November 6, 2023

Federal Trade Commission Expands Reach of Safeguards Rule to Require More Entities to Report Data Security Breaches

On October 27, 2023, the Federal Trade Commission ("FTC") announced an amendment to the Safeguards Rule (the "Rule"), promulgated under the Gramm-Leach-Bliley Act ("GLBA") of 1999, expanding reporting requirements for non-banking financial institutions.[1] Under the Rule, entities such as mortgage brokers, motor vehicle dealers, and payday lenders are now required to implement comprehensive data security programs and to report cybersecurity breaches to the FTC. These new reporting requirements, which take effect 180 days following publication in the *Federal Register*, impose significant new obligations on businesses, including those not traditionally subject to extensive data privacy regulation.

Overview of Rule Changes

The new rule requires financial institutions to report notification events to the FTC as soon as possible, but no later than 30 days following discovery of an event.[2] An event is considered discovered as of the first day it is known to any person, other than the person committing the breach, who is the employee, officer, or other agent of a financial institution.[3] A notification event is defined as the unauthorized acquisition of unencrypted customer information pertaining to at least 500 customers.[4] Notice to the FTC must include: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information that were involved in the notification event; (3) the date or date range of the notification event, if it is possible to determine this information; (4) the number of consumers affected; (5) a general description of the notification event; and, if applicable, whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the FTC to contact the law enforcement official.[5] Notice must be filed electronically through a form on the FTC's website.[6]

---

1 *See* Federal Trade Comm'n, *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches* (Oct. 27, 2023), available here; *see also* FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314 (2023), available here.

2 Federal Trade Comm'n, *supra* note 1.

3 16 C.F.R. Part 314 at 22.

4 Federal Trade Comm'n, *supra* note 1.

5 16 C.F.R. Part 314 at 4.

6 *Id.* at 5.

In a previous expansion of the Safeguards Rule, announced on October 27, 2021, the FTC required non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain measures to protect customer information.[7] The most recent update to the Rule subjects those same non-banking financial institutions to the new reporting requirements.[8]

The amended Safeguards Rule requires notification where "customer information" is subject to unauthorized acquisition.[9] The Safeguards Rule adopts a broad definition of "customer information," including any "personally identifiable financial information."[10] The Rule further states that "personally identifiable financial information" includes any consumer information:[11]

(i) provided by a consumer to obtain a financial product;

(ii) associated with any transaction involving a financial product or service between a non-bank financial institution and a consumer; or

(iii) otherwise obtained in connection with providing a financial product or service to that consumer.

This expansive definition could include any information about a consumer that is collected in relation to the provision of financial services to them, including transaction history, account balance, and account status.

The Rule does not limit the notification requirement to incidents that the affected institution has concluded pose a risk of harm to consumers.[12] The FTC reasoned that requiring financial institutions "to assess the likelihood of misuse … would [allow] financial institutions to underestimate the likelihood of misuse, and, thereby, the need to report [a] security event."[13]

Impact of Reporting Requirements

The new reporting requirements are novel in their scope, both in terms of the types of entities they regulate and the types of cyber incidents for which they mandate notification. To avoid running afoul of FTC regulations, non-bank financial institutions, including entities like car dealers and mortgage brokers, will need to be ready to notify the agency following any cyber incident involving the unauthorized access of any information that falls under the definition of "customer information." Since the requirement to report is not based on a risk assessment before noticing a breach under the Rule, companies are incentivized to take a broad approach when determining what breach incidents require notification.

New Rule May Require Businesses to Report to Multiple Regulators and Result in Enhanced Scrutiny from State Regulators

The regulatory notification requirements set forth in the amended Safeguards Rule do not supplant state regulations. In the event of a cyber incident triggering notification requirements under both the amended Safeguards Rule and a state's cybersecurity regulation, the affected company would be obligated to provide notifications under both laws.

---

7 *See* Federal Trade Comm'n, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), available here.

8 *See* Federal Trade Comm'n, *supra* note 1.

9 16 C.F.R. Part 314 at 17.

10 *Id.*

11 16 C.F.R. 314.2(n)(1).

12 16 C.F.R. Part 314 at 15.

13 *Id.*

However, given the relatively permissive standard for FTC notification under the Safeguards Rule, there is a strong possibility that entities will be required to notify the FTC of data incidents that they are not currently required to report to state regulators. The FTC has stated its intention to "enter notification event reports into a publicly available database."[14] Companies can thus expect inquiries by state regulators into incidents published on the FTC's database, even if the affected entity has not reported the breach to the state. The increased number of public notices of data incidents could further lead to a higher volume of civil actions against companies affected by data breaches.

Takeaways

Given the relatively expansive notification standard it articulates, the amended Safeguards Rule will likely require non-bank financial institutions to make additional investments in cyber security compliance, and in establishing efficient reporting mechanisms to meet the FTC's relatively short reporting timeframe. Companies should establish mechanisms to facilitate notification of the FTC in a timely manner following any covered security incident. Companies should also make sure they are equipped to make timely determinations as to whether the FTC should be notified, and in particular whether any "customer information" has been implicated in a data incident.

Companies should also be alert to possible future changes in state notification requirements in response to the Safeguards Rule and the potential for state regulators to initiate investigations into incidents reported to the FTC but that are not required to be reported under state laws. Under the Rule, the FTC will publish data incident reports in a publicly available database, heightening regulated entities' exposure to both state regulatory inquiries and civil suits, and potentially incentivizing more liberal interpretations of their obligations under state notification requirements. We will continue to monitor actions taken by FTC in this area and provide further updates as appropriate.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Yahonnes Cleary
+1-212-373-3462
ycleary@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Alexander B. Polsky and Neil Chitrao contributed to this Client Memorandum.

[14] 16 C.F.R. Part 314 at 26.