

EXPLAINER

Incident notification: 72 hours, 36 hours, and what the board should hear when

The regulator notification rules for credit unions and banks, and how to make sure the board is told in time to do its part.

Current as of October 13, 2026 · 3 minute read

When a serious cyber incident happens, two clocks start. One is the regulator's. The other is the board's: how soon directors hear, and what they are expected to do. The first is set by rule. The second is set by the board, and is often never written down.

	Federally insured credit unions	Banks
Rule	12 CFR 748.1(c)	Computer-Security Incident Notification rule: 12 CFR Part 53 (OCC), 225.300-303 (Fed), 304.21-24 (FDIC)
Deadline	No later than 72 hours after the credit union reasonably believes a reportable cyber incident occurred	As soon as possible and no later than 36 hours after the bank determines a notification incident occurred
What counts	A substantial loss of confidentiality, integrity or availability; a disruption of operations or member services; or a disruption or unauthorized access through a CUSO, cloud provider, other third party or the supply chain	An incident that has materially disrupted, or is reasonably likely to, the ability to serve a material portion of customers, a material business line, or US financial stability
In force since	September 1, 2023	April 1, 2022 (compliance from May 1, 2022)

Details that catch institutions out

- **Third parties.** For a credit union, when the incident is at a CUSO, cloud provider or other third party, the 72 hours can run from when that party tells you. For banks, service providers must tell their bank customers as soon as possible when covered services are disrupted for four hours or more.
- **Testing is not an incident.** Penetration tests and similar work done at the institution's request are excluded from the credit union rule.
- **Members and customers.** Separately, the response program rules (Part 748 Appendix B; the Interagency Guidelines' Supplement A) expect notice to members or customers as soon as possible when sensitive information has been, or is reasonably likely to be, misused.
- **Suspicious activity reports.** An incident may also require a SAR. FinCEN's 2016 advisory says a SAR is required for a cyber-event meant to affect transactions of \$5,000 or more.
- **Public holding companies.** A bank holding company listed with the SEC also has a four business day disclosure rule for material incidents.

What the board should hear, and when

- 1 Immediately: any incident that meets, or may meet, the notification threshold. Agree the threshold in advance, in writing.
- 2 Who starts the clock: a named person who decides when the institution reasonably believes, or determines, that an incident has occurred.
- 3 The board's role in the first 48 hours, as distinct from management's: who is told, who decides on outside help and communication, and when the board meets.
- 4 Afterwards: what happened, what it cost, what changed, and whether the plan worked.

Test it

An escalation path that has only been written down has not been tested. A tabletop exercise that includes directors, with what it found tracked until closed, is the best evidence that the board can do its part on the day.

BoardAlign checks the board's incident plan and its approval date against your charter's clock, and asks directors whether they know it.

Sources

12 CFR 748.1(c), NCUA. <https://www.ecfr.gov/current/title-12/chapter-VII/subchapter-A/part-748>

NCUA final rule, 88 FR 12811 (March 1, 2023). <https://www.govinfo.gov/content/pkg/FR-2023-03-01/html/2023-03682.htm>

12 CFR Part 53 (OCC). <https://www.ecfr.gov/current/title-12/chapter-I/part-53>

12 CFR 225.300 to 225.303 (Federal Reserve). <https://www.ecfr.gov/current/title-12/chapter-II/subchapter-A/part-225/subpart-N>

12 CFR 304.21 to 304.24 (FDIC). <https://www.ecfr.gov/current/title-12/chapter-III/subchapter-B/part-304/subpart-C>

Final rule, 86 FR 66424 (November 23, 2021). <https://www.federalregister.gov/documents/2021/11/23/2021-25510>

FinCEN Advisory FIN-2016-A005. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005>

SEC cybersecurity disclosure fact sheet. <https://www.sec.gov/files/33-11216-fact-sheet.pdf>

General information for directors, not legal advice. Current as of October 13, 2026. Rules change: check the cited source before relying on it.