

APRIL 8, 2021

For more information,
contact:

Carmen Lawrence
+1 212 556 2193
clawrence@kslaw.com

Russell Johnston
+1 212 827 4081
rjohnston@kslaw.com

Russ Ryan
+1 202 626 5457
rryan@kslaw.com

Russell Sacks
+1 212 790 5369
rsacks@kslaw.com

Michael Watling
+1 212 827 4082
mwatling@kslaw.com

Ana Daily
+1 212 556 2140
adaily@kslaw.com

Steve Miller
+1 212 790 5363
smiller@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

SEC and FINRA Emphasize Cybersecurity, AML, and Reg BI as Key Areas of Focus for Broker- Dealer Examinations in 2021

INTRODUCTION

The U.S. Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) have each published their annual examination priorities for 2021, signaling areas of scrutiny that broker-dealers should expect in upcoming regulatory exams. Both sets of priorities offer a road map of the issues of concern to regulators and provide guidance on what market participants – particularly broker-dealers – can do to anticipate those concerns and mitigate regulatory risks. Given the shared focus of both the SEC and FINRA in certain areas, broker-dealers should pay close attention to aspects of their businesses where these shared priorities overlap. This alert explores several of these areas of mutual concern, namely (i) information protection and cyber security, (ii) anti-money laundering policies, and (iii) sales practices, especially as they relate to Regulation BI obligations. We conclude by offering some practical takeaways to help broker-dealers mitigate risks and establish credible evidence of their compliance efforts to comply during regulatory examinations.

OVERLAPPING PRIORITIES

Information Protection and Cybersecurity

The SEC and FINRA both highlighted information protection and cybersecurity as key areas of focus for their 2021 examinations, especially as remote work environments persist. In its report titled “2021 Examination Priorities” (the “SEC Report”), the SEC’s Division of Examinations conveyed its increased concerns about endpoint security, data loss, remote access, use of third-party communication systems, and vendor management.¹ Looking ahead, the SEC will examine whether firms took “appropriate measures to: (1) safeguard customer accounts and prevent account intrusions, including verifying an investor’s identity to prevent unauthorized account access; (2) oversee vendors and service



providers; (3) address malicious email activities, such as phishing or account intrusions; (4) respond to incidents, including those related to ransomware attacks; and (5) manage operational risk as a result of dispersed employees in a work-from-home environment.”²

The SEC Report clarifies the agency’s expectation that broker-dealers will identify and mitigate risks beyond changed circumstances caused by the pandemic. As normal business operations remain disrupted for many financial services companies, the report puts firms on notice that the SEC’s Division of Examinations will review registrants’ business continuity and disaster recovery plans and cautions “systemically important registrants” in particular that they should ensure their plans account for the “growing physical and other relevant risks associated with climate change.”³ This caution is an important one inasmuch as the regulators are signaling that, having functioned wholly or partly remotely during the pandemic, firms will now be expected to retain and implement such working procedures quickly.⁴

FINRA identified additional cybersecurity concerns in its own “2021 Report on FINRA’s Examination and Risk Monitoring” (the “FINRA Report”).⁵ Regarding oversight of vendors, the FINRA Report notes that some firms lack formal policies and procedures for reviewing vendor cybersecurity controls, adding that firms are expected to manage the “lifecycle” of their engagement with all vendors from onboarding through relinquishment or destruction of all non-public client information.⁶ The report also identifies inadequacies concerning data loss prevention and access management, as some firms failed to encrypt confidential data and implement controls over who can access sensitive data.⁷ Finally, the FINRA Report highlights emerging risks related to increasingly sophisticated ransomware and phishing emails.⁸

Given the shared focus of the SEC and FINRA on risks associated with data protection and cybersecurity, broker-dealers should consider periodically evaluating whether their written policies and procedures effectively address these concerns, especially in light of recent operational and technological challenges that will likely persist into the foreseeable future.

Best practices suggested by both the SEC and FINRA include establishing and regularly testing formal incident response plans and implementing policies and procedures to protect non-public investor information.⁹ Further, to avoid some of the examination pitfalls addressed in the FINRA Report, and to enhance operational procedures relating to cybersecurity, firms should consider reviewing the effects of information silos within their institution: collaboration and information sharing between business departments – including technology, risk, compliance, fraud, and internal investigations – is frequently being identified as a best practice in cybersecurity assessments. When implementing these practices, firms should pay particular attention to incidents such as systemwide outages, email/account takeovers, fraudulent wire requests, imposter websites, and ransomware.

Anti-Money Laundering (AML)

AML compliance is another longstanding area of common concern for both the SEC and FINRA. The SEC Report makes clear that the agency continues to assess whether broker-dealers are complying with their AML obligations under the Bank Secrecy Act (BSA).¹⁰ Specifically, the agency’s Division of Examinations will review whether firms have policies and procedures that are reasonably designed to verify customer identities and the beneficial owners of legal entities; are conducting due diligence in line with the BSA’s Customer Due Diligence rule; are monitoring for suspicious activity and meeting their obligations to file Suspicious Activity Reports (SARs); and are independently testing their AML programs.¹¹

The FINRA Report highlights several areas in which FINRA examiners have observed AML deficiencies by broker-dealer firms. For example, some firms failed to properly document investigations of suspicious activity, while others did not require staff to notify the firm’s AML department or file SARs when appropriate, and/or improperly relied on clearing firms to monitor transactions and file SARs.¹² The FINRA Report also identifies other notable deficiencies including inadequate surveillance tools, insufficient program testing, and unclear delegation of responsibilities within AML programs and financial crime compliance departments.¹³ Of particular interest, recent enforcement action in the area



has cited that, as firms grow, they are expected to expand their anti-money laundering compliance and monitoring functions accordingly.

The FINRA Report references several ongoing AML risks, including the frequently cited risks relating to transactions in microcap securities through omnibus accounts at non-U.S. financial institutions and non-U.S. affiliates of U.S. broker-dealers.¹⁴ It also mentions risks associated with firms' rapidly expanding use of special purpose acquisition companies (SPACs) without adequate written supervisory procedures (WSPs) to address due diligence and fraud detection in connection with SPAC-related transactions.¹⁵

Given these SEC and FINRA concerns, broker-dealers are wise to focus on tailoring their procedures and on periodic AML training to ensure their employees understand the firm's obligations. Finally, meaningful and independent testing of AML controls, which is required by the BSA, is critical to evaluating whether policies and procedures are reasonably designed to detect, investigate, and report suspicious activity.

Sales Practices and Regulation Best Interest (Reg BI)

Finally, both the SEC and FINRA continue to be focused on policing retail sales practices, especially following the adoption of Regulation BI. For broker-dealers, the dominant sales practice focus for the 2021 examination cycle will likely be compliance with the newly promulgated "best interest" standard of conduct for customer recommendations. Under Reg BI,¹⁶ broker-dealers and associated persons subject to Reg BI have four primary obligations:

- **Disclosure** – A broker-dealer must provide a retail customer, either before or at the time of a recommendation, a "written, full and fair disclosure" of all material facts related to the scope and terms of its relationship with the customer, and all material facts relating to any conflicts of interest associated with the recommendation.
- **Care** – A broker-dealer must exercise reasonable diligence, care, and skill when making a recommendation to a retail customer. That includes evaluating the potential risks, rewards, and costs associated with the recommendation in light of the customer's investment profile.
- **Conflicts of Interest** – A broker-dealer must establish, maintain, and enforce written policies and procedures reasonably designed to address conflicts of interest associated with its recommendations to retail customers.
- **Compliance** – A broker-dealer must establish, maintain, and enforce written policies and procedures reasonably designed to achieve compliance with Reg BI as a whole.¹⁷

During the past year, regulatory exams related to Reg BI focused on the efforts firms were making to *implement* the new regulation. This year, the SEC says it will "expand" its focus to assessing whether firms are *complying with* Reg BI.¹⁸ Specifically, exams will assess whether broker-dealers are in fact making recommendations only when they have a "reasonable basis" to believe those recommendations are in their customers' best interests, and they will evaluate broker-dealers' processes for Reg BI compliance.¹⁹ The SEC also says its examiners will conduct enhanced transaction testing to evaluate the "recommendation of rollovers and alternatives considered, complex product recommendations, assessments of costs and reasonably available alternatives, how sales-based fees paid to broker-dealers and representatives impact recommendations, and policies and procedures regarding how broker-dealers identify and address conflicts of interest."²⁰

FINRA is similarly promising an expansion of its Reg BI exams this year "to effect a more comprehensive review of firm processes, practices, and conduct."²¹ The FINRA Report includes a practical list of questions for broker-dealers to consider in determining whether they are complying with Reg BI.²² Those questions include, among others, whether the firm has adequately trained its sales and supervisory staff on Reg BI, whether firm policies and procedures adequately



address Reg BI's recordkeeping and disclosure requirements, and whether firm policies and procedures continue to address compliance with FINRA suitability requirements (which still govern recommendations to non-retail customers).

Firms would be well-advised to review and consider each of the questions itemized in this section of the FINRA Report well in advance of their next anticipated examination. And as with other areas of novel regulatory scrutiny, firms should consider whether their documentation of measures taken to comply with Reg BI – including documentation relating to particular customers and transactions – will provide the foundation of a compelling response when examiners ask questions in this area.

CONCLUSION

The SEC and FINRA examination priorities reports provide market participants with a useful road map of the issues on which these regulators are most likely to focus in 2021. Firms subject to examination by these regulators should carefully review both past examination results and the guidance offered in these reports, particularly in the areas of cybersecurity, anti-money laundering, and compliance with Reg BI.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising." View our [Privacy Notice](#).

ABU DHABI	CHARLOTTE	GENEVA	MOSCOW	RIYADH	TOKYO
ATLANTA	CHICAGO	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
AUSTIN	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	
BRUSSELS	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE	

¹ SEC Division of Examinations, 2021 Examination Priorities (Mar. 3, 2021), <https://www.sec.gov/files/2021-exam-priorities.pdf>. See also K&S Client Alert, "SEC Division of Examinations – 2021 Priorities" (Apr. 1, 2021), <https://www.kslaw.com/news-and-insights/sec-division-of-examinations-2021-priorities>.

² *Id.* at 24.

³ *Id.* at 25.

⁴ The admonition here is more than symbolic: securities regulatory agencies are cautioning their regulated entities to expect more frequent disruption of the kind caused by severe weather, and signaling that, post-pandemic, firms will be expected to have BCPs in place to switch to remote functioning quickly in response to such disruptions.

⁵ FINRA, 2021 Report on FINRA's Examination and Risk Monitoring Program (Feb. 2021), <https://www.finra.org/sites/default/files/2021-02/2021-report-finras-examination-risk-monitoring-program.pdf>.

⁶ *Id.* at 9.

⁷ *Id.*

⁸ *Id.* at 10. While the lion's share of concern relating to data loss and ransomware attacks is reserved for retail firms, and the protection of retail investors, it is noteworthy that ransomware and data theft attacks are often targeted at institutional firms, which can serve as a repository for material non-public information.



⁹ See SEC Report at 24; FINRA Report at 10.

¹⁰ SEC Report at 27.

¹¹ *Id.* The Division of Exams also published a Risk Alert on March 29, 2011 titled “Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers” (available at <https://www.sec.gov/files/aml-risk-alert.pdf>).

¹² FINRA Report at 5-6.

¹³ *Id.*

¹⁴ *Id.* at 7.

¹⁵ *Id.* The SEC is also very focused on the use of SPACs, as evidenced by its recently announced inquiry into how underwriters are managing risks. The SEC also issued an investor alert on March 10, 2021 regarding celebrity involvement with SPACs, and the Division of Corporate Finance released disclosure guidance for SPAC sponsors, underwriters, and other market participants on December 22, 2020. See SEC Investor Alerts and Bulletin, *Celebrity Involvement with SPACs – Investor Alert* (March 10, 2021) available at <https://www.sec.gov/oiea/investor-alerts-and-bulletins/celebrity-involvement-spacs-investor-alert>, and SEC Div. of Corporation Finance, *CF Disclosure Guidance: Topic No. 11, Special Purpose Acquisition Companies* (Dec. 22, 2020) <https://www.sec.gov/corpfin/disclosure-special-purpose-acquisition-companies>.

¹⁶ General Rules and Regulations, Securities Exchange Act of 1934, 17 CFR Part 240 (2021).

¹⁷ For a more complete description of Regulation BI, see Russell D. Sacks, “Private Banking and Wealth Management” in *Broker-Dealer Regulation* (Practising Law Institute, July 2020).

¹⁸ SEC Report at 20. We believe that, as has been past practice with respect to the implementation of significant new regulation, FINRA and SEC Examination Staff have been cataloging perceived best practices during initial (i.e., 2020) examinations, and will be seeking to compare firms’ compliance to other firms’ best practices.

¹⁹ *Id.*

²⁰ *Id.*

²¹ FINRA Report at 2.

²² *Id.* at 18.