COMPLIANCE GUIDE · 2026 EDITION

2026 Compliance Guide

For the Founder Who's Also the CCO

Small & Mid-Sized Registered Investment Advisers

COMPLIERS CONSULTING SERVICES, LLC

You're Not Just the Compliance Officer

If you're a founder-CCO at a small or mid-sized RIA, you already know the job description on paper doesn't match the job in practice. You're building the investment process, running the business, talking to clients — and somewhere in there, you're also responsible for a compliance program that regulators expect to look no less rigorous than one built by a firm ten times your size.

That last part is the one worth sitting with. Size changes your resources. It does not change what examiners expect of you. Fiduciary duty, accurate disclosures, documented policies, cybersecurity controls, and — new for 2026 — AI governance apply whether you manage $30 million or $300 million.

This guide is built for exactly that reality: limited time, lean resources, and no compliance department to hand things off to. Every figure in it comes from a primary regulatory source — the SEC, FINRA, or FinCEN directly — cited as we go, not secondhand. Where the numbers floating around the industry right now don't match what regulators actually published, we say so.

Let's get into what actually changed heading into 2026, what didn't, and what to do about both.

Where Enforcement Actually Stands

You've probably seen the headline: SEC enforcement activity dropped sharply in fiscal 2025. That's true — but "dropped sharply" gets measured a few different ways in the SEC's own release, and each one tells a slightly different story about how much enforcement appetite the Commission actually has heading into 2026.

Here's what the SEC's own April 2026 enforcement results release actually says about FY2025 (the year ended September 30, 2025): [1]

456
Total enforcement actions filed — down 22% from FY2024, and the lowest in at least 20 years

303
Standalone actions, down from 431 in FY2024 (a 30% drop)

On dollars, the release actually reports two different totals worth telling apart. Total monetary relief ordered — the number that tends to make headlines — came to $17.9 billion ($10.8B in disgorgement and prejudgment interest plus $7.2B in civil penalties). But $14.9 billion of that is a single matter: the FY2025 judgment closing out *SEC v. Stanford International Bank*, a Ponzi-scheme case first filed in 2009. Exclude that one case and FY2025 relief ordered was roughly $2.7 billion. [1]

Separately, the SEC also reports total monetary **settlements** — a narrower measure of negotiated resolutions rather than relief ordered through litigation — and that figure fell to $808 million, down 46% from FY2024's $1.5 billion and the lowest since 2012. [1] Both numbers are real; they're just

answering different questions. Relief ordered captures everything the Commission won, including one 16-year-old case that happened to close out this year. Settlements captures what the SEC negotiated directly with respondents in FY2025 alone. If you've seen a 2026 compliance guide cite "lowest since 2012," that's almost certainly this settlements figure, not an error — but it's worth knowing which measure you're looking at before drawing conclusions about exam risk from either one on its own.

$2.7B
Monetary relief ordered, excluding the one Stanford Ponzi-case judgment closed out in FY2025

$808M
Total monetary settlements — down 46% from FY2024, the lowest since 2012

Chairman Paul Atkins has been explicit about the shift: the drop reflects a move away from "regulation by enforcement" and toward cases involving genuine fraud, market manipulation, and breaches of fiduciary duty — not a lower bar. Nearly two-thirds of FY2025 standalone actions charged an individual, a 27% year-over-year increase. That's a message worth hearing if you're the individual whose name is on the ADV. [1]

SMALL FIRM ≠ SMALL TARGET

State regulators run their own exam programs, independent of the SEC, and small RIAs are their primary constituency. The SEC also continues to prioritize examinations of never-examined and recently registered advisers every single year. If your firm has operated for a few years without an exam, that's not evidence you're off the radar — it may mean you're due.

FINRA's 2025 numbers tell a similar story: fewer cases, sharper focus. [2]

625
New disciplinary actions filed in 2025, down 14% from 730 in 2024

$99.6M
Total fines and disgorgement, up from $75.6M in 2024 — almost entirely one outlier fine

AML
The single largest category of 2025 fines by dollar amount

That fines figure is less reassuring on close inspection: $26 million of it — more than a quarter of the total — came from a single March 2025 action against Robinhood Financial and Robinhood Securities for AML, supervisory, and disclosure failures. [3] Exclude that one case and 2025's fines actually fell roughly 15% year-over-year. Most small, state-registered RIAs aren't FINRA members, so this activity won't touch you directly. But it's a preview of what state and SEC examiners are looking for too: weak written supervisory procedures, recordkeeping gaps, and thin AML programs. The failure patterns repeat across regulators even when the jurisdiction doesn't.

What Regulators Are Actually Watching in 2026

The SEC's Division of Examinations published its FY2026 priorities in December 2025, [4] and FINRA followed with its own Annual Regulatory Oversight Report the same month. [5] Strip away the volume and both point at the same handful of things.

Fiduciary duty, still at the top of the list

- Whether investment advice is consistent with your fiduciary obligations, including how conflicts of interest are handled.
- Whether you're seeking best execution for clients.
- The documented rationale behind recommendations — especially for alternative investments, complex or higher-cost products, and advice to older investors or those saving for retirement.

This is the most foundational obligation you carry as a founder-CCO. Every recommendation needs a documented "why," not just a defensible one in your head.

Whether your program is actually followed, not just written

Examiners assess whether policies are implemented and enforced — not whether a manual exists. A policy written at registration and never revisited doesn't reflect an effective program, and an attestation that testing happened is not the same as evidence that it happened.

Never-examined and recently registered advisers

The Division has prioritized this group for years running. First examinations tend to set the tone for your regulatory relationship going forward — a firm that shows up with a thoughtful, documented program from day one starts that relationship from a position of credibility.

The two issues everyone's compliance calendar needs in 2026

- **AI governance.** For the first time, both the SEC's exam priorities and FINRA's oversight report contain dedicated attention to artificial intelligence — covered in the next section. [4] [5]
- **Cybersecurity, including AI-specific threats.** The SEC's 2026 priorities call out training and security controls to identify and mitigate risks from both AI misuse and traditional malware. [4] FINRA's report separately flags phishing, account takeovers, deepfake-enabled fraud, ransomware, and “Cybercrime-as-a-Service,” where ready-made attack tools are sold to less sophisticated actors. [5]

Neither of these is a large-firm problem. Small firms are frequently more exposed, not less, because they lack dedicated security infrastructure — a point both regulators have made explicitly.

AI Governance Is Not a Large-Firm Problem

This is the genuinely new obligation heading into 2026, and the most common mistake founder-CCOs make about it is assuming it scales with firm size. It doesn't. It scales with use. If anyone at your firm uses AI for any business purpose, you have a governance obligation right now — regardless of your AUM.

What counts as "using AI"

You don't need a proprietary AI system to trigger this. Drafting a client email with ChatGPT, summarizing research with Claude or Gemini, or running meeting notes through an AI note-taker all count. And free, consumer versions of these tools can use whatever you type as training data for the underlying model — meaning client information or firm strategy entered into a free tool may have left the building with no audit trail and no data protection agreement behind it. That's a confidentiality issue, a recordkeeping issue, and a real liability, in that order.

What a defensible — not sophisticated — program looks like

- **An inventory.** A list of every AI tool anyone at the firm uses for any business purpose, including AI embedded inside third-party platforms you already use.
- **A one-page policy.** Which tools are approved, what can never be entered into them (client data, MNPI, proprietary strategy), and who owns oversight.
- **Accurate disclosures.** If AI shows up anywhere in your Form ADV or marketing, your actual practice needs to match what's on the page — AI misrepresentation is already an established enforcement category, not a hypothetical one.
- **Vendor oversight.** If your portfolio analytics, CRM, or compliance technology has AI baked in, you're responsible for understanding how your client data is used and protected by that vendor.
- **A human review step.** Any AI output that touches a client or an investment decision needs a documented human check before it goes out the door.

WHY THIS MATTERS MORE FOR TOOLS THAT ACT, NOT JUST ANSWER

A chatbot that drafts a reply is a different risk profile than an “agentic” tool that executes multi-step actions across your systems with limited human oversight. If any vendor you use is moving toward agentic AI features, ask directly what controls govern it before you flip that switch on.

The bar here isn't sophistication. It's evidence — that you've thought about the obligation, put structure around it, and can produce that structure the moment an examiner asks.

Cybersecurity & Regulation S-P: Two Deadlines That Have Already Passed

Regulation S-P was amended in 2024 to significantly expand how registered investment advisers must protect customer information. [6] Four requirements came out of that amendment:

- **A written incident response program** covering how you detect, contain, and recover from unauthorized access to customer information.
- **Client notification within 30 days** of discovering that customer data was, or may have been, accessed without authorization — describing what happened and how to contact the firm.
- **Written documentation of your safeguarding practices**, including records of any detected unauthorized access and the response taken.
- **Service provider oversight**, including a requirement that vendors notify you of a security incident within 72 hours of discovery.

Both compliance deadlines have now come and gone:

Dec 3, 2025
Deadline for larger entities ($1.5B+ RAUM) — passed

Jun 3, 2026
Deadline for smaller entities (under $1.5B RAUM) — also passed

If you're a smaller entity and the written incident response program, client-notification procedure, and vendor-oversight framework aren't fully in place, this is no longer a planning item on next quarter's calendar — it's an open compliance gap an examiner can cite today. Close it now, and be prepared to show your work on when and how you did. [6]

Most state-registered advisers aren't directly subject to Reg S-P (though many states have their own, similar requirements). But if you're approaching the $100 million RAUM threshold covered in the next section, Reg S-P will apply to you the moment SEC registration is effective. Building the incident response program, vendor oversight framework, and documentation before that happens — rather than the week before your first SEC exam — is the difference between a mature program and a rushed one.

A practical floor for every small RIA

- A written incident response plan, even a simple one, covering detection, response, and client notification.
- A policy governing what data employees can and can't share with third-party vendors and AI tools.

- Multi-factor authentication on every system that touches client data.
- Vendor contracts reviewed for data protection language, especially for any vendor using AI in its product.

Crossing $100 Million: The State-to-SEC Transition

For growing RIAs, this is the milestone that changes almost everything about your regulatory world. Here's how the thresholds actually work under current rules: [7]

- **Below $100 million RAUM:** state registration, in your home state and any state where you have clients.
- **$100–$110 million RAUM:** a buffer zone — SEC registration is optional, not required.
- **$110 million or more:** SEC registration becomes mandatory. You must file within 90 days of your fiscal year-end.
- **Below $90 million** (if already SEC-registered): you may be required to transition back to state registration.

One exception worth knowing: firms operating in 15 or more states may be eligible for SEC registration even below the $100 million threshold, which can meaningfully cut the burden of multi-state compliance.

A RELATED DEVELOPMENT WORTH TRACKING

On January 7, 2026, the SEC proposed raising the RAUM threshold that defines a “small entity” for Regulatory Flexibility Act purposes — from $25 million to $1 billion. That's a different threshold from the $100M/$110M SEC-registration trigger described above, and it doesn't change who has to register where. But it signals real momentum toward recalibrating size-based thresholds that haven't moved since 1998, and it's worth watching alongside the separate, still-unresolved question of whether the $100 million registration threshold itself gets raised. The comment period on this specific proposal closed March 13, 2026; as of August 2026, no final rule has been adopted. [8]

What actually changes once you're SEC-registered

- Your examiner changes — from your state regulator to the SEC's Division of Examinations, a larger organization whose first exam can reach back up to five years of firm history.
- Regulation S-P applies in full, including the incident response and vendor oversight requirements above.

- Rule 206(4)-7's formal annual review requirement kicks in — if you've been running a lighter version as a state-registered adviser, this is the point to formalize it.
- SEC-specific rules around marketing (Rule 206(4)-1) and custody may require real updates to your compliance manual, even where the underlying substance overlaps with state rules.

The firms that navigate this cleanly start six to twelve months before crossing the mandatory threshold: a gap assessment against SEC requirements, a Reg S-P program built in advance, and a Form ADV that's been genuinely reviewed for accuracy rather than just refiled.

What Actually Changed — and What Didn't

The change in administration brought real deregulatory movement. On June 12, 2025, the SEC formally withdrew fourteen outstanding rule proposals from the prior administration — not just the handful most commonly cited. Among them: [9]

- Conflicts of Interest Associated with Predictive Data Analytics (broker-dealers and advisers)
- Enhanced ESG Disclosures by Certain Investment Advisers and Investment Companies
- Outsourcing by Investment Advisers
- Safeguarding Advisory Client Assets (the proposed custody rule overhaul)
- Ten additional proposals spanning other parts of the rulebook

Withdrawal means exactly that: any future rule on these topics has to start over, with a fresh proposal and a new comment period. It does not mean the underlying conduct these rules targeted is now unregulated.

That distinction matters, because a deregulatory environment creates a specific and predictable risk: treating silence as permission. Fiduciary duty, accurate disclosure, written supervisory procedures, and cybersecurity obligations are all fully in force and under active examination regardless of what got withdrawn. Examiners are trained to spot exactly this pattern — a firm that quietly let something slide because the headline rule went away.

The one true delay: FinCEN's AML rule

The rule that would have formally defined certain registered investment advisers and exempt reporting advisers as “financial institutions” under the Bank Secrecy Act — requiring AML programs and suspicious activity report filing — was delayed a second time, with FinCEN finalizing a two-year postponement to January 1, 2028. FinCEN has been explicit that it intends to use the extra time to further tailor the rule and coordinate with the SEC on the related investment adviser CIP rule, not to abandon it. [10]

Use the runway. Don't treat it as permission to ignore where your firm's AML exposure already sits today.

Ten Moves to Make Before Year-End

Prioritized and sized for a firm where you're the only one who can act on most of these. Each one addresses a gap examiners are actually finding, not a hypothetical.

1. Build the AI inventory first, then the policy

List every AI tool anyone at the firm uses for any business purpose, including free consumer tools. That list is the foundation everything else depends on — you cannot supervise what you haven't inventoried. A one-page policy naming approved tools, off-limits data, and an accountable owner beats no policy every time.

2. Re-review your marketing materials against the Marketing Rule

The SEC issued its fourth Risk Alert on the Marketing Rule in December 2025, this one focused on testimonial, endorsement, and third-party rating disclosures — four alerts on one rule since 2022 is not a coincidence. [11] If testimonials, Google reviews, LinkedIn recommendations, or performance figures appear anywhere in your materials, confirm disclosures are in place and your review process is documented, including for AI-drafted content.

3. Treat your Form ADV update as an accuracy audit, not a filing exercise

Fees, conflicts of interest, services offered, AI representations, and disciplinary history are the areas examiners cite most often. Your ADV should tell an accurate, current story before an examiner ever reads it.

4. Write (or refresh) a real risk assessment

Without one, your policies are educated guesses. It doesn't need to be elaborate — it needs to be current, honest, and something you can hand an examiner when they ask how you decide what to test.

5. Prove your policies are actually followed

Schedule time to verify, at least annually, that what you said you'd do actually happened — and document that verification. A policy manual that's never been tested against real practice is not a compliance program.

6. Close the Reg S-P gap immediately if you haven't already

The June 3, 2026 compliance deadline for smaller entities has passed. A written incident response plan, client-notification procedures, MFA on client-data systems, and reviewed vendor contracts are the floor, not the ceiling — and the longer this sits open, the more it looks like an oversight rather than a timing issue.

7. Build exam readiness as a year-round posture

Keep your compliance manual current, your documentation organized, and a short first-day overview of your business ready to hand an examiner. If you've never run a mock exam or gap analysis, this is one of the highest-value investments a lean firm can make before a real one shows up.

8. Start SEC-transition prep six to twelve months early if you're approaching $100M

A gap assessment against SEC requirements, an early Reg S-P build-out, and an ADV review sized for SEC-level scrutiny all belong on this list well before the mandatory threshold, not after.

9. Keep your own knowledge current

There's no degree in this job. Reading SEC Risk Alerts and FINRA Notices as they're published, maintaining a professional designation, and staying connected to other founder-CCOs are not optional extras in a year where the rules keep moving.

10. Scale the program as you scale the business

Firms rarely get into trouble by ignoring compliance from day one. They get into trouble by building a solid program early, then letting it quietly fall behind as headcount, strategies, and client jurisdictions grow. Revisit the program every time the business changes shape — not once a year on autopilot.

The Bottom Line

2026's compliance landscape for small and mid-sized firms is defined less by what regulators pulled back and more by what they didn't. Fiduciary duty, accurate disclosure, documented policy, cybersecurity, and AI governance are all fully in force and under active examination — regardless of your AUM.

Being small doesn't mean being exempt. It means being resourceful: using the plays in this guide to build a program that's defensible, current, and genuinely reflects how your firm operates — not a manual that's been sitting untouched since registration.

HOW COMPLIERS CAN HELP

We work with founder-led broker-dealers and RIAs on exactly the gaps this guide covers — AI governance frameworks, Reg S-P build-outs, SEC transition readiness, and outsourced or fractional CCO support for firms that need real expertise without a full-time hire. If any part of this list feels like it's been sitting on the back burner, that's exactly what we help firms move to the front.

Ready to talk it through? Schedule a meeting at calendly.com/david-compliers/introduction or email us directly at info@compliers.com.

Compliers is a compliance consulting firm; this guide is provided for general informational purposes and is not legal advice. Figures and regulatory citations reflect publicly available SEC, FINRA, and FinCEN sources as of the dates referenced and are current as of August 2026.

References & Sources

Every figure in this guide was checked directly against the primary regulatory release where one exists — the SEC, FINRA, or FinCEN's own publications — rather than taken from secondary summaries. The two exceptions are noted below: the FY2025 FINRA disciplinary-action comparison and the full list of withdrawn SEC rule proposals, where we relied on independent analysis of FINRA's and the SEC's public filings by named third parties because no single regulator publication aggregates those figures. All sources were accessed in August 2026.

[1] U.S. Securities and Exchange Commission, "SEC Announces Enforcement Results for Fiscal Year 2025," Press Release No. 2026-34, Apr. 7, 2026. sec.gov/newsroom/press-releases/2026-34 — cross-referenced against U.S. Securities and Exchange Commission, "SEC Announces Enforcement Results for Fiscal Year 2024," Press Release No. 2024-186, Nov. 2024. sec.gov/newsroom/press-releases/2024-186

[2] FINRA disciplinary-action filings for calendar years 2024–2025, as compiled from FINRA's monthly "Disciplinary and Other FINRA Actions" reports and analyzed in Hyman Cotter PC, "Study of FINRA 2025 Disciplinary Actions Finds Decrease in Cases and Restitution, but Increase in Fines," Apr. 2026. securitieslaw.com

[3] FINRA, "FINRA Orders Robinhood Financial to Pay $3.75 Million in Restitution to Customers; Fines Robinhood Financial and Robinhood Securities for Anti-Money Laundering, Supervisory and Disclosure Violations," News Release, Mar. 7, 2025. finra.org/media-center/newsreleases/2025

[4] U.S. Securities and Exchange Commission, "SEC Division of Examinations Announces 2026 Priorities," Press Release No. 2025-132, Dec. 2025. sec.gov/newsroom/press-releases/2025-132

[5] FINRA, "2026 FINRA Annual Regulatory Oversight Report," published Dec. 9, 2025. finra.org/rules-guidance/guidance/reports/2026-finra-annual-regulatory-oversight-report

[6] U.S. Securities and Exchange Commission, "SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information," Press Release No. 2024-58, May 16, 2024, and Final Rule Release No. 34-100155. sec.gov/newsroom/press-releases/2024-58; compliance-date confirmation via FINRA, "Cybersecurity Advisory — Reminder: SEC Regulation S-P Compliance Date Approaching for Some Member Firms," Nov. 14, 2025. finra.org

[7] 17 C.F.R. § 275.203A-1, "Eligibility for SEC registration; switching to or from SEC registration." ecfr.gov/current/title-17/chapter-II/part-275/section-275.203A-1

[8] U.S. Securities and Exchange Commission, "SEC Proposes Amendments to the Small Entity Definitions for Investment Companies and Investment Advisers for Purposes of the Regulatory Flexibility Act," Press Release No. 2026-1, Jan. 7, 2026. sec.gov/newsroom/press-releases/2026-1

[9] SEC withdrawal of fourteen outstanding rule proposals, June 12, 2025, as reported in Sullivan & Cromwell LLP, "SEC Withdraws 14 Proposed Rules," Jun. 2025. sullcrom.com/insights/memo/2025/June; individual proposal titles and dates confirmed against the SEC's public rulemaking history.

[10] Financial Crimes Enforcement Network, final rule delaying the effective date of the AML/CFT program and suspicious activity report filing requirements for registered investment advisers and exempt reporting advisers to January 1, 2028 (issued Dec. 31, 2025; published in the Federal Register Jan. 2, 2026). federalregister.gov/documents/2026/01/02/2025-24184

[11] U.S. Securities and Exchange Commission, Division of Examinations, "Additional Observations Regarding Advisers' Compliance with the Advisers Act Marketing Rule," Risk Alert, Dec. 16, 2025. sec.gov/newsroom/whats-new/additional-observations-regarding-advisers-compliance-advisers-act-marketing-rule