SULLIVAN & CROMWELL LLP

S&C memo

November 1, 2023

Federal Trade Commission Requires Non-Bank Financial Institutions to Report Certain Data Breaches

Amendment to the Safeguards Rule Will Require Reporting of Breaches of Unencrypted Customer Information Affecting at Least 500 Consumers

SUMMARY

On October 27, 2023, the Federal Trade Commission ("FTC") voted to approve supplemental amendments to the Safeguards Rule (the "Final Rule") that will require non-bank financial institutions to notify the FTC electronically as soon as possible, and no later than 30 days after discovery, of any unauthorized acquisition of unencrypted customer information that affects at least 500 consumers.[1] The breach notification must include certain information about the event, including a description of the event and the number of consumers affected or potentially affected. Notably, the FTC has stated that it intends to make the notifications publicly available through an online database.[2] The Final Rule will become effective 180 days after publication in the Federal Register.

BACKGROUND

The Gramm-Leach-Bliley Act (the "GLBA") provides a framework for the regulation of financial institutions' privacy and information security practices. The FTC enforces the GLBA with respect to non-bank financial institutions such as mortgage brokers, money transmitters, payday lenders, automotive dealerships, retailers that directly issue consumer credit cards, and tax preparers.[3]

The FTC promulgated the Safeguards Rule in 2002 under Subtitle A of Title V of the GLBA, which directs the FTC and other federal financial regulators to establish standards relating to administrative, technical and physical safeguards for certain information.[4] The Safeguards Rule requires non-bank financial

institutions to develop, implement and maintain a comprehensive security program to keep their customers' information safe.[5]

As described in our earlier memorandum to clients, in December 2021, the FTC updated the Safeguards Rule in significant ways, including by adding more detailed requirements for the development and establishment of a non-bank financial institution's information security program, and by expanding the definition of "financial institution." At that time, the FTC also requested comment on proposed supplemental amendments that it has now adopted, with only minor changes, in the Final Rule.[6]

FINAL RULE

Notification Event and Timing

The Final Rule requires non-bank financial institutions to notify the FTC electronically within 30 days of discovery of a "notification event" that involves the information of at least 500 consumers.[7] With respect to the definition of "notification event":

- a "notification event" is defined in the Final Rule as the "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains."[8];
- "customer information" is defined in the Safeguards Rule as "non-public personal information" about a customer, which includes "personally identifiable financial information," that is not publicly available[9];
- "acquisition" of customer information, pursuant to the FTC's adopting release, "will be presumed to include unauthorized access" to such information unless the financial institution "ha[s] reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information"[10] ; and
- customer information will be considered unencrypted, pursuant to the FTC's adopting release, if the encryption key was accessed by an unauthorized person.[11]

The Final Rule will apply to all non-bank financial institutions, regardless of their size.[12]

With respect to when the 30-day timeframe for notification begins, the adopting release provides that a notification event will be considered to have been discovered "as of the first day on which such event is known" to the financial institution, which will be deemed to have knowledge if such event is known "to any person, other than the person committing the breach, who is an employee, officer or other agent of the financial institution."[13] In the adopting release, the FTC notes that while certain commentators argued that the 30-day period "should not begin until [the financial institution] has determined that security event meets notification requirements,"[14] the FTC believes that a deadline of 30 days from the date of discovery "properly balances the need for prompt notification with the need to allow financial institutions to investigate a security event, determine whether the information was acquired without authorization and how many consumers were affected, and learn enough about the event to make the notification to the Commission meaningful."[15]

Notification Contents

The Final Rule requires that the notice include:

- the name and contact information of the reporting financial institution;
- a description of the types of information that were involved in the notification event;
- if the information is possible to determine, the date or date range of the notification event;
- the number of consumers affected or potentially affected by the notification event;
- 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.

Publication of Notices

In the adopting release, the FTC notes that it "intends to enter notification event reports into a publicly available database."[16] The FTC does not specify precisely when the reports will be made publicly available relative to when they are submitted, but the Final Rule provides that publication of the reports may be delayed only as follows:

- for up to 30 days following the date when the notice was provided to the FTC if requested by a law enforcement official;
- for an additional 60 days if the law enforcement official seeks such an extension in writing; and
- for an additional period of time if the FTC staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

The Final Rule does not require notification directly to affected consumers given that, as noted in the adopting release, such a requirement would be "largely duplicative" of existing state laws.[17]

IMPLICATIONS

The Final Rule adds to a range of overlapping data breach notification laws that have complicated the challenge for companies responding to significant cybersecurity and data privacy incidents. For example, all 50 states require reporting of data breaches to affected consumers, and many separately require reporting to state Attorneys General, but in circumstances that vary among the states in terms of the nature of compromised data that triggers notification, the content of the required notice, and the timing in which notice must be provided. Notably, the Final Rule's definition of "customer information," a breach of which may require notification, is broader than many states' definition of the types of personal data that give rise to a notification obligation. As a result, in addition to the analyses they may need to conduct under relevant state laws to determine whether notice to consumers or Attorneys General is required, companies that have experienced a breach involving personal information will need to engage in a separate analysis to determine whether notification is required under the Final Rule.

In addition to these overlapping state law requirements for consumer notification, non-bank financial institutions may be subject to additional notification requirements. For example, when providing services to banks or other regulated financial institutions, non-bank financial institutions may be subject to certain data breach notification requirements imposed on bank service providers by banking regulators that incorporate different standards as to when notification is required. Furthermore, public companies will be subject to the Securities and Exchange Commission's new cybersecurity disclosure rules, which include a requirement to disclose material cybersecurity events. The need for companies to conduct analyses of compromised data sets under multiple different legal and regulatory standards, and to do so within a prescriptive timeframe such as that imposed by the Final Rule, will add to the complexity and burden of responding to relevant incidents.

The FTC's decision to make the notifications available in a public database may further complicate the challenge for companies responding to data breaches given that these notifications may become available before notice to affected consumers is required or would be expected to be provided under relevant state laws. Even where a company is able to determine an approximate number of individuals affected in a particular compromise such that it can provide timely notification to the FTC under the Final Rule, it can take significantly more time in certain circumstances for the company to determine and prepare the required content of a notification to affected individuals. For example, the company may need to do significant additional work, depending on the circumstances, to determine which individuals were affected, what types of data of each individual were affected, and where affected individuals reside such that notice to affected individuals made be provided pursuant to state law. The discrepancy between when information is made public through the FTC database and when the company is in a position to notify affected consumers individually may create challenges for a company in responding to customers' requests about the incident and whether the incident affected them. These challenges could expose the company to reputational or other harms, and divert internal resources and attention at a time when the company is already strained in responding to a cybersecurity incident.

The Final Rule's 30-day deadline may also be challenging to comply with in some circumstances. The question of whether a notification event has occurred, or whether 500 or more consumers have been affected by such an event, may not be easy to determine depending on the facts, and the facts and the company's understanding of the nature and impact of a security breach may quickly evolve. The Final Rule places additional pressure on these determinations given that the FTC has made clear that the 30-day timeframe begins running when any employee at the company has relevant knowledge. Accordingly, non-bank financial institutions covered by the Final Rule should confirm they have clear procedures that apply to all employees so that any potential notification events can be raised to appropriate personnel.

* * *

ENDNOTES

1 *See* Fed. Trade Comm'n, *Final Rule: Standards for Safeguarding Customer Information*, RIN 3084-AB35 (Oct. 27, 2023) ("Adopting Release") *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/p145407_safeguards_rule.pdf.

2 *Id.* at 26.

3 16 C.F.R. § 313.3(k) (2021).

4 15 U.S.C. 6801(b).

5 16 C.F.R. § 314 (2021).

6 Standards for Safeguarding Customer Information, Supplemental Notice of Proposed Rulemaking and Request for Public Comment, Federal Trade Commission, 86 Fed. Reg. 70,062, 70,067 (Dec. 9, 2021).

7 Adopting Release at 20.

8 The proposal would have required financial institutions that become aware of a security event to promptly determine the likelihood that customer information has been or will be misused. Reporting would have been triggered upon a financial institution determining that, among other conditions, "misuse of customer information ha[d] occurred or . . . [was] reasonably likely [to occur]." The FTC agreed with certain commenters that the proposed approach required clarification, including because "the ambiguity [in the proposal] could have been used as an opportunity to circumvent the reporting requirement." *Id.* at 12.

9 *Id.* at 17.

10 The FTC agreed with certain commenters that notification need not be required "when harm to consumers is rendered extremely unlikely because the customer information is encrypted." *Id.* at 16.

11 *Id.* at 12.

12 *Id.* at 20.

13 *Id.* at 22.

14 *Id.* at 20.

15 *Id.* at 20-21.

16 *Id.* at 26.

17 *Id.* at 27.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.