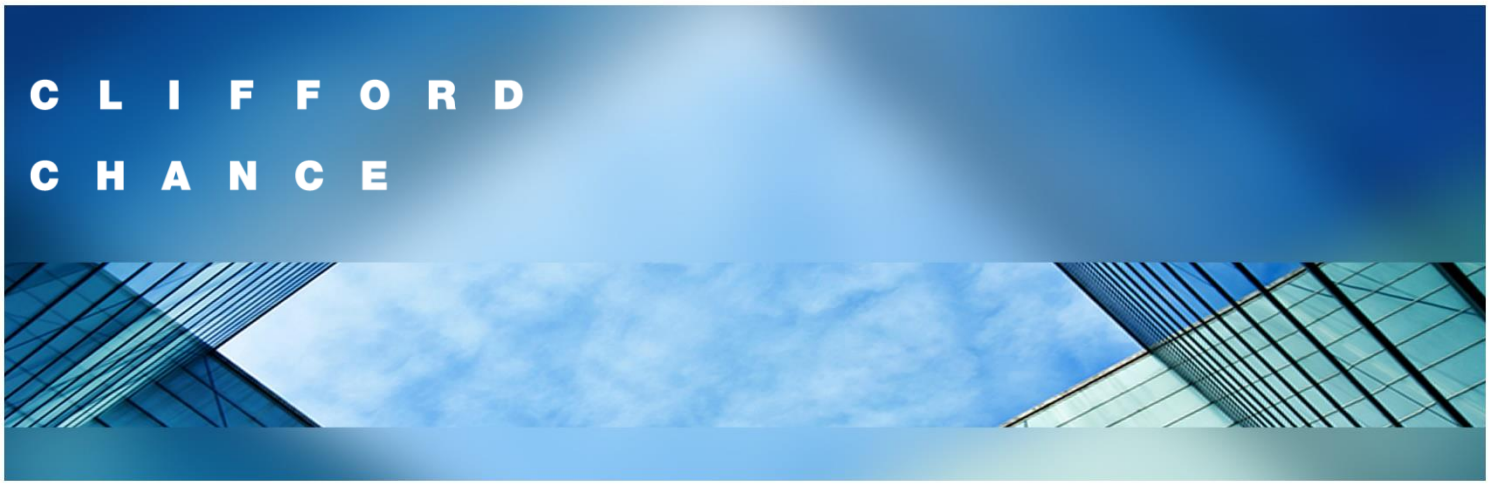

FEDERAL TRADE COMMISSION PROPOSES NEW AMENDMENTS TO SAFEGUARDS AND PRIVACY RULES AMIDST CALLS FOR FEDERAL LEGISLATION AND INTERNAL DISSENT

Last month, the Federal Trade Commission (FTC) issued notices requesting comments on proposed amendments to its Financial Privacy and Safeguards Rules, regulations promulgated under the Gramm-Leach-Bliley Act ("GLBA") that aim to protect the privacy and security of customer information held by financial institutions. While the proposed revisions to the Financial Privacy Rule[1] are relatively minor,[2] the revisions to the Safeguards Rule will have significant impacts on covered financial institutions if they are adopted. The proposed amendments draw heavily from the cybersecurity regulations issued by the New York Department of Financial Services ("NYDFS Cybersecurity Regulations") and the insurance data security model law issued by the National Association of Insurance Commissioners ("NAIC Model Law") and enumerate specific requirements for security measures covered financial institutions are required to take, such as having a data incident response plan. The notices also seek comment on whether to adopt certain additional requirements such as requiring entities that suffer a data security incident to report it to the FTC. The proposed amendments are the latest in a string of developments

1 13 CFR Part 313.

2 The proposed revisions to the FTC's Financial Privacy Rule are aimed at aligning the text of the Rule to the fact that since the passage of the Dodd-Frank Act, the Rule only applies to some motor vehicle dealers. The revisions remove examples and references to other entities that are extraneous and may cause confusion. The proposed amendment also incorporates a provision of the Fixing America's Surface Transportation Act (FAST Act) that exempts certain entities from the GLBA's annual notice requirements.

aimed at strengthening the patchwork of data privacy and cybersecurity laws that protects data in the US.

The Safeguards Rule: Background

The Safeguards Rule[3] requires certain financial institutions[4] to have measures in place to keep nonpublic personal information (NPPI) secure. The current version of the Rule does not prescribe specific measures entities must take, instead opting to provide general requirements and guidance so that entities can have the flexibility to design their information security programs in a way that is most suited to their particular business needs. The Rule requires that the programs be written and readily accessible, and that the safeguards adopted be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of the NPPI involved.

The Rule was promulgated by the FTC in 2002 under the authority granted by the GLBA, and the Commission sought comment on the rule in 2016 as part of its periodic review of its rules and guides. In the notice describing the proposed revisions, the FTC summarizes and responds to the comments submitted during the 2016 review.

Proposed Revision #1: More Specific Requirements

The most notable proposed amendment to the rules is the addition of more specific security requirements for those entities covered by the Safeguards Rule. The FTC explained that including these requirements would provide covered entities with more “guidance and certainty” as to what was required by the Rules. This proposal goes against most of the comments the FTC received in 2016 regarding the Safeguards Rule. Commenters who opposed such a revision worried that this would not only take away the existing flexibility of the rules, but it may also cause companies to be complacent if the standards were set too low and were not updated frequently enough to match a rapidly evolving cybersecurity landscape. To mitigate these concerns, the FTC explained that the proposed amendments would remain process-focused, identifying risks that must be addressed, as opposed to requiring specific solutions to those risks. As for concerns raised by the commenters about the burden of overhauling existing programs to accommodate these requirements (and the significant costs associated with such an overhaul), the FTC also explained that the amendments would “build on existing requirements” and thus require less additional work than commenters may have originally feared.

Drawing primarily from the NYDFS Cybersecurity Regulations[5] and the NAIC Model Law,[6] the FTC’s proposed amendments would require financial institutions covered by the rule to have:

---

3 16 CFR Part 314.

4 "Financial institution" includes any business that is "significantly engaged" in providing financial products or services. The FTC's broad interpretation of this definition includes check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, courier services, credit reporting agencies, and ATM operators.

5 For more information about the NYDFS Cybersecurity Regulations see our earlier piece discussing the rule.

6 For more information about the NAIC Model Law, see our piece here.

- A single specific employee responsible for data security[7] *(i.e.*, a Chief Information Security Officer, or "CISO");
- Written risk assessments that inform the entity's information security program, including periodic reassessments;[8]
- Specific safeguards to address risks identified in an initial risk assessment, including:
    - Access controls, including on physical locations and devices that store customer data;
    - Data and IT infrastructure mapping;
    - Encryption;
    - Security policies for in-house application development;
    - Multi-factor authentication;
    - Audit trails and logs to detect and respond to security events;
    - Data retention and disposal policies;
    - Change management procedures for changes to an entity's IT infrastructure; and
    - Monitoring of activity related to customer data;
- Continuous monitoring or annual penetration testing and biannual vulnerability assessments;[9]
- Training and education of all employees on cybersecurity and data privacy, and specific training for information security personnel, who must be qualified to manage the company's information security risks;[10]
- Oversight of service providers who handle customer data, including periodic assessments based on the risk they pose to the data;[11] and
- A yearly written report by the entity's CISO regarding the overall status of the company's IT security program, compliance with the Safeguards Rule, and specific material matters relating to information security risks.[12]

Given the significant additions in requirements related to data security and privacy, the proposed amendments would provide certain exemptions for covered entities that maintain small amounts of customer data. Covered entities that maintain customer information of fewer than five thousand customers would be exempt from having to have (1) written risk assessments; (2) continuous monitoring or annual penetration testing and biannual vulnerability assessments; and (3) yearly written security reports.

---

7 The current Rule allows the responsibility to be shared by more than one employee.
8 The current Rule already required risk assessments, but it does not require periodic reassessments.
9 This would be a new requirement.
10 These would be new requirements.
11 The current Rule does not require periodic assessments of service providers.
12 This would be a new requirement.

Proposed Revision #2: Incident Response Plan

The second major proposed revision to the Safeguards Rule is the requirement that covered entities have an incident response plan. This is an unexpected revision, because covered entities are already required to have an incident response plan under many state laws; in fact, as many commenters pointed out, this requirement is arguably already included in the existing rule's requirement for covered entities to have a "reasonable information security program." In the FTC's commentary on this proposed revision, the FTC acknowledged that many entities are already required to have incident response plans. However, it explained that in addition to making the requirement explicit—and thus eliminating any doubt or confusion over whether an institution was required to have an incident response plan—the proposed revision would allow the FTC to require incident response plans to have specific provisions, including:

- Specific goals for the plan;
- Defined internal processes for responding to a security event;
- Clear roles, responsibilities, and levels of decision-making authority;
- Processes for communications and information sharing, both externally and internally;
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- Documentation and reporting regarding security events and related incident response activities;
- Evaluation and revision of the plan following a security event.

The FTC also stated that it was considering (but had not yet proposed) requiring covered entities to report certain cybersecurity incidents to the Commission. The FTC noted that the NYDFS Cybersecurity Regulations required reporting to NYDFS and asked commenters whether the Commission should follow the NYDFS model—and if so, what the reporting threshold should be (*e.g.,* should all cybersecurity events be reported, or only those that involve a certain number of customers); what the appropriate deadline for reporting events (NYDFS requires reporting within 72 hours); and whether such reports should be made public.

The FTC also acknowledged concerns that requiring an incident response plan as part of the Rule may preempt certain state laws requiring the same. The FTC's notice seeks comment on whether this revision may have a detrimental effect on cybersecurity due to state law preemption, and if so, what that effect will be.

Other Proposed Revisions

The FTC notice also describes other proposed revisions the Commission is considering, including whether the Rules should require, incorporate, or reference any other information security standards or frameworks, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standard. The FTC explained that at this time, it was not inclined to reference any of these standards or frameworks, including by creating a "safe harbor" for covered entities that can demonstrate compliance with

any of these frameworks, as some commenters had suggested or hoped for during the 2016 comment period. However, the notice seeks comments on adding such a provision, suggesting that the FTC could be persuaded to adopt such a provision if given the right reasoning to do so.

The FTC is also proposing to include—and modify—the definition of "financial institution"[13] in the Rule. Previously, the definition had cross-referenced the one in the Financial Privacy Rule. This is confusing now, because after the passage of the Dodd-Frank Act, the Financial Privacy Rule no longer applied broadly to financial institutions, meaning that the definition cross-referenced was no longer operative in the Financial Privacy Rule itself. The proposed revision to the Safeguards Rule eliminates the confusion and establishes the definition in the text of the Rule itself. In addition to removing the cross-reference, the FTC also proposes including "incidental" activities in its definition of "financial institution," thus slightly broadening the scope of the rules. Many of the 2016 commenters had opposed such a change, worrying that the Rules would apply too broadly and sweep in entities not meant to be covered by the GLBA such as convenience stores or securities firms. However, the FTC explained that the revised definition was aimed specifically at making clear that the Rules also applied to finders[14] and not any other type of entity or activity. The FTC also explained that this revision would bring the Safeguards Rule in line with other agencies' rules promulgated under the GLBA.

Dissenting Statement & Opposing Comments

In a rare and surprising move, the proposed revisions to the Safeguards Rule were accompanied by a dissenting statement by two of the five commissioners. The statement reiterated the concerns of many commenters that adopting a more prescriptive approach to data security as proposed in the revisions would make the Rules too inflexible and disproportionately affect small companies, who will be less able to absorb the increased compliance costs these revisions would require than their bigger competitors. The dissenting commissioners also worried that these revisions would stifle innovation among companies looking to disrupt their industries, for fear of violating data privacy and security-related rules. The statement noted that if the FTC wanted to provide guidance to companies on how to comply with the Rule, the FTC already had access to effective tools such as public speeches, reports, and published information about factors the FTC considers when pursuing investigations, all of which can set expectations and provide guidance without being too prescriptive or inflexible.

The dissenting statement also criticized the proposed revisions as premature. The dissenting commissioners noted that neither the NYDFS Cybersecurity Regulations nor the NAIC Model Rules had been in force for long enough to properly test the effectiveness of their requirements. The statement also expressed that the dissenting commissioners "strongly support" the FTC's calls for federal data security legislation, which if passed may eliminate the need for these rules.

---

13 See note 4.

14 The FTC's press release announcing the notice explains that a "finder" is an entity that charges a fee to connect consumers who are looking for a loan to a lender. The notice explained that such entities collect and store sensitive consumer information that needed to be protected from unauthorized disclosure.

Implications & Conclusions

While the timing of these proposals may seem odd—it has been almost three years since the FTC sought and received comments on the rule—there is good reason for the FTC to have finally acted.[15] Last year, the 11th Circuit dealt a blow to the FTC's enforcement authority in *LabMD, Inc. v. Federal Trade Commission*. 894 F.3d 1221 (11th Cir. 2018). In that decision, the court found that the FTC's order requiring LabMD to implement a data security program that was "reasonable and appropriate" was too vague to be enforceable. The FTC's order was issued under the Commission's authority under § 5(a) of the FTC Act to protect consumers from "unfair" practices, which the 11th Circuit described as violating "*statute, judicial decisions—i.e., the common law—or the Constitution*." The proposed revisions to the Safeguards Rule would allow the FTC to avoid the concern in *LabMD* for covered financial institutions by providing specific requirements that these institutions would have to implement. Until a federal law is passed, these proposed amendments would ensure that the FTC's enforcement authority in the area of data privacy remains effective—at least as far as financial institutions are concerned.

As for companies not covered by the GLBA, the *LabMD* decision may explain why the FTC is so keen on federal data privacy legislation, especially as the patchwork of state and federal laws and regulations keeps getting more complex. Last June, California passed the strongest state privacy law in the US, the California Consumer Privacy Act of 2018 (CCPA).[16] Since then, a number of states have introduced or passed similar legislation. These laws are more comprehensive than the FTC's proposed revisions (since states are not restricted by the FTC's rulemaking authority) and include provisions such as giving individuals certain rights to their data or creating private rights of action. All of this creates a massive headache for those in charge of corporate compliance, who are probably hoping for a more standardized federal law just as much as the FTC is.

In the meantime, as everyone waits to see if and how Congress will act, financial institutions impacted by the Safeguards Rule should begin considering how to bring their existing programs and policies up-to-date. The comment period is underway and will continue for another month, and any revisions will only go into effect six months after publication of a final rule, so companies do have some time before they must act. However, as recent experience with the EU's General Data Protection Regulation counsels, it is never too early to plan for compliance, particularly with regards to the requirements that may prove particularly onerous to implement, such as the proposed training and staffing requirements.

---

15 This dissenting statement may also help explain why the FTC waited so long to propose these revisions: it probably took some time to put together a set of amendments that had the support of the majority of the FTC commissioners—and even this set only barely got that support with a 3-2 vote.

16 For more on the CCPA, see our earlier briefing.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Alice Kane
Counsel

T +1 212 878 8110
E alice.kane@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin@cliffordchance.com

KEY CYBERSECURITY CONTACTS

Alexander Anichkin
Partner, Moscow

T +7 495 258 5089
E alexander.anichkin@cliffordchance.com

Carlo Felice Giampaolino
Partner, Milan

T +39 064229 1356
E carlofelice.giampaolini@cliffordchance.com

Megan Gordon
Partner, Washington, DC

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Tim Grave
Partner, Sydney

T +61 2 8922 8028
E tim.grave@cliffordchance.com

Luke Grubb
Partner, Singapore

T +65 6506 2780
E luke.grubb@cliffordchance.com

Ling Ho
Partner, Hong Kong

T +852 2826 3479
E ling.ho@cliffordchance.com

Jonathan Kewley
Partner, London

T +44 20 7006 3629
E jonathan.kewley@cliffordchance.com

Celeste Koeleveld
Partner, New York

T +1 212 878 3051
E celeste.koeleveld@cliffordchance.com

Anita Lam
Consultant, Hong Kong

T +852 2825 8952
E anita.lam@cliffordchance.com

Markus Muhs
Partner, Munich

T +49 89 21632 8530
E markus.muhs@cliffordchance.com

Lena Ng
Partner, Singapore

T +65 6410 2215
E lena.ng@cliffordchance.com

Masayuki Okamoto
Partner, Tokyo

T +81 3 6632 6665
E masayuki.okamoto@cliffordchance.com

Daniel Royle
Partner, Abu Dhabi

T +966 11481 9756
E daniel.royle
@cliffordchance.com

Dessislava Savova
Partner, Paris

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com

Daniel Silver
Partner, New York

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Natsuko Sugihara
Partner, Tokyo

T +81 3 6632 6681
E natsuko.sugihara
@cliffordchance.com

Luke Tolaini
Partner, London

T +44 20 7006 4666
E luke.tolaini
@cliffordchance.com

Arun Visweswaran
Senior Associate, Dubai

T +971 4503 2748
E arun.visweswaran
@cliffordchance.com

Donna Wacker
Partner, Hong Kong

T +852 2826 3478
E donna.wacker
@cliffordchance.com