POLSINELLI. What a law firm should be.™

Looking Ahead to the FTC's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions

Beginning on May 13, 2024, nonbanking "financial institutions" must notify the Federal Trade Commission ("FTC") within 30 days of discovering a data breach involving the nonpublic personal information of at least 500 consumers. These covered organizations can include a wide variety of companies that engage in financial activities but that are not directly regulated by federal banking regulators, including automobile dealerships, higher educational institutions participating in federal student financial aid programs, mortgage lenders or brokers, tax preparation firms, travel agencies, and others. These organizations are already required to implement certain information security protections pursuant to the FTC's Safeguards Rule.[i] The FTC's new data breach notification requirement will provide the FTC with a critical tool to ensure that organizations are properly safeguarding consumer data.

Background

All fifty states have enacted some form of a data breach notification law. Certain industries are also subject to data breach notification obligations at the federal level. The Gramm-Leach-Bliley Act ("GLBA") imposes certain privacy and data security obligations on covered "financial institutions."[ii] Under the GLBA, financial institutions are broadly defined to include any institutions engaging in activities that are financial in nature or incidental to such financial activity.[iii] For banking (typically depository) financial institutions, the GLBA provides enforcement authority to the federal banking regulators (the Federal Deposit Insurance Corporation, Federal Reserve, Office of the Comptroller of the Currency, and National Credit Union Administration). For all other types of financial institutions, the GLBA provides enforcement authority to the FTC.[iv]

Under the FTC's existing Safeguards Rule, covered financial institutions must develop, implement and maintain an information security program that includes nine specific elements.[v] On October 27, 2023, the FTC adopted an amendment to the FTC's Safeguards Rule that will increase the number of organizations subject to federal data breach reporting requirements, including many organizations that may not realize they are considered a "financial institution" under the GLBA's broad definition.

Requirements Under the Amended Safeguards Rule

The amended Safeguards Rule requires financial institutions to report any instance of the unauthorized acquisition of unencrypted customer information of at least 500 consumers to the FTC as soon as possible but in no event later than thirty days following discovery of the incident. The rule broadly defines customer information to include any nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form.[vi] This includes any information provided by the customer in order to obtain a financial product, information about a customer resulting from any transaction involving a financial product or service, and any other information obtained about the customer in connection with providing the financial service.

The 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), (4) the number of consumers affected, (5) a general description of the event, and (6) if applicable, whether any law enforcement official has provided the institution with a written determination that notifying the public of a breach would impede a criminal investigation.

Anticipating FTC Investigations and Public Disclosure Under the New Rule

Once an organization notifies the FTC of a data breach under the new rule, it will then face risks associated with the public disclosure of the notice and a potential FTC investigation. The FTC intends to publicly post the data breach notices it receives.[vii] These postings will increase the risk of litigation and media attention arising out of the data incident.

The FTC is also likely to initiate investigations into many of the reported breaches.[viii] Consistent with how the FTC has investigated prior data security incidents and consistent with how other federal regulators investigate reported incidents, reporting organizations should expect the FTC to conduct a three-pronged inquiry following a data breach report. First, the FTC will likely request information about how the organization responded to the incident, including how it conducted its investigation, how it ensured that its systems were secure, and whether and how it notified potentially affected individuals. Second, the FTC is likely to seek information about the organization's underlying information security program and compliance with the FTC's Safeguards Rule. Finally, the FTC may seek information about the organization's overall data privacy compliance program under the FTC's jurisdiction to investigate and prohibit unfair or deceptive acts or practices in commerce.[ix] The FTC's inquiry into these areas can be quite detailed.

Preparing for the New Rule

As a threshold matter, all organizations should determine whether they are subject to the FTC's Safeguards Rule well in advance of any data security incident. The new data breach notification requirement is only one part of the more comprehensive set of data security requirements under the Safeguards Rule. Covered organizations must implement an information security program that contains nine specific elements. This new reporting rule provides the FTC with a new method to identify and investigate financial institutions that may not be compliant with the Safeguards Rule.

Covered organizations should ensure that their data security incident response plans address the new rule by incorporating the definitions and reporting time frames under the FTC rule and other applicable law. As with any external notice regarding a data security incident, notices to the FTC should be timely, factual and accurate. The organization should identify the person or team who will be responsible for leading the organization's incident response and ensuring that regulators are notified in accordance with applicable law.

The organization should distribute the updated incident response plan to all individuals who may be required to execute on the plan in both physical and digital formats. Once the plan is adopted, organizations should ensure that the plan is routinely tested to identify potential gaps and to increase the effectiveness of the response plan under an actual crisis.

---

[i] 16 C.F.R. Part 314.
[ii] 15 U.S.C. §§ 6801-6809.
[iii] 15 U.S.C. § 6801(3).
[iv] 15 U.S.C. § 6805.

[v] 16 C.F.R. § 14.4
[vi] 16 C.F.R. § 314.2.
[vii] 88 Fed. Reg. 77,506 (Nov. 13, 2023).
[viii] 88 Fed. Reg. 77,501 (Nov. 13, 2023).
[ix] 15 U.S.C. 45.