Regulatory Compliance Watch

January 22, 2024 • **Insight, guidance and best practices**

SUBSCRIBER-REQUESTED STORY

Backtesting to satisfy SEC valuation rule

A common method of testing the accuracy of a fund's valuation is backtesting—essentially comparing the price a security sold at with what the fund adviser's fair valuation method came up with.

If you scour Investment Company Act ***rule 2a-5*** (fair value determination and readily available market quotations), which took effect in 2022, you won't find the word "backtesting." But the rule does require fund boards or their designees (often a fund's investment adviser) to periodically review "the appropriateness and accuracy of the [fair value] methodologies selected and making any necessary changes or adjustments."

Gotta love 'flexibility'

The ***final rule***'s release gave the **SEC** an opportunity to "clarify" its position on backtesting. "While we believe that calibration and back-testing are methods that should be used for testing the appropriateness and accuracy of funds' fair value methodologies in many circumstances, the final rule does not require calibration and back-testing …. The final rule provides flexibility to allow funds to use new, appropriate testing methods."

Flexibility carries the day. "The SEC does not require a specific method or frequency" of testing, says **Paul Balynsky**, CFA, CPA/ABV managing director at **Valuation Research Corporation** in New York. The onus falls upon the mutual fund board to lay out the valuation process—or its designee.

Backtesting is "the predominant way of doing testing," states **Benjamin Haskin**, a partner with **Willkie Farr & Gallagher** in Washington, D.C. "It's the most intuitive testing that you could do," comparing actual transactions with your fair-valued pricing.

Compliance around rule 2a-5 is important because it's a focus of examiners (***RCW***, Oct. 16, 2023). The SEC's exam division, in its 2024 ***priorities***, promises

Whistleblower protection violations cost J.P. Morgan $18M, page 3.

Content

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.

to "review registered investment company valuation practices, particularly for those addressing fair valuation practices (e.g., implementing board oversight duties, setting recordkeeping and reporting requirements, and overseeing valuation designees), and, as applicable, will assess the effectiveness of registered investment companies' derivatives risk management and liquidity risk management programs."

An adviser CCO, who asked not to be identified, tells ***RCW*** of a recent exam that deeply probed the adviser's due diligence into its pricing services used for establishing valuations.

Best practices

The CCO's firm relies heavily on a pricing vendor to establish valuations. He says the vendors expect adviser due diligence and readily share their SOC or SSAE16 reports. Others welcome site visits.

Your board and the adviser can decide on the frequency of such due diligence, but the CCO recommends that you risk assess and rank each of your pricing vendors. At his firm, the job of conducting the due diligence falls to the financial department and not compliance.

"We're not backtesting the prices pulled down" through the pricing service the firm uses, says the CCO.

However, the adviser conducts valuation due diligence. Its valuation committee meets monthly to ponder the fair value of its securities. If securities are off by a certain percentage over time, say, 5% or 10%, the staff would peer into why the discrepancies exist.

In some cases, the adviser may even hire a second pricing vendor to work up its own value on a troubled security or its own auditors will delve into pricing discrepancies.

Variances in pricing, of course, are to be expected. Haskin even recommends that "testing in multiple environments probably adds a lot of values in making the process work well," meaning to weigh "different market circumstances" e.g., a sharp market drop or stable markets.

Your annual report to the board should include a summary of your testing around fair valuation, he counsels. Some advisers look at pricing variations when they periodically test their valuation services, he adds. Rule 2a-5 requires reporting to the board on these issues at least quarterly.

Go low, middle and high

Another approach that some advisers use is to gain a low-, mid- and high-point valuation for harder-to-value securities, notes Balynsky. Testing can spot which point came closest to accuracy after a security is sold or after market conditions change.

"If you're seeing a consistent, material difference" between valuations and a security's end price, that's when the fund board needs to ask why, he advises. You also could consider additional testing of your process.

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*

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).

At the very least, the board should review your valuation P&Ps, update them as necessary, and ensure the P&Ps are being followed and cross-referenced to the requirements of rule 2a-5, continues Balynsky.

The key is to take a reasonable, consistent and "a very well-documented approach," he recommends. You should be able "to supply an audit trail for the SEC" if examiners ask, he counsels.

CCOs "should be a voice in the room" but the real responsibility falls upon the board, he maintains. However, a CCO can ensure that the adviser's valuation P&Ps match the nomenclature of the rule. At a minimum, SEC examiners would want to see this.

RCW has provided past guidance for satisfying the tenets of rule 2a-5 (***RCW***, March 4, 2021 and ***RCW***, Aug. 25, 2022. **Valuation Research Corporation** also offers ***guidelines*** and other ***guidance***.

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

Impeding potential whistleblowers costs

Confidential release agreements that did not permit clients to voluntarily contact the **SEC** have caused **J.P. Morgan Securities** to run afoul of the whistleblower protection rule. The firm agreed to pay an $18 million penalty. The Jan. 16 announcement came with a strong caution from the Commission warning that investors "must be free to report complaints to the SEC without any interference."

The SEC charged JPMS ($212.9B in RAUM) with "impeding hundreds of advisory clients and brokerage customers from reporting potential securities law violations to the SEC." The Commission found that for an over three-year period spanning March 2020 through July 2023, the dual registrant "regularly" asked its retail clients to sign confidential release agreements if they had been issued a credit or settlement from JPMS of more than $1,000.

The SEC determined that from 2020, at least 362 JPMS clients signed a release. Amounts received under the releases ranged from $1,000 to $165,000. Despite reporting some of the disputes to **FINRA**, the SEC said the reporting "does not in any way mitigate the language in the release that impeded clients from reporting potential securities law violations to the Commission."

The provisions of the agreements proved particularly problematic in the eyes of the Commission. Under the agreements, clients were required to keep confidential "the settlement, all underlying facts relating to the settlement, and all information relating to the account at issue." **The kicker**: even though the agreements permitted JPMS clients to respond to SEC inquiries, the agreements did not permit clients to voluntarily contact the SEC.

The ***settlement***, under which JPMS neither admitted or denied the Commission's findings, noted that the confidential release agreements "required the clients to keep confidential not only the release itself, but also all information relating in any way to the specified account at JPMS."

Whistleblower protections

The SEC reminded that Exchange Act ***rule 21F-17***—which became effective in August 2011—states that "no

Whistleblower case prompts plea for TCRs

The **SEC** used the occasion of the Jan. 16 enforcement action against **J.P. Morgan Securities** for whistleblower protection rule violations to "strongly" encourage the submission of tips, complaints, and referrals to the Commission (see related story, this page). SEC Chairman **Gary Gensler** has said TCRs are essential to the Commission's "work as a cop on the beat."

In ***remarks*** delivered shortly after the SEC's 2023 fiscal year closed, Gensler noted that the Commission received more than 40,000 TCRs in the previous FY. He added that more than 18,000 of the submissions came from "critical whistleblowers."

Record payouts

Last year was a busy one for the SEC's Office of the Whistleblower, which was created in 2011. In May, the office awarded its highest payout to date at $279 million. You can look for more of the same in 2024. Just last month, the SEC announced awards of more than $28 million to seven individuals whose information led to a successful enforcement action.

The SEC reminds that whistleblowers can be eligible for an award when voluntarily providing the Commission with "original, timely and credible information that leads to a successful enforcement action." Awards can range from 10% to 30% of the money collected when sanctions exceed $1 million.

Tips, complaints, and referrals can be submitted via ***www.sec.gov/tcr***. The SEC pledges to protect the confidentiality of whistleblowers.

person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement … with respect to such communications."

Either-or proposition

"For several years, [JPMS] forced certain clients into the untenable position of choosing between receiving settlements or credits from the firm and reporting potential securities law violations to the SEC," said SEC Enforcement Division Director **Gurbir Grewal**. "This either-or proposition not only undermined critical investor protections and placed investors at risk, but was also illegal," he added.

The case offers the lesson to go back and re-read client confidentiality agreements. "Those drafting or using confidentiality agreements need to ensure that they do not include provisions that impede potential whistleblowers," cautioned **Corey Schuster**, co-chief of the Enforcement division's asset management unit.

JPMS has since revised the release to add language affirmatively advising clients that they are not prohibited from disclosing information to any governmental or regulatory authority, the SEC reported in the settlement. ■

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.

SCOTUS weighs omission standard for PF suits

The **U.S. Supreme Court** is wrestling with a case that could have major implications for financial services firms on either side of private securities lawsuits.

The central question in **Macquarie Infrastructure Corp.**, *et al. v.* **Moab Partners**, et al. is whether evidence of a violation of Item 303 under **SEC** rule S-K—which requires public companies to disclose "known trends or uncertainties that have had or that are reasonably likely to have a material favorable or unfavorable impact" in their periodic regulatory filings—can be used to support private litigation under the antifraud provisions of the Exchange Act.

If the justices answer in the affirmative, Macquarie and its allies are worried, it will "open the floodgates to potentially crippling private securities fraud liability," the company's lawyers said in their brief. Moab and its allies argue that an answer in the negative "would create broad immunity any time an issuer fraudulently omits information Congress and the SEC require it to disclose."

The SEC, through the **U.S. Solicitor General**'s office, is backing Moab. It has urged the justices to go even further than Moab's position. The Commission says it cannot police every single public filing. Plaintiff's suits are a useful supplement to the Commission's enforcement authority.

A ruling against Moab and its fellow plaintiffs could "allow unscrupulous parties to exploit the very trust that disclosure requirements are designed to foster by engaging in strategic omissions that they expect investors to misconstrue," government lawyers said in their amicus brief.

The high court held oral arguments in the case Jan. 16.

Divided industry

The case has literally divided the private funds industry. Moab is an SEC-registered private fund adviser, and some of its fellow plaintiffs include public pension funds. Macquarie is a publicly traded company managed by its largest shareholder, a Sydney-based private infrastructure fund adviser.

In 2018, Moab filed a class-action suit against Macquarie, claiming that the company should have disclosed the impact of then-pending international rules limiting high-sulfur fuel oils on Macquarie's business. Most of Macquarie's profits had been driven by a subsidiary in the business of storing one of those fuels, known as "No. 6 fuel oil."

In a 2012 earnings call, Macquarie told investors there was a risk that demand for "heavy oil residual product" might fall, but said it had no plans to convert its subsidiaries' heavy oil tanks. Between 2012 and 2018—the international regulations curbing high-sulfur fuel oils took effect in 2016—Macquarie officials didn't mention the regulations or its No. 6 storage business but said more than once they weren't worried about price changes for crude oil or petroleum products.

In February 2018, Macquarie announced that its No. 6 storage business had fallen, that the company had missed its financial projections and that it would cut dividends. Two days later, the company's stock fell by more than 40%.

Moab and its allies claim that Macquarie's refusal to disclose the potential damage from the anti-sulfur regulations was materially misleading, tantamount to fraud under Exchange Act rule 10b-5. A judge in the **Southern District of New York** tossed the suit, ruling that Moab had failed to prove scienter. But a unanimous panel of the **Second Circuit U.S. Court of Appeals** overturned the dismissal, ruling that the court should've rationally concluded that Macquarie's material omissions were evidence for scienter. Macquarie appealed to the Supreme Court.

'Hard to apply'

Macquarie lead counsel **Linda Coberly**, a partner at **Winston & Strawn**, reminded the justices that they are usually "loath to expand" private rights of action—but Chief Justice **John Roberts** opened arguments by telling Coberly "the distinction you draw between sort of half-truths and omissions strikes me as one that might be hard to apply in practice."

Justices **Clarence Thomas** and **Brett Kavanaugh** seemed most worried about whether the SEC should be in charge of enforcing Item 303. "If pure omissions are misleading—it seems as though you're saying the mere fact that it is an omission makes it misleading," Thomas told Moab lead counsel, **Kellog, Hansen, Todd, Figel & Frederick** partner **David Frederick**, "Can you—is there a limit to that?"

Kavanaugh wanted to know, "can we just say that an omission alone is not good enough, you have to identify a statement as well, and send it back?" When Frederick responded that such a ruling would not help, Kavanaugh said, "It'll help us," drawing laughs.

Both Thomas and Kavanaugh pressed **Ephraim McDowell**, who argued for the solicitor general's office, on how the government could argue that a public statement that omitted a fact would render the whole disclosure misleading without it containing an otherwise false statement.

'Verbal junk'

Advocates on both sides are watching the case closely. **SIFMA**, the **U.S. Chamber of Commerce** and the **Business Roundtable**, among others, ***filed*** an amicus brief supporting Macquarie. The business trio say they're worried that a ruling for Moab will sow even more confusion amongst investors.

"The Second Circuit's erroneous rule means that public companies must *overdisclose* or incur risk simply by omitting a disclosure in any remotely doubtful case," the groups said in their brief. "Such overdisclosure is hardly benign. This court, the SEC, and scholars have all warned against bloated disclosures that bury actually useful information in a pile of verbal junk."

In a separate amicus brief, 10 different pension funds—including New York Comptroller **Thomas DiNapoli** in his capacity as trustee to New York's public pension plan—and three investment advisers ***said*** the Second Circuit got things right. "Amici institutional investors, their investment advisors, and investment professionals generally, rely heavily not only on the accuracy of the information disclosed under this regime, but also on the *completeness* of those disclosures," the funds and fund advisers said. "Item 303 disclosures are particularly important. Most information provided under federal securities law is backward-looking. That information is important, but stock valuations are principally based on a prediction of future performance."

Motions to dismiss

Among those watching the case is **Troutman, Pepper** partner **Jay Dubow**. He says how a fund manager views the case will depend on their business model. Activist, disruptive fund managers are more likely to support Moab. Portfolio managers are more likely to support Macquarie.

The difficulty is that the Second Circuit seems to have determined that an omission is *per se* evidence of fraud. That makes it much easier for class-action lawsuits to survive motions to dismiss, which in turn puts enormous pressure on companies to settle such actions.

"The big thing in these securities cases, plaintiffs just want to get past the motion to dismiss," Dubow says. "These cases almost never go to trial. The cases usually settle, because there's going to be lots of expensive discovery involved."

Like SIFMA, Dubow says he worries that a decision for Moab could force companies to make all kinds of useless disclosures. "I think the potential for having companies having to make all kinds of unnecessary, extra disclosures, could really dilute the usefulness of disclosures," he says.

The Supreme Court's decision in *Macquarie* is not likely to land until April. ■

2024 RISK ALERT

Some swap dealers fall short on compliance

The Times Square ball may hardly be back in storage but the **SEC**'s Division of Examinations has already released its first risk alert of the year. It targets security-based swap dealers, and castigates some for falling down on compliance.

The seven-page alert, ***Observations Related to Security-Based Swap Dealers***, recounts the fundamental compliance rules under the SEC's security-based swaps regime, and points out where some swap dealers are coming up short, including failing to accurately and timely report their "security-based swap transactions to a registered security-based swap data repository."

The guidance comes after some initial exams of swap dealers following the long-awaited adoption of *Dodd-Frank* rules by the SEC, and also "ad-hoc outreach" to the industry by the division.

Examiners probed for compliance with ***Regulation SBSR***, as well as recordkeeping and reporting ***rules*** that took effect in 2021. These rules required dealers to create compliance P&Ps "reasonably designed" to avoid violations. The risk alert highlights six areas for P&Ps, including that the dealers, at least on "an annual basis," conduct "an internal review of security-based swap business reasonably designed to detect and prevent violations of applicable securities laws, rules, and regulations."

Small but mighty firms

There are only 51 registered security-based swap dealers. ***Here's a list of them***. Many of them, such as **Goldman Sachs**, **Morgan Stanley**, **Merrill Lynch** and **Wells Fargo**, are among the largest financial firms and also operate SEC-registered investment advisers.

Examiners found some dealers failed to satisfy the rules, e.g., by neglecting to record "the name and address of" each counterparty, develop standards to prevent supervisors from overseeing their own activities, to keep current blotters, report swap trades to swap data repositories "within required timeframes," and for listing "inaccurate notional amounts, including miscalculated notional amounts."

The blame for these failures falls upon "weak internal controls and processes for ensuring that information reported was accurate," the alert reads.

Other errors found by examiners included failures "to account for recorded telephone conversations of associated persons or used generic search terms to identify communications for review," and to have "an independent auditor perform periodic audits of security-based swap trading relationship documentation policies and procedures."

The DOE encouraged swap dealers "to review and strengthen their policies, procedures, internal controls, and security-based swap reporting capabilities."■

A look at AI and financial services

Predictions already note that as more of the financial services industry adopts artificial intelligence technologies, the bad guys will as well. Envision dueling AI.

"We have basically an arms race between detection [of financial fraud] and evasion [using AI], in which we don't know what the outcome is going to be," described **Michael Wellman**, a professor of Computer Science & Engineering at the **University of Michigan**. "We should be prepared to deal with some super manipulators."

He spoke Jan. 9 before the **CFTC**'s Technology Advisory Committee, when it considered the implication of AI on financial markets.

When humans place second

One challenge is the technology can move faster than the economy. "All kinds of strategies that were not possible under human time scales, could become possible with computer time scales," Wellman forecast. AI "enables taking humans out of the loop, in fact, it necessitates taking humans out of the loop because response times by people are not fast enough to" compete.

An advantage offered by AI is it can "replicate and scale" an algorithm "very fast," said Wellman. However, that ability can be used by both good and bad actors.

The industry is "already highly infiltrated by AI," Wellman told committee members. "The stakes involved have attracted a lot of investment."

These stakes are lured by the prospect of big profits—both by the good guys, and the bad guys using AI.

Of course, there will be new scams perpetrated by the use of AI, Wellman admitted. And the technology will move faster than the ability of laws and regulations to keep up, he predicted.

Risks of sophisticated market manipulation

"AI can be used on the part of an adversary to manipulate, attacking markets, but [it] also can be used to defend them, for example, by developing detectors," sketched out Wellman, who said he has studied algorithmic trading for 15 years.

A study Wellman engaged in recently tested the ability of AI to detect potential market manipulation, and discovered that AI used by the study's purported adversary also very quickly deduced ways to avoid that detection.

The arms race Wellman spoke of stems from this seeming ability of AI to "immediately" move to hide wrongdoing flagged by AI tools—meaning both sides will use the technology for and against each other into the faraway future.

Current regulations obviously already outlaw market manipulation and fraud but **SEC** regulations also present a potential "loophole" when it comes to the use of AI for sinister means because the regulations were designed for human behavior and may not measure up against machine-generated wrongdoing, he continued.

"It's inevitable that mistakes will be made with regulation of AI," Wellman opined. First, regulators will discover if current rules are adequate, especially given that AI could generate misbehavior that's unique. "We have to be watching for them," he advised.

He warned, though, that relying only on machine learning to detect wrongdoing won't be enough.

A question directed at Wellman asked if the SEC's planned consolidated audit trail may be "outdated already" given AI's trajectory. "Imagine where we'd be without the consolidated audit trail to deal with some of these issues," Wellman responded.

Hoarding data

Another concern raised by Wellman focuses on the fear that some parties may monopolize information that would nourish their AI efforts. "We may need to worry about the concentration, ownership of large bodies of non-public information that have … strategic value," which could give some parties overwhelming advantages over others, he said.

What could financial regulators do? For one thing, they could offer "case studies and lessons" around how financial services handles AI that could assist other industries where the technology has yet to take root, he noted. ■

SEC social media account hacked

SEC Chairman **Gary Gensler** has made clear that he wants the financial services industry to tighten up its cybersecurity defenses with a suite of rule proposals, exams and enforcement crackdowns, but the chairman has just learned that sometimes the tweet is coming from within the house.

Two statements issued on the Commission's official account on social media site **X** (formerly known as **Twitter**) announcing that regulators had given permission for a **Bitcoin** exchange-traded fund were the work of hackers, an agency spokeswoman announced late Jan. 9.

"The SEC's @SECGov X/Twitter account has been compromised," a spokeswoman said in an e-mail. "The unauthorized tweet regarding bitcoin ETFs was not made by the SEC or its staff."

The tweets went out some time after 4 p.m. on Jan. 9. The first one said, "Today the SEC grants approval for #Bitcoin ETFs for listing on all registered national securities exchanges. The approved Bitcoin ETFs will be subject to ongoing surveillance and compliance measures to ensure continued investor protection." The second one merely said, "$BTC," a reference to Bitcoin as a business on the social media platform.

Unknown party 'terminated'

The hacker would turn out to be right—the Commission ended up announcing its approval for Bitcoin's ETF on Jan. 10—but it was a fresh embarrassment for Gensler and his team in a sensitive area. Gensler has been an open skeptic of the asset class, saying it's rife with fraud. Crypto advocates, including fellow SEC Commissioner **Hester Peirce**, have blasted Gensler for insisting that crypto companies come into compliance with SEC registration rules while denying every petition for registration that has come his way.

The on-again, off-again tweets sent Bitcoin shares soaring, and then crashing to the ground. About $3 billion was lost to investors, published reports claim.

The SEC spokeswoman said an "unknown party" had briefly hacked the Commission's official account, but the agency has since "terminated" the party's access. "The SEC will work with law enforcement and our partners across government to investigate the matter and determine appropriate next steps relating to both the unauthorized access and any related misconduct," the spokeswoman added.

"The SEC takes its cybersecurity obligations seriously,"

Gensler said in a statement posted to the agency's web site Jan. 12. "Commission staff are still assessing the impacts of this incident on the agency, investors, and the marketplace but recognize that those impacts include concerns about the security of the SEC's social media accounts. The staff also will continue to assess whether additional remedial measures are warranted." ■

OBAs: a top regulator focus

Outside business activities appear yet again on **FINRA**'s list of priorities for 2024 and recent enforcement actions undertaken by the SRO back this up. FINRA rule 3270 requires registered persons to notify their firms in writing of proposed OBAs so firms can determine whether to prohibit, limit or allow those activities. But some firms are falling short of the mark in establishing, maintaining, and enforcing a supervisory system tied to OBAs.

The newly released *2024 FINRA Annual Regulatory Oversight Report* flags both OBAs and private securities transactions (PSTs) as focus areas this year (***RCW***, Jan. 11, 2024). The SRO recommends firms consider what methods they use to identify individuals involved in undisclosed OBAs and PSTs. Also, determine whether your firm's WSPs "explicitly" state when and how registered persons must notify your firm of a proposed OBA or PST, the ***report*** suggests.

Clear WSPs

As an "effective practice," FINRA noted the clear identification in WSPs of the types of activities or investments that would constitute an OBA or PST. Defining selling compensation and providing FAQs reminding employees of scenarios that they might not otherwise consider implicating ***rule 3270*** (Outside Business Activities of Registered Persons) and ***rule 3280*** (Private Securities Transactions of an Associated Person) were also touted.

Other effective practices identified in the report included, among other things:

- **Questionnaires**. This included requiring registered persons and other associated persons to complete upon hire, and periodically thereafter, detailed, open-ended questionnaires with regular attestations regarding their involvement in new or previously disclosed OBAs and PSTs.
- **Due Diligence**. Learn about all OBAs and PSTs at the time of initial disclosure to the firm and periodically thereafter.
- **Training**. Conduct training on OBAs and PSTs during onboarding and periodically thereafter.
- **Disciplinary Action**. Heightened supervision, fines, or termination could all be considered for persons failing to notify firms in writing of their OBAs and PSTs.

Crypto activities

Newly identified in this year's OBAs/PSTs findings was "no review and recordkeeping of crypto asset-related activities." FINRA reported seeing firms failing to disclose, approve or follow required rule steps for crypto asset-related OBAs and PSTs. The making of a false statement related to OBAs or PSTs involving crypto assets on firms' annual attestations was also called out by the SRO.

Enforcement actions

Enforcement is clearly dialed in to the handling of OBAs. Earlier this month, **MMA Securities** was charged by FINRA with failing to establish, maintain, and enforce a supervisory system, including WSPs, "reasonably designed" to achieve compliance with the rules governing OBAs. The SRO found that from January 2018 to the present, the failed to evaluate and document its evaluation of OBAs as disclosed by its registered reps.

MMA did have WSPs requiring it to review disclosed OBAs to ensure that they did not "compete with the firm's business, use firm resources, or present a potential conflict of interest," the ***settlement*** notes. However, MMA approved at least 37 OBAs without evaluating and documenting its evaluation. These failures cost MMA $30,000.

Not evaluating OBAs also tripped up the Greenwich, Conn.-based **SRT Securities**. In an enforcement action brought in December, FINRA said SRT did not evaluate three registered reps engaged in an OBA involving an investment advisory business or another rep who was engaged in an OBA for which he planned to solicit investments in a hedge fund. In a ***settlement***, SRT, without admitting or denying FINRA's findings, also agreed to a $30,000 fine. ■