SmartSuite

Framework / Privacy / Global Privacy Regulations

SEC Regulation S-P (17 CFR 248)

SEC Regulation S-P (17 CFR Part 248): privacy notices, opt-outs, safeguards and 30-day breach notice for broker-dealers, funds, advisers and transfer agents.



What it is

SEC Regulation S-P (17 CFR Part 248, Subpart A: Privacy of Consumer Financial Information and Safeguarding Personal Information) is the Securities and Exchange Commission's rule under Title V of the Gramm-Leach-Bliley Act. It requires broker-dealers, investment companies, SEC-registered investment advisers and, since the 2024 amendments, transfer agents to give privacy notices, honor opt-outs, safeguard customer information, respond to breaches and dispose of information securely.

At a glance

PUBLISHER
U.S. Securities and Exchange Commission (rule under Title V of the Gramm-Leach-Bliley Act, enacted by the U.S. Congress)

TYPE
Regulation

VERSION
17 CFR Part 248, Subpart A (as amended 2024)

EFFECTIVE
November 13, 2000; amendments August 2, 2024

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
United States

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: ecfr.gov/current/title-17/chapter-II/part-248

Why it matters

- **One rule for notices and safeguards** Privacy notices, opt-outs and the safeguards program sit in the same Subpart, so the customer-facing promise in the §248.6 notice and the security program behind it are examined together.
- **A defined response program** §248.30(a)(3) requires procedures to assess the nature and scope of an incident, identify the systems and types of customer information involved, contain and control the incident, and notify affected individuals.
- **A fixed notice deadline** Notice as soon as practicable and no later than 30 days after becoming aware of unauthorized access or use, unless the firm determines after a reasonable investigation that the sensitive customer information is not reasonably likely to be used to cause substantial harm or inconvenience (§248.30(a)(4)).

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Reg S-P

Privacy Notice and Opt-out Register

Hold the current initial and annual notice text, the §248.6 content checklist, opt-out elections and the §248.5(e) exception analysis in Privacy Management.

Safeguards Policy Set (§248.30(a)(1))

Keep the written administrative, technical and physical safeguards as controls with owners, testing and evidence in Compliance Management.

Incident Response Program (§248.30(a)(3))

Run assessment, containment and the notification decision as a workflow, with the reasonable-investigation finding documented when notice is not given.

30-day Individual Notice (§248.30(a)(4))

Track the awareness date, affected individuals or systems, the notice contents, any Attorney General delay and the delivery record.

Service Provider Oversight (§248.30(a)(5))

Record due diligence, monitoring, the 72-hour notice obligation and any written delegation of customer notice in Third Party Risk Management.

Examination Records

Assemble policies, incident documentation, determinations, delays and agreements for the record periods §248.30(c) and the firm's books-and-records rules require.

Common framework mappings

CCPA/CPRA · GDPR · GLBA Safeguards Rule (16 CFR Part 314) · ISO 27001:2022 · ISO 27701 · NIST Privacy Framework v1.0 · NIST 800-53 Rev.5 · SOC 2

Official resources

SEC Regulation S-P

Defines consumer financial information privacy requirements for U.S. financial institutions.

ecfr.gov/current/title-17/chapter-II/part-248

Federal Register: Regulation S-P amendments (89 FR 47688, June 3, 2024)

The SEC's adopting release of May 16, 2024 for the incident response program, customer notification and service provider oversight amendments, with the compliance dates.

federalregister.gov/documents/2024/06/03/2024-11116/regulation-s-p-privacy-of-consumer-financial-information-and-safeguarding-customer-information

eCFR: 17 CFR 248.30 Procedures to safeguard customer records and information; disposal

The safeguards rule, incident response program, customer notification, service provider oversight and disposal provisions as amended.

ecfr.gov/current/title-17/chapter-II/part-248/subpart-A/subject-group-ECFR83262a0bce5ffaa/section-248.30

Frequently asked questions

Who is a covered institution under Regulation S-P?

For the safeguards, response program and disposal rules, §248.30(d)(3) defines a covered institution as any broker or dealer, any investment company, and any investment adviser or transfer agent registered with the Commission or another appropriate regulatory agency. The privacy notice and opt-out provisions in §248.1 apply to brokers, dealers, investment companies and SEC-registered investment advisers, including foreign ones registered with the Commission, for consumers who obtain products or services for personal, family or household purposes.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What did the 2024 amendments add, and when do they apply?

Release 34-100155 (adopted May 16, 2024, published at 89 FR 47688 on June 3, 2024, effective August 2, 2024) added the §248.30(a)(3) incident response program, the §248.30(a)(4) individual notice within 30 days, the §248.30(a)(5) service provider oversight with a 72-hour notice, brought transfer agents into the safeguards and disposal rules, extended customer information to other institutions' customers, added recordkeeping and conformed the annual notice exception. Compliance was required by December 3, 2025 for larger entities (for example fund groups with $1 billion or more in net assets and advisers with $1.5 billion or more under management) and by June 3, 2026 for smaller entities.

When must customers be notified of a breach?

§248.30(a)(4) requires a clear and conspicuous notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization, as soon as practicable and no later than 30 days after the firm becomes aware of the incident. Notice is not required if, after a reasonable investigation, the firm determines the information is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience. The U.S. Attorney General may delay the notice for national security or public safety reasons by 30 days, a further 30 days and, in extraordinary circumstances, 60 more.

What must service providers do under Regulation S-P?

§248.30(a)(5) requires the covered institution's response program to include written policies for oversight of service providers through due diligence and monitoring, reasonably designed to ensure they protect customer information and notify the institution as soon as possible and no later than 72 hours after becoming aware of a breach in security resulting in unauthorized access to a customer information system they maintain. The institution then starts its own response program; it may contract with the provider to notify individuals on its behalf, but the obligation to ensure notice stays with the institution.

When is an annual privacy notice not required?

§248.5(e) excuses the annual notice when the firm provides nonpublic personal information to nonaffiliated third parties only under the exceptions in §248.13, §248.14 and §248.15, and has not changed the policies and practices disclosed under §248.6(a)(2) through (5) and (9) in its most recent notice. A firm that later changes those practices must resume the annual notice under the timing rules in §248.5(e)(2); the initial notice under §248.4 is still required.

License included / downloadable: Yes Regulation S-P is a U.S. federal regulation published free in the Code of Federal Regulations and in the SEC's releases; the platform links to the official text.

Full framework page and mappings: smartsuite.com/frameworks/sec-regulation-s-p-privacy-of-consumer-financial-information