Securities Regulation Law Journal

Volume 52 Number 3 Fall 2024

Thomson Reuters™

Quarterly Survey of SEC Rulemaking and Major Court Decisions (April 1, 2024 – June 30, 2024)

By Kenneth M. Silverman and Kerrin T. Klein[*]

This issue's Survey focuses on the U.S. Securities and Exchange Commission's ("SEC") rulemaking activities and other decisions relating to the Securities Act of 1933, as amended (the "1933 Act"), the Securities Exchange Act of 1934, as amended (the "1934 Act"), and other federal securities laws from April 1, 2024 through June 30, 2024.

This quarter, the SEC proposed one new rule and approved two final rules. In relevant part, this quarter the SEC has largely focused on addressing the increased security threats and potential of criminal activity faced by the nation's financial systems and its customers.

Final Rule

Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

On May 16, 2024, the SEC adopted amendments to Regulation S-P for the first time since the privacy-focused rules were originally adopted in 2000. In notable part, the amendments mandate that broker-dealers (including fund portals), investment companies, registered investment advisers ("RIAs") and transfer agents (collectively, "covered institutions") adopt incident response programs that are reasonably designed to detect and address security breaches of customer information. Additionally, the amendments expand the scope of the safeguards and disposal rules set forth under Regulation S-P, set new standards for recordkeeping and modify Regulation S-P's annual privacy notice delivery requirements.

Regulation S-P governs how certain financial institutions treat customers' non-public personal information. As originally adopted, Regulation S-P is composed of three major provisions: (i) a requirement that covered institutions adopt written policies

---

[*]Mr. Silverman and Ms. Klein are members of the New York Bar and Partners at Olshan Frome Wolosky LLP. Associates Zachary Freedman, Tamar Prince and Law Clerk Samantha Haquia assisted the authors.

reasonably designed to protect customer records and information (the "safeguards rule"); (ii) a requirement that covered institutions properly dispose of consumer report information to protect against unauthorized access or misuse (the "disposal rule"); and (iii) a requirement that broker-dealers, investment companies and RIAs provide an annual privacy policy notice to customers, subject to opt-out provisions implemented by Congress in the Fixing America's Surface Transportation Act of 2015.

Seeking to modernize Regulation S-P in response to significant technological developments in how financial institutions obtain, share and manage customers' personal information in the last 20 years, the SEC first proposed amendments to Regulation S-P on March 15, 2023. The final amendments largely mirror those initially proposed by requiring financial institutions to: (i) develop incident response programs that address incidents of unauthorized access to or use of customer information; (ii) expand the scope of protections of the safeguards and disposal rules established under Regulation S-P; and (iii) modify certain recordkeeping and notice requirements.

Incident Response Program

The final rule requires that covered institutions establish and implement written policies and procedures to create incident response programs that address and prevent breaches of customer information. An incident response program must be reasonably designed to detect, respond to and recover from unauthorized access to or use of customer information. The SEC recognized in the adopting release that covered institutions need flexibility to adopt programming that suits their size and the scope of their activities. Thus, the final amendments establish general elements that covered institutions must follow in establishing an incident response plan regarding assessment, containment and control, notice and applicability to third-party service providers.

The final rule mandates that incident response programs assess the nature and scope of incidents involving unauthorized access to or use of customer information and identify the "customer information systems" that may have been accessed or used. The rule defines the term customer information (except as it pertains to transfer agents) as any record of a covered institution containing non-public personal information about a customer (i.e., a consumer who has a customer relationship with the institution) in any form that is possessed by the covered institution or handled on its behalf. For transfer agents, the definition of customer information is identical with the exception that a customer is defined to be any natural person who is a security holder of an issuer for which the transfer agent acts. The rule

references the term "sensitive" customer information as information that, alone or in conjunction with any other information, could create a reasonably likely risk of substantial harm or inconvenience to the individual identified with the information. The SEC declined to define "substantial harm or inconvenience," concluding that a covered institution's determination of whether a release of specific information could create a substantial risk of harm or inconvenience is ultimately a fact-specific inquiry. To properly assess and identify any potential incident, covered institutions must be able to identify the types of customer information used (i.e., standard "customer information" versus "sensitive" customer information) and the information systems that may have been accessed.

Incident response programs must include appropriate steps to contain and control a security incident. The goals of containment and control are to mitigate the immediate impact of a security incident and prevent further loss of customer information or systems integrity. In the high-pressure environment following an identified security incident, containment and control procedures must provide a framework to expedite remediation. The SEC provided a few examples of strategies in the final rule that covered institutions may use for containing and controlling an incident, including isolating compromised systems, enhancing the monitoring of intruder activities, searching for additional compromised systems or changing system administrator passwords.

Covered institutions must provide clear and conspicuous notice to affected individuals whose *sensitive* information may have been used or accessed, with some narrow exceptions. The final rule requires that incident response programs address incidents involving any form of customer information, but notification under such programs is only required when there has been a breach or misuse of sensitive customer information. Notice is presumptively required once a security incident that involves sensitive customer information has occurred. However, this presumption may be rebutted if the institution conducts a reasonable investigation and concludes that sensitive customer information has not been, or is not reasonably likely to be, used in a manner that would result in substantial harm.

If a covered institution cannot identify the specific individuals whose information may have been subject to unauthorized use or access, the institution must provide notice to all individuals whose information resides in a system that was, or may have been, compromised. The notice must include details about the incident, the breached data, how affected individuals can respond to the breach to protect themselves (e.g., by placing a fraud alert

on their accounts), and how affected individuals can contact the covered institution to discuss the incident. Moreover, institutions are required to provide notice as soon as practicable, but no later than 30 days after the covered institution learns that a security incident has occurred or is reasonably likely to have occurred. Notice may be delayed in very limited circumstances, such as in the event of a major customer security breach where the U.S. Attorney General determines that notice within the 30-day timeframe would pose a substantial risk to national security or public safety.

Incident response programs must include establishing and enforcing written policies designed to require monitoring of service providers. A service provider is "any person that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution." Although covered institutions are not required to enter into a written contract with service providers to provide notice to affected individuals in the event of a data breach, a covered institution's written policies and procedures must be designed to ensure the protection against unauthorized access to or use of customer information and prompt notification to the covered institution in the event of a security breach. This includes a mandatory provision that a service provider used by a covered institution must provide notice to such covered institution in the event of security breaches of its own "as soon as possible, but no later than 72 hours" after becoming aware of a security breach resulting in unauthorized access to a customer information system maintained by such service provider.

Safeguards and Disposal Rules

The final rule primarily modifies the safeguards and disposal rules under Regulation S-P by broadening the scope of both rules to apply to the information of a covered institution's own customers and to the information of customers of other financial institutions. Each rule provides requirements that covered institutions (now including transfer agents) adopt written policies and procedures (in addition to those policies and procedures to be established in connection with incident response programs) to protect the maintenance and disposal of customer records and information. Customer information is protected under the safeguards and disposal rules, regardless of whether that information pertains to "(a) individuals with whom the covered institution has a customer relationship or (b) the customers of other financial institutions where such information has been provided to the covered institution." As noted above, the definition of "customer information" is expanded under the final rule to include

information that is handled by service providers or other third parties. For covered institutions, other than transfer agents, "customer information" means "any record containing non-public personal information about a customer of a financial institution, whether in paper, electronic, or other form."

Prior to adoption of the final rule, the safeguards rule did not apply to transfer agents, and the disposal rule applied only to transfer agents registered with the SEC. The final rule establishes that both the safeguards and disposal rules apply to transfer agents, even if the transfer agent is registered with another regulatory agency. The SEC reasoned that the rules should apply equally to transfer agents, where systems maintained by transfer agents are subject to the same threats Regulation S-P aims to address. Considering the nature of transfer agents' work, the SEC adopted a definition of "customer" that is unique to transfer agents as described above (i.e., "any natural person who is a securityholder of an issuer for which the transfer agent acts or has acted as a transfer agent").

Recordkeeping and Annual Privacy Notice Requirements

The final rule requires that covered institutions make and maintain written records documenting compliance with the safeguards and disposal rules. The stated purpose of the recordkeeping requirements is to ensure that covered institutions have the records necessary to assess the effectiveness of their safeguarding and disposal programs. The recordkeeping requirements vary by covered institution. For example, registered and unregistered investment companies must generally keep records for six years, with the most recent two years kept in an easily accessible place. For RIAs, this requirement is for five years, and for broker-dealers and transfer agents it is three years. RIAs, broker-dealers and transfer agents must also keep the most recent two years of records in an easily accessible place.

Before the adoption of the final rule, Regulation S-P required broker-dealers, investment companies and RIAs to provide customers with annual notices regarding the institution's privacy practices ("annual privacy notice"). Institutions may be exempt from the annual privacy notice requirement if the institution (1) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (2) the institution has not changed its policies and practices about disclosing non-public personal information from its most recent disclosure sent to customers.

Though the final rule substantially mirrors the amendments as proposed, the SEC made certain changes in response to public comment. In particular, the final rule eliminates the proposed

requirement that covered institutions enter into written agreements with service providers to protect customer information and streamlines the proposed notification requirements. When initially proposed in 2023, individual and public interest group commenters generally supported the amendments. However, several industry commenters expressed concern about how the amendments, as proposed, might create redundant or conflicting obligations for covered institutions. For example, commenters noted that state laws regulating data breaches already address the issues raised in the proposed amendments. The SEC reasoned that because state laws are inconsistent on the issues addressed in the proposed amendments, the amendments will provide for more robust consumer protections nationwide. Additionally, commenters posited that the notice requirements may have conflicted with other statutes and federal safeguarding standards, like the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and the Consumer Financial Protection Bureau rules. Seeking to resolve the commenters' concern about conflicting or redundant requirements, the SEC edited the final amendments to align with corresponding standards set by other federal regulatory agencies.

Effective Dates

The final rule was published in the Federal Register on June 3, 2024, and will become effective on August 2, 2024. In response to certain public comments to the proposed amendments regarding the compliance burden these amendments will impose, for "larger entities" including investment companies with net assets of $1 billion or more, RIAs with $1.5 billion or more under management and all broker-dealers and transfer agents that are not small entities under the 1934 Act for purposes of the Regulatory Flexibility Act, such institutions will be required to start complying with the final rule by February 2, 2026. Small covered institutions will be required to start complying with the final rule by August 2, 2026.

Proposed Rule

Customer Identification Programs for Registered Investment Advisers and Exempt Reporting Advisers

On May 13, 2024, the SEC and the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") jointly proposed a new rule that would require RIAs and exempt reporting advisers ("ERAs") to establish written customer identification programs ("CIPs"). The proposed rule aims to provide further safeguards against illicit finance activity in the investment adviser industry.

In February 2024, the U.S. Department of Treasury issued its 2024 Investment Adviser Risk Assessment, which identified that the investment adviser industry has served as an entry point into the U.S. market for illicit proceeds associated with foreign corruption, fraud and tax evasion. Shortly thereafter, FinCEN proposed a rule to designate RIAs and ERAs as "financial institutions" under the Bank Secrecy Act of 1970, as amended (the "Bank Secrecy Act"), and subject such entities to several requirements, including anti-money laundering ("AML") and countering the financing of terrorism ("CFT") program requirements. As part of this February 2024 proposal, FinCEN would be required to "prescribe rules that establish minimum standards for covered investment advisers regarding the identities of customers when they open an account." The rules jointly proposed by FinCEN and the SEC in May 2024 set forth these minimum standards. If adopted, the rule will require RIAs and ERAs to implement a CIP that includes customer verification procedures. Additionally, RIAs and ERAs will have to maintain records of information used to verify customer identity, in a manner that is largely consistent with existing CIP requirements for entities such as broker-dealers. Of note, RIAs and ERAs have not previously been subject to CIP requirements, though many advisers likely have identification verification systems in place.

Proposed CIP Requirements

Under the proposed rule, RIAs and ERAs would be required to implement a written CIP that includes "reasonable procedures" for verifying the identity of persons seeking to open an account "to the extent practicable." The SEC makes clear in the proposed rule that the CIP is not a separate program but should be incorporated into an investment adviser's existing AML and CFT programs.

The proposed rule sets forth four main minimum CIP requirements: (i) identification verification; (ii) risk assessment; (iii) recordkeeping; and (iv) notice. Regarding identification verification, a CIP would need to include procedures to verify the identity of customers within a reasonable time before or after the customer's account is opened. At a minimum, the investment adviser must obtain the customer's name, date of birth for an individual or the date of formation for any person other than an individual, address and identification number, which could be an individual's social security number or an entity's taxpayer identification number. Advisers may verify identifying information through documents, non-documentary means or both. At the verification stage, a CIP should include procedures for determining whether a customer appears on any government list of known or suspected terrorists or terrorist organizations.

In creating a CIP that complies with the minimum requirements noted above, the proposed rules prescribe that RIAs and ERAs should ensure that their CIPs are informed by the relevant risks specific to their business. Risk factors may include the types of accounts managed, the methods of opening accounts, the various types of identifying information available, and the adviser's size, location and customer base. Under the proposed rule, an investment adviser should obtain additional information in its CIP if, after considering these risk factors, they determine that additional information is required to form a reasonable belief that the adviser knows the true identity of the customer.

An investment adviser's CIP would also need to include procedures for (i) verifying customer's identity and assessing risks and (ii) creating and maintaining a record of all information collected at the verification and risk assessment stages. Generally, investment advisers would be required to retain this information while the account remains open and for five years after the account is closed.

Finally, investment advisers would be required to notify customers that customer information is being requested to comply with the proposed rule. Notice may be posted on a website, inserted in an account application or through any other form of written or oral notice. The proposed rules do not require a review of already-opened accounts unless an investment adviser cannot ascertain the true identity of a customer using the identity verification methods noted above. In such instances, and with the exception of trusts or similar beneficiary accounts, an investment adviser would be obligated to seek further information regarding the identity of the customer, including following the due diligence process set forth in the CIP for new customers.

The SEC noted in the proposed rule that there may be instances when an adviser relies on another financial institution for some or all elements of a CIP process in a manner that seeks to protect institutions from engaging in duplicative or unnecessary efforts. The proposed rule permits reasonable reliance on information provided by other institutions so long as the other institution is also required to adhere to AML/CFT compliance program requirements under the Bank Secrecy Act. Additionally, there must be a contract between the parties that requires annual certification to the RIAs or ERAs that the other party has implemented a compliant AML/CFT program and will perform the requirements of the RIAs' or ERAs' CIP. Under these circumstances, RIAs and ERAs would not be held responsible for failures of contracted financial institutions to fulfill such CIP responsibilities.

The comment period for the proposed rule ends on July 22, 2024.

On the Horizon

Spring 2024 Reg-Flex Agenda

On July 8, 2024, the SEC released its Spring 2024 Reg-Flex Agenda (the "Spring Agenda"), which included proposed and final rules the SEC expects to consider in the next 12 months.

The forthcoming SEC rule proposals noted in the Spring Agenda cover a broad array of topics including data collection and incentive-based compensation practices, and many seek to require increased disclosure requirements in contentious areas such as board and nominee diversity and human capital management. The proposed rules noted in this release are expected to be released for public comment between October 2024 and April 2025 but may be delayed or redeveloped as the Spring Agenda was drafted prior to recent decisions of the U.S. Supreme Court in late June 2024.

Major Court Decisions

U.S. Supreme Court Holds that Pure Omissions Are Not Actionable Under Rule 10b-5(b)

On April 12, 2024, the Supreme Court of the United States held that pure omissions are not actionable under Securities and Exchange Commission (the "SEC") Rule 10b-5(b). The Court found that the U.S. Court of Appeals for the Second Circuit erred in concluding that omissions of statements in violation of Item 303 could sustain a claim under § 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5(b). Writing for a unanimous court, Justice Sonia Sotomayor explained "Rule 10b-5(b) . . . covers half-truths, not pure omissions . . . [because] the Rule requires identifying affirmative assertions (*i.e.*, 'statements made') before determining if other facts are needed to make those statements 'not misleading.' "

Petitioner Macquarie Infrastructure Corporation ("Macquarie") owns a subsidiary whose largest product is storage terminals for a particular type of fuel oil, No. 6 fuel oil, containing a typical sulfur content of about 3%. In 2016, the United Nation's International Maritime Organization adopted IMO 2020, a regulation that capped sulfur content in fuel oil at 0.5% by 2020. Following its adoption, Macquarie did not mention IMO 2020 in any of its public offering documents. However, in February 2018, Macquarie announced that the storage capacity contracted for use by its subsidiary's customers dropped in part due to the decline in the No. 6 fuel oil market, and Macquarie's stock price fell by approximately 41%.

Because Item 303 requires companies to disclose known trends likely to impact revenue, Respondents Moab Partners, L.P. ("Moab") et al. argued that the omission of IMO 2020 from Macquarie's public offering documents violated disclosure obligations of Item 303, and thus violated Rule 10b-5(b). The U.S. District Court for the Southern District of New York dismissed Moab's complaint and the Second Circuit reversed. On appeal, the Supreme Court considered whether a company's failure to disclose information required by Item 303 can support a private cause of action under Rule 10b-5(b), even if the omission does not make any "statement made" misleading.

The Supreme Court held that Rule 10b-5(b) does not impose liability for pure omissions, even if those omissions may violate Item 303. Instead, the plain language of Rule 10b-5(b) prohibits only half-truths: "representations that state the truth only so far as it goes, while omitting critical qualifying information." Notably, other provisions of the Securities Act of 1934 explicitly impose liability for plain omissions, particularly Section 11(a), which prohibits a registration statement that "omit[s] to state a material fact required to be stated therein." The absence of similar language in § 10(b) and Rule 10b-5(b), the Court concluded, suggests that neither Congress nor the SEC intended for these provisions to create liability for pure omissions.

To illustrate the distinction between actionable half-truths and non-actionable pure omissions, Justice Sotomayor, writing for the Court, provided an analogy: "[T]he difference between a pure omission and a half-truth is the difference between a child not telling his parents he ate a whole cake and telling them he had dessert." The Court ultimately held that a pure omission does not give rise to liability under Rule 10b-5(b). The Court did not opine whether half-truths, rather than pure omissions, could give rise to liability under the facts alleged in this case. The Court also did not opine on whether Rules 10b-5(a) and 10b-5(c) support liability for pure omissions.

Macquarie Infrastructure Corporation et al. v. Moab Partners, L.P. et al., Case No. 22-1165, in the Supreme Court of the United States.

Second Circuit Holds Amended Schedule 13D Can Moot Claims Alleging Section 13(d) Violation

On May 20, 2024, the U.S. Court of Appeals for the Second Circuit affirmed the judgement of the U.S. District Court for the Southern District of New York, which dismissed as moot Plaintiff-Appellant Nano Dimension Ltd.'s ("Nano") claims that Defendants-Appellees Murchinson Ltd., EOM Management LTD, Nomis Bay Ltd., BPY Limited Boothbay Fund Management, LLC,

Boothbay Absolute Return Strategies, LP, Boothbay Diversified Alpha Master Fund, LP, Anson Advisors Inc., Anson Funds Management LP, and Anson Management GP LLC (collectively, the "Defendants") violated Section 13(d) of the Securities Exchange Act of 1934 by failing to disclose group status in their Schedule 13D filings. Further, the Second Circuit held that the alleged Section 13(d) violation was cured when Defendants amended their Schedule 13D filings by attaching Nano's complaint and asserting that the allegations contained therein were without merit. Additionally, the Second Circuit denied Nano's claims for retroactive relief, citing as dispositive the effective Schedule 13D amendments, a lack of irreparable harm, and no change in control.

Plaintiff-Appellant Nano is an Israeli 3D printing and manufacturing company that trades on the NASDAQ stock exchange. In September 2022, Defendants collectively acquired more than five percent of Nano's American Depository Shares (ADSs). On January 22, 2023, Murchinson called for a special meeting ("Special Meeting") of Nano's shareholders, which was held in March 2023 and involved the election of two of seven directors. On January 23, 2023, Murchinson filed its initial Schedule 13D.

Nano then brought suit against Defendants pursuant to Section 13(d), alleging Defendants started violating Section 13(d) when they collectively acquired more than five percent of Nano's ADSs. Nano sought an order directing Defendants to disclose their group status on amended Schedule 13Ds and an injunction prohibiting Defendants from acquiring more ADSs or voting their existing ADSs pending the amended filings. Thereafter, Defendants amended their Schedule 13D filings, which attached Nano's complaint and disputed the allegations therein. The District Court dismissed Nano's Section 13(d) claims with prejudice, finding they were moot following Defendants' amended filings. On appeal, the Second Circuit considered two issues: first, whether Defendants' amended Schedule 13Ds were ineffective because they merely disclosed and denied Nano's allegations, but did not disclose whether Defendants were acting as a group, and second, whether Nano should be entitled to equitable relief, namely the recission of Defendants' ADSs and the vacatur of their votes at the Special Meeting.

As to the first issue, the Second Circuit found that Defendants' amended Schedule 13Ds were effective because the filings served the informative purpose of Section 13(d). The amended filings disclosed the possibility of a disputed fact. Moreover, the Second Circuit relied on *Avnet, Inc. v. Scope Industries*, 499 F. Supp. 1121, Fed. Sec. L. Rep. (CCH) P 97691 (S.D.N.Y. 1980), to support the conclusion that in instances of a good faith dispute as to

group status, an amended Schedule 13D appending the complaint and disputing plaintiff's allegations satisfies Section 13(d).

As to the second issue, the Second Circuit held that Nano was not entitled to equitable relief. Since the required disclosures were made, Nano failed to show the irreparable harm required to receive an injunction for a Section 13(d) violation. Additionally, the Second Circuit has previously held that Nano's requested relief—"injunctive share sterilization"—is unavailable where, as here, corrective disclosures have been made, the vote in question did not affect a change in control over the issuer, and the vote in question has already taken place. In its decision, the Second Circuit affirmed the District Court's order and reiterated that amendments to Schedule 13Ds can serve as effective remediation in the face of potential Section 13(d) violations.

Nano Dimension Ltd. v. Murchinson Ltd. et al., Case No. 23-1141-cv, in the U.S. Court of Appeals for the Second Circuit.

Fifth Circuit Vacates SEC Rule Regarding Private Fund Advisers

On June 5, 2024, the U.S. Court of Appeals for the Fifth Circuit vacated a final rule promulgated by the Securities and Exchange Commission ("SEC" or "Commission") in August 2023. The rule, entitled "Private Fund Advisors; Documentation of Registered Investment Adviser Compliance Reviews" (the "Final Rule"), related to the regulation of private fund advisers. The Fifth Circuit found that the Commission lacked the statutory authority to enact the Final Rule under Section 211(h) and Section 206(4) of the Investment Advisers Act ("Advisers Act"). The three-judge panel unanimously agreed with Petitioners, which included the National Association of Private Fund Managers, noting that the statutory provisions the Commission cited to have "nothing to do with private funds."

In February 2022, the Commission proposed a new rule under the Advisers Act, which the Commission stated aimed to prevent fraud in the private fund advisor industry, citing Section 211(h) and Section 206(4) of the Advisers Act as support for its statutory authority. After the public comment period ceased, the SEC formally adopted the Final Rule in August 2023. Shortly thereafter, Petitioners sued the SEC, challenging the rule on the basis that the Commission exceeded its statutory authority and that the rule was "arbitrary and capricious" under the Administrative Procedure Act. The prevailing issue facing the Fifth Circuit was whether Sections 211(h) (codifying Section 913(h) of the Dodd-Frank Act) and 206(4) of the Advisers Act provided the SEC with the statutory authority to promulgate regulations of private fund advisers.

The Fifth Circuit vacated the Final Rule, noting that neither Section 211(h) nor Section 206(4) of the Advisers Act authorized the Commission to promulgate it. Importantly, the Fifth Circuit rejected the Commission's argument that Section 211(h) of the Advisers Act applies to private investors, noting that the plain language of the provision applies only to retail customers and not private investors. Thus, the Commission did not have statutory authority to promulgate a Final Rule regarding private fund investors under Section 211(h).

As to Section 206(4), the Fifth Circuit also rejected the Commission's argument that this provision granted the SEC with the statutory authority to promulgate the Final Rule to prevent fraud. Notably, the court found that the SEC failed to articulate a rational link between the Final Rule and the prevention of fraud. Since Section 206(4) requires the Commission to define a practice as "fraudulent, deceptive, or manipulative" before promulgating a rule to prevent such practice, the statute did not authorize the Final Rule without a rational link. Furthermore, the Fifth Circuit concluded that Final Rule is not "reasonably designed" to address fraud as required by Section 206(4) because private funds are exempt from federal regulation of their internal governance structure. In its opinion, the Fifth Circuit decidedly vacated the Commission's Final Rule regulating private fund advisers, marking another instance in which a federal court strikes down the Commission's rulemaking.

National Association of Private Fund Managers et al. v. Securities and Exchange Commission, Case No. 23-60471, in the U.S. Court of Appeals for the Fifth Circuit.