Rule	Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers [Final Rule]	Requirement that FIs Report Notification Events to the FTC [Final Rule]
Agency	OCC, FRB, and FDIC	FTC
Effective Date	Effective date: April 1, 2022; Compliance date: May 1, 2022	May 13, 2024
Applicability	(1) ***Banking organization*** means a national bank, Federal savings association, or Federal branch or agency of a foreign bank; provided, however, that no designated financial market utility shall be considered a banking organization. (2) ***Bank service provider*** means a bank service company or other person that performs covered services; provided, however, that no designated financial market utility shall be considered a bank service provider.	Financial institutions over which the FTC has jurisdiction. These entities include, but are not limited to: mortgage lenders, ‘‘pay day’’ lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the SEC, and entities acting as finders.
Notification Event	***Financial Institutions*** For covered banking organizations, the new notification requirements are triggered in the event a bank experiences a “notification incident” defined as a security event resulting in actual harm to the confidentiality, integrity or availability of the bank’s information system or the information that the system processes, stores or transmits and which has—or is reasonably likely to—disrupt or degrade its: ability to carry out banking operations or deliver banking products or services to a material portion of its customers; business lines which, upon failure, would result in a material loss of revenue or franchise value; or operations which, upon failure or discontinuance, would pose a threat to the financial stability of the nation. ***Bank Service Providers*** For service providers, the new notification requirements are triggered when a service provider experiences an incident resulting in actual harm to the confidentiality, integrity or availability of the service provider’s information system or the information that the system processes, stores or transmits and which has—or is reasonably likely to—disrupt or degrade the services it provides for a period of **4 or more hours**.	Notification event means acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person. Unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information. A notification event shall be treated as discovered as of the first day on which such event is known to you. You shall be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent.

Notification Obligations	***Financial Institutions*** Banking organizations are required to notify the appropriate agency or agency-designated point of contact of the incident (the primary federal regulator), which can be accomplished through email, telephone or similar methods prescribed by the agencies. The bank must provide its notice no later than **36 hours** after a determination has been made that a notification incident has occurred. ***Bank Service Providers*** In the event of a triggering security incident, service providers are required to provide notice of the incident to at least **1 bank-designated point of contact at each affected bank customer**. **In the event no bank-designated point of contact has been supplied to the service provider, notification must be made to the bank's CEO and CIO or 2 individuals** of comparable responsibility and can be accomplished "through any reasonable means." In terms of timing, service providers are only required to supply the requisite notice "as soon as possible" after a determination has been made that a triggering security incident has occurred. The 36-hour time limitation imposed on banks does not, however, extend to service providers.	Upon discovery of a notification event, if the notification event involves the information of at least **500 consumers**, you must notify the Federal Trade Commission as soon as possible, and no later than **30 days** after discovery of the event. The notice shall include the following: (i) The name and contact information of the reporting financial institution; (ii) A description of the types of information that were involved in the notification event; (iii) If the information is possible to determine, the date or date range of the notification event; (iv) The number of consumers affected or potentially affected by the notification event; (v) A general description of the notification event; and (vi) 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 Federal Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.