



FTC APPROVES AMENDMENT TO SAFEGUARDS RULE

The Federal Trade Commission (“FTC”) has announced new amendments to the Safeguards Rule to go into effect 180 days after publication in the Federal Register. Over the last few years we have reported on amendments to the Safeguards Rule. See, e.g. our Alerts dated [Nov. 17, 2021](#) and [Oct. 5, 2022](#). Notably in 2021 the FTC amended the Safeguards Rule to, among other things, expand the definition of “financial institution” to include entities engaged in activities the Federal Reserve Board determines to be incidental to financial activities, which adds “finders”—companies that bring together buyers and sellers of a product or service—within the scope of the Rule. The 2021 amendments also added provisions to provide more guidance on how to develop and implement aspects of an information security program, such as access controls, authentication and encryption. Most of the 2021 amendments went into effect in December 2022.

In the last several years, the FTC has issued Notices of Proposed Rulemaking, held workshops and conducted panels with information security experts to solicit comments regarding cybersecurity programs and proposed amendments. The FTC has noted that several federal agencies and the New York Department of Financial Services’ Cybersecurity Regulations (one of the model regulations for the recent amendments to the Safeguards Rule) require covered entities to report any security event to the regulator directly.

After additional review of comments regarding the proposed reporting requirements, the FTC has announced its Final Rule. The new amendments to the Safeguards Rule will require a financial institution to submit a notice to the FTC of any unauthorized acquisition of *unencrypted* customer data, referred to as a “notification event,” that involves 500 or more customers. The FTC will require a financial institution to submit the following information in the electronic form located on the FTC’s website within 30 days of discovery of the notification event:

- (1) The name and contact information of the reporting financial institution;
- (2) A description of the type(s) of non-public personal information involved in the notification event;

- (3) The date or date range of the notification event, if available;
- (4) The number of consumers affected;
- (5) A general description of the notification event; and
- (6) Information regarding any law enforcement involvement in the notification event (specifically, whether a law enforcement official has determined public disclosure of the breach would interfere with a criminal investigation or cause a threat to national security).

The FTC stated in the final notice that the required notification will streamline and strengthen its ability to monitor security breaches. The FTC noted that state security breach notification statutes vary greatly and not all states require publication of security breaches, making it difficult for the FTC to monitor trends in security breaches. According to the FTC, by requiring reporting directly to the FTC, investigations can be conducted more quickly and efficiently. The FTC indicated it intends to enter reported notification events into a publicly available database.

Financial institutions should periodically review cybersecurity programs for compliance with the Safeguards Rule and other state privacy and security laws. If you have any questions regarding compliance with the Safeguards Rule or other privacy and security laws, please do not hesitate to contact us.

✧ *Elizabeth Anstaett and Kimberly Tomkies*

Darrell L. Dreher
ddreher@dtlaw.com

Elizabeth L. Anstaett
eanstaett@dtlaw.com

Mercedes C. Ramsey
mramsey@dtlaw.com

Susan L. Ostrander
sostrander@dtlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DTLAW.COM

To see previously sent ALERTS, visit our website at www.dtlaw.com

To decline future ALERTS, please contact us at ALERTS@DLTLAW.COM.
This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

Michael C. Tomkies
mtomkies@dtlaw.com

Judith M. Scheiderer
jscheiderer@dtlaw.com

Robin R. De Leo
robin@deher-la.com