Jun. 4, 2026

Retailization

The SEC's Growing Focus on Retailization, AI, Cybersecurity and Private Credit

By Michael Washburn, *Hedge Fund Law Report*

A wave of developments at the SEC, including public speeches in favor of deregulation; guidance on cybersecurity and closed-end funds investing in private funds; and the agency's invitation of comments on adding private credit reporting to Form PF, are rich with implications for private fund managers. The current zeitgeist heavily favors broadening retail investor access to private funds and encouraging technological innovation in ways scarcely envisioned under prior administrations. At the same time, the agency maintains a firm stance on the need to tailor compliance programs for cybersecurity preparedness and to adopt best practices around artificial intelligence (AI), retailization and private credit.

All those points came across in a May 2026 media roundtable held by ACA Group, which featured Patrick Olson, vice chairman; Carlo di Florio, president; Aaron Pinnick, senior manager of thought leadership; Christine Tetherly-Lewis, partner and head of cybersecurity and the risk advisory division; and Nikolay Kojuharov, partner in product developments. This article summarizes key takeaways from their discussion.

See "New Guiding Principles and Priorities of the SEC Enforcement Division" (Apr. 9, 2026).

Growth of AI

The number of firms making use of AI in their day-to-day operations has grown dramatically in recent years, Pinnick observed. When ACA Group canvassed clients in 2023 to get a sense of how many of them used AI, about 20 percent said they made use of it, he shared. According to results from a 2026 survey, however, the number has grown to more than 80 percent, he said. Firms surveyed cited ChatGPT, Claude and Gemini as programs they made use of regularly, but that should not be taken to mean their AI is holistic across all research, analytical and compliance tasks, he added.

"It is a very broad trend in terms of adoption, but when you look at firms that are using AI for advanced or sophisticated use cases, that is very rare. Only about 11 percent of firms in our research

group use AI for some sort of client-based interaction," Pinnick observed. "There is not a lot of deep integration of AI, so AI adoption is a mile wide and an inch deep."

"That is not necessarily a bad thing, when you think of this new technology. Obviously, there should be rigorous coverage, rigorous testing, there should be a lot of caution when firms begin using" AI systems and protocols, Pinnick added.

Burden of Compliance

Yet another reason for the highly incremental, phased adoption of AI on the part of so many firms has to do with the circumspect approach of many compliance departments when it comes to the deployment and adoption of AI programs and models, Tetherly-Lewis shared. "The compliance side faces so much pressure to implement the tool, use the tool and create efficiencies around the tool that use cases have already been deployed," she said. However, there is still a learning curve, and some compliance teams are still "playing catch-up" when it comes to mastery of various AI uses and functions.

"They want to embrace the technology and want to support the endeavor" of broader AI adoption, Tetherly-Lewis observed. "But they're scratching their heads and saying, 'How do I know what data it's using? How can I be confident that there won't be data leakage? Who is using the AI, and what are the use cases? Do the use cases put us in jeopardy with potential regulatory issues?'"

Hence, Tetherly-Lewis said, she and her colleagues have been engaged in a heavy volume of conversations with clients seeking to understand not only the fast-evolving technology but also the corporate governance issues that come into play when a firm expands into AI or adds to an existing AI infrastructure. "We are seeing a proliferation of not just deploying a technology on everyone's desktop but also going in deeper, understanding the data that they are using and understanding every department's use case for adopting that technology and making sure that people are minding" all the nuances of AI use, she explained.

In some cases, Tetherly-Lewis added, people using AI are asking questions that they now realize ideally should have been asked sooner. "They are asking, 'Did we let this genie out of the bottle?'" she shared. "And you can't really put it back in. So the question now is, how do we go about making sure that people are good citizens about using the technology and making sure that the use cases are appropriate for the business in question?"

See "Benchmarking AI Uptake by Compliance Functions" (Dec. 4, 2025).

Increased Vigilance

Notwithstanding public statements from current SEC officials about fostering innovation, ensuring due process and avoiding regulation through enforcement, such granular attention to AI and its uses is not a luxury but a necessity for firms nowadays given the increasing attention that the SEC is paying to the issue, in di Florio's view.

Besides governance and an oversight framework, di Florio observed, the SEC is taking an increased interest in the model testing and validation systems and methodologies that firms use. "The SEC is also asking questions about cybersecurity and vendor management with regard to AI," he noted.

If a firm has been proactive about those areas, then that tends to suggest to the SEC that the firm "is trying to do the right thing around AI in terms of governing and controlling its use," di Florio shared. "But if the firm doesn't have an answer about its approach to these issues – or has only thought about the front-end use cases but not really the importance of governance and controls – then that can raise concerns."

Rather than undertaking active investigations into such matters, the SEC's stance on the issue at present is generally one of cautious inquiry through examinations, di Florio posited. "The SEC has continued to look at AI practices through its exam program. It's possible that, at some point, they may publish a risk alert sharing key observations from the exams, both in terms of potential areas of deficiency and effective practices that they observed," he opined.

The issue is particularly acute for U.S.-based entities that have offices and/or nexuses of operations in foreign jurisdictions, Tetherly-Lewis added. In some instances, the strictness of regulations overseas may even present a case of "the tail wagging the dog," in which a relatively small foreign office of a large stateside firm shoulders the largest compliance burden and helps guide and shape compliance for the entire organization, she shared.

See "The Core Benefits and Burdens of AI Use in Financial Services" (Apr. 23, 2026).

"We're seeing huge responsibilities [come into play] with AI and its influence on third parties," Tetherly-Lewis observed. She cited "third-party regulations in the European Union, all over the United Arab Emirates and on the part of the Dubai Financial Services Authority and the Financial Services Regulatory Authority in Abu Dhabi."

"And so the pressure is there, if there is an extended presence on the part of U.S.-based companies, even if the SEC may not yet apply quite the same pressures," Tetherly-Lewis reflected. "We're seeing offices of companies in those regions grapple with those regulatory pressures."

Third-Party Exposure

Many firms still have a lot of catching up to do with regard to their third-party exposure, Pinnick said. A recent ACA Group survey found that only 24 percent of respondent firms had a policy in place addressing the use of AI on the part of third parties, he noted.

"Now we have machines talking to each other, potentially sharing customer information. So, again, the issue here goes back to governance. It goes back to establishing access controls, policies and procedures and rigorous testing and monitoring of your third parties," Pinnick observed. "There may not have been enforcement actions yet" directly related to the issue, "but I expect that the SEC would treat third-party vendors that have access to customer information, and are putting an AI tool to use, the same as any other third party."

The third-party issue is all the more urgent given the growing burdens that AI operations and compliance are placing on many firms in the market, Kojuharov noted. The challenges of integrating multiple data sources to harness the full power of AI has driven a shift in their approach to the logistical side of AI adoption, he said. "They shift from actually doing the work to supervising and guiding big AI, which is performing the work," he stated.

With that shift comes an array of subsidiary questions, continued Kojuharov. "Are they going to build the infrastructure themselves? Are they going to handle compliance themselves? A lot of firms don't have massive IT divisions that can just dedicate themselves to compliance," he noted.

"Early on, a lot of firms were really afraid to use external AI. There were a lot of concerns about privacy and using sensitive data to train models and data escaping through the models," Kojuharov elaborated. "But these days, the concerns are more and more about burglars – third parties – stealing data, and that is adding other challenges. Firms sometimes use AI vendors that they don't really have control over. And that adds complexity around transparency, validation and accountability."

See "Contracting With Vendors to Mitigate Third-Party AI Risk" (May 21, 2026).

Regulation S-P

In di Florio's view, the responsibility to ensure the cybersecurity and oversight of third-party relationships is even more important given the SEC's May 16, 2024, adoption of enhancements to Regulation S-P, which expanded what were already quite considerable responsibilities on the part of firms following the detection of a cyber breach. Those enhancements added a requirement for firms to have policies and procedures in place that are reasonably designed to notify customers of a breach as soon as practicable and not more than 30 days after the detection of the breach. The customers to be notified include all whose sensitive data was, or was reasonably likely to have been, affected by the incident.

See "Best Practices for Complying With Regulation S-P's New Notification Requirements" (Feb. 12, 2026).

In the context of Regulation S-P and other rulemakings and enhancements of existing rules, the SEC tends to pursue a graduated approach to scrutinizing market participants – "conducting initial examinations to understand how firms are complying with the new requirements and then following up with more in-depth exams and scrutiny," di Florio shared. "Regulation S-P has led many firms to map out and understand where specifically they have sensitive customer information stored, both internally at the firm as well as with third-party vendors and service providers."

"First and foremost, clients have to get their hands around all of their vendors. Then they have to figure out what kind of data they have" entrusted to those vendors and track the uses and security of that data, Tetherly-Lewis concurred. In some cases, that diligence may entail reassessing which vendor relationships are considered important and which are seen as minor, she elaborated. In the context of cybersecurity and Regulation S-P compliance, there is really no such thing as an inconsequential vendor relationship.

"Historically, many firms were focused on making sure that their 'top' vendors – the vendors that potentially had data that they were nervous about – were well cared for, but those middle-tier or lower-tier vendors, not so much," Tetherly-Lewis reflected. "This Regulation S-P update has definitely called to the forefront the need to look at all of them, A to Z," with the same thoroughness and acuity, she stressed.

"Get them all in one place, identify the data, chart it, do the data mappings," Tetherly-Lewis advised. "Now add a column to find out if they have AI tools. And, if so, are there AI disclosures? Have you tracked that? Is that a diligence priority for the firm? So this [compliance area] just continues to add more 'clicks,' in terms of the responsibility."

See "SEC Staff Discuss Regulation S-P Amendments and Related Examination Processes" (Oct. 23, 2025).

Retailization

401(k) Plans and Alternative Assets

As the administration of President Donald J. Trump, the SEC and the Department of Labor (DOL) revise existing rules and propose new rules in favor of facilitating greater retail investor access to the private funds realm, "there has never been so much support behind enabling retail investors to access alternative investments," observed di Florio.

"We've had prior iterations of trying to get to retail alts, but here you have got an executive order from the White House, saying, 'We think retail investors in America should have access to alternative investments,'" di Florio noted, alluding to the president's August 7, 2025, executive order, "Democratizing Access to Alternative Assets for 401(k) Investors."

The DOL, on March 30, 2026, put forward a proposed rule (Proposal) setting forth steps that managers of employer-sponsored 401(k) plans must follow to incorporate alternative assets into plans they manage in accordance with the terms of the Employee Retirement Income Security Act of 1974 (ERISA). Among other provisions, the Proposal would establish safe harbors that such fiduciaries can use to avoid any claims they have violated their duty of prudence in the course of selecting alternative assets to include in their plans, di Florio noted.

See our two-part series on the SEC Private Markets Roundtable: "Valuation and Liquidity Concerns in Retailization of Private Markets" (Apr. 23, 2026); and "Fund Governance Issues for Retailization of Private Markets" (May 7, 2026).

The SEC and CE-FOPFs

Although the full implications of the DOL's Proposal – and whether it will become law as written – remain to be seen, the SEC's views are at least partly aligned when it comes to the desirability of expanding retail investor access to private funds, continued di Florio. One important sign here was

the SEC's release of Accounting and Disclosure Information 2025-16 (ADI), which reversed the agency's longstanding position on registered closed-end funds that invest in private funds (CE-FOPFs).

For more than two decades, CE-FOPFs that invested more than 15 percent of their assets in private funds had been required to market and sell only to investors meeting the "accredited investor" standard as set forth in Regulation D under the Securities Act of 1933 and who made initial investments of at least $25,000. Taking into account far-reaching changes in CE-FOPF regulation since the first registration statement of such a vehicle in 2002, the ADI decreed that the agency will no longer provide comments requiring CE-FOPFs to either keep the investor threshold at that level or limit their investments to 15 percent of their assets.

"So now the door is wide open for closed-end funds, such as interval funds, tender offer funds and business development companies, to become the vehicles of choice to provide retail investor access to alternative investments," di Florio noted. "And they are also revising co-investment rules to permit registered funds to co-invest with private funds, which is significant relief."

"At the same time that the government is expanding retail investor access to alternative investments, we have seen significant investor and market concerns in the private retail space and with regard to valuations in the private fund space more broadly," continued di Florio. "What the SEC is very focused on now are the guardrails to address valuation, liquidity, conflicts of interest, performance and marketing, among other issues."

See "SEC Eases Some Requirements for Registered Closed-End Funds Investing in Private Funds" (Nov. 6, 2025).

Private Credit

Yet another significant development on the retailization front is the SEC's decision, in recently proposed changes to Form PF, to invite comments on including private credit as a category in which firms can report information to assist regulators in monitoring systemic risk, di Florio observed. "The SEC chair has said they do not see systemic risk issues in the private credit market at present, but they are closely evaluating and monitoring private credit."

"Private credit is an asset class that is perfectly aligned with retirement, in terms of being a long-term asset versus a long-term liability," Olson concurred. "It is a massive market – about $20 trillion in size."

Change in Focus

The SEC's openness to retailization and general alignment with the pro-business and anti-overreach stance of the current administration is also evident in its new memorandum of understanding with the CFTC and its release of its fiscal year 2025 enforcement results, both of which articulated a

shift in its approach to enforcement matters – emphasizing the pursuit of serious cases of fraud and investor harm, while de-emphasizing "novel cases of negligence or broken-window violations," di Florio acknowledged. "This is a significant departure from the enforcement approach of the prior Gensler administration."

See "SEC's Latest Enforcement Results and Budget Request Affirm Focus on Fraud" (May 21, 2026).