Due diligence checklist: Computer-Security Incident Notification Rule

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers. OCC, Federal Reserve and FDIC, the United States.

Regime	Computer-Security Incident Notification Rule
Regulator	OCC, Federal Reserve and FDIC
Country	the United States
Regulator's page	https://www.fdic.gov/news/financial-institution-letters/2021/fil21074.html
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/us-incident

What it is

Bank service providers notify the bank as soon as possible of an incident that disrupts service for four hours or more.

Who it applies to

Applies to banks and mutuals and credit unions in the United States.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	Notice to the institution as soon as possible after a computer-security incident likely to disrupt service for four hours or more	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.