

# AMENDED REGULATION S-P: WHAT SMALL RIAs NEED TO KNOW AND WHY IT MATTERS FOR MANAGEMENT LIABILITY INSURANCE

The SEC's 2024 amendments to Regulation S-P mark a meaningful shift in how Registered Investment Advisers (RIAs) are expected to manage and respond to cybersecurity and data privacy risks. For small advisers (under \$1.5B in AUM), the compliance deadline arriving this summer introduces not only operational and regulatory challenges, but also a measurable expansion of liability exposure.

While Regulation S-P has historically focused on safeguarding client information, the amended rule formalizes incident response, mandates federal breach notification timelines, and extends accountability to third-party service providers. These changes effectively elevate cybersecurity from an IT function to a firm-wide compliance obligation with direct implications for Cyber Liability, Directors & Officers (D&O) and Errors & Omissions (E&O) insurance programs.

## What Changed Under Amended Regulation S-P

For most RIAs, the amendments to Regulation S-P do not introduce entirely new concepts but they do formalize and standardize expectations in ways that increase accountability and potential liability. At a high level, the rule now:

- **Codifies incident response** – Firms must maintain written programs to detect, respond to, and remediate cybersecurity incidents
- **Imposes a federal 30-day notification requirement** – Creating a uniform and compressed timeline for client disclosure
- **Expands the scope of protected information** – Including former clients, third-party data, and information received from other institutions
- **Extends responsibility to service providers** – Requiring ongoing vendor oversight and due diligence
- **Enhances documentation expectations** – Establishing a clear record of decisions and actions during incidents

Taken together, these updates do less to change what firms should be doing and more to define how well and how quickly they must do it - with clearer standards that can be evaluated by regulators and, importantly, by plaintiffs.

## Why This Matters: A Shift in Liability Exposure

The amended rule does not simply increase compliance requirements; it redefines the liability landscape for RIAs in three key ways:

1. **Cyber incidents become regulatory events by default**
2. **Clear standards make negligence easier to prove**
3. **Third-party failures become first-party responsibility**

These shifts have direct and material implications across management liability insurance lines.

## Implications for Cyber Liability Insurance

- **Increased Claim Frequency** – Mandatory notification requirements mean that more incidents will trigger response costs, be disclosed to clients and potentially lead to claims
- **Expansion of First-Party Costs** – compliance with the amended rule inherently requires forensic investigations, client notification, credit monitoring and legal costs
- **Increased Vendor Risk** – a breach at a third-party vendor can trigger the adviser's policy and due diligence failures may impact coverage or underwriting.

## Cyber Insurance Considerations

Small RIAs should ensure that:

- Policies can operationally support the 30-day notification deadline
- Vendor-originated breaches are covered
- Response panel vendors align with regulatory timelines
- Privacy regulatory inquiries are covered
- Sub-limits for notification and monitoring/remediation are adequate

The cost of a single incident can exceed annual compliance or IT budgets without proper insurance support.

## Implications for Directors & Officers (D&O) Insurance

- **Elevation of Cybersecurity to the Board Level** – No longer purely an operation concern. Under Reg S-P it becomes a matter of governance, oversight and risk management. Firm leadership may be exposed to claims alleging failure to implement required policies, inadequate oversight of cybersecurity risks and weak vendor governance
- **Increased Regulatory Scrutiny** – The SEC now has a clear framework for evaluating compliance which may lead to more frequent deficiencies, heightened enforcement and formal investigations following incidents. D&O policies are often the first line of defense for regulatory inquiries and enforcement proceedings.

- **Investor and Client Litigation Risk** – For RIAs with institutional client or pooled vehicles, potential claims include misrepresentation of cybersecurity controls, failure to adhere to stated policies and inadequate risk disclosure. These claims often target firm leadership directly, reinforcing the importance of robust D&O coverage.

## D&O Insurance Considerations

Smaller RIAs should confirm that:

- Regulatory investigations are covered (to the extent possible)
- Conduct exclusions require final adjudication
- Individual insureds are protected even if the firm faces financial strain following a cyber incident
- Board or management meeting records reflect active oversight of Regulation S-P readiness

## Implications for Errors & Omissions (E&O)

- **Creation of a Defined Standard of Care** – Amended Regulation S-P establishes clear expectations for safeguards, incident response, vendor oversight and notification timing. In the event of a breach, plaintiffs can now argue that the firm failed to meet explicit regulatory requirements and did not act within mandated timeframes. This reduces ambiguity and strengthens claims of professional negligence or breach of fiduciary duty.
- **Broader Claim Triggers** – E&O policies may be implicated in scenarios such as failure to implement adequate data protection controls, delays in breach notification, inadequate vendor due diligence and misrepresentation of cybersecurity practices to clients
- **Overlap with Cyber Coverage** – The amended rule increases the likelihood of coverage intersection between E&O and Cyber around third-party liability arising from breaches, client lawsuits following notification and contractual obligations tied to data protection.

## E&O Insurance Considerations

RIAs under \$1.5B should review:

- Whether privacy or data-related claims are excluded or limited
- How regulatory inquiries tied to client data incidents are treated
- The interaction between E&O and Cyber policies for defense and response costs
- Contractual liability exclusions where client agreements reference data protection

## Key Takeaways for Small RIAs

As the compliance deadline approaches, small advisers should focus on the intersection of operational readiness and insurance protection.

### 1. Cyber Risk is Now Compliance Risk

A cybersecurity incident is no longer just a technical failure, it is a potential regulatory violation.

### 2. Vendor Risk is Your Risk

Third-party relationships must be actively managed, as their failures can directly impact your firm's liability.

### 3. Documentation Matters

Regulators and plaintiffs will evaluate not just what happened, but how the firm responded and documented its actions.

### 4. Insurance Programs Must Evolve

Traditional approaches to Cyber, E&O, and D&O insurance may not fully account for the expanded exposure created by amended Regulation S-P.



For any questions or to discuss in more detail, please reach out:

**Damian Clar**  
Executive Leader | RIA Specialist  
[dclar@amimdp.com](mailto:dclar@amimdp.com) | 443-305-6204

