ALERT MEMORANDUM

# SEC Adopts Amendments to Reg S-P

*May 23, 2024*

On May 16, 2024, the Securities and Exchange Commission (the "Commission" or "SEC") adopted a final set of amendments (the "Final Amendments") to Regulation S-P ("Reg S-P") to require "covered institutions," which include SEC-registered investment advisers ("RIAs") and broker-dealers, to adopt an incident response program for incidents involving unauthorized use of or access to customer data. The Final Amendments also require customer notification where the covered institution determines the compromise of such data could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information .

Importantly, as discussed in more detail below, the Final Amendments will apply to RIAs' relationships with natural person investors in their private funds, notwithstanding that an adviser's only "clients" for Advisers Act purposes may be private funds themselves, to which Reg S-P does not apply.

The Final Amendments largely track the SEC's March 2023 proposal (discussed here), with a few targeted changes to address concerns raised by industry comments. One notable change is that the Commission declined to define "substantial harm or inconvenience" for purposes of the notice requirement, citing concerns that the proposed definition was simultaneously overly broad and narrow. In the Final Amendments, the Commission instead took the approach of various federal banking regulators in similar rules in not defining the term. The Commission also removed the requirement that customer notices following a data breach must include information on the steps that have been taken to protect customer data—a change that may be welcome news to registered firms concerned that such disclosures would have in fact heightened security risks.

The Final Amendments become effective 18 months following publication in the Federal Register for large institutions (RIAs with AUM of at least $1.5B and broker-dealers that are not considered small entities under the Exchange Act) and 24 months for small institutions (*i.e.*, those below such thresholds). We note that this is a longer period than the timelines in other recent rules. This may signal a reversion to more workable compliance periods, although it remains to be seen whether this will become a trend.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

WASHINGTON

**Robin M. Bergen**
+1 202 974 1514
rbergen@cgsh.com

**James R. Burns**
+1 202 974 1938
jrburns@cgsh.com

**Brant K. Brown**
+1 202 974 1694
bkbrown@cgsh.com

**Amber V. Phillips**
+1 202 974 1548
avphillips@cgsh.com

**Anna Bintinger**
+1 202 974 1602
abintinger@cgsh.com

NEW YORK

**Rachel Gerwin**
+1 212 225 2723
rgerwin@cgsh.com

In this Client Alert, we discuss (1) which institutions and relationships are covered by the Final Amendments, (2) the various requirements that will take effect, and (3) key takeaways for registered firms to consider.

## Who Is Covered?

The current version of Reg S-P contains two primary components: a "safeguards rule" that requires covered institutions (explained below) to adopt written policies and procedures to safeguard customer information and a "disposal rule" that requires covered institutions to dispose properly of consumer report information.

The Final Amendments introduce new requirements for covered institutions and also standardize the definitions in the safeguards and disposal rules. Both rules will now apply to "customer information" as defined in the Final Amendments, regardless of whether affected individuals are customers of a covered institution *or* customers of another financial institution whose information was provided to the covered institution. In other words, the Final Amendments expand the definition of "customer information" to include information about individuals who may not even be customers of the covered institution.

The Final Amendments define "covered institution" to mean any (1) broker-dealer or funding portal; (2) investment company; (3) RIA; or (4) transfer agent registered with the SEC or another relevant agency. Exempt reporting advisers are not in scope. Unlike recent rule releases such as the Private Fund Adviser Rules, the Commission did not distinguish between RIAs based in the United States and offshore RIAs based in other jurisdictions, nor did it distinguish between U.S. and non-U.S. customers; accordingly, absent further guidance from the SEC to the contrary, the requirements will apply to all RIAs and with respect to customers from any jurisdiction. The adopting release reiterates the SEC's position that private funds themselves are not considered "covered institutions" under Reg S-P.

Under the Final Amendments, broker-dealers that are only notice-registered (*i.e.*, CFTC-registered futures commission merchants and introducing brokers that are permitted to register as broker-dealers by filing a notice with the SEC for the limited purpose of effecting security futures products transactions) will be excluded from the scope of the disposal rule, but will continue to be subject to the safeguards rule. In a nod to harmonization of regulatory frameworks, the SEC stated that notice-registered broker-dealers will continue to be deemed in compliance with Reg S-P if they are subject to and comply with the financial privacy rules of the CFTC.

The SEC noted in the adopting release that many covered institutions may be subject to other, broader requirements relating to cybersecurity and/or protection of customer information, such as the EU's General Data Protection Regulation ("GDPR") and other regimes applicable to firms operating outside of the United States. The adopting release acknowledges that covered institutions may therefore already have protective frameworks in place, but the Final Amendments do not include specific exemptions for firms that comply with GDPR or other non-U.S. regulations.

### What Updates Will Be Required to Firms' Policies and Procedures and Compliance Programs?

#### *New Incident Response Program*

The Final Amendments require covered institutions to establish, maintain, and enforce policies and procedures that include an incident response program for unauthorized access to or use of customer information and customer notifications of incidents. The policies and procedures must be "reasonably designed to detect, respond to, and recover from both unauthorized access to and unauthorized use of customer information" and must cover:

— An **assessment** of the nature and scope of any incident involving access to or use of customer information systems, including an assessment of the types of customer information that may have been accessed or used;

— Appropriate steps to **contain and control** the incident to prevent further unauthorized access to or use of customer information;

— **Notification** to each affected individual whose "sensitive" customer information was, or is, reasonably likely to have been accessed or used without authorization.

The assessment requirement mandates that covered institutions conduct an assessment upon becoming aware of any unauthorized access to or use of customer information, with the scope of the assessment (as well as the response itself) dependent on the nature of the unauthorized access or use. (Inadvertent access by an employee, for example, would likely require a different type of assessment and response than would intentional access by a malicious actor.) A covered institution's policies and procedures must also require a reassessment of its notification determinations if it becomes aware of new facts that are potentially relevant to such determinations.

Taking a more principles-based approach, however, neither the Final Amendments themselves nor the adopting release prescribes how to determine the appropriate contain-and-control steps that follow an assessment. The Commission declined to require specific steps in a response program or to require that firms designate specific individuals or functions with oversight responsibility for all or part of the response program. Instead, the adopting release indicates that the appropriate steps necessary to contain and control a security incident will vary based on the type of incident, and may include "isolating compromised systems, changing system administrator passwords, rotating private keys, and changing or disabling default user accounts and passwords." Finally, the adopting release suggests that covered institutions "consider reviewing and updating the containment and control procedures periodically to ensure that the procedures remain reasonably designed."

***Notice Requirement***

The Final Amendments, consistent with the proposal, require covered institutions to notify each affected individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization. The scope of the notification requirement is narrower than the scope of incidents requiring an assessment: while assessments are required for any unauthorized use of or access to customer information, notice is required where *sensitive* customer information is used or accessed without authorization.

The Final Amendments define sensitive customer information as "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."

As mentioned above, the Commission did not adopt its proposed definition of "substantial harm or inconvenience" and explicitly declined to define this term. The adopting release notes that the ultimate determination of substantial harm or inconvenience depends on the facts and circumstances of the unauthorized access or use. In the absence of a specific definition, covered institutions will have some latitude to determine the scope of the effects of an incident. These judgment calls will, of course, potentially be subject to challenge by the Commission with the benefit of additional hindsight.

Covered institutions must provide the notifications as soon as practicable, but (with some specific exceptions) no later than 30 days following the covered institution becoming aware that unauthorized access to or use of sensitive customer information has occurred or is reasonably likely to have occurred. This timeline is consistent with the Commission's approach in other rules, *e.g.*, the Private Fund Adviser rules and Form ADV, which may signal a more general standard for "prompt" obligations under the Advisers Act. This is, notably, a shorter time period than required under many state laws, which often allow for 45- or 60-day time periods for notice.

Finally, although the Commission did not prescribe a specific format for required notices, it did emphasize that notice must be provided in a clear and

conspicuous manner by means designed to ensure that the customer can reasonably be expected to have received actual notice of the incident in writing. The notice must be reasonably understandable and designed to call attention to the nature and significance of the information required to be provided.

The Final Amendments removed the requirement that the notice describe what the firm has done to protect the customer information from further unauthorized use. The Commission noted that this was in response to industry comments that voiced significant concern regarding the security risks of publicizing remedial actions, in addition to potential commercial sensitivities.

***Service Providers***

The Final Amendments require covered institutions to establish, maintain, and enforce written policies and procedures reasonably designed to require oversight of service providers, including through due diligence and monitoring. "Service provider" is defined in the Final Amendments as "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." This reflects a significant change from the proposal, which would have required a written contract with applicable service providers; however, covered institutions' policies and procedures must cover the same scope of procedures as proposed for such contracts: service providers must both protect against unauthorized access to or use of customer information, and provide notification to the covered institution as soon as possible, no later than 72 hours, after becoming aware of a breach in security that results in unauthorized access to a customer information system maintained by the service provider.

Covered institutions can delegate to service providers the obligation to send the customer notifications, but the covered institutions remain ultimately responsible.

The Commission removed the reference to third parties that was in the proposed definition to clarify that service providers can include affiliates of a covered institution.

***Recordkeeping***

Covered institutions are required to make and maintain written records documenting their compliance with the requirements of Reg S-P's safeguards rule and disposal rule. These requirements are generally consistent with existing recordkeeping obligations under other rules for each covered entity. RIAs must keep all required records for five years, the first two in an easily accessible place; broker-dealers are required to keep all records for three years in an easily accessible place. The records that covered institutions are required to keep include copies of policies and procedures pursuant to the Final Amendments, written documentation of any detected unauthorized access to or use of customer data, documentation of investigations into whether notice is required pursuant to the Final Amendments, copies of any notice provided to customers, and documentation of any contract or agreement pursuant to the Final Amendments between a covered institution and a service provider.

**Key Takeaways from the Final Amendments**

RIAs and broker-dealers that are covered institutions under Reg S-P should begin to consider:

— Which entities within their structures are considered "covered institutions";

— For RIAs that possess information relating to natural person investors, whether the adviser already has policies and procedures in place to comply with GDPR, state law, or other rules or regulations;

  - If so, how to undertake a gap analysis and address any conflicts;

— What updates should be made to existing policies and procedures to incorporate the new assessment, response, notification, and recordkeeping requirements; and

— What service provider relationships would be considered in scope, and for those that are, how to ensure that ongoing diligence and monitoring is sufficient to meet the new requirements under Reg

S-P, and whether any enhancements should be made to documentation.

Looking ahead, RIAs should also expect to see new SEC Advisers Act rules relating to cybersecurity as well as to outsourcing, each of which may have implications for the policies and procedures related to Reg S-P and some substantive overlap with the Final Amendments' requirements. The anticipated Outsourcing Rule, for example, may also set forth diligence and monitoring requirements for third-party service providers that handle sensitive information. RIAs to private funds will need to consider carefully how to establish a compliance program that addresses all of the newly-introduced requirements, even where they may differ across rules.

…

CLEARY GOTTLIEB