PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

August 2, 2019

Before the
Federal Trade Commission
Washington, D.C.

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

Thank you for the opportunity to provide comments on proposed amendments to the FTC's Safeguards Rule under the Gramm-Leach-Bliley Act. We commend the FTC for addressing the timely issue of information security at financial institutions, and we support the Commission's efforts to strengthen the effectiveness of the current Safeguards Rule framework.

We are researchers associated with the Center for Information Technology Policy (CITP) at Princeton University. In keeping with Princeton's tradition of service, CITP has launched a new Technology Policy Clinic that provides nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. These comments are a product of that Clinic and reflect the independent views of the undersigned scholars.

We write to express our general support for the Commission's proposed amendments to the Safeguard Rule, as well as to offer specific recommendations for improving the Rule based on significant technical and legal expertise in the field of information security. Our comment focuses on the benefits of requiring financial institutions to adopt robust security measures to protect customer information. Bad actors, whether commercially motivated or state-sponsored, have targeted financial institutions with some success in recent years. But companies can take specific, well established, and cost-effective measures to safeguard customer information and mitigate the negative consequences of a security breach.

As we explain further below, the proposed amendments to the Safeguards Rule promote necessary and appropriate actions for financial institutions to take when implementing a comprehensive information security program. Taken together, these actions would significantly reduce data security risks for the customers of financial institutions. We offer recommendations for refining and strengthening the proposed

amendments, and we further recommend that the FTC establish a shorter review cycle for updating the Rule so that it can keep current with the evolving threat environment.

1. Risk-Based Information Security

We support the FTC's continued reliance on a risk-based approach to information security. We know that no information security measure can guarantee that a system is immune from intrusion or unauthorized access. What good security design can do is avoid single points of failure and limit the fallout from any potential breach by avoiding the risk of cascading failures.

As the field of information security has developed, practitioners have identified specific policy and practice safeguards that are effective, cost-effective, and have withstood the test of time. We support the NPRM's proposal to task financial institutions with implementing a number of such practices. We do not view these proposed amendments as endorsing a "check the box" approach. To the contrary, the proposal requires financial institutions to conduct rigorous risk assessments and implement appropriate safeguards. The NPRM's process-based approach is especially important given that security standards are evolving continually.

We encourage the Commission to augment its discussion of risk-based information security with two specific concepts: threat modeling and defense in depth. Threat modeling is a valuable practice of rigorously identifying discrete information security risks and mitigations in information security.[1] Defense in depth is the concept that information security should involve multiple, overlapping precautions, since one safeguard might be disabled, insufficient, or ineffective. Like threat modeling, defense in depth is a frequently used concept in the implementation of risk-based information security.

Recommendations:

- Require institutions to explicitly incorporate threat modeling and defense in depth in their security risk assessments.

[1] *See* Threat Modeling: Designing for Security, Adam Shostack (Wiley 2014).

2. Security Across All Networks

As currently drafted, the amendments appear to codify a distinction between "internal" and "external" networks (usually referred to as the "perimeter" security model). For example, the proposed provisions on encryption in transit and multi-factor authentication would only apply to "external" networks. With the rise of mobile computing, however, business data routinely leaves the workplace—and increasingly appears on personal devices as employers adopt bring-your-own-device policies. The distinction between internal and external networks has, as a consequence, blurred beyond recognition.

Furthermore, the notion that internal networks have heightened security is no longer supported. It is routine for information security attackers to obtain access to internal networks, then leverage that position to obtain sensitive data. Internal networks can also be inadvertently exposed to the public internet or exploited by rogue employees.

The modern practice in information security has been to move away from perimeter security, and to instead focus on protecting data within a firm's control—regardless of who owns the network that the data is transiting or the device where the data is stored. We encourage the Commission to follow this modern practice and eliminate the distinction between internal and external networks.

Recommendations:

- The NPRM's provisions on encryption and multi-factor authentication should apply to any network (internal or external) that covered information transits and any system that stores covered information.

3. Encryption

The proposed revisions to the Safeguards Rule requires financial institutions to encrypt data in transit and at rest. This makes sense. Encryption minimizes the risk of harm even if the system or network is breached, since properly encrypted information would be unreadable by an attacker. Moreover, the costs associated with implementing encryption have significantly decreased in recent years, and those costs are outweighed by the security value (including avoided costs from failures).

Encryption is, however, not a cure-all. In our experience, encryption is at times implemented poorly. For example, some firms do not securely manage cryptographic material (e.g., encryption keys), such that attackers can obtain the keys in conjunction with encrypted data—defeating the purpose of encryption. Firms can also implement outdated or non-standard encryption, introducing vulnerabilities.

Recommendations:

- Revise the definition of "encryption" to clarify that encryption must be consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

4. Access Controls

We support the Commission's proposal to incorporate access controls into the Safeguards Rule. Access controls are a foundational element of information security, minimizing the risk that data will be exposed to an unauthorized person.

A recent information security incident involving First American Financial Corporation highlights the importance of appropriate access controls.[2] First American exposed information on millions of real estate transactions to anyone on the web who could simply modify the URL for a document, giving them unauthenticated access to highly sensitive data, including bank account numbers and statements, mortgage and tax records, social security numbers, wire transaction receipts, and driver's license images.

We recommend that the Commission strengthen the proposed provision on access controls by incorporating the Principle of Least Privilege, a widely accepted security maxim that a person's access to a system, network, or data should be no greater than necessary for legitimate business purposes. The Principle of Least Privilege is especially important for employees and service providers; it mitigates the risk of insider attacks and the consequences of breaches involving service providers.

Recommendations:

[2] *See* "Security Gap Leaves 885 Million Mortgage Documents Exposed," Nicole Perlroth and Stacy Cowley, New York Times, May 24, 2019, https://www.nytimes.com/2019/05/24/technology/data-leak-first-american.html.

- Require financial institutions to design access controls that incorporate the Principle of Least Privilege, i.e., a person's access to a system, network, or data should be no greater than necessary for legitimate business purposes.

5. Information Security Testing

We support the Commission's proposal to incorporate continuous monitoring, penetration testing, and vulnerability assessments into the Safeguards Rule. Routine testing is an invaluable component of a comprehensive information security program. Mistakes happen and technology changes rapidly, necessitating recurring checks.

We recommend that the Commission strengthen its proposal by requiring *both* continuous monitoring *and* penetration testing. Continuous monitoring, in our experience, is most effective at identifying obvious vulnerabilities (e.g., out-of-date software), misconfigurations (e.g., a public management interface), and threats (e.g., malware that matches a signature) in individual, off-the-shelf systems. Continuous monitoring can be less effective for checking the interaction between systems, proprietary systems, or subtle security issues.

By contrast, penetration testing can provide in-depth assessment of particular systems, and enables a firm to benefit from a distinct attacker perspective and skillset. But penetration testing tends to be (relatively) infrequent and limited in scope. These are two distinct types of security testing with relative strengths and cumulative value; financial services firms should implement both.

Notably, the Commodity Futures Trading Commission has found that both routine monitoring and periodic independent testing are appropriate for entities that it regulates under the Gramm-Leach-Bliley Act,[3] as well as under the Commodity Exchange Act.[4]

Recommendations:

- Require that information security testing involve *both* continuous monitoring *and* penetration testing.

[3] *See* https://www.cftc.gov/sites/default/files/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.
[4] *See* https://www.govinfo.gov/content/pkg/FR-2016-09-19/pdf/2016-22413.pdf.

6. Multi-factor Authentication

The NPRM's amendments would require multi-factor authentication before accessing customer information held in internal databases. In our experience, multi-factor authentication is a highly effective and comparatively inexpensive means of reducing the risk of unauthorized access to systems.

We note that, as currently drafted, the proposed provison is ambiguous about whether the multi-factor authentication requirement extends to customer access to covered information. We recommend that the Commission clarify the amendment by expressly requiring multi-factor authentication for customer access. Research and industry experience have repeatedly demonstrated that multi-factor authentication is an important safeguard for customers, especially against phishing and password reuse attacks.

Because users have differing devices, financial backgrounds, and accessibility requirements, there is no one-size-fits-all approach to customer multi-factor authentication. We recommend that the Commission reflect these considerations in the Safeguard Rule, encouraging financial institutions to provide multi-factor authentication that is easy to use and accessible to all customers.

The NPRM's definition of multi-factor authentication includes, at minimum, a challenge based on two of three categories of information: knowledge, possession; and inherence. We support this flexibility, with a recommended addition: institutions should not rely on factors that can be readily acquired, spoofed, or manipulated.

It is important to note that authentication best practices are constantly evolving, and vulnerabilities can become apparent for factors that were previously considered secure. In accordance with that view, we support the Commission's decision to omit SMS one-time passcodes as an authentication factor, and we encourage the Commission to clearly and affirmatively exclude telephony-based authentication factors.

The information security community now recognizes that that proving device possession via SMS (or a phone call) has security risks, including SIM swap, number porting, and SS7 rerouting attacks. As a result, NIST has recommended restricted use of the practice as an authentication factor, with a long-term aim of no longer relying on the practice.[5] These vulnerabilities are not hypothetical, especially in the context of financial

[5] *See* Section 5.1.3.3, NIST Digital Identities Guidelines (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. Indeed, the FTC's former

services; there are recurring news reports of financial fraud that involves circumventing SMS-based authentication. While SMS is convenient, our assessment is that in the context of protecting financial information, that convenience is outweighed by the ready availability of more secure alternatives (e.g., software tokens, authentication apps, hardware tokens, and U2F/FIDO2 keys) that can also be conveniently deployed.

Recommendations:

- Clarify that multi-factor authentication is required for customer access to reduce the risk of unauthorized access;
- Require that financial institutions avoid authentication factors that can be readily acquired, spoofed, or manipulated.

7. Incident Response Plan

There is little debate that a written incident response plan is an essential component of a good security system. The proposed rule appropriately sets forth a few basic requirements of such a written plan, including that it provides clear lines of responsibility in often chaotic situations and that it include a process for evaluation and revision after a security incident to remediate the damage and prepare for the next attack.

We also suggest the Rule amendments require that financial institutions report security events to the Commission**.** Such reports would provide the Commission with valuable information about the scope of the problem and the effectiveness of security measures across different entities. It will also help the Commission coordinate responses to shared threats. We further recommend that all security events that could affect a certain number of customers (e.g., 500) should be reported without regard to the likelihood of harm. Basing the reporting threshold on the likelihood of consumer harm could disincentivize receiving timely and comprehensive reports as that could require making a more involved legal judgment. Finally, we encourage the FTC to make these reports available to the public to further enhance transparency and accountability.

Recommendations:

Chief Technology Officer was herself a victim of a SIM-swap attack: https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief.

- Report all security events to the Commission that could affect a certain number of customers (e.g., 500) without regard to the likelihood of harm to enhance transparency and accountability.

8. Audit Trails

Audit trails are crucial to designing effective security measures that allow institutions to detect and respond to security incidents. The trails help understand who has accessed the system and what activities the user has engaged in. We support the FTC's approach to requiring institutions to record such information at a sufficient level of detail that will be useful in identification and remediation of breaches.

9. Security Updates

We recommend that the Commission include a provision in the Rule about timely installation of security updates. A recurring issue in data breaches is that attackers are able to exploit a known security vulnerability, because the firm failed to apply necessary updates to address the vulnerability. For example, in the recent incident at Equifax, the company had failed to patch its system to account for known vulnerabilities. The result was one of the most significant data breaches ever involving a financial institution.

Recommendations:

- Explicitly include a provision that requires financial institutions to timely install security updates.

10. Data Retention

The proposed amendment requires financial institutions to develop procedures for the secure disposal of customer information. The FTC requested comments on whether there should be a requirement for destroying data after a fixed period, or an affirmative obligation on the part of the institution to demonstrate a current need for that data. We suggest a hybrid approach, where the institution has to institute a policy for mandatory deletion after a fixed time and then it may demonstrate, on a case-by-case basis, why that policy should not be followed.

We also recommend that the Commission institute a requirement that institutions periodically review their data practices to minimize data collection or

retention in areas that are unnecessary or unrelated to a legitimate business purpose. And, to the extent financial institutions collect and process data from non-traditional data sources to service their customers, that they protect that information with the same safeguards that are used to protect personally identifiable financial information.

Recommendations:

- Adopt a hybrid approach to data retention policies where the institution has to institute a policy for mandatory deletion after a fixed time and then it may demonstrate, on a case-by-case basis, why that policy should not be followed;
- Require financial institutions to periodically review their data practices to minimize data collection or retention.

11. Definition of Personally Identifiable Financial Information

We recommend that the data retention policies also apply to aggregate or "anonymized" customer information because there is a significant risk of future reidentification if the data is not destroyed securely.[6]

At present, the Rule's proposed definition of customer information excludes "[i]nformation that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses." 16 CFR § 313.3(o)(2)(ii)(B). We recommend the Rule clarify that if financial institutions rely on this exemption, they must demonstrate that the aggregate or blind data is not "reasonably linkable" to individuals.[7] The FTC's existing framework addresses that concern and requires that the company (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the

[6] Arvind Narayanan and Vitaly Shmatikov, Myths and Fallacies of "Personally Identifiable Information," 53 COMM.OF THE ACM 24, 26 (2010).

[7] The EU General Data Protection Regulation ("GDPR") addresses similar concerns by exempting from regulation data that "does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable." GDPR Recital ¶ 26. It then formulates an intermediate category, pseudonymized data, for de-identified data may be re-linked to individuals. This category is still subject to the regulations and is defined as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." GDPR Art. 5.

data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.[8]

Recommendations:

- Clarify that the definition of customer information encompasses data that can be reasonably linked to individuals.

12. Periodic Review of Safeguards Rule

Finally, we suggest the FTC establish a shorter review cycle for the Rule given the rapid technology developments in the space. Specifically, we recommend the FTC revisit the Safeguards Rule every three years to determine whether the prescriptive measures are still necessary and effective.

Respectfully submitted,

Ryan B. Amos
Graduate Student, Department of Computer Science

Tithi Chattopadhyay
Associate Director, Center for Information Technology Policy

Edward W. Felten
Robert E. Kahn Professor of Computer Science and Public Affairs

Mihir Kshirsagar
Technology Policy Clinic Lead, Center for Information Technology Policy

Jonathan Mayer
Assistant Professor of Computer Science and Public Affairs

Arvind Narayanan
Associate Professor of Computer of Science

[8] *See* FTC Report Protecting Consumer Privacy in an Era of Rapid Change (2012): https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Contact:

Website: https://citp.princeton.edu
Phone: 609-258-5306
Email: mihir@princeton.edu