FTC AI-exposure threshold exercise

FTC-covered financial institutions' incident and compliance teams

Read the complete guide on aona.ai

For a covered institution, the FTC notification requirement applies to a notification event involving at least 500 consumers. The rule concerns unauthorised acquisition of unencrypted customer information, including its access presumption and encryption-key condition. Notify as soon as possible and no later than 30 days after discovery when the requirement applies.

Three fictional variants show why the threshold and reliable-evidence analysis must be documented separately.

Entirely synthetic data counts and incidents. No actual breach determination, provider response or FTC notification is represented.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Establish the notification-event facts**

Record authorisation, acquisition/access, encryption and key access, with the evidence supporting any exception.

☐ **Count distinct consumers**

Reconcile the payload and duplication rather than equating rows with people.

☐ **Assign the FTC notice process**

Record discovery, the responsible owner, deadline and updates; check other notification regimes separately.

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

Condition or variant	Invented facts	Decision path
Scope check	The fictional firm is assumed FTC-covered for this exercise.	A real case must establish institutional and customer-information scope.

Condition or variant	Invented facts	Decision path
Variant A: threshold met	620 distinct consumers; qualifying unauthorised acquisition established in the scenario.	Meets the numerical trigger; assign FTC notice as soon as possible within the 30-day outer limit.
Variant B: below this threshold	420 distinct consumers; same assumed acquisition conditions.	This FTC numerical trigger is not met; investigate and assess other applicable duties.
Variant C: access with contrary evidence	620 consumers; access occurred but reliable technical evidence may establish no acquisition.	Assess that evidence against the rule; do not infer an exception from a lack of known misuse.
Encryption check	A separate scenario involves encrypted data and an exposed decryption key.	Treat the key-access condition as part of the unencrypted-information analysis.
Discovery and report	Relevant employee, officer or agent discovery is recorded, excluding the person committing the breach; some scope facts remain uncertain.	Assign the owner, report known required facts when applicable and update rather than waiting for perfect certainty.

Three decisions, one record

- **Scope:** Covered institution and customer information
- **Event:** Acquisition, access presumption and encryption
- **Threshold:** At least 500 distinct consumers
- **Action:** FTC notice owner and discovery-based timing

Synthetic count reconciliation

File rows: 800
Distinct invented consumers: 620
Duplicate rows: 180
Scenario A acquisition: assumed established for teaching
Scenario A numerical finding: at least 500 consumers

Case record fields

Record the institution and scope, discovery evidence, data types, distinct consumer count, acquisition/encryption findings, reliable contrary evidence if any, notification owner, known facts submitted and subsequent updates.

No notice is generated or sent by this worksheet.

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 decide FTC reportability, determine every affected consumer or submit the notification.

FTC: Safeguards Rule, what your business needs to know. Covered institutions, customer information, service-provider oversight and the notification threshold and process.

16 CFR 314.2: Definitions. Customer information, financial-institution scope and the definition and acquisition presumption for a notification event.

16 CFR 314.4: Information-security programme elements. Service-provider oversight under paragraph (f), and FTC notification timing, content and discovery under paragraph (j), including the exclusion of the person committing the breach from deemed institutional knowledge.