Updates
November 02, 2023
FTC Announces Data Breach Reporting Obligation Under GLBA Safeguards Rule

Under an amendment to the Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA) announced on October 27, 2023, the Federal Trade Commission (FTC) will require a broad range of nonbank financial institutions to notify the FTC of instances of the unauthorized acquisition of unencrypted, personally identifiable, nonpublic financial information of more than 500 customers.

The new notification obligation will be a significant change for financial institutions covered by the FTC's Safeguards Rule, as the universe of reportable incidents is vastly broader than is currently covered by other state or federal requirements, notification must be made quickly, and such reports will generally be made public by the FTC.

Who Must Comply

The new notification obligation applies to nonbank financial institutions that are subject to the FTC's existing Safeguards Rule. *See* 16 C.F.R. § 314.1(b). The new notification obligation thus applies to a broad range of entities such as mortgage brokers, certain fintech companies, nonbank lenders, credit reporting agencies, accountants and tax preparation services, real estate appraisers, auto dealers that engage in certain leasing activities, and credit counselors. *See* 16 C.F.R. § 314.2(h)(1) (listing examples of covered entities).

What Type of Information Triggers Notification?

The notification obligation applies to "customer information," which is nonpublic, personally identifiable financial information that is maintained about a "customer," which is a consumer with whom the institution has a continuing relationship to provide financial products or services for personal, family, or household purposes. Nonpublic, personally identifiable financial information, commonly referred to as "NPI," includes *any* information that a consumer provides to a financial institution to obtain a financial product or service or that the

financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer. *See id*. § 314.2(c)-(e), (l), (n).

Notably, the definition of the type of information covered by the notification obligation is *significantly* broader than under state breach notification laws. It includes all nonpublic information about an institution's customers that is personally identifiable, instead of just the types of information specifically listed in state breach notification laws. It could include, for example, contact information, cookie and browsing information tied to customers, and the mere fact that an individual has obtained a product or service from the institution. *See id.* § 314.2(n).

What Type of Event Triggers Notification?

Notice is required for a "notification event" affecting the customer information (see above) of at least 500 consumers. A "notification event" is any "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains." In the event of unauthorized *access* to customer information, the onus is on the affected company to demonstrate that unencrypted customer information was not or could not reasonably have been *acquired*. Otherwise, the incident is presumed to involve unencrypted customer information. *See id.* §§ 314.2(m) (to be codified), 314.4(j) (to be codified).

Notably, the definition of "notification event" covers not only data breaches and security incidents as traditionally understood, but also voluntary and/or intentional sharing of customer information by a financial institution if done without the customer's authorization. The FTC similarly took this type of unconventional approach to "breach" reporting in its proposed amendments to the Health Breach Notification Rule (HBNR). It attempted to explain this expansive approach as an effort to "make clear to the marketplace that a breach includes an unauthorized acquisition . . . that occurs as a result of a data breach or an unauthorized disclosure, such as a voluntary disclosure . . . not authorized by the consumer." However, in the GLBA context, this type of disclosure has traditionally been considered a privacy rather than a security issue, and it has been addressed by the FTC's GLBA *Privacy* Rule, 16 C.F.R. § 313, which establishes requirements for when covered financial institutions can disclose NPI and the type of notice and consent they must obtain to do so, with established remedies for any failures to comply.

Left unsaid in the announcement of the amended Safeguards Rule is the relationship between the new notification obligation for "unauthorized" sharings and the Privacy Rule's long-standing provisions. In addition, the FTC does not explain what standard governs whether customers authorized a sharing, who decides if it was unauthorized, and whether a notification obligation is triggered if such determination is made long after the event concludes (e.g., as a result of a separate legal proceeding).

There Is No Harm Threshold

The proposed rule would have required notice only for incidents that were reasonably likely to result in misuse of the information, a standard somewhat akin to that of many other breach notification laws. However, this was removed from the final rule, and thus all incidents, even those with no risk of harm, must be disclosed. The FTC believes that it will "lower the burden" to assess incidents without such a threshold. The comments suggest the FTC believes that the number of incidents currently reported to state agencies is a reasonable guideline as to how many reports will be required under this rule, but with much broader data in scope and no harm threshold, that assumption is likely misguided.

Required Contents of the Notification

Notice to the FTC must include: (1) the name and contact information of the reporting company; (2) a description of the information involved in the event; (3) the date range of the event if it can be determined; (4) the number of affected consumers; (5) a general description of the event; and (6) whether a law enforcement official has informed the company in writing that notifying the public would "impede a criminal investigation or cause damage to national security," along with contact information for any such law enforcement official. Notification must be conducted via an online reporting form to be made available on FTC.gov. *See* 16 C.F.R. § 314.4(j)(1)-(2) (to be codified).

Timeline for Notification

Notification events must be reported to the FTC as soon as possible and no later than 30 days after they are discovered. Discovery occurs on "the first day on which such event [i.e., the notification event] is known" to the affected company or any of its employees, officers, or agents. While this timeline is not as short as some timelines in, for example, international regulations, most notification regimes with short notification timelines do not make such notifications public (see below). *Id.*

Notice to the FTC Will Be Public

The FTC considered but declined to impose a requirement for companies to individually notify affected consumers. But, the FTC plans to publish notification event reports in a publicly available database, with a limited exception if law enforcement indicates that notice to the public would impede a criminal investigation or harm national security. *Id.* Because of the broader scope of required notifications than under state breach notification laws, publication by the FTC means that the public could learn of an incident from the FTC-published report, even for incidents for which no one will receive individual notice under state law and for which, because of the lack of risk, there are no actions that individuals can or should take to protect themselves.

Takeaways

The Commission voted 3-0 in favor of the amended Safeguards Rule. The amendment becomes effective 180 days after publication of the amended rule in the *Federal Register*. Coupled with the new data security obligations under the Safeguards Rule that the FTC announced in December 2021 (see our prior Update) and which are in effect as of June 2023, the new notice obligations result in a significant expansion of the requirements that apply to financial institutions subject to the FTC's Safeguards Rule.

Covered financial institutions should take steps to evaluate and prepare for the notification obligation under the amended Safeguards Rule, including consideration of whether incident response plans should be updated.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Financial Transactions

Related insights

Update

Trump’s FDA and USDA: Five Key Issues To Watch in 2025

Update

The Dismantle DEI Act: One Potential Blueprint for Forthcoming Attacks on DEI