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

The FTC's Safeguards Rule covers financial firms no bank regulator supervises: tax preparers, mortgage brokers, auto dealers that arrange financing, finance companies, collection agencies and some investment advisers. Since May 2024, an unauthorized acquisition of unencrypted customer information involving 500 or more consumers must be reported to the FTC on its online form no later than 30 days after discovery. The FTC says a report "may be made public," and its staff can compel documents. Not every report draws a request. If yours does, these are the documents the rule requires. Firms holding information on fewer than 5,000 consumers are exempt from items 2, 7 and 10.

The FTC's own count of GLBA cases.

About 35 since 2005

cases under the GLB Act and both its rules together (FTC Privacy and Data Security Update, March 2024).

Data security cases of every kind.

90+ since 2000

data security actions in all industries (FTC report to Congress, January 2026). No Safeguards-only count is published.

ITEM & DESCRIPTION	REGULATION (16 CFR 314)
☐ **1. Who is in charge.** The person who oversees the program, and who oversees them if outsourced. → Have it ready: the Qualified Individual designation, and the provider contract if outsourced.	314.4(a)
☐ **2. Written risk assessment.** The risks you found, how you judged them, what you decided. → Have it ready: the current assessment with its date, plus earlier versions.	314.4(b)
☐ **3. What data you hold and who can reach it.** The data and systems inventory, and the access rules. → Have it ready: the data inventory, the access policy and the last access review.	314.4(c)(1), (c)(2)
☐ **4. Encryption and MFA.** Encryption in transit and at rest; multi-factor authentication for every user. → Have it ready: encryption settings, the MFA enrollment report, any written approvals of alternatives.	314.4(c)(3), (c)(5)
☐ **5. Retention, disposal and change control.** Disposal within two years of last use; a record of system changes. → Have it ready: the retention schedule, disposal logs and change tickets.	314.4(c)(6), (c)(7)
☐ **6. Logs for the incident window.** Monitoring of user activity and detection of intrusions. → Have it ready: the logs and alerts for those days, and your IT vendor's incident report.	314.4(c)(8)
☐ **7. Testing.** Continuous monitoring, or a yearly penetration test and scans every six months. → Have it ready: the test reports and what was fixed after each.	314.4(d)
☐ **8. Training.** Security awareness training kept current with your risks. → Have it ready: rosters, dates and the materials used.	314.4(e)
☐ **9. Vendor oversight.** How you chose providers, what their contracts require, how you check them. → Have it ready: the vendor list, contracts with safeguard clauses, assessment notes.	314.4(f), (g)
☐ **10. Response plan, board report and the notice itself.** The plan as it stood that day, the latest board report, the form you filed. → Have it ready: the plan, the incident timeline, the board report and a copy of the FTC submission.	314.4(h), (i), (j)

IF YOU ONLY DO ONE THING

Write down what customer information you hold and where it sits, then do the risk assessment on that list. The FTC's small-business guide says you cannot build a program until you know what you have and where it is.