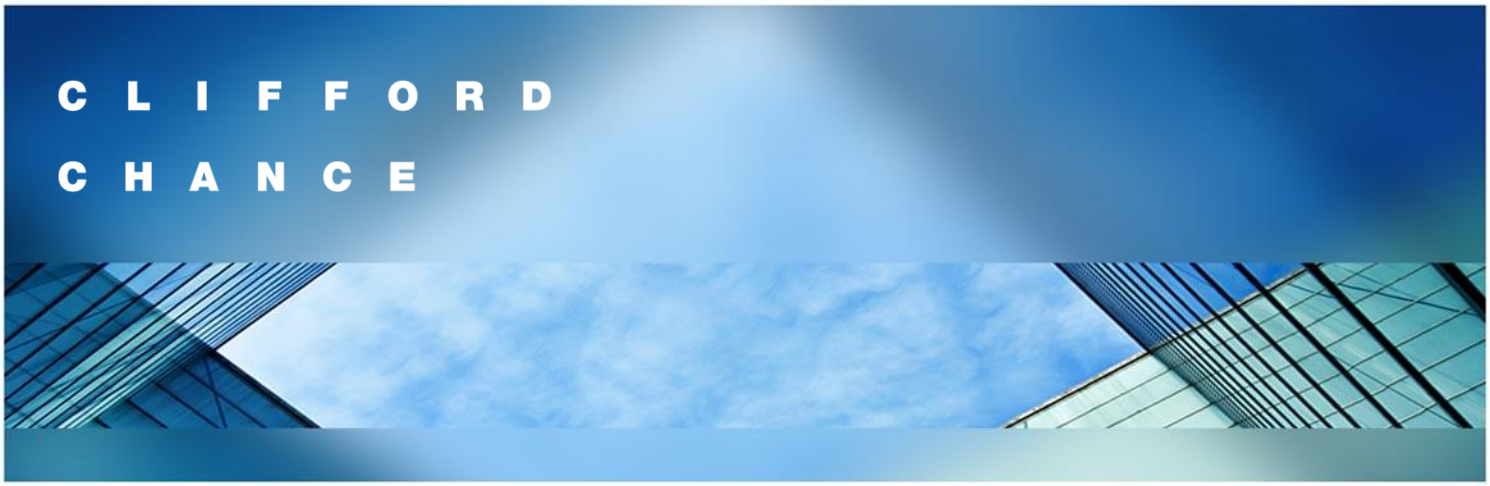

UPDATE: RECENT AMENDMENTS TO REGULATION S-P

On May 16, 2024, the Securities and Exchange Commission ("**SEC**") issued important amendments ("**Amendments**") to Regulation S-P, a set of privacy rules that regulate covered institutions' treatment of non-public personal information about consumers. A "**covered institution**" is a broker, dealer, investment company, SEC-registered investment adviser, funding portal[1], or transfer agent registered with the SEC or another appropriate regulatory agency, as defined in the Securities Exchange Act of 1934 ("**transfer agent**"). The Amendments are designed to modernize and enhance Regulation S-P protections, initially put in place 24 years ago, and respond to expanded use of technology and corresponding risks to consumers.

Broadly, the Amendments update the requirements of (1) the "safeguards" rule, which requires brokers, dealers, investment companies, and SEC-registered investment advisers to adopt written policies and procedures addressing administrative, technical, and physical safeguards to protect customer records and information; and (2) the "disposal" rule, which requires institutions covered by the safeguards rule and transfer agents to appropriately dispose of consumer report information.

The Amendments contain five key elements.

These are:

1. **Incident Response Program**. Covered institutions are required to develop, implement, and maintain written policies and procedures for an incident response program reasonably designed to detect, respond to, and recover from unauthorized access to or use of

[1] Under Regulation Crowdfunding, funding portals must comply with the Regulation S-P requirements applicable to brokers. See 17 CFR 227.403(b).

customer information. Such a program must include policies and procedures to:

- Assess the nature and scope of an incident and identify impacted customer information systems and types.
- Take appropriate steps to contain and control the incident to prevent further unauthorized access and use of customer information.

The program policies and procedures should be reviewed and updated periodically to ensure that they remain "reasonably designed".

"**Customer information**" is:

- **For any covered institution other than a transfer agent**, any record containing non-public personal information about a customer of a financial institution, in any form, in the possession of the covered institution or handled or maintained by it, or on its behalf, regardless of whether the covered institution has a customer relationship with such individual.
- **For a transfer agent**, any record containing non-public personal information identified with any natural person who is a security holder of an issuer for which the transfer agent acts, in the possession of or handled or maintained by the transfer agent, or on its behalf, regardless of whether the transfer agent has a customer relationship with such individual.

2. **Notification requirement**. The incident response program must also include policies and procedures to notify all individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization, unless:

   - A covered institution determines after reasonable investigation, that such information has not been and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience. Each institution has flexibility to define, based on facts and circumstances, what constitutes a "reasonable investigation" and whether information is "reasonably likely" to have been used in a prohibited manner.
   - The SEC receives a written request from the Attorney General that customer notification would pose a substantial risk to national security or public safety. In this instance, the covered institution may delay customer notice for a maximum of three times and thereafter, if needed, continue to work with the Attorney General. The SEC has established an inter-agency communication process with the Department of Justice to effectuate this requirement.

   "Sensitive customer information" is "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the

information."[2] This definition is broader than that used by some states and the Banking Agencies' Incident Response Guidance. For example, "substantial harm or inconvenience" is not defined and would be subject to the facts and circumstances surrounding an incident.[3]

Broadly, the notification requirement is intended to give affected individuals an opportunity to mitigate risks by taking timely action, including through credit monitoring, fraud alerts, and change of passwords, while incentivizing covered institutions to conduct thorough investigations. If a covered institution is unable to determine which individuals are affected by an incident, it must provide notice to all individuals whose sensitive customer information is stored in the system that was, or is reasonably likely to have been compromised. Also, since the requirement applies to customer information even in the absence of a relationship between a covered institution and an impacted individual, a covered institution may need to collaborate with another institution where the individual does have a relationship—to obtain contact information or for the other institution to provide notice.

Notice to impacted individuals must be clear, and conspicuous, and provided as soon as practicable, but no later than 30 days after the covered institution becomes aware[4] of the incident. Notice must also be provided by a means designed to ensure that the affected individual can reasonably be expected to receive it. The Amendments do not prescribe a specific format, but do require the notice to include key information about the incident, the breached data, and how the affected individual can respond, including contact information sufficient to enable inquiry about the incident and recommended steps and explanations about review of account statements for suspicious activity, requests for credit reports and protection against identity theft.

3. **Service providers**. As a new obligation, covered institutions are required to establish, maintain, and enforce written policies and procedures reasonably designed to oversee, including through due diligence and monitoring, their service providers. A "**service provider**" is "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution." Affiliates of covered institutions can be subject to this definition.

   Policies and procedures must be reasonably designed to ensure that service providers take appropriate measures to protect against unauthorized access to or use of customer information and provide notice to a covered institution within 72 hours of becoming aware[5] of a potential breach in security resulting in unauthorized access to a customer information system the service provider maintains.

---

2 The Amendments include examples of this information that can be used alone (e.g., Social Security number) or in combination with other information (e.g., name or online username in combination with access code or mother's maiden name).

3 Examples noted in the Adopting Release include fraud, theft, harassment, physical harm, damaged reputation, or misuse of an individual's account.

4 The Adopting Release discusses the difference between the "becoming aware" standard and the reporting trigger in the Public Company Cybersecurity Rules and notes that the difference is intentional because the Amendments and these other rules have different purposes.

5 This standard aims to enable a covered institution to implement an incident response program expeditiously.

To enable flexibility for covered institutions in their service provider arrangements, there is no requirement for covered institutions to enter into written agreements with their service providers. Although covered institutions may arrange for service providers to provide notice to affected individuals, covered institutions remain primarily responsible and liable for compliance with the Amendments.

4. **Scope**. The Amendments adjust the scope of the safeguards and disposal rules to:
    - Align protections under both rules to apply to the newly defined "customer information". Previously, Regulation S-P's protections applied to different, though at times overlapping, sets of information with, for example, the safeguards rule only protecting records and information of covered institutions' customers.
    - Extend Regulation S-P's requirements to transfer agents. Transfer agents maintain sensitive and detailed information about security holders, which is subject to similar risks as customer information maintained by other covered institutions.
    - Extend Regulation S-P's protections to transfer agents' customers.
5. **Recordkeeping and Annual Notice Amendments**. Covered institutions, other than funding portals, must maintain written records documenting compliance with the Amendments. These include policies and procedures; documentation of any detected unauthorized access to or use of customer information; documentation of any investigations; and contracts between covered institutions and service providers. The length of time for which records must be kept varies:
    - Registered investment companies and unregistered investment companies must keep records for six years in an easily accessible place.
    - Registered investment advisers must keep records for five years, in an easily accessible place for the first two years.
    - Broker dealers and transfer agents must keep records for three years in an easily accessible place.

    The Amendments also codify an existing statutory exception to the annual privacy notice requirement.

Compliance period

The period to come into compliance with the Amendments varies depending on entity size. Larger entities have 18 months to comply following the date of the Amendments' publication in the Federal Register on June 21, 2024, and other entities have 24 months to comply following such date. "Larger entities" are defined to include investment companies with net assets of $1 billion or more; registered investment advisers with $1.5 billion or more in assets under management; all brokers, dealers and all transfer agents that are not small entities under the Securities Exchange Act of 1934.

Next steps

Covered institutions are advised to review the Amendments and map the new requirements to institutions' policies and procedures. Note should be taken of the expanded definition of "customer information", scope of attendant requirements as well as the new customer notification requirements. Covered institutions should also revisit their service provider arrangements to ensure compliance with the Amendments.

Clifford Chance would be pleased to advise on the various aspects of the Amendments and practical implications for our clients.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Devika Kornbacher
Partner

T +1 713 821 2818
E devika.kornbacher
@cliffordchance.com

Ricky Legg
Associate

T +1 202 912 5943
E ricky.legg
@cliffordchance.com

Brian Yin
Associate

T +1 202 912 5902
E brian.yin
@cliffordchance.com

Inna Jackson
Tech Knowledge &
Innovation Attorney –
Americas

T +1 212 878 3292
E inna.jackson
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Two Manhattan West, 375 9th Avenue, New York, NY 10001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.