TABLE OF CONTENTS

Articles »

Six Things to Know about Arbitrating Diminished Capacity Issues in FINRA Customer Cases
By Josh Jones
Unique situations arise when litigating competency issues in the FINRA forum.

Is It Your First Time Having a Client under Investigation by FINRA?
By Joseph S. Simms and Andrew T. Illig
Here’s what you need to know, from receipt of an 8210 letter to the hearing in the enforcement action.

The U.S. Supreme Court Case That Could Significantly Expand Civil Liability under the Federal Securities Laws
By Jessica Ortiz, Caleb Hayes-Deats, and Michelle Parthum
Private plaintiffs could become able to pursue claims in D.C., Alabama, Florida, and Georgia that would be legally insufficient elsewhere.

FINRA’s New Report on Broker-Dealer Cybersecurity Practices
By John E. Clabby
The report’s key points and some observations from the author’s practice.
Six Things to Know about Arbitrating Diminished Capacity Issues in FINRA Customer Cases
By Josh Jones

Litigation before the Financial Industry Regulatory Authority (FINRA) involving the elderly and other vulnerable clients is likely to increase significantly in the coming years given the aging of the investing population, that population’s unique vulnerabilities, and their substantial wealth. In addition to financial elder abuse claims, disputes are likely to involve competing claims to assets or claims that the firm wrongfully prevented a customer from making transactions or distributions. One thing is clear: Issues involving the competency of the elderly and vulnerable clients are certain to become more common in arbitration.

Senility and its effect on a person’s competency to direct his or her affairs raise complicated medical issues and unique concerns in litigation and arbitration. The following is a quick discussion of several of these concerns, along with a number of practical considerations for lawyers in this space.

1. Potential Litigation Concerns Associated with 2018 Changes to FINRA Rules
In February 2018, FINRA implemented Rule 2165, which enables member firms to place a temporary hold on disbursements from accounts based on a reasonable belief “that financial exploitation of the Specified Adult has occurred, is occurring, has been attempted, or will be attempted.” The rule applies only to “specified adults” or those who are either (1) age 65 and older or (2) age 18 and older and “who the member reasonably believes has a mental or physical impairment that renders the individual unable to protect his or her own interests.”

As part of the same process, FINRA amended Rule 4512 to add section (a)(1)(F). This amendment requires that firms request the contact information of “a trusted contact person age 18 or older who may be contacted about the customer’s account” from clients in connection with the account opening process. Moreover, firms must inform clients upon opening the account that firms may reach out to the trusted person when they suspect that the client is being financially exploited.

Rule 2165 is permissive in that it does not require firms to place a hold on assets or accounts even if the firm suspects that a vulnerable client is being financially exploited; it simply permits such holds. If implemented in good faith, such holds provide firms with a safe harbor from certain FINRA rules regarding improper use of client accounts and funds, expedition of certain customer requests regarding the transfer of securities, and its general provision relating to standards of commercial honor and just and equitable principles of trade. However, firms that implement Rule 2165 must maintain certain records as well as develop written supervisory procedures and training policies.

© 2019 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
From a firm’s perspective, there are several potential litigation concerns raised by the rule changes:

- As noted above, FINRA Rule 2165 does not require a hold even when a firm suspects financial exploitation. However, firms should anticipate that counsel for adverse parties will argue that the rule provides firms with a means of safeguarding assets and that a firm’s failure to protect a vulnerable client even when it suspects or is actually aware of financial exploitation constitutes negligence or a breach of some duty owed under the law or equity.

- The rule requires that a firm’s belief regarding the exploitation be reasonable. Similarly, a firm’s belief that an adult under the age of 65 is covered by the statute must be based on a reasonable belief that person suffers from an impairment that prevents the person from being able to protect his or her interests. Firms should anticipate attacks on the reasonableness of their beliefs by supposed victims who now allege that they have been damaged by the wrongful freezing of their assets or a firm’s refusal to enter trades or other transactions on their behalf. In such cases, claimants are likely to assert claims for lost profits or other resulting damages.

- The supplementary materials to Rule 2165 provide that firms implementing the rule “must develop and document training policies or programs reasonably designed to ensure that associated persons comply with the requirements of this Rule.” Firms can expect to see claims that the training policies and programs were somehow defective or negligently implemented, as well as discovery directed to these issues.

- Rule 4512 could also create litigation concerns given that it is quite often someone close to the client, including children, who are exploiting the client. What happens when the “trusted contact” cannot be trusted? Firms must be wary of assisting the fox with guarding the henhouse.

- In addition, what happens when a client who may be showing some signs of diminished capacity wants to change an account beneficiary in a way that affects the trusted contact, favorably or unfavorably? Fact patterns could involve a client disinheriting a trusted contact, or a firm reaching out to a trusted contact to discuss a change that could dramatically affect the trusted contact in the future. These scenarios are not difficult to hypothesize, but they could be very difficult to address in real time or in hindsight when in a FINRA arbitration.

- Litigants should also be aware of the distinctions between the requirements under FINRA rules and the various state statutes designed to prevent exploitation of seniors and other vulnerable clients.

2. The Importance of Recognizing the Sensitive Nature of These Issues
Cases involving financial exploitation of vulnerable adults can be difficult cases to try. Parties and witnesses are litigating in what is often a very emotional context involving loved ones who may have suffered and declined for a number of years. And the process does not necessarily lend itself to addressing what are often long-held family tensions and underlying issues in personal,
and what are normally private, relationships. Lawyers trying these cases are well served to approach these issues with the delicacy and tact that they warrant.

Practitioners must also recognize the potential strong reaction that arbitrators may have to these issues. It is quite possible that the arbitrators themselves have seen someone whom they care about affected by dementia. According to the Alzheimer’s Association’s 2018 Alzheimer’s Disease Facts and Figures, roughly 5.7 million people in the United States suffer from Alzheimer’s dementia. That number is expected to exceed 7 million by 2025. Hearing testimony about a person’s decline or medical evidence regarding cognition or even seeing a witness become emotional on the stand can affect an arbitrator—just as it would any caring person.

The following issues merit consideration:

- Are potential arbitrators more likely than most to have dealt with diminished capacity issues in their profession? These could include estate attorneys, regulators, medical professionals, brokers, caregivers, and advocates for the elderly.
- Is it possible that the arbitrators themselves have begun to experience some diminution of their faculties? FINRA has recognized that the arbitrator pool contains a significant number of seniors. I regularly see panels with arbitrators in their late seventies or eighties.
- Consider how your panel might be affected by these issues. If they have seen a loved one suffer from Alzheimer’s, they will almost certainly feel some sympathy both for the person suffering and for those who care for the person. Accordingly, they might look harshly at the loved one, financial advisor, or third party whom they view as attempting to take advantage of the victim. Similarly, they might appreciate a firm’s reasonable attempts to prevent such exploitation but fault a firm that stood by and did nothing. Practitioners should consider the effect that firsthand experience with dementia can have on a panel’s decision-making process.
- An aging panelist might very well resent a firm’s efforts to place limits on an elderly investor who is vigorously asserting his or her competency to decide his or her own financial affairs, when the firm has concerns that person is being exploited or otherwise appears unable to maintain his or her investment accounts. Such cases can be very difficult to litigate or resolve, particularly in instances in which the client appears to have “good days and bad days.”

3. Cases Are Generally Won on the Facts
As with most FINRA arbitrations, these cases are generally won on the facts. For that reason, you will want to make sure that you have a fully developed record from which the panel can draw its decision.

- The financial advisor will likely be a key witness. It is helpful for a panel to understand the length and depth of the client relationship. Of particular interest are in-person meetings supported by the broker’s communications, notes, and calendar, and any
recordings. Other fact witnesses in the branch could include the client associate and managers who interacted directly with client.

- Documents to consider include other agreements entered into during the time frame at issue. For instance, if a beneficiary change is being challenged, did the client execute a will around the time of the change, or open a bank account, take out a loan, buy real estate, or otherwise contract to legally bind himself or herself? Similarly, financial records can be critical. Did the client manage his or her personal checking account, file tax returns, operate a business, or direct investments at another firm? All of the above could shed light on the client’s competency to direct his or her affairs.

- Others potential witnesses could include those who knew the client over time, including professionals (lawyers, accountants, other advisors), family, neighbors, and friends. I have examined witnesses who were visitors at the hospital during a client’s final days.

- Medical personnel may also offer key testimony. Was the client capable of making binding medical decisions? Did the doctors or nurses (who are often better witnesses, in my experience, given the nature of the patient relationship) believe that the client was competent? Did that change over time?

- Along these lines, medical records are critically important. If you are in litigation with an estate, it should be able to access and produce the decedent’s medical records. If you are not able to secure medical records from the parties, you will need to seriously consider availing yourself of the subpoena process outside the scope of FINRA orders of production and appearance.

- Finally, firms need to consider the possibility of testimony by the person or persons within the firm who made a decision at issue in the case. For instance, who made the decision not to release funds requested by a client or to freeze a client’s account pending direction from a court? Such decisions may lie at the heart of the litigation, but of course firms will struggle with issues relating to the attorney-client privilege, work product, and related concerns. The last place that most attorneys or even non-attorney compliance professionals want to be is on the witness stand, and firms are right to be concerned about opening their decision-making processes to discovery.

- FINRA Rule 2165 contains a retention provision that requires firms to maintain a number of records relating to requests for disbursement that may constitute financial exploitation, the basis of the firm’s belief that the requests constitute exploitation, and other related information. Firms can likely anticipate discovery requesting production of the materials and information required to be retained.

4. Potential Need for Expert Witnesses
Cases involving competency issues may also require expert testimony. For instance, parties on both sides may call industry experts to discuss industry standards, best practices, rules, and regulations. Depending on when the events giving rise to the claim occurred, such testimony may also need to address how the industry’s understanding of these topics and implementation of related processes have changed over time.
Parties also need to consider whether to call a psychiatrist to opine on issues relating to competency. Although such an expert likely will not offer an ultimate opinion on competency, he or she can expound on the record before the panel, including explanation of medical records and summarizing important takeaways from the testimony of both lay witnesses and medical personnel. Testimony from a recognized expert that the record before the panel does or does not support a finding of competency can be quite persuasive while also serving to focus the panel’s attention on the key factors at play.

5. When the Money Is Still There . . .
Consider a common fact pattern in cases involving diminished capacity issues: Someone alleges that he or she is the rightful beneficiary on an account despite a firm’s records reflecting otherwise. In cases in which the moneys have not been distributed, firms are advised to consider interpleading the funds when available or otherwise seeking a court order directing the distribution of the proceeds. Firms may also consider seeking such guidance from an arbitration panel. Issues to consider with this approach include whether a firm can compel a nonparty to arbitrate such a dispute, a FINRA panel’s limited ability to grant equitable remedies available to a court, and enforcement of the panel’s order. Difficulty can arise when a firm seeks to secure direction from a court while also maintaining its ability to arbitrate claims that it damaged a party through its actions or inaction. Along these lines, firms may also face claims in arbitration brought by purported beneficiaries or other parties who are not its customers and with whom they are not required to arbitrate under FINRA Rule 12200. Such disputes can lead to sometimes tricky litigation in court when a firm seeks declaratory or other relief directing that it not be compelled to arbitrate against noncustomers.

6. Once the Money Is Gone . . .
A firm’s exposure increases substantially once the funds are withdrawn or disbursed from the account. I have litigated beneficiary disputes in cases in which the money is sitting in the account waiting on a court or arbitrator order directing disbursement, as well as cases in which the moneys had long since been disbursed and spent soon thereafter. You can guess which causes more sleepless nights for in-house counsel and their business clients.

Under Rule 2165, the hold placed by a firm expires “not later than 15 business days after the date that the member first placed the temporary hold” unless “otherwise terminated or extended by a state regulator or agency of competent jurisdiction or a court of competent jurisdiction[,]” In addition, the hold may be extended for an additional 10 business days if the firm’s internal review supports its reasonable belief as to exploitation. So firms have roughly a month from the initial hold to take action seeking direction from a court or regulator that would serve to protect the investor’s assets, which could also serve to limit a firm’s potential exposure in the event of litigation.

Conclusion
Unique issues arise when litigating competency issues in the FINRA forum. Practitioners would be wise to give them due consideration given the likelihood that they will be addressing them
soon enough with an aging investor population, increased regulatory scrutiny, and growing realization of the need to recognize and prevent exploitation.

Josh Jones is a principal with Bressler Amery Ross in Birmingham, Alabama.
Is It Your First Time Having a Client under Investigation by FINRA?

By Joseph S. Simms and Andrew T. Illig

Receiving an inquiry from a regulatory agency or self-regulatory organization can make anyone nervous. Questions immediately arise as to what to do, how to respond, how to determine the reason for the investigation, and what steps to take. Using Financial Industry Regulatory Authority (FINRA) procedures as an example, we look to answer some of these questions, with an eye toward the overarching obligation of registered representatives and member firms to fully cooperate and respond to FINRA’s inquiries.

FINRA’s 8210 Letter

Most FINRA investigations start with a so-called 8210 letter. This letter is typically issued by a FINRA investigator in the Department of Enforcement and requests documents and information related to an investigation. Certainly, the first step in preparing to respond to an inquiry is to identify, to the extent possible, the subject matter of the investigation and whether the recipient of the inquiry is a subject of the investigation or a witness (although that can—and frequently does—change during the course of the investigation). Firms and individuals should also immediately identify and preserve relevant and responsive documents, data, and information, and identify witnesses with pertinent knowledge and custodians who may have possession of or access to relevant documents and information. With the assistance of counsel, witness interviews should be undertaken to determine the “who, what, when, where, why, and how” of what occurred. Also with counsel’s involvement, documents should be gathered and prepared for production—perhaps with the assistance of an outside vendor, depending on the scope—to ascertain what is at issue. Time usually is of the essence, and care should be taken to protect against destruction or spoliation of evidence.

FINRA Rule 8210 states that FINRA staff has the authority to request that any person subject to FINRA’s jurisdiction provide information orally, in writing, or electronically, and testify under oath with respect to any matter involved in the investigation, complaint, examination, or proceeding. Modifications to the rule, passed in 2013, have broadened FINRA’s authority to request documents and information. This expansion requires a recipient to produce (1) documents in his or her possession and (2) documents in the possession of someone else if he or she “has a right to demand them.”

A recipient of an 8210 letter has limited options. A FINRA member is obligated to cooperate with FINRA during an investigation. FINRA Rule 8210(c) provides that “[n]o member or person shall fail to provide information or testimony or to permit an inspection and copying of books, records, or accounts pursuant to this Rule,” and further states that “any failure on your part to satisfy these obligations could expose you to sanctions, including permanent bar from the securities industry.” Unfortunately, an 8210 letter does not specify whether the recipient is the target of an investigation or merely an innocent third party asked to provide relevant information.
All too often, registered representatives see an 8210 letter and think that responding themselves (without counsel) will make the investigation go away or that they can personally explain away whatever situation is being investigated. Unfortunately, these responses often do not address the most important legal points in the investigation and fail to properly articulate the relevant facts to the FINRA investigator. Regardless of a firm’s desire and effort to cooperate, these investigations and inquiries present nuanced issues of law such that the experience of counsel is desirable. Any recipient of an 8210 letter, or a similar letter from the Securities and Exchange Commission, state Department of Insurance, or state Department of Securities, would be wise to immediately consult with counsel to ensure a written response is thoughtfully drafted and to work cooperatively with the investigator to discuss any issues with the document requests to fully comply in a way that directly responds to the investigator’s inquiries without exposing the respondent to unnecessary risk. Care and consideration must be afforded to the scope and timing of the response, narrative descriptions that may accompany a document production, and the scope of objections, if any, to the requests.

Based on the written response, the documents produced, and conversations between counsel and the FINRA staff, FINRA can choose to pursue enforcement, close its investigation, or continue the investigation by requesting on-the-record (OTR) interviews.

FINRA’s On-the-Record Interview
An OTR is similar, but not identical, to a deposition in a civil lawsuit with a witness responding under oath to questions posed by a FINRA investigator. The OTR will delve into the witness’s background and qualifications, work experience, and the subject matter of the investigation itself. Questions may relate specifically to documents the witness produced in response to the 8210 letter or to documents FINRA received in response to 8210 letters directed to other individuals or entities. Keep in mind that the FINRA investigator typically gathers documents and information from multiple sources. Anyone submitting to an OTR would be wise to consult with counsel before providing testimony to properly prepare for what will be the only opportunity (outside of an 8210 letter response) to explain facts to the FINRA investigator before an enforcement action could be filed. As in the response to the 8210 letter, care should be taken to provide full and accurate responses to any questions posed, subject to objections, if any, to the scope, subject matter, or form of the questions.

In an OTR—unlike a civil deposition, where objections may be made for a myriad of reasons—there are limited bases for counsel to object to questions posed by the FINRA investigator. Because of this, counsel’s role is better appreciated from the standpoint of preparing for the OTR and in negotiating a potential dismissal or resolution, as opposed to simply protecting the client during the OTR itself. Should someone invoke the Fifth Amendment privilege against self-incrimination, FINRA may view such invocation as a lack of cooperation and issue harsh sanctions for doing so, including a permanent bar from the securities industry. OTRs also differ from civil depositions in that FINRA will provide the witness an opportunity to make a closing statement, which may be used to further explain prior testimony or to address issues or considerations that were not touched on in the questioning. The decision to make such a
statement, and what to include in this statement, will depend on the facts and circumstances of each case and the performance of each individual witness. Because of these unique issues, care should be taken in deciding whether to make such a statement and, if so, what to include. It is advisable for a witness to consult with counsel both prior to and during the OTR to make this determination.

After the OTRs, FINRA will typically decide whether to dismiss the case, pursue sanctions through settlement discussions, or take it to the next level by filing an enforcement action.

**FINRA Enforcement Actions**
If a FINRA investigation is not dismissed or resolved after the 8210 letter or OTR, it will turn into a formal enforcement action. Customarily, but not necessarily, the respondent is put on notice of an impending enforcement action by means of a Wells notice—a notification from a regulator of its intent to pursue enforcement and the nature of the alleged violations that are believed to have occurred. A recipient of such a notice has the opportunity to respond to it by means of a Wells submission designed to convince the regulator to forgo, alter, or reduce its allegations of wrongdoing against the recipient. Oftentimes, and for many different reasons, respondents choose not to submit a response to a Wells notice because they are neither privileged nor confidential, and anything set forth in a Wells submission can be used against the respondent in a subsequent enforcement proceeding. And they are discoverable and can be used against the respondent in private civil litigation. Of course, there are many circumstances in which a Wells submission is advisable, and the determination whether to make a Wells submission should be the result of careful consideration and analysis.

If the Wells submission is not successful and the dispute cannot be resolved, the Department of Enforcement initiates an enforcement action by filing a complaint against the member or associated person. After the complaint is filed, the material phases of an enforcement action are as follows:

1. **Answer:** The defendant (or defendants) will have an opportunity to file an answer to the complaint, admitting, denying, or stating a lack of sufficient information to admit or deny the allegations.
2. **Selection of panel:** The chief hearing officer will appoint a hearing panel or an extended hearing panel to oversee the hearing.
3. **Conferences:** The parties will participate in an initial pre-hearing conference to discuss a litigation schedule and any other material issues.
4. **Motion practice:** The defendant may file a motion for summary disposition, which is similar to a state court or federal court motion for summary judgment, when there is no genuine issue in dispute with regard to any material fact, and the issues may be decided as a matter of law.
5. **Discovery:** The defendant will have the opportunity to obtain documents prepared or obtained by FINRA staff in connection with the investigation, request that FINRA compel the production of documents or testimony at the hearing from persons over whom

© 2019 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
FINRA has jurisdiction, or file a written motion requesting that FINRA produce for inspection and copying any witness statements from witnesses who will be called at the hearing.

6. **Pre-hearing submissions:** The parties will submit pre-hearing submissions and exchange witness and exhibit lists, documents to be used during the hearing, an outline or narrative summary of a party’s case or defense, the legal theories on which a party will rely, and other information called for in FINRA Rule 9242.

7. **Hearing:** At the hearing, the parties will have an opportunity to call witnesses and introduce evidence. Within 60 days after final disposition, the hearing officer will issue a written decision.

8. **Appeal:** Either party may appeal the decision within 25 days to the National Adjudicatory Council.

Ultimately, under its [Sanction Guidelines](May 2018), FINRA may impose one or more of the following sanctions for each violation of FINRA rules: (1) censure, (2) a monetary fine, (3) suspension, (4) expulsion, (5) a temporary or permanent cease-and-desist order, or (6) any other fitting sanction. As in civil litigation, the opportunity for resolution exists at every stage of the proceeding. However, care should be taken to ensure that settlement discussions occur at the proper time to maximize the likelihood of a mutually acceptable outcome.

*Joseph S. Simms* and *Andrew T. Illig* are with Reminger Attorneys at Law in the firm’s Cleveland, Ohio, office.
The U.S. Supreme Court Case That Could Significantly Expand Civil Liability under the Federal Securities Laws

By Jessica Ortiz, Caleb Hayes-Deats, and Michelle Parthum

Can the Securities and Exchange Commission (SEC) penalize an investment banker on the ground that, even though he did not “make” false statements under *Janus Capital Group v. First Derivative Traders*, his distribution of false statements constituted a “device, scheme, or artifice to defraud” or an “act, practice, or course of business which operates . . . as a fraud or deceit” under subsections (a) and (c) of Rule 10b-5? On December 3, 2018, the Supreme Court heard oral argument on that question in *Lorenzo v. SEC*. The stakes in *Lorenzo* are high. The SEC argues that prohibiting it from penalizing distributors of false statements will create a significant hole in its enforcement authority. Lorenzo responds that penalizing mere distributors under Rules 10b-5(a) and 10b-5(c) will render *Janus* a nullity, erode the Supreme Court’s limitations on liability for aiding and abetting, and lead to a deluge of private securities litigation. The Supreme Court’s anticipated decision will have a significant impact on liability for distributors of false statements.

Background

Petitioner Lorenzo was the director of investment banking at Charles Vista LLC, a registered broker-dealer. Lorenzo’s client, Waste2Energy Holdings, Inc. (W2E), claimed to have developed technology that could generate electricity by converting trash into gas. That technology never materialized, however, and W2E issued a Form 8-K—which Lorenzo received—in which it changed its valuation of the technology from $10 million to nothing.

After learning that W2E had written off this $10 million asset, Lorenzo sent two emails to potential investors marketing a W2E debenture offering. The emails itemized several “layers of protection” that investors would enjoy and attributed a $10 million value to the asset Lorenzo knew was worthless. The other promised layers of protection also did not exist. The emails stated that they were sent at the request of Charles Vista’s president. However, Lorenzo signed the emails with his name and title, and invited the recipients to call him with questions.

Lower Court Decisions

Based on the false statements in Lorenzo’s emails, the SEC commenced cease-and-desist proceedings against him, charging him with violations of section 17(a)(1) of the Securities Act of 1933, section 10(b) of the Securities Exchange Act of 1934, and Rule 10b-5. Lorenzo proceeded to a hearing before an administrative law judge (ALJ). The ALJ found that (1) Charles Vista’s president had drafted the emails, which contained numerous false statements; (2) Lorenzo had sent the emails at the president’s request; and (3) Lorenzo had, at a minimum, acted recklessly in so doing. Based on those findings, the ALJ fined Lorenzo and banned him from participating in the securities industry. The SEC sustained the ALJ’s decision, finding that Lorenzo knew that the emails’ key statements were false.
A divided panel of the D.C. Circuit agreed in part. The court found that substantial evidence supported the SEC’s determination that Lorenzo acted with knowledge of the emails’ falsity. Nonetheless, applying the Supreme Court’s decision in Janus—which held that the “maker” of a statement for purposes of Rule 10b-5(b) is the person or entity with “ultimate authority” over that statement—the court concluded that Charles Vista’s president, not Lorenzo, had “made” the false statements in the emails. Thus, it rejected the SEC’s finding that Lorenzo had violated Rule 10b-5(b).

The court further held, however, that Lorenzo’s knowing dissemination of false statements constituted a violation of section 17(a)(1), section 10(b), and Rules 10b-5(a) and 10b-5(c) (the “scheme liability provisions”). Unlike Rule 10b-5(b), the court explained, the scheme liability provisions do not require a violator to “make” a false statement. Instead, those provisions are violated by any “device, scheme, or artifice to defraud” or by conduct that “operate[s] as a fraud or deceit.” The court concluded that Lorenzo’s conduct fit within those prohibitions.

The third member of the panel, then judge Brett Kavanaugh (who has recused himself from the proceedings before the Supreme Court), dissented. He argued that permitting the SEC to penalize someone under the scheme liability provisions for a false statement that is not actionable under Rule 10b-5(b) undermines the distinction between primary and secondary liability, i.e., liability for aiding and abetting.

Issues Presented and Oral Argument
In his briefing and argument before the Supreme Court, Lorenzo argues that penalizing him under the scheme liability provisions for false statements he did not “make” will undercut the Supreme Court’s decision in Janus. That decision limited liability under Rule 10b-5(b) to the “makers” of deceptive statements in order to preserve the distinction between primary actors and those who only aid and abet. This distinction matters, in no small part, because investors have a private right of action against primary actors, whereas only the SEC can pursue aiders and abettors. Lorenzo argues that if someone who did not make a false statement can be held primarily liable for that statement under the scheme liability provisions, then the SEC could repackage defective Rule 10b-5(b) claims by arguing that actions that merely aided and abetted a fraud—such as Lorenzo’s emails—instead constituted a primary fraudulent scheme. This, Lorenzo argues, would destroy the distinction between primary and secondary liability that the Court sought to preserve in Janus. To avoid such an outcome, Lorenzo would interpret only Rule 10b-5(b) to cover fraudulent misstatements and would read the scheme liability provisions to require some additional conduct beyond a mere statement.

The SEC responds that the different provisions of Rule 10b-5 have overlapping coverage and that penalizing Lorenzo under the scheme liability provisions will not undermine the distinction between primary violators and aiders and abettors. According to the SEC, knowingly distributing the false statements of others in an effort to induce investment “fits comfortably” within an ordinary understanding of a “device, scheme, or artifice to defraud” or an “act, practice, or course of business which . . . would operate as a fraud,” making Lorenzo a primary violator of
the scheme liability provisions. The SEC contends its enforcement efforts would be undermined if it could not penalize fraudulent conduct under the scheme liability provisions simply because, under Rule 10b-5(b), the relevant person did not “make” the false statements at issue. Specifically, the SEC warns of a “loophole” that will arise if the Court accepts Lorenzo’s position. To hold someone liable for aiding and abetting pursuant to 15 U.S.C. §78t(e), the SEC must first prove a primary violation. If the person who “makes” the relevant statement does not know it is false, no primary violation will occur. Thus, those who distribute the statement with knowledge of its falsity cannot be held liable for aiding and abetting.

During oral argument, several members of the Court viewed Lorenzo’s argument skeptically. Justices Elena Kagan, Sonia Sotomayor, and Samuel Alito each suggested that sending a false email is an “act” that can properly give rise to primary liability under Rule 10b-5(c). Justices Ruth Bader Ginsburg and Stephen Breyer, too, emphasized Lorenzo’s active role in sending the emails, suggesting that his conduct was properly penalized as a primary violation of the securities laws—not an instance of mere aiding and abetting. Justices Kagan and Sotomayor also challenged Lorenzo’s reliance on Janus, emphasizing that its limitation of liability to “makers” of false statements was explicitly based on the term “make” in Rule 10b-5(b), which does not appear in the scheme liability provisions and thus does not apply to those provisions.

Justice Neil Gorsuch, by contrast, indicated some receptiveness to Lorenzo’s argument that the D.C. Circuit had blurred the distinction between primary and secondary violators. Justice Gorsuch noted that the only “acts” alleged were the statements in the emails—which, under Janus, Lorenzo did not “make”—and thus Lorenzo might be more properly characterized as an aider/abettor than a primary violator.

**What Is at Stake?**

The Supreme Court’s decision in Lorenzo will have important implications for the scope of securities fraud liability. If Lorenzo prevails, then liability for isolated deceptive statements will be limited to those who “make” them, a narrow class that includes only those with “ultimate authority” over the contents of a statement. Those who do nothing more than knowingly distribute false statements “made” by others will not face private civil liability under Rule 10b-5, although the SEC could still prosecute them as aiders and abettors if it can show a primary violation by another.

On the other hand, if the Supreme Court adopts the SEC’s position, then distributors of false statements will be subject to liability under the scheme liability provisions, even if they lacked ultimate authority over the statements’ contents and did not in fact draft the statements. Such a ruling may encourage the SEC and private plaintiffs to recast actions that were previously understood as aiding and abetting others’ misstatements as “schemes” or “practices” that independently violate Rules 10b-5(a) and 10b-5(c). Courts may thus have to identify the point at which promotion of others’ misstatements ceases to simply aid and abet, and instead becomes a separate deceptive scheme.
Because Justice Kavanaugh has recused himself from consideration of the case, Lorenzo will be decided by an eight-member Court. Should the Court split 4–4, the D.C. Circuit’s decision holding that Lorenzo’s statements violated the scheme liability provisions would remain undisturbed. In that case, a circuit split would remain in place, with the D.C. and Eleventh Circuits holding that false and misleading statements are actionable under the scheme liability provisions, and the Second, Eighth, and Ninth Circuits holding that something more is required to violate those provisions. Private plaintiffs thus would be able to pursue claims under the scheme liability provisions in D.C., Alabama, Florida, and Georgia that would be legally insufficient elsewhere.

Jessica Ortiz, Caleb Hayes-Deats, and Michelle Parthum are with Molo Lamken LLP in New York City, New York; Washington, D.C.; and Chicago, Illinois.
FINRA’s New Report on Broker-Dealer Cybersecurity Practices
By John E. Clabby

The protection of customer personal data continues to be a priority for the Financial Industry Regulatory Authority (FINRA), primarily from an examination perspective and, the author predicts, increasingly from an enforcement perspective. In its December Report on Selected Cybersecurity Practices—2018, FINRA shares information learned during its examinations to help broker-dealer firms to increase the effectiveness of their cybersecurity programs. Attention to this report will assist even the most sophisticated firms in both strengthening their data security controls and responding to FINRA examination requests.

This article first summarizes the key regulations that govern broker-dealers’ data management and protection efforts. The article then describes the key points of the report. Finally, it offers some observations from the author’s practice, to amplify the suggestions in FINRA’s report.

The Legal Landscape for Protection of Customer Data
With respect to member cybersecurity practices, FINRA has focused its efforts on ensuring compliance with Security and Exchange Commission (SEC) regulations on privacy and data integrity and security. The main three of those regulations, as listed by FINRA in its public statements on cybersecurity, are described below.

First, Regulation S-P (17 C.F.R. § 248.30) requires, among other things, that firms adopt written policies and procedures to secure the confidentiality of customer records and information, and to protect those records against anticipated threats and unauthorized access. Regulation S-P also demands immediate and annual disclosure to customers of a firm’s privacy policies and practices. In addition, the regulation governs the disclosure of nonpublic personal information and account number information that is permitted to unaffiliated third parties.

Second, Regulation S-ID (17 C.F.R. § 248.201–202) requires that securities firms implement a written program to detect, prevent, and mitigate identity theft in connection with certain customer accounts. Those accounts include retail brokerage accounts or any other personal accounts with a reasonably foreseeable risk to customers from identity theft.

Third, the Securities Exchange Act of 1934 (17 C.F.R. § 240.17a-4(f)) requires that firms that keep records by means of “electronic storage media” maintain those records in a “non-rewriteable, non-erasable format” and in such a way that it will “verify automatically the quality and accuracy of the storage media recording process.” The requirement to preserve electronic records in this way, sometimes known as the “write once, read many” (or “WORM”) format, was the basis for the $14.4 million in fines against 12 firms that FINRA announced in December 2016.
Of these regulations, perhaps Regulation S-P is the most important to examinations, as it is broadest in scope and can often be made to fit, fairly or unfairly, a wide range of a firm’s data protection conduct.

**FINRA’s Report on Selected Cybersecurity Practices—2018**

FINRA’s review of cybersecurity programs under these regulations is, perhaps surprisingly, technical in nature. That is, it includes not just an assessment of systems governance, policies and procedures, and staff training, but also a review of risk assessments, technical controls, and system change management. Examinations may also test incident response planning, vendor management, and active data loss prevention.

Member firms facing these inquiries will find that responding to some are straightforward, such as proving both staff trainings and risk assessments, because those tasks can be largely outsourced to third parties along with the proof of same. But other areas of cybersecurity readiness must be integrated into business practices on a continual basis, including general technology governance and incident response preparedness. Those are also harder for a firm to track over time and for FINRA to measure and benchmark.

It is into this regime that FINRA’s new report, released on December 20, 2018, enters. It is the first such report in three years, and it goes into considerable detail on what FINRA has learned from its examination program. A practitioner in this area should study it in its entirety, but a few highlights follow.

First, the report observes that “some firms face challenges maintaining effective cybersecurity controls at their branch locations.” FINRA notes that branches tend to have less developed cybersecurity controls than the home office and that an effective practice would include developing “branch level” written supervisory procedures (WSPs) addressing “comprehensive guidance.” The report also suggests that an “asset inventory” be completed at the branch level so that the firms know “the scope of assets they need to protect.” Finally, FINRA names as an effective practice that the home office conduct “periodic exam visits or risk-based audits” at each of the branches.

Second, the report discusses “phishing”—the use of deceptive emails or other e-messages to spread malware or fraudulently obtain information or money—as “one of the most common cybersecurity threats firms have discussed with FINRA.” Consistent with common guidance for controls against social engineering cyber attacks, FINRA names the following, among others, as effective practices: training, email scanning and filtering, simulated attacks, segmenting customer assets and information, and multifactor authorization.

Third, the report details the causes of, and possible prevention and mitigation of, insider threats, which are threats to data security from those who already have access to firm systems and can therefore circumvent many firm controls designed only to repel third-party access. FINRA recommends ensuring “proper access” to data, including “that systems entitlements are aligned
with specific job functions and assigned only on a need-to-know basis.” This is sometimes known as the “policy of least privilege,” and in its simplest form, it ensures that a summer intern, for example, is not provided a username and password that would allow unlogged access to account data for the firm’s entire customer and lead database.

Fourth and finally, the report describes the risk and potential controls over threats to data integrity from the proliferation of mobile devices. FINRA notes as effective practices robust “bring your own device” standards, removal of applications that violate the firm’s policies, and reporting procedures for lost or stolen devices, including personal devices with access to firm data.

**Additional Considerations for the Industry**

In light of FINRA’s conclusions in its report, and in consideration of the author’s observations from practice, there are four additional points to consider. Because the report focuses in large part on prevention rather than on mitigation during a breach, the first two suggestions that follow attempt to highlight the critical role that breach response can have in limiting the scope of a data loss incident.

First, each firm should review, test, and, if necessary, revise its incident response plan. This plan is in addition to the WSPs, which should set out the cybersecurity controls themselves. The incident response plan should focus instead on what to do in the event of an actual or suspected breach of customer personal information. The incident response plan should be a user-friendly document that sets out a process for how data security incidents are identified, reported, escalated, mitigated, and remediated.

To this end, most incident response plans benefit from having at least the following two attachments. The first is the internal list of contacts to join the incident response team in the event of a data security incident, with after-hours contact information and secondary contacts for each position. The plan itself would offer guidance by role and responsibility, but this attachment should have the actual names and mobile numbers of the primary and secondary employees. The second attachment should include the preapproved vendors to assist in the event of a data breach, including insurance broker, cybersecurity expert, legal assistance, and media relations team. An additional best practice: The key contact could call those individuals periodically to check in and remind them that they may receive an emergency call.

As a second key point, each firm should name a single point of contact for interaction with the regulators in the event of a data incident, and train that individual as part of the incident response planning. The report suggests in a few places that a firm designate an individual officer (or branch manager) as being ultimately responsible for cybersecurity, which is sound advice. But this suggestion is for a different role. Rather than being the person responsible for the cybersecurity controls, this person is ultimately responsible for reporting an incident to FINRA or other third parties, which often requires a different, nontechnical skill. This professional need not be—and often should not be—a cybersecurity expert, because during an incident, the
technical cyber expert will be working on investigating and remediating the incident. The suggested role may be better suited for the employee who has regular interaction with the firm’s FINRA regulatory coordinator. This person should also receive training on, and perhaps meet in advance with, the local Federal Bureau of Investigation field office, which is typically the point of contact for larger-scale data security incidents affecting the securities industry or markets.

As a third key point from the report, certain firms have a profile that makes an incident more likely or, if it occurs, more damaging to the customers and the firms. The report noted the risks from branch offices. Three additional profiles include those firms experiencing rapid growth, those serving aged investors, and those undergoing a merger with other firms. Rapid-growth firms are often adding customers and opportunities faster than their technical systems can grow to match. Elder investors present particular challenges for data security, including an increased risk of being a victim of identity theft, Internet-related scams, and other forms of elder abuse that manifests as a threat to data integrity. Finally, firms that are merging or acquiring or being acquired may see technical challenges to protection (or risk inadvertent disclosure) in the integration of systems. Firms with these profiles need to be particularly attendant to cyber risk.

As a fourth key observation, mentioned in a few areas in the report, firms should focus resources on vendor management for cybersecurity. This is when a firm studies the data security controls of those with whom it contracts or subcontracts to process, collect, or hold customer data or those third parties that, through contract relationships with the firm, have access in some capacity to its systems. This inquiry would include ensuring not only that vendors trusted with the firm’s customer data have sufficient technical controls but also that vendors—including those that do not possess the firm’s customer data—cannot be used as a bridge to access data on the firm’s servers. Such a focus would include reviewing vendor contracts to determine whether vendors have agreed to appropriate data management practices, to specify how notice will be made to firm customers in the event of an incident at the vendor affecting customer data, and to shift liability as appropriate between the firm and the vendor. A firm with several vendors, each of which holds its customers’ personal information or has system access in whole or in part, will typically benefit from a review of the overall relationship structure and possible consolidation.

Conclusion
The new FINRA Report on Selected Cybersecurity Practices provides granular, technical advice to broker-dealers on developing and strengthening cybersecurity protections for customers. While FINRA was not explicit that this list of “effective practices” would be the basis for potential investigations and enforcement actions in the future, it is a fair inference from the report’s detail that these examples and trends are more than just general nudges toward better practices. Indeed, FINRA’s 2019 Risk Monitoring and Examination Priorities Letter indicates that the report’s suggestions may form the basis, in whole or in part, for future, more detailed regulation of industry participants.

John E. Clabby leads Carlton Fields’s Securities & Derivative Litigation Practice Group from the firm’s Tampa, Florida, office.
This article was drafted in conjunction with an ABA regional CLE workshop, “Second Annual Current Issues in FINRA Arbitration and Enforcement,” held February 22, 2018, in Tampa, Florida. The workshop was cosponsored by the Securities Litigation Committee and the Privacy & Data Security Committee of the Section of Litigation.
EDITORIAL BOARD

Committee Cochairs: Julie Firestone, Peter M. Adams
Journal Editors: Noah Katsell, Breton Leone-Quick, Takeo Kellar, Jessica Valenzuela Santamaria
Web Editors: Patrick G. Rideout
Staff Editor: Steve Gartland

The views expressed herein are those of the author(s) and do not necessarily reflect the positions or policies of the American Bar Association, the Section of Litigation, this committee, or the employer(s) of the author(s).

ABA Section of Litigation Securities Committee
https://www.americanbar.org/groups/litigation/committees/securities/