Regulation S-P AI incident insert

SEC-covered institutions' privacy, incident-response and compliance teams

Read the complete guide on aona.ai

For a covered institution, an AI-related customer-information incident belongs in the Regulation S-P response programme. Assess its nature and scope, contain it and determine the affected-individual notice obligation. The reasonable-investigation exception, 30-day outer notice limit and service-provider notification duties are distinct from the FTC's 500-consumer rule.

A fictional covered institution investigates a spreadsheet of 40 invented customers sent through an unapproved AI feature. The count is deliberately below the separate FTC threshold.

Synthetic event, customers and roles. No actual investigation finding, notice, provider assurance or control result is represented.

Your review

Reviewer: ____________________ Date: ____________________

Organisation or team: ______________________________________

☐ **Verify the legal and data scope**

Identify covered institution status, customer information and potentially affected individuals without borrowing another rule's threshold.

☐ **Track separate notice duties**

Record provider awareness, institution awareness, responsible recipients and the applicable timing.

☐ **Evidence any exception**

A reasonable investigation must support the relevant conclusion; a lack of reported misuse alone is not the record.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: ____

Evidence to collect: ____

Owner and next review date: ____

Review matrix

Response step	Worked insert for the fictional event	Owner and evidence
Identify scope	Record the institution, AI account, feature, spreadsheet and potentially affected information.	Compliance and incident lead establish the actual rule and system scope.

Response step	Worked insert for the fictional event	Owner and evidence
Contain and preserve	Stop additional uploads and preserve relevant facts without spreading the spreadsheet.	Incident team records timing, payload evidence and completed actions.
Investigate sensitive information	Determine what was accessed or used and assess the substantial-harm-or-inconvenience standard.	Privacy/legal owner documents the reasonable investigation and any exception conclusion.
Assess individual notice	Do not treat 40 consumers as automatically below a Regulation S-P threshold.	Notice owner applies the actual rule and relevant 30-day outer limit.
Coordinate provider notice	Obtain the service-provider facts and assess the applicable 72-hour provider-notification requirement.	Vendor owner separates provider notice from notices to affected individuals.
Close and improve	Retain decisions, actual notices if any and the remediation record.	Response owner updates the plan; no live notice is generated by this exercise.

Keep the notice paths distinct

- **Service provider:** Notify the institution under the applicable provider provision

The described outer limit is 72 hours.

- **Covered institution:** Assess, contain and investigate
- **Affected individual:** Receive required notice from or on behalf of the institution

Apply the separate notice conditions and timing.

Fictional response-plan insert

Trigger: employee reports using an AI feature with a spreadsheet containing 40 invented customer records.
Immediate routing: incident lead, privacy/compliance owner and vendor owner.
Evidence questions: which account and feature; what information; what actually reached the provider; which recipients and copies; what access/use occurred; what mitigation is evidenced.
Notice analysis: apply Regulation S-P's affected-individual and investigation conditions. Do not apply the FTC 500-consumer threshold.
Provider coordination: document the separate provider-to-institution notice and facts.
Final decision: no live determination or notice in this exercise.

This insert supplements an existing institution-specific plan; it does not replace its roles, legal assessment or notice procedures.

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information, not professional approval or a completed control test. It does not determine Regulation S-P notice obligations, conduct the institution's legal investigation or send notices.

17 CFR 248.30: Customer-information safeguards and response. Covered institutions, customer and sensitive customer information, response and notice duties, investigation exception and service-provider oversight.

SEC: Regulation S-P final rule, 3 June 2024. Final amendments and the 18-month larger-entity and 24-month smaller-entity compliance periods from publication; distinct from the proposal.