Passing the Exam: What You Need to Know

By Joshua Horn, Ernest E. Badway and Christopher Varano

Being examined by the SEC or FINRA is never a fun process. Further, the frequency of their knocking at your proverbial door is only likely to increase in the future. In fact, the SEC has stated that it will prioritize never-before-examined investment advisers and investment companies this year.

Collectively, the SEC and FINRA conduct thousands of examinations of regulated entities each year. They demand to review your books and records, interview your firm's management and employees, analyze your firm's operations, and, in many instances, conduct an onsite visit of your offices. In the end, rarely do you get off without any additional action. The most typical outcome of an examination by the SEC's Office of Compliance Inspections and Examinations ("OCIE") is a deficiency letter, requiring prompt action by your firm to correct any of the items noted in the letter. FINRA similarly concludes with an Examination Report summarizing any risk areas that it found and requiring you to submit formal written response identifying corrective actions that you have taken or plan to take.

Thus, firms must take steps now to prepare for and avoid any potential fines or enforcement actions that could result from a failed examination. The SEC and FINRA have each outlined their 2016 examination priorities, and we have identified two topics likely to be high on these regulators' list: protecting senior investors and cybersecurity compliance.

Senior Investors

The SEC and FINRA have clearly prioritized assessing how retail firms are dealing with their older clientele. Over the past few years, these regulators have conducted exam sweeps focused on how firms conduct business with senior investors ("investors aged 65 years old or older") as they prepare for and enter into retirement. In general, the SEC and FINRA's past examinations have focused on a broad range of topics, such as: a) the types of securities being sold to senior investors; b) training of firm representatives with regard to senior specific issues and how firms address issues relating to aging (e.g., diminished capacity and elder financial abuse or exploitation); c) use of senior designations, firms' marketing and communications to senior investors; d) types of customer account information required to open accounts for senior investors; e) suitability of securities sold to senior investors; f) disclosures provided to senior investors; g) complaints filed by senior investors and the ways firms tracked those complaints; h) and supervision of registered representatives as they interact with senior investors.

The SEC and FINRA are now narrowing their focus to divide and conquer. In the coming year, the SEC will be focused on assessing firm controls related to retirement investments and the type of retirement advice being given to clients of investment advisors and broker-dealers. In particular, the SEC is planning on continuing their "ReTIRE" initiative, which it launched in June 2015 as a multi-year examination initiative, focusing on SEC-registered investment advisers and broker-dealers and the services they offer to investors with retirement accounts. As part of the ReTIRE initiative, OCIE will examine the types of retirement services being offered, focusing on whether there is a reasonable basis for recommendations, conflicts of interest, supervision and compliance controls, as well as marketing and disclosure practices.

FINRA is taking a more direct approach, focusing directly on senior investors themselves. Last April, FINRA launched its Securities Helpline for Seniors. According to FINRA's year-end report for the Helpline, FINRA received calls on topics ranging from how to review an investment account statement, to assistance with lost securities, to concerns of potential unsuitable recommendations, fraud, or illegal activity involving brokerage accounts and investments, as well as abuse and exploitation of seniors by persons outside of the securities industry. In particular, FINRA noted that it addressed instances where registered representatives have borrowed large sums of money from elderly clients, taken control of assets through Powers of Attorney and other mechanisms, or recommended products that are not suitable for an elderly investor but provide high commissions and payouts to the salesperson. Indeed, FINRA has reported that some of these calls resulted in follow-up calls from FINRA and ultimate referral to federal and state authorities.

In preparing for its upcoming examinations, FINRA is advising firms to monitor senior investors' accounts for red flags of possible abuse, such as overly aggressive investments or unusual asset movements, including to recipients outside of the country. The scope of FINRA's 2016 examinations in this area will include suitability and concentration concerns related to senior investors, as well as recommendations regarding higher-cost products that may drive unsuitable recommendations and affect product performance to the detriment of the investor.

Our Take: If you have not already done so, it is critical that you revisit your policies and procedures relating to senior clients. If you do not have policies and procedures, you need them. At a minimum, you should consider placing all accounts of anyone 65 years old and over on some form of heightened supervision. By doing so, you are in a better position to learn about issues before they become a problem and, worse yet, get reported to FINRA through the hotline. Senior investors are actively seeking FINRA's assistance on issues from the mundane to the serious. Regarding those more serious issues, FINRA has demonstrated its intention to address a variety of those issues directly. However, many of these issues can be avoided by simply improving the lines of communication with your senior clients.

From our perspective, one of the biggest issues will be the suitability of investment recommendations. By having policies and procedures that demand your attention to this issue (such as heightened supervision), you may avoid liability and regulatory issues in the future. Thus, it may be time to dust off your Written Supervisory Procedures (WSPs) and take a hard look at how they address elder and retirement account issues.

Cybersecurity

In the wake of numerous data breaches and scandals, cybersecurity has become an even more heightened area of focus for the SEC and FINRA. In September 2015, the SEC launched a Cybersecurity Examination Initiative focused on the following areas:

ABOUT THE AUTHORS

Joshua Horn and **Ernest E. Badway** are Partners in the litigation department of Fox Rothschild LLP, www.foxrothschild.com. They can be reached at jhorn@foxrothschild.com and ebadway@foxrothschild.com respectively. **Christopher Varano** is an Associate om the Litigation Department of Fox Rothschild. He can be reached at cvarano@foxrothschild.com.

1. Governance and Risk Assessment: does a registrant have adequate governance and risk assessments processes and policies in place to address the following points.

2. Access Rights and Controls: does a registrant have basic controls to prevent unauthorized access to the systems and information.

3. Data Loss Prevention: does a registrant have an adequate program to monitor electronic data that is sent out of the firm by employees or through third parties; are there unauthorized transfers being made.

4. Vendor Management: does a registrant have practices and controls related to vendor management, such as due diligence as to vendor selection, oversight and contract terms.

5. Training: does a registrant have an adequate training program for those employees and vendors who could put the firm's data at risk.

6. Incident Response: does a registrant have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events.

Not to be outdone, FINRA also remains focused on firms' cybersecurity preparedness. FINRA is concerned with risks that firms face from unauthorized internal and external access to customer accounts, online trading systems and asset transfer systems, as well as in the management of their vendor relationships. Thus, in the coming year, FINRA plans to review firms' approaches to cybersecurity risk management and examine one or more of the following topics: governance, risk assessment, technical controls, incident response, vendor management, data loss prevention and staff training. Additionally, as part of its examinations, FINRA may also assess firms' abilities to protect the confidentiality, integrity and availability of sensitive customer and other information.

Our Take: The SEC and FINRA have given you a guidepost for your own internal review to ensure that you are focused on the importance of implementing certain cybersecurity measures. We anticipate that the SEC and FINRA will start issuing heavy sanctions upon non-compliant firms in the coming months and years. Here are some tips for being prepared:

Conduct a Risk Assessment: Know what you have on your systems that need protection. You cannot protect what you do not even know that you have, so undertake an internal review of the data that you collect and store on your firm's systems. You must then test, retest, and retest your systems (including your staff) for gaps and vulnerabilities. Hackers are very sophisticated. Do what you can to stay ahead of the curve on understanding the risks to your systems and staff.

Written Policies and Procedures: Be certain that you have detailed written policies and procedures on cybersecurity, including what must be done in the event of a breach. These policies should also detail the known risks – such as working with third parties – and how the firm intends to address them. Importantly, develop an incident response plan. An incident response plan is like insurance; you make a large investment that you hope you never have to use. If you have a breach, then you have to have a detailed plan on what you are going to do about it. The plan should detail what you will do in the event of a breach (vis-à-vis your regulators, your employees and your customers), how you will fix the gap and prevent it from happening again.

Education and Training: Educate your employees on data security issues. Strong cybersecurity policies and procedures will not serve their purpose unless you provide your employees with adequate education and training. Be sure to communicate your cybersecurity policies and procedures to all individuals associated with your firm. Thereafter, conduct adequate and recurring training on those policies, and emphasize the importance of diligence when it comes to cyber-awareness. A well-trained staff can help you avoid such things as phishing scams and missteps in the event of a breach.

Strong Passwords and Encryption: Insist on your employees using secure passwords. Many phishing schemes will poke and prod a firm until a weak link in your employ is exposed. One way to prevent this is to have your IT or security consultant conduct a phishing scam directed to your employees to figure out who may be a weak link, and then address those weak links. Also, ensure that your systems (including portable devices) have adequate encryption. Otherwise, should an unprotected device be stolen and information exposed, you can bet your regulator will have an issue.

Insurance: Do not assume that your current insurance policy covers the aftermath of a cyber-event. If you think you have coverage, make sure you document that understanding so that you do not have a shock when it is too late to do anything. A sound policy will cover, among other things, the costs of notifying your customers of a breach and the costs of technical support to close the gap.

Client Involvement: Your cybersecurity plans should extend outside your firm as well. In order to have sound cybersecurity protocols, you need to do more than just physically protect your systems and have written supervisory programs. Specifically, you need to fully engage your clients to be part of the protocol. Their participation can make your program work that much better than without them. Every firm should educate their clients of what type of materials, electronic or otherwise, that the client should expect to receive from the firm. You should likewise tell clients to report back to you if they receive something not in keeping with the list you previously provided. For example, clients should be reminded that trades and money transfers are not handled via email. Any email solicitation of trades or transfers should be reported to the firm because that may reflect a security gap.

Many clients have access to their accounts online. These clients should be reminded not to share their passwords with anyone. Likewise, the firms should have a multiple verification process to allow clients to access their statements online (i.e., a password and a security question to which only the client would know the answer). Finally, you should consider having a standard presentation that you can provide clients about your cyber-security protocols. In other words, let your clients know what you have and what you are doing to protect their data.

In short, any sound data security program is going to engage a firm's clients as much as its own internal systems, programs and policies. A collective effort is the best course to protect firm and client data. Without this joint engagement, you only run a greater risk of client harm when you have a breach. Additionally, you can use your cybersecurity as a way to market to your clients, which may also help recoup some of the cost associated with bolstering your policies and procedures. Indeed, clients are well aware of these issues and want to have some sort of assurance if they are going to trust you with their money. If your firm does not have these key elements in its data security program, you have set yourself up for disaster. Take the time, spend the funds necessary; protect yourself and your clients.

Final Thought

In sum, firms need to be prepared for the coming onslaught of examinations from both the SEC and FINRA focusing on senior and cybersecurity protections. Act now; do not wait for the SEC or FINRA to pay you a visit. Protect your firm, protect your clients, and avoid enforcement actions by your regulators. The SEC and FINRA have each painted a picture for you. You would only have yourself to blame if you do not act now before you hear from your regulator. ✦