ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

NOVEMBER 13, 2023

FTC Approves New Data Breach Notification Requirement for Nonbanking Financial Institutions

by *Lance Taubin*, *Kim Peretti*, *Kate Hanniford*, *Kathleen Benway*, and *Amy Mushahwar*

On October 27, 2023, the Federal Trade Commission (FTC) approved an amendment to the Safeguards Rule requiring that nonbanking financial institutions notify the FTC of a defined "notification event" when customer information of 500 or more individuals was subject to unauthorized acquisition. The amendment becomes effective 180 days after publication in the *Federal Register*. Importantly, the amendment requires notification only to the FTC – which will post the information publicly – and not to potentially impacted individuals.

Financial institutions subject to the Safeguards Rule are those not otherwise subject to enforcement by another financial regulator under Section 505 of the Gramm–Leach–Bliley Act (GLBA). The Safeguards Rule within the FTC's jurisdiction includes mortgage brokers, payday lenders, auto dealers, nonbank lenders, credit counselors, and other financial advisors and collection agencies. The FTC made clear that one primary reason for adopting these new breach notification requirements is so the FTC could monitor emerging data security threats affecting nonbanking financial institutions and facilitate prompt investigations following major security breaches – yet another clear indication the FTC intends to continue focusing on cybersecurity and breach notification procedures.

Key aspects of the amendment include that:

- The FTC approved its first explicit data breach notification requirement for nonbanking financial institutions.
- Notification is triggered when customer information of 500 or more individuals was subject to unauthorized acquisition. "Customer information" is more broadly defined than "sensitive customer information" (under the GLBA's Interagency Guidelines Establishing Information Security Standards) and "personal information" (under the state data breach notification laws).
- Nonbanking financial institutions will need to conduct a separate analysis of their FTC notification requirements from their state data breach notification analysis.

Notification to the FTC

Under the amendment, notification to the FTC is required upon a notification event, which is defined as the acquisition of unencrypted customer information without authorization that involves at least 500 consumers. If the customer information was encrypted, notification is not triggered so long as the encryption key was not accessed by the unauthorized third party. As a new twist, the amendment specifies that unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless the financial institution has evidence that the unauthorized party only accessed but did not acquire the information.

The presumption of unauthorized acquisition based on unauthorized access is, in part, intended to eliminate the financial institutions' difficult assessment of whether access to the customer information led to acquisition. For example, the financial institution may have evidence of unauthorized access to a certain file containing customer information, but not be able to determine whether the unauthorized third party acquired (via downloading, printing, or even screenshotting) the customer information due to technical limitations. The presumption of unauthorized acquisition based on unauthorized access is consistent with the FTC's Health Breach Notification Rule and HIPAA's Breach Notification Rule, but not state data breach notification laws or the GLBA's Interagency Guidelines.

The FTC considered removing the threshold of "500 or more consumers" within the definition of a notification event (meaning notification would have been required if only one consumer's information was subject to unauthorized acquisition). The FTC also considered a higher threshold of 1,000 or more consumers but ultimately seemed to strike a middle ground of 500 or more consumers in what seems to have been another effort to align with the FTC's Health Breach Notification Rule and HIPAA Breach Notification Rule.

Individual notification requirements for nonbanking financial institutions will continue to be governed by state data breach notification statutes and are not otherwise included in the amendment. The inclusion of a federal regulatory notification requirement and not an individual notification requirement in the amendment is similar to the Computer-Security Incident Notification, which requires banking organizations to notify their primary federal regulator (OCC, Federal Reserve, and FDIC), but not individuals. On the other hand, this is a departure from the Interagency Guidelines that apply to banking financial institutions and the SEC's proposed rules that would require individual and regulatory reporting by registered investment advisers and broker-dealers.

Expansive Definition of Triggering Customer Information

Again departing from preexisting notification triggers of sensitive customer information in the Interagency Guidelines or personal information under state data breach reporting laws, the FTC's rule requires notification to the FTC if customer information is subject to unauthorized acquisition. "Customer information" is defined as "non-public personal information," which is further defined to be "personally identifiable financial information"; both of these definitions remain unchanged from the existing Safeguards Rule.

Under the FTC's rule, "personally identifiable financial information" is broadly defined to be (1) information provided by a consumer to obtain a service or product from the reporting entity; (2) information obtained about a consumer resulting from any transaction involving a financial product or service from the nonbanking financial institution; or (3) information the nonbanking financial institution obtains about a consumer when providing a financial product or service to the consumer.

Unlike the Interagency Guidelines, which define "sensitive customer information" as a specific subset of data elements ("customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account"), the FTC's definition of personally identifiable financial information is much broader. For example, personally identifiable financial information could include information a consumer provides on a loan or credit card application, account balance information, overdraft history, the fact that an individual has been one of your customers, and any information collected through a cookie.

The FTC received several comments arguing that notification should only be triggered for a narrower subset of information that is more "sensitive" in nature. The FTC disagreed, stating that customer information is already a subset of the information nonbanking financial institutions obtain from customers and the unauthorized acquisition of customer information is serious, warranting the need for notification to the FTC. This broad definition may trigger notification obligations for a wider variety of data events, compared to data breach notifications for banking financial institutions under the Interagency Guidelines or state data breach notification laws. Nonbanking financial institutions should consider reviewing and revising their incident response procedures so that they can be prepared to conduct a separate analysis of FTC notification requirements under the amendment, as distinct from state-law notification requirements.

No Risk of Harm Provision

Although the FTC considered whether to include a "risk of harm" standard for notifying the FTC, it ultimately decided against including one to avoid any ambiguity or the potential for nonbanking financial institutions to underestimate the likelihood of misuse. However, numerous state data breach reporting statutes contain risk-of-harm provisions that excuse notice to individuals and state regulators if the unauthorized acquisition and access of personal information is unlikely to cause substantial harm (such as fraud or identify theft) to the individual. This divergence between FTC notifications and state law has set the stage for the possibility that a reporting nonbanking financial institution could be required to report to the FTC, but not to potentially affected individuals and state attorneys general pursuant to state law.

Timing and Content for Notice to FTC

Nonbanking financial institutions must notify the FTC as soon as possible, and no later than 30 days after discovery of the notification event. Discovery of the event is deemed to be the "first day on which such event is known … to any person, other than the person committing the breach, who is [the reporting entity's] employee, officer, or other agent." The FTC's timeline is similar to the timeline dictated for notifying state attorneys general under most state data breach notification laws (either explicitly or implicitly), but a key difference from the Interagency Guidelines, which require notification to the bank's primary federal regulator "as soon as possible."

The notification must be submitted electronically on a form on the FTC's website and include the following information, which will be available to the public: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information involved in the notification event; (3) the date or date range of the notification event (if available); (4) the number of consumers affected or potentially affected; (5) a general description of the notification event; and (6) whether a law enforcement official (including the official's contact information) has provided a written determination that notifying the

public of the breach would impede a criminal investigation or cause damage to national security. Making this type of information about a data security incident available to the public is not part of any current U.S. regulatory notification structure.

Law Enforcement Delays Public Disclosure by FTC, Not FTC Reporting

A law enforcement delay may preclude public posting of the notification event by the FTC for up to 30 days but does not excuse timely notification to the FTC. A law enforcement official may seek another 60 days' extension, which the FTC may grant if it determines that public disclosure of the notification event "continues to impede a criminal investigation or cause damage to national security." Many commentators argued that financial institutions should be permitted to delay (or withhold) notification to the FTC at the request of law enforcement or if notification would interfere with a law enforcement investigation, consistent with many state data breach notification laws.

The FTC ultimately concluded that notification to the FTC should not be delayed or withheld, but in an effort avoid any interference with a law enforcement investigation, the FTC would delay making the notification available to the public. This approach, the FTC believes, is consistent with the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule (summarized here), which permits a delay in disclosing material cybersecurity incidents (in a Form 8-K) if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety.

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**.

ALSTON & BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: Vantage South End ■ 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: City Center Fort Worth ■ Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7DE ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333