Data Security Déjà Vu: FTC Finalizes Notification Event Amendment to Safeguards Rule

December 29th, 2023 | and K. Dailey Wilson

Does anyone else feel like Bill Murray in *Groundhog Day*, where his character keeps experiencing the same day over and over and over again? It seems like the Federal Trade Commission just amended the Safeguards Rule yesterday, and now the agency is at it again. On October 27, 2023, exactly two years after releasing the first set of amendments to the Safeguards Rule, the FTC finalized its amendment requiring entities to notify the agency upon the occurrence of certain types of security events. This article will break down the requirements of the 2023 amendment to help you make the changes necessary to your compliance policies and procedures.

What is a "notification event"?

Financial institutions subject to the Safeguards Rule, including auto dealers who offer financing and finance companies, are required to notify the FTC upon discovery of a "notification event" involving at least 500 consumers. The term "notification event" means the acquisition of unencrypted customer information, or encrypted information along with the encryption key, without the authorization of the individual to which the information pertains. This definition is much broader than most breach definitions under state data breach statutes, requiring notification for the unauthorized access of *any* customer information. Remember, the Safeguards Rule defines the term "customer information" to essentially mean any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates. In layman's terms, "customer information" can include:

- information that a consumer provides to you on an application to obtain a credit transaction;
- payment history;
- account balance information;
- the fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- any information that a consumer provides to you or that you or your agent otherwise obtain(s) in connection with collecting on or servicing a credit account;
- any information in connection with a financing transaction that you collect through an Internet "cookie"; and
- information from a consumer report.

When is notification required?

You are required to notify the FTC “as soon as possible” but no later than 30 days after discovery of the notification event. A notification event is considered “discovered” as of the first day on which you receive knowledge of the event. You are deemed to have knowledge of a notification event if the event is known to any employee, officer, or other agent of your company (other than the person committing the breach).

What notification is required?

The rule requires the FTC to make an electronic form available on its website for you to make the required notification. The notification must include the following:

- your company’s name and contact information;
- a description of the types of information that were involved in the notification event;
- the date or date range of the notification event, if that information is possible to determine;
- the number of consumers affected or potentially affected;
- a general description of the notification event;
- whether any law enforcement official has provided you 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.

The rule allows a law enforcement official to request an initial delay in notifying the public of up to 30 days following the date when the notice was provided to the FTC. This initial delay may be extended for an additional 60 days if the law enforcement official seeks an extension in writing and the FTC has determined that public disclosure of the breach continues to impede a criminal investigation or cause damage to national security.

What do you need to do next?

The requirement to notify the FTC upon the occurrence of a notification event will be effective May 13, 2024. Before the compliance date, you’ll need to review your Safeguards Rule policies and procedures and your information security program and then make any changes necessary to incorporate the requirement to notify the FTC when you experience a notification event. You’ll also want to review and revise the written incident response plan that you put in place following the 2021 amendments to the Safeguards Rule to address these new requirements.