How Breach Reporting Is Changing For Financial Institutions

By **Evan Yahng and Kurt Hunt** (March 6, 2024)

Evan Yahng

Kurt Hunt

Expanding its ability to detect and pursue security incidents, the Federal Trade Commission finalized an amendment to the Safeguards Rule on Oct. 27, 2023, requiring nonbanking financial institutions to report certain data breaches.[1]

By extending this data privacy protection to customers of all financial institutions, this amendment demands fintech firms across the country revisit their cybersecurity and incident response policies.

Background

Since the passage of the Gramm Leach Bliley Act in 1999, the Federal Deposit Insurance Corporation, Federal Reserve, and the Office of the Comptroller of Currency have required banking institutions to report certain data breaches to regulators.[2]

Meanwhile, the GLBA vests authority to regulate nonbanking financial institutions with the FTC. Such financial institutions are not banks, but significantly engage in activities that are financial in nature or that are incidental to financial activities. This includes, among others:

- Retailers that issue their own credit cards directly to consumers;
- Mortgage brokers and lenders;
- Certain tax preparation firms;
- Payday lenders;
- Check cashers;
- Nonfederally insured credit unions;
- Finders;[3]
- Automobile dealerships that lease vehicles for more than 90 days;
- Personal property or real estate appraisers;
- Wire transferors; and
- Collection agencies.

New Data Incident Reporting Obligations

Until now, the FTC's Safeguards Rule only required these financial institutions to develop, implement and maintain information security programs that contain certain administrative, technical and physical safeguards to protect customer information. The FTC did not impose any data breach notification obligations separate from those that already might exist under state or other laws.

That will change in May, when the recently finalized Safeguards Rule amendment takes effect. The amendment requires financial institutions to report to the FTC any incident in which unencrypted customer information involving 500 or more consumers is acquired without the authorization of the individual associated with the information.

Companies that are subject to the rule and experience an incident must report to the FTC:

- The institution's name and contact information;
- A description of the types of information involved in the incident;
- The date or date range over which the incident took place;
- The number of affected consumers;
- A general description of the incident; and
- Whether a law enforcement official has made a written determination that notifying the public of the incident would either impede an ongoing criminal investigation or cause damage to national security, and, if so, contact information for said law enforcement.

Companies must report the incident as soon as possible, but no later than 30 days after the date the incident is discovered. An incident is discovered on the first day such event is known to any person, other than the person committing the breach, who is the financial institution's employee, officer or other agent. Breaches may be reported through the FTC's website.

While the FTC intended for the amendment to extend the data protections that apply to information held by banks to information held by nonbanking financial institutions, in some critical aspects the amendment sweeps even more broadly:

- "Customer information" protected by the rule is defined broadly, and includes any record of nonpublic personal information — personally identifiable financial information about a consumer obtained in connection with a financial product or service, regardless of who shared that information with the company — that is handled or maintained by the financial institution or its affiliates.
- The FTC will consider customer information unencrypted if an unauthorized person accessed the encryption key.

- The FTC will presume that unauthorized access resulted in unauthorized acquisition unless the financial institution has reliable evidence otherwise.

- There is no "risk of harm" prerequisite to triggering the reporting requirement.

- The FTC intends to publish a publicly available database of notification event reports on its website, with the aim to provide more information to consumers and incentivize companies to better protect consumer information.

The amendment will not require notification of the affected individuals. However, companies should expect many of these obligations to flow down to their service providers, affiliates and third-party vendors. A company's burden might also dramatically expand depending on whether its affiliates or service providers are deemed to be agents whose knowledge of a breach triggers the notification clock.

Conclusion

The FTC has stated that the intent of the amended Safeguards Rule is to incentivize financial institutions to use strong data security measures, and that "[r]eceipt of these notices will enable the Commission to ... facilitate prompt investigative response to major security breaches."[4]

The FTC may not only investigate security breaches, but is also authorized to bring enforcement actions under Section 5 of the FTC Act against companies that fail to properly provide notice of a data incident or otherwise run afoul of the amended rule.

Given the ever-increasing rate of cybersecurity incidents and the costly — and also public — consequences of failing to adhere to the applicable regulations, it is critically important to be proactive.

As the effective date for the new Safeguards Rule approaches, fintech firms and other companies subject to the rule should promptly revisit their security practices and compliance strategies, including updating their security incident response plans to include the new definitions, deadlines and penalties and preparing to disclose new kinds of information to regulators if and when an incident occurs.

After a security incident it's often too late to address many of these issues, and no one wants to be the company the FTC uses as an example to demonstrate the power of their new regulations.

Evan J. Yahng is an associate and Kurt R. Hunt is a partner at Dinsmore & Shohl LLP.

of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] 16 C.F.R. 314 et seq.

[2] See, e.g. 12 CFR 53.3; 12 CFR 225.302; 12 CFR 304.23.

[3] The FTC defines a "finder" as a company that brings together buyers and sellers of a service or product.

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/p145407_safeguards_rule.pdf.