After a breach report: what a bank regulator is likely to ask for

Since May 2022 a bank must tell its primary federal regulator (OCC, Federal Reserve or FDIC) "as soon as possible and no later than 36 hours" after it determines that a computer-security incident has materially disrupted, or is reasonably likely to disrupt, its operations, a business line or a material part of its customers. A federally insured credit union has 72 hours from the moment it "reasonably believes" a reportable cyber incident has happened. A bank service provider must tell each affected bank when a covered service is down four hours or more. Behind the clock sit the 2001 Interagency Guidelines and the 2005 Response Program guidance, and the examiner's authority runs to "books, records, or documents of any type."

FDIC notifications, the only bank count published.

7 notices

met the 36-hour threshold in the rule's first ten months, to 31 March 2023 (FDIC 2023 Report on Cybersecurity and Resilience). The OCC and the Federal Reserve publish no count.

NCUA incidents, latest year published.

588 incidents

reported by credit unions 1 May 2025 to 30 April 2026 (NCUA 2026 Cybersecurity and Credit Union System Resilience Report). Of the prior year's 1,072, 742 were third-party related.

ITEM & DESCRIPTION	REGULATION
☐ **1. The notification record.** What was sent, to whom and when, against the 36- or 72-hour clock. → Have it ready: the email or call log and the dated determination memo.	12 CFR 53.3, 225.302, 304.23; 748.1(c)
☐ **2. Incident response program.** Written procedures to assess, contain, notify the regulator, file a SAR and tell customers. → Have it ready: the approved plan and the incident timeline showing each step.	2005 Guidance; 748 App. B
☐ **3. Information security program.** The written program the board approved, and the approval. → Have it ready: the current program and the board minutes.	12 CFR 30 App. B; 748 App. A
☐ **4. Risk assessment.** Foreseeable threats, their likelihood and damage, and control adequacy. → Have it ready: the latest assessment and its update after the incident.	12 CFR 30 App. B; 748 App. A
☐ **5. Customer or member notice and the list.** The misuse finding, the notice with the required elements, the list, any law enforcement delay request. → Have it ready: the finding, the letter, the mailing list and dates.	2005 Guidance; 748 App. B
☐ **6. Service provider contracts and oversight.** Due diligence, security and incident-notice clauses, monitoring. → Have it ready: the contract, the provider's four-hour notice and oversight records.	12 CFR 53.4; 12 USC 1867(c)
☐ **7. Access control evidence.** Who could reach the affected systems and how they were authenticated. → Have it ready: access lists, MFA and privileged-account records.	12 CFR 30 App. B, III.C
☐ **8. Logs and the forensic report.** Preserved evidence, the engagement and the findings. → Have it ready: the logs, the report and the chain of custody.	2005 Guidance; 12 CFR 30 App. B
☐ **9. Business continuity plan and tests.** The plan, the last test and how recovery went this time. → Have it ready: the plan, test results and the recovery timeline.	12 CFR 30 App. B
☐ **10. Annual report to the board.** Program status, risk assessment, provider oversight and incidents. → Have it ready: the most recent report and the board's receipt of it.	12 CFR 30 App. B; 748 App. A

IF YOU ONLY DO ONE THING

Document the clock. The bank rule runs 36 hours from when you "determine," the credit union rule 72 hours from when you "reasonably believe," and customer notice is due when misuse "has occurred or is reasonably possible." One dated timeline of when you knew, decided, called the regulator and told customers answers the first question every examiner asks, and the other nine items hang off it.