Published on *The National Law Review* https://natlawreview.com

New FTC Rule Requires Certain Financial Institutions to Report Loss of Unencrypted Customer Data

Article By:

Christina Grigorian

Trisha Sircar

Eric R. Hail

Ted Huffman

On October 27, the Federal Trade Commission (FTC or Commission) published a final rule expanding data breach notification requirements for certain financial institutions (Final Rule).[1] *Federal Register*, will require entities within its scope to report the following to the FTC no later than 30 days[2] after unencrypted customer information involving more than 500 consumers is acquired without authorization:

(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) if the information is possible to determine, the date or date range of the notification event;

(4) the number of consumers affected;

(5) a general description of the notification event; and,

(6) 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.

Importantly, the FTC adopted a reporting requirement that is triggered based on acquisition, not misuse. However, the acquisition of encrypted information does not trigger a reporting requirement if the lost customer information is encrypted, so long as the encryption key was not also accessed or compromised by an unauthorized person.

Why it Matters

In its adopting commentary, the FTC states that the rule was necessary because it would allow the Commission to "monitor for emerging data security threats affecting financial institutions and to facilitate prompt investigative response to major security breaches." This is meritorious. To the extent the FTC can use such notifications to track perpetrators or provide warnings or advice to other financial institutions, it will benefit providers of consumer financial products and services and, by extension, their customers. However, the FTC's decision to *make public* these filings through access to a publicly available database presents an important aspect of the rule that compels the encryption of nonpublic personal information throughout its life cycle, including when such data is at rest. Not only does enterprise-wide use of encryption technology protect a financial

institution's data generally, the broadest possible adoption of such technological safeguards will assist in minimizing the potential that reporting obligations under the Final Rule are triggered given that encrypted data losses are only "reportable" if the corresponding encryption key is also lost or compromised.

1 Note that the FTC does not have enforcement authority over banks or credit unions. However, it does have authority over other non-bank providers of consumer financial products and services, such as non-bank lenders and debt collectors.

2 Under the Final Rule, a notification event shall be treated as discovered as of the first day on which such event is known. Covered financial institutions must report such events "as soon as possible," but no later than 30 days after discovery of the event.

National Law Review, Volume XIII, Number 305