforcement agency determines after a reasonable investigation that a security system breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals."); Conn. Gen. Stat. § 36a-701b(b)(1) ("Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."); Fla. Stat. § 501.171(4)(c) ("Notwithstanding paragraph (a), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed."); Wash. Rev. Code § 19.255.010(1) ("Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm.").

[34] Supplemental NPRM at 70,064 (emphasis added).

[35] Similarly, the proposed rule could also be read to apply even where it is not confirmed that customer information has been misused. For example, the proposed language provides that an organization must report if it "determine[s] that misuse of customer information has occurred or is reasonably likely." *Id.* at 70,067. Again here, coupled with a broad definition of "security event" that includes system disruptions, this standard is too attenuated, moving the proposed requirement even further from the tether of security breaches that are likely to cause harm to consumers.

events. At the same time, the proposed requirement would not meaningfully improve the security of customer information, so would have no added consumer protection benefit.

Finally, the FTC's current proposal hinges on a definition of "security event" that is extremely broad and the vague standard of "misuse" of customer information. We note that the FTC's authority under GLBA is limited to establishing safeguards regarding certain personally identifiable financial information, so any reporting rule must be confined to that authority.[36]

2. *Any FTC Reporting Requirement Must Provide a Reasonable Reporting Timeline Beginning When a Financial Institution Confirms a Covered Security Breach*.

As proposed, the FTC's rule would require reporting 30 days after discovery of the event.[37] But security events are often complex and ongoing, so assessing security incidents—both their nature and impacts on data—often takes more time. To allow for a covered financial institution to adequately understand any given breach—and facilitate that institution's ability to focus on mitigating potential harms—the FTC should consider two changes to its proposed reporting timelines.

*First,* the clock should not commence on a reporting requirement until the incident has been confirmed. A confirmation trigger, as opposed to a discovery trigger, would ensure that financial institutions are able to focus on investigating and responding to a security breach, which requires significant resources. Moreover, a confirmation trigger provides clarity to financial institutions and reduces subjectivity from the determination as to whether a report is required. A clear, objective standard for the commencement of the reporting timeline is a necessary element of any incident reporting regulatory regime.

[36] *See* 15 U.S.C. §§ 6801, 6809(4).

[37] Supplemental NPRM at 70,067.

*Second*, the FTC should allow for reasonable delays in reporting for important law enforcement purposes. Given the sensitive nature of law enforcement investigations, it is important that any reporting requirement that the FTC adopts sufficiently protects the integrity of these investigations and avoids inadvertently jeopardizing federal and state efforts to hold criminals accountable.

### C. The FTC Should Not Centralize and Publish Information About Financial Institutions' Security Breaches, Which Could Increase Security Risks to Businesses and Consumers Following Breaches.

In the Supplemental NPRM, the FTC proposes to "input the information it receives from affected financial institutions into a database that it will update periodically and make available to the public."[38] The FTC should not move forward with this proposal, as publicly posting security breaches in a single database presents more risks than benefits.

A public database of the financial institutions that have suffered a data breach could be a useful data source for cyber criminals, essentially tipping off bad actors to be able to more easily exploit and re-victimize both financial institutions and their customers. Unfortunately, it is not uncommon to see customers who have been harmed by a breach be preyed on by fraudsters. For example, fraudsters reach out to these customers pretending to offer some kind of assistance or remediation post-breach. These kinds of practices already occur, but centralizing breach information in a public database would likely facilitate them. Likewise, re-victimization of companies is also a serious threat post-breach. Publicly releasing information about breaches is a roadmap for hackers, often at a very critical time when the company is trying to resolve similar or related issues. Indeed, once hackers know the details of one exploit, they usually pivot to finding the next one, often while the business is still reacting to the first breach. For example, a

[38] *Id*. at 70,064.

business could have a breach of one application programming interface ("API"), and while it is patched in the case of the breached API, the business may not immediately have the opportunity to make that same fix across the board for all APIs. Post-breach, federal partners should be working with impacted companies to contain the threat and mitigate the effects of the attack, not centralize and hand over valuable information that can help criminals continue to victimize companies and customers already suffering harms.

Further, public databases provide little if any net benefit to consumers because consumers already receive direct notifications of data breaches under state law. While certain states have chosen to publish lists of the notifications made under their breach notification laws,[39] in these states, there is no indication that publishing these lists has provided tangible benefits to consumers that are already receiving notifications from the victim organization. Furthermore, the FTC should not penalize financial institutions that are victims of cyber-attacks by subjecting them to this type of "name and shame" approach. FTC enforcement actions become public when there is a consent decree or litigation based on assessed violations; there is no need to create a public database of data breach victims.

### D. There Is No Need for the FTC To Expand Its Proposal to Include Consumer Notification Requirements.

Finally, the Supplemental NPRM asks if notification to consumers should also be required, in addition to the proposed rule requiring notice of security events to the FTC.[40] As detailed above, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted data breach notification laws that require covered organizations—which encompasses far more than just financial institutions—to notify consumers in the case of a

[39] *E.g.*, Delaware Data Security Breaches; Maryland Information Security Breach Notices.

[40] Supplemental NPRM at 70,064.

security breach.[41] While CTIA and its members support a uniform, federal data breach notification requirement that would preempt this patchwork of state laws, it does not support a federal requirement that simply adds to these obligations and that is overly broad, such as the current proposal in the Supplemental NPRM. Beyond the burdens on covered financial institutions, multiple and duplicative consumer notification requirements would also risk consumer confusion and notice fatigue, which undermine security efforts rather than bolstering them.

## IV. CONCLUSION

CTIA appreciates the opportunity to comment on the Supplemental NPRM and looks forward to continued engagement with the FTC on this important issue. The FTC should not adopt a new and additional reporting requirement for financial institutions. However, if it moves forward with a reporting requirement, it should: establish a simple notification requirement linked to existing legal obligations to report breaches of information covered under the GLBA, or at a minimum, should significantly narrow its proposal for a stand-alone reporting requirement. In any case, it should not compile breach information in a publicly available database and should not establish a requirement for consumer notifications.

[41] *See* NCSL Security Breach Notifications Laws.

Respectfully submitted,

*/s/ Melanie K. Tiano*
Melanie K. Tiano
Assistant Vice President, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

**CTIA**
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

February 7, 2022