Regulatory Compliance Watch

May 20, 2024 • **Insight, guidance and best practices**

RCW EXCLUSIVE: PART 1 OF 2

New Form ADV data: Benchmarks to use

The industry rebounded slightly in 2023 after a down year, with the biggest firms showing the best AUM growth.

RCW's exclusive annual analysis of new Form ADV data reveals that, overall, total AUM managed by **SEC** RIAs grew only 1% in the aggregate last year–from $127T to $128T. At least that meager growth bests the prior year's 7% decline in total AUM (***RCW***, May 11, 2023). But it pales compared with the 2023 jump in the Dow of 10.2%.

Yet the biggest firms did even better. The box on page 3 shows the results for the largest 10 RIAs. Their total assets grew 18% when comparing the latest Form ADV data for 2023 with 2022's.

Examining new data

In this part one of our annual series, we look at freshly reported Form ADV data from more than 15,000 SEC RIAs. That's 96% of all RIAs–reflecting the majority that must update their forms by the end of March.

The AUM results varied by sector as well. For example, the nearly 200 firms that reported more than $100B in AUM, saw their total assets fall nearly 1%. Advisers with under $100M in assets suffered the largest loss in total AUM: down 17.5%.

The best gain, among the sectors, came among firms managing between $500M-$999M. Their gross AUM jumped 7.2%. Of course, many reasons could explain such increases and decreases in AUM.

Numbers of clients

Of the total 108 million clients reported by RIAs (and this number must include duplicates as some clients turn to multiple advisers), 45 million are described as non-high-net-worth individuals. The aggregate AUM for these clients topped $7T.

High-net worth individuals placed, numbering 7.8 million ($12.6T in AUM). Assets managed by advisers of mutual funds took first place with $42T, just ahead of pooled



Joint SEC/FinCEN proposal would mandate RIA CIPs, page 3.

Content

3 **SEC/FinCEN joint rulemaking Proposal would mandate RIA CIPs**

5 **Judge tosses FTC's private equity claims**

6 **AI triggers advertising regulation FAQs**

7 **SoFi self-reports on customer ID program**

8 **Homeland Security proposes cyber rules**

The electronic edition of this *RCW* weekly briefing can be found at *regcompliancewatch.com*, along with our compliance toolbox, archive, advanced search features and more.

investment vehicles. The 93,000 investors in private funds held an aggregate AUM of $33T.

Some of these investors are outside the U.S. On average, 12% of an adviser's clients are "non" U.S. persons. But most advisers serve only U.S. clients. Nearly one-third of advisers reported some non-U.S. clients, while more than 1,800 advisers reported at least half their clients are non-U.S. persons; 417 advisers–3% of all RIAs–serve *only* non-U.S. persons.

Use of advertising

The new data allow an opportunity to examine how advisers are using the new marketing rule. One Form ADV question asks about use of performance results. Sixty percent answered they do not advertise performance. Nearly 80% don't showcase specific investment advice. Advisers have not embraced sharing testimonials (92% don't), endorsements (85% don't) or third-party ratings (83% don't).

About half of the advisers answered a Form ADV question about compensating for testimonials, endorsements or ratings. Of these, 69% indicated they don't compensate people for providing testimonials.

In part 2 of our series, we'll look at the data just from private fund advisers–and how their advertising answers differ from their peers'. Some 36% of RIAs noted that they advise at least one private fund.

Outsourced CCOs

For years, Form ADV has asked a question about whether a firm's CCO is compensated or employed (e.g., outsourced compliance officers) by another entity. This year, only 6% indicated that this is the case with their CCO.

Here's a rundown of more takeaways from the new Form ADV data:

- Payment for 95% of advisers comes from a percentage of AUM. Only 2% accept commissions.
- The average RIA employs 65 staff but the median number is 8. On average, 35 provide IA functions (median: 5). This makes sense as most advisers are smaller firms.
- An average of 27 employees are registered B-D reps. Seventeen on average are licensed insurance agents.
- On average, three persons solicit advisory clients for their firms.
- Nearly half (47%) of advisers report that they have custody of assets.
- Some 17% of advisers sell other products or services to their IA clients.
- Only 13% of advisers participate in wrap fee programs.
- Only 16% engage in derivatives transactions for their SMA clients.

Regulatory Compliance Watch

Group Publisher: Hugh Kennedy
Direct: 202-908-6212
Hugh.k@pei.group

Publisher: Carl Ayers
Direct: 202-908-6194
carl.a@pei.group

Editor: Bill Myers
Direct: 202-908-6191
William.m@pei.group

RCW strives to provide you with accurate, fair and balanced information. If for any reason you believe we are not meeting this standard, please let us know.

Regulatory Compliance Watch
130 W 42nd Street, Suite 450,
New York, NY 10036

Subscriptions:
For questions about newsletter delivery, address changes or online access, contact Customer Service at 202-908-6192 or e-mail: *subscriptions@peimedia.com*

Site Licenses for your firm:
If you are a member, additional staff at your firm qualify for a multi-user site license at a significant discount. Call our Site License Department toll-free at 800-455-5844, option 2, prompt 1 and get access tomorrow by 7am ET.

The ***RCW*** weekly briefing is a general circulation weekly focused on regulatory and compliance issues in the investment adviser community. Nothing within should be interpreted as offering investment advice or legal counsel.

Find us at *www.regcompliancewatch.com*

Copyright 2024 *RCW*

The ***RCW*** weekly briefing is published weekly, part of the subscription service of Regulatory Compliance watch (*www.regcompliancewatch.com*). The yearly membership rate is $3,195. ***RCW*** is owned by PEI Media (subscriptions@peimedia.com).

COPYRIGHT NOTICE 2024. No portion of this publication may be reproduced or distributed without the written permission of the publisher. ***RCW*** shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic distribution.

To report violations, contact: Carl Ayers, 130 W 42nd Street, Suite 450, New York, NY 10036; Confidential line: 202-908-6194 E-mail: carl.a@pei.group. For photocopying and electronic redistribution permission, please contact Publisher Carl Ayers at 202-908-6194 or e-mail *carl.a@pei.group*

How the Top 10 SEC RIAs fared in 2023 in total AUM

Firms	2024	2023	% Difference
1 The Vanguard Group	$7.9T	$6.6T	19%
2 Fidelity	$3.9T	$3.1T	26%
3 BlackRock Fund Advisors	$3T	$2.4T	27%
4 Capital Research and Management Co.	$2.9T	$2.7T	7%
5 PIMCO	$2.6T	$2.2T	16%
6 J.P. Morgan Investment Management	$2.5T	$2T	27%
7 T. Rowe Price Associates	$1.7T	$1.5T	16%
8 Goldman Sachs Asset Management	$1.6T	$1.5T	5%
9 Morgan Stanley Smith Barney	$1.4T	$1.1T	18%
10 BlackRock Financial Mgmt.	$1.2T	$1.1T	11%

Source: ***RCW*** analysis of **SEC** Form ADV data

- Just under 8% of advisers engage in principal transactions; and 2.3% execute agency cross transactions.
- Nearly 70% of advisers recommend B-Ds to their clients.
- Only 2.7% of SEC RIAs are also broker-dealers.
- AUM held by non-U.S. persons managed by advisers totals $26.6T, or about 20% of all AUM.
- Ninety-one percent of advisers maintain at least one website.
- Nearly half of advisers keep books and records somewhere other than their principal office.
- Fewer than 7% of advisers are also registered with a foreign financial regulator.
- Only 23 advisers indicated they're part of a public company.
- Only 3% of advisers hold more than $1B in their own assets; 89% of these manage between $1B-$10B in AUM.
- Only 36% of advisers answered that they use soft dollar benefits.
- One in four will compensate, either "directly or indirectly," for client referrals.
- Cryptocurrency investing crept up slightly compared with recent years, but the numbers remain scant. About 35 advisers noted they place clients in such investments, with 15 specifically citing Bitcoin.



Editor's note: Next week's analysis focuses on Form ADV responses from Schedule D and private fund advisers.

*What do you think about this story? Please, **share your thoughts** with Publisher* **Carl Ayers**. ■

SEC/FINCEN JOINT RULEMAKING

Proposal would mandate RIA CIPs

For some reason, federal regulators have long left out **SEC** RIAs when requiring financial institutions to maintain customer identification programs (CIPs). This would end should the SEC and **FinCEN** adopt a new proposal directed at both SEC RIAs and exempt reporting advisers.

The two regulators May 13th jointly announced a ***proposed rule*** that would work in tandem with FinCEN's proposal earlier this year to require RIAs to maintain an anti-money laundering program (***RCW***, March 27, 2024).

Indeed, the latest proposal stresses the CIP couldn't be separate but would have to be incorporated into an RIA's AML program, should both rules eventually be finalized.

Many forward-thinking RIAs already run AML/CIPs as a best practice, or perhaps because they had anticipated the day would come when these rules would encompass them.

BSA, not Advisers Act

The May 13th proposal would create a rule for advisers under the *Bank Secrecy Act*; not the Investment Advisers Act. The new rule would be BSA ***rule 220*** (customer ID programs for RIAs/ERAs). Among other things, this proposal would mandate that advisers must verify a customer's or an entity's identity "within a reasonable time before or after the customer's account is opened."

The CIP must operate on written compliance P&Ps that, among other things, would lay out what information would have to be sought, including a person's:

- Full legal name, and perhaps any aliases or DBAs names;
- Date of birth;
- Residential or business address; and
- Taxpayer identification number (if one is available or applied for).

For entities, an adviser would have to verify the corporation's, partnership's or trust's "principal place of business, local office, or other physical location."

Records that would have to be considered to verify a "non-U.S. person" could include "a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard," according to proposed rule 220.

The justification

The regulators noted that the "scale of money laundering in the United States is large," in justifying expanding the BSA CIP rule to SEC RIAs/ERAs. Many other financial institutions—from mutual funds to broker-dealers, travel agents to casinos—already must run CIPs.

In a regulator ***fact sheet***, they contended that if the CIP rule is finalized, it "would make it more difficult for criminal, corrupt, and illicit actors to use investment advisers as an entry point into the U.S. financial system."

You wouldn't have to re-verify an existing customer's identify when they opened a new account as long as you have confirmed their identity with procedures similar to the proposal in the past and you have a "reasonable belief" that you know the person's true identity.

The "proposed rule would provide investment advisers with the flexibility to use a risk-based approach to determine when the identity of a customer must be verified relative to the opening of an account," reads the proposal's preamble.

Two required methods

While you would get some flexibility in devising your CIP, it would have to include two methods of verifying a customer's identity: (1) using documents (e.g., eying "an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport") and (2) relying on non-documentary methods, such as "contacting a customer; independently verifying the customer's identity through the comparison of information provided with respect to the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; or obtaining a financial statement."

The ID inquiry would be limited to accountholders and not extend to those who have authority or "control over the accounts," like trustees.

A firm's compliance P&Ps would have to spell out what happens if a customer's identity couldn't be substantiated, including perhaps declining to open the new account.

Another step required would be to check if a customer opening a new account appears on any government lists, like **Treasury**'s OFAC (***RCW***, April 11, 2011). It is recognized in the proposal that many IAs already have such procedures in place.

You also could rely on a customer's ID verification previously confirmed by "another financial institution." While an adviser wouldn't be held responsible for the other party's failure to do so, it would be "responsible for ensuring compliance with the proposed rule."

Compliance Toolbox

Find tools-you-will-use at ***www.regcompliancewatch.com***. Visit our ***Compliance Toolbox***. Five examples of what you'll find in our toolbox are below. Or visit our website and find the tools you need.

- ***Client Release Form***
- ***Soft Dollars P&Ps***
- ***Robo Advisor Exam Letter***
- ***Holdings Report Form***
- ***Small Firm Cybersecurity Checklist***

Join our community and help your peers. ***Share your favorite tool***. Direct us to keep your contribution anonymous if you'd like.

Recordkeeping requirements

Advisers also would have to keep records of each verification for at least five years, and even five years after an account is closed. This would have to include a description of "any measures undertaken to verify the identity of the customer."

Another piece of the proposal would require that customers be notified of a firm's CIP procedures. The proposal includes sample notification language.

The regulators welcome your comments, and they'd have to be received within 60 days after the proposal appears in the *Federal Register*. The effective date of any final rule also could be 60 days, the proposal reads, but the compliance date would extend out six months.

Early reaction

The **Investment Adviser Association** expressed concerns "that the sweeping proposal will capture virtually all SEC Advisers and will not accomplish the stated policy goals because it lacks sufficient tailoring to the unique business models and risk profiles of SEC Advisers." It also urged FinCEN to reopen the comment period for its AML proposal and for FinCEN/SEC to consider the two proposals "holistically."

*What do you think about this story? Please, **share your thoughts** with Publisher* **Carl Ayers**. ■

Judge tosses FTC's private equity claims

The **Biden Administration's** crusade to roll back private equity's power in American healthcare markets has suffered its first defeat after a federal judge dismissed an antitrust suit against a fund manager that regulators claimed had formed an illegal monopoly on Texas anesthesiology practices.

The **Federal Trade Commission** filed suit against **Welsh, Carson, Anderson & Stowe** and the portfolio company it founded, **U.S. Anesthesia Partners**, last year (***RCW***, Oct. 10, 2024). Commission lawyers claimed Welsh, Carson's and USAP's years-long roll-up strategies violated Sec. 13(b) of the *FTC Act*. On May 13, U.S. District Judge **Kenneth Hoyt** dismissed the claims against Welsh, Carson.

Shares divested

Since forming USAP in 2012, Hoyt ruled, Welsh, Carson had divested most of its shares in the firm—it now owns 23% of the firm through one of its funds—and the FTC had not proved that Welsh, Carson's stake meant it could be held accountable for any ongoing (and yet-to-be-proven) anticompetitive behavior.

"The FTC's authorities discuss only one merger to roll back, where rolling back the merger resolves the ongoing violation," Hoyt wrote in his 23-page decision. "Not so here; the FTC's theory would require rolling back Welsh, Carson's

New FAQs on remote inspections' pilot

The FAQs are flying out of **FINRA** these days (see related story, page 6). The latest guidance out of the SRO touches on FINRA's remote inspections' pilot program. The temporary relief to conduct remote inspections of offices sunsets June 30, when firms can no longer fulfill inspection obligations remotely unless they elect to participate in the pilot program.

The May 13 release of the ***FAQs*** confirms that starting July 1, a firm that doesn't elect to affirmatively participate in the pilot program will be required to conduct inspections of all office and locations subject to rule 3110(c) in an "on-site manner."

Flexibility afforded

The three-year pilot program allows eligible firms the option of fulfilling their obligation under rule 3110(c) by conducting inspections of some or all branch offices, including offices of supervisory jurisdiction and non-branch locations remotely without on-site visits (***RCW***, Feb. 8, 2024). The pilot affords firms the flexibility to conduct inspections remotely or on-site, on a location-by-location basis.

Opt-in availability

FINRA noted that the pilot program doesn't change the current inspection cycles. The SRO reported that it is currently developing functionality in FINRA Gateway to allow firms to provide an "opt-in notice" to FINRA. It is anticipated that the functionality will be available to firms by June 1.

The 13 questions appearing in the FAQs also address additional enrollment and withdrawal issues, and data and information to be collected. FINRA said a core use of the data and information it receives will be used to "assess the effectiveness of remote inspections relative to on-site inspections to help shape any amendments to Rule 3110(c) that would help to modernize an inspection program in the evolving workplace environment."

acquisition of USAP stock and USAP's *own* acquisitions."

"Again," Hoyt added, "this Court will not be the first to use this specialized statute to expand antitrust liability to reach active investors in companies that are alleged to violate antitrust law. The FTC does not articulate why it cannot return with a new lawsuit under Section 13(b) if and when Welsh, Carlson signals – beyond mere speculation and conjecture – that it is actually about to violate the law."

A big win

Hoyt's decision allows the FTC to pursue its claims against USAP. It also points Washington's army of antitrust enforcers to potential suits against more hands-on fund managers. Yet it is still a big win for the private equity industry, which sees the FTC's crusade as an existential threat.

Among those fighting alongside Welsh, Carson was the **American Investment Council**. It filed a friend-of-the-court brief that urged Hoyt to toss the FTC's claims.

"Private equity investors have the same obligations as any market actors to abide by the antitrust laws, but they are entitled to the equal application of those laws," the brief stated. "Enforcement of those laws should be aimed at supporting competition, not at generalized and unfounded concerns about a business model. While it is not, of course, the role of courts to adjust a government agency's enforcement priorities, when those priorities are enforced through lawsuits based on novel liability theories without a sound basis – as is the case here… – courts should not allow such cases to proceed."

Investigations and inquiries

An FTC spokeswoman declined to comment. The agency has made clear that Welsh, Carson is only a small part of their order of battle. The Trade Commission, along with the **Justice Department** and the **Department of Health and Human Services** are in the middle of a public inquiry into private equity's role in healthcare (***RCW***, April 1, 2024). Separately, the Senate Budget Committee has opened its own investigation into private equity and healthcare.

In an e-mail, a Welsh, Carson spokeswoman said the firm was "gratified" by Hoyt's decision. **"**As we have said from the beginning, this case was without factual or legal basis," the spokeswoman said. ■

AI triggers advertising regulation FAQs

Artificial intelligence was flagged as an "emerging risk" in the *2024 FINRA Annual Regulatory Oversight Report* and the SRO cautioned that the use of AI tools "could implicate virtually every aspect of a firm's regulatory obligations." In a bid to inform on AI implications on advertising, **FINRA** released May 10 two new ***FAQs*** on advertising regulation tied to supervising chatbot communications and AI-created communications.

The first new FAQ addresses how a firm using AI technology to create chatbot communications with investors should supervise this activity. FINRA advises that "depending on the nature and number of persons receiving the chatbot communications, they may be subject to FINRA communications rules as correspondence, retail communications, or institutional communications." That means firms must supervise chatbot communications in accordance with applicable FINRA rules.

Reviewing correspondence

One of these rules cited by the SRO is rule 3110(b)(4). FINRA reminds that rule 3110(b)(4) requires firms to establish, maintain and enforce written procedures for the review of incoming and outgoing written (including electronic) correspondence relating to the firm's investment banking or securities business that must be appropriate for the firm's business, size, structure, and customers. The content also must be consistent with rule 2210(d).

The other new FAQ concerns whether a firm is responsible for the content of communications created using AI technology. FINRA confirms that "regardless of whether they are generated by a human or AI technology" firms are responsible for their communications.

AI-created communications

Firms must ensure that AI-generated communications they distribute or make available comply with applicable federal securities laws and regulations and FINRA rules, the SRO states. The obligation includes compliance with supervision requirements, applicable FINRA and **SEC** recordkeeping requirements, and content standards in rules 2210 and 2220. FINRA reminds that the content standards "generally require that communications be fair and balanced and prohibit the inclusion of false, misleading, promissory or exaggerated statements or claims."

In its annual regulatory oversight report, FINRA acknowledged that AI tools can create operational efficiencies and aid in better serving customers while cautioning that their development has been "marked by concerns about accuracy, privacy, bias and intellectual property, among others."

Broad implications

In addition to advertising, FINRA suggested that firms

should consider paying particular attention to these areas when considering use of AI:

- Anti-money laundering.
- Books and records.
- Business continuity.
- Customer information protection.
- Cybersecurity.
- Model risk management.
- Research.
- Regulation Best Interest.
- Supervision.
- Vendor management.

FINRA suggested that firms should keep an eye on the regulatory landscape for AI as "it may change as this area continues to develop." Interestingly, the SEC's latest Regulatory Flexibility agenda did not contain the Commission's proposed AI rule (***RCW***, Aug. 10, 2023). ■

SoFi self-reports on customer ID program

The San Francisco-based **SoFi Securities** self-reported to **FINRA** that third parties had fraudulently transferred funds from accounts at unaffiliated financial institutions without authorization to SoFi Money, the firm's cash management brokerage accounts. A subsequent investigation by the SRO led to charges of deficient customer ID and identity theft prevention programs and a $1.1 million fine assessed against the firm.

The enforcement action yet again offers the lesson learned to continually check the veracity of your automated processes and to scrutinize the work of your third-party vendors. FINRA found that SoFi's "largely automated process" to approve the opening of SoFi Money accounts was not "reasonably designed to verify the customers' identity." This flaw in the process made the new accounts vulnerable to fraud perpetrated by third parties using fictitious or stolen identities.

Transfers subsequently withdrawn

The ***settlement agreement*** reveals that over a five-month period covering December 2018 through April 2019, SoFi approved the opening of 800 accounts that third parties then used to transfer $8.6 million from the accounts of customers at other financial institutions without authorization. It was determined that $2.5 million of those transfers were subsequently withdrawn by the third parties from the SoFi Money accounts.

Remediation lessons

The withdrawal of the stolen funds was accomplished through ACH transfers, ATM withdrawals, and debit card purchases. Fortunately, SoFi responded relatively quickly once it detected the fraud. The steps taken, which offers additional lessons, included:

- Increasing its staff trained to review fraud alerts.
- Improving its CIP and ITPP systems and procedures.
- Upgrading its fraud identification tool to perform additional verification of customer identity.
- Changing its customer verification logic to systematically decline certain applicants.
- Hiring third-party consultants to help address the significant volume of fraud alerts that had been generated and assisting with SoFi's remediation efforts.
- Reviewing activity in thousands of high-risk accounts.
- Making the self-report to FINRA.

SoFi's identity theft prevention program also was found wanting by FINRA. The program issues resulted in the SRO charging the firm with violating rule 201 of Regulation S-ID and FINRA rule 2010.

Identity theft program expectations

Via the settlement, FINRA reminded that in designing its ITPP, firms are expected to "consider a number of factors, including the methods of accessing covered accounts, the detection of red flags of identity theft in connection with authenticating customers, the types of covered accounts it offers or maintains, and its previous experiences with identity theft."

The ***2024 FINRA Annual Regulatory Oversight Report*** (***RCW***, Jan. 11, 2024) contained a section devoted to the "emerging risk" of new account fraud that may warrant another look in the wake of the SoFi case. ■

Homeland Security proposes cyber rules

Thousands of fund managers and other companies would be required to report cyber-hacks to the federal government within 72 hours of learning about them, and to report any ransomware payments they make within 24 hours under new rules the **Biden Administration** is weighing.

Officials in the **Department of Homeland Security**'s **Cybersecurity and Infrastructure Agency** say the ***proposed rules*** will help the U.S. protect its "critical" infrastructure from cyber-baddies. They define a "critical" company as any firm that either a) is larger than a "small business" as defined by the **Small Business Administration**, or b) works in one or more of 13 different "critical" sectors, including financial services, healthcare, energy and transportation.

Under the proposal, a "critical" company would be required to notify CISA officials of a "substantial cyber incident" within 72 hours of learning about it. Companies would have to report any ransomware payments within 24 hours of paying them. The rules give CISA broad authority to enforce its rules and penalize companies for failing to report incidents properly. There are criminal penalties for anyone who lies or misleads regulators about the incidents.

As a practical matter, the new rules may sweep up thousands of private equity managers or their portfolio companies. CISA says the rules, as written, will affect more than 316,000 companies, and cost industry $1.4 billion over the next decade to implement. The rules are the most sweeping cyber regulations in U.S. history, and land atop of some three dozen already existing federal cybersecurity reporting rules across several agencies. Last summer, the **SEC** adopted ***similar rules***—with a 72-hour reporting window—for public companies.

"What we're seeing is more and more regulating bodies implementing reporting requirements with specific timelines," says **Jeremy Swan**, a partner with **CohnReznick**.

The emerging body of cyber laws and rules goes straight to the heart of funds' fiduciary duties, Swan says. "And part of that means protecting your investors' privacy," he says.

That, in turn, means private equity managers must take cybersecurity seriously, too, says **Emilie Abate**, a former SEC examiner who is now a director with compliance consulting firm **Iron Road Partners**. "You need firm leadership doing cybersecurity diligence," Abate says. "This is what your work is, every single day. It's definitely a senior leadership task."

"From an SEC perspective, they're certainly curious about whether your compliance officer is on top of this," Abate adds. "I think the SEC is still going to ask, 'How are you going to protect information of your investors?' Compliance staff need to be armed with enough information so that they can look at their programs annually and know where the gaps are."

A 'death knell'

In its rulemaking proposal, CISA cites a study it commissioned on the damage hackers cause to American business. The study found that between 2012 and 2021, there were 1,893 "cyber events" resulting in compromised firm data. System intrusion was the most common attack, accounting for nearly half of all incidents, and the average hack cost more than $25 million.

"What happens if they get into a portco and then can get into you, and access information on your investors?" CohnReznick's Swan says. "That's a death knell. Imagine if you're a private equity firm and you have CalPERS as an investor. If the hackers get into you and then swim upstream to CalPERS, good luck raising your next fund with CalPERS."

Indeed, last year, the SEC ***launched*** its own exam sweep of private funds, asking probing questions about how they were managing the risk of AI and monitoring their third-party IT vendors. Separately, the Commission is weighing rules that would require registered investment advisers – including some 5,600 private fund managers – to vet all their vendors for conflicts and other risks, and re-vet them regularly.

"Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors," Commission Chairman **Gary Gensler** said after he and his colleagues adopted the new public company reporting rules.

'A multiplier technology'

Artificial intelligence's scale also presents internal risks of its own, says **Mushegh Hakhinian**, chief information officer at **73 Strings**, a tech firm that offers valuation, data collection and monitoring software to private fund managers. "This is a force multiplier technology," Hakhinian says. "And a small private data leak, if ends up in an amplifier like AI, may have a huge impact."

At the same time, ransomware attackers have gotten more sophisticated in their demands. It's still rare that private equity managers carry cyber-insurance, Abate says, but one of the first places hackers have begun to look once they breach a company's defenses is at the company's insurance policies. The ransom demands increasingly conform neatly to the outlines of those policies, she says. ■