After a breach report: what the SEC is likely to ask for

Two SEC rules reach a breach. A public company must file Form 8-K Item 1.05 within four business days of deciding an incident is material, a decision made "without unreasonable delay." Investment advisers, broker-dealers, funds and transfer agents must, under Regulation S-P as amended in 2024, run a written incident response program and tell affected customers "as soon as practicable, but not later than 30 days" after learning of unauthorized access; their service providers must report to them within 72 hours. Larger firms have been on the amended rule since December 2025, smaller firms since June 2026. These are the records the rules require, so they are what an examiner asks for.

The SEC's own enforcement count, fiscal 2025.

456 actions

enforcement actions in the year to 30 September 2025, with $17.9 billion in financial remedies ordered (SEC release, 7 April 2026). No cyber-only figure is broken out.

The clocks the rules set.

30 days

to tell affected customers under Regulation S-P, from awareness. Four business days for the Form 8-K after the materiality decision. 72 hours for a service provider to tell you.

ITEM & DESCRIPTION	REGULATION
☐ **1. The materiality decision, dated.** When you learned of the incident, who assessed it, and why it is or is not material. → Have it ready: the memo with discovery date, decision date and participants.	Form 8-K Item 1.05, Instr. 1
☐ **2. The 8-K and the minutes behind it.** The filed report, any amendment, and the board record of the decision. → Have it ready: the EDGAR copy and the minutes or consents.	Item 1.05(a), Instr. 2
☐ **3. Incident response program.** Written procedures to detect, respond to and recover from unauthorized access, and to notify. → Have it ready: the current version, prior versions and approval dates.	17 CFR 248.30(a)(3)
☐ **4. Customer notice and the log of who got it.** The notice, its contents, who received it, when and how, or the written finding that no notice was needed. → Have it ready: the template, recipient list and send dates.	248.30(a)(4)
☐ **5. Service-provider oversight.** Due diligence, monitoring, and contracts that require 72-hour notice to you. → Have it ready: the vendor inventory, contracts and review notes.	248.30(a)(5)
☐ **6. The safeguards policies.** Written administrative, technical and physical safeguards for customer information. → Have it ready: the policy set and evidence it is in use.	248.30(a)(1), (a)(2)
☐ **7. Disposal records.** The written disposal policy and proof it is followed. → Have it ready: destruction logs or vendor certificates.	248.30(b)
☐ **8. The retention set.** All of the above, kept for the years the rules require. → Have it ready: an index of where each record sits.	248.30(c); Rules 17a-4, 17ad-7, 31a-1, 204-2
☐ **9. The annual cyber disclosure.** Last 10-K text on risk processes, board oversight and management expertise, and the facts behind it. → Have it ready: the filed text and the risk assessment it rests on.	Reg S-K Item 106(b), (c)
☐ **10. The forensic report.** The investigator's findings on scope and the data affected. → Have it ready: the final report, its scope letter and dates.	Supports 248.30(a)(3) and Item 1.05(a)

IF YOU ONLY DO ONE THING

Keep one dated log. Both rules run on clocks, and Regulation S-P requires written records of the incident, the response and the notice decision. A log with each date, decision, reason and recipient answers most of what an examiner can ask for.