Rule	Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers [Final Rule]	Proposal for Requirement that FIs Report Security Events to the FTC [Supplemental NPRM]
Agency	OCC, FRB, and FDIC	FTC
Effective Date	Effective date: April 1, 2022; Compliance date: May 1, 2022	6 months after publication of a final rule
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.	FI's over which the FTC has jurisdiction - those 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**.	When FI becomes aware of a security event, must promptly determine the likelihood that customer information has been or will be misused. If FI determines that misuse of customer information has occurred or is reasonably likely and that at least **1,000** consumers have been affected or reasonably may be affected, notification obligations are triggered.
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.	Must notify the FTC as soon as possible, and **no later than 30 days after discovery of the event**. The notice shall be made electronically on a form to be located on the FTC's website. The notice shall include the: (1) The name and contact information of the reporting financial institution; (2) A description of the types of information that were involved in the security event; (3) If the information is possible to determine, the date or date range of the security event; and (4) A general description of the security event.