Professional Perspective

Work From Anywhere Compliance

Marc Gilman, Theta Lake

Bloomberg Law

Work From Anywhere Compliance

Contributed by Marc Gilman, Theta Lake

The Covid-19 pandemic has proved disruptive to nearly every industry and organization, including financial services regulators. Case in point. The Financial Industry Regulatory Authority (FINRA) typically publishes a set of Exam Findings and Observations in November and follows up with Exam Priorities for the coming year in January. However, in 2021 FINRA has taken a different approach. No findings were published in 2020, keeping the industry in suspense as the year closed. On Feb. 1, 2021 FINRA released a comprehensive Report on Examination and Risk Monitoring Program (2021 Report), combining retrospective observations and forward-looking exam priorities in a single document. As a result, the 2021 Report provides member firms with a one stop shop to understand the struggles of the last year and FINRA's exam priorities in the coming year.

The 2021 Report and Remote Work

Sifting through the 2021 Report as well as several Covid-19 FAQs released during 2020 demonstrates FINRA's focus on providing guidance to help firms adapt to a new work from anywhere business environment. Indeed, it seems that the establishment of remote work business models signal a longer term transformation of the traditional office. This transformation will include, at minimum, hybrid setups where office presence may be required periodically with equal reliance on home offices, co-working spaces, or anywhere with a stable internet connection. The newfound flexibility of anywhere work will continue to present challenges for firms as the permanence of previously a temporary office arrangement sets in.

The purpose of this article will be to distill the guidance of the relevant sections of FINRA's 2021 Report into a set of compliance best practices for firms navigating work from anywhere issues. A nuanced understanding of the technical, operational, and security ramifications of the topics discussed in the 2021 Report will facilitate an informed and meaningful dialogue between compliance departments and other firm stakeholders, to allow organizations to make informed decisions about how to further adopt remote work in alignment with FINRA's expectations.

Since the 2021 Report incorporates what was previously contained in two separate publications, we'll narrow our focus to the portions that have a direct impact on remote work. As such, this article will emphasize sections dedicated to firm operations and communications and sales. Within those categories, we'll examine the sections on cybersecurity, books and records, Regulation Best Interest, and communications with the public given their collective relevance to work from anywhere. While the discussions of market integrity and financial management are of equal import generally, the related compliance concerns are less significant for remote work.

2021 Report Structure

FINRA has structured each section of the 2021 Report consistently, to provide a common format for digesting information. Each section includes an outline of the defined regulatory obligations in each domain, exam observations and effective practices, a sub-section on emerging risks, and a list of additional reference resources.

Cybersecurity

The cybersecurity section kicks off with a reiteration of firms' obligations under the SEC's Regulation S-P, business continuity obligations pursuant to FINRA Rule 4370 as well as general oversight obligations under FINRA Rule 3110 on Supervision. As part of the introduction, FINRA draws a direct line between cybersecurity and remote work, stating that "[g]iven the increase in remote work and virtual client interactions, combined with an increase in cyber-related crimes, we encourage member firms to review the considerations, observations and effective practices noted in the Report." FINRA outlines several cybersecurity considerations for firms to take into account like incident identification and response, data loss prevention (DLP), encryption controls as well as tracking methodologies to determine the severity and status of risks within the organization.

Several findings from last year's examinations center around the protection of customer data. For example, a finding around DLP notes a deficiency for "[n]ot encrypting all confidential data, including a broad range of non-public customer information in addition to Social Security numbers (such as other account profile information and firm information)." From a process perspective, FINRA also observed change management failures resulting in "[i]nsufficient supervisory oversight

for application and technology changes (including upgrades, modifications to or integration of firm or vendor systems), which lead to violations of other regulatory obligations, such as those relating to data integrity, cybersecurity, books and records, and confirmations."

Finally, FINRA suggests a range of effective practices for firms to consider that include cross-functional work on managing insider threats, upleveling incident response planning, improved asset inventories, and better change management protocols.

From a compliance perspective, the cybersecurity guidance is extremely instructive. Across the board firms have deployed a range of new applications to support remote work such as collaboration tools like Zoom, Microsoft Teams, and Cisco Webex. The proliferation of Zoombombing attacks and other unauthorized meeting access means that continued rollout and maintenance of these platforms must take into account guidance around change management, system patching, and asset inventories. Monitoring and enabling uniform controls across collaboration tools to protect against Zoombombing risks is absolutely essential. Moreover, understanding if malware or malicious websites are being displayed during collaboration conversations is critical.

As it pertains to DLP, firms must consider remote work cybersecurity risks related to protecting customer data and firm confidential information from distribution during collaboration conversations and rethinking how applications containing sensitive data may be available to geographically distributed staff. The multiplicity of new data leakage vectors introduced by remote work requires a thoughtful and comprehensive response. FINRA's focus on the procedural aspects of application management and onboarding as well as technical controls that can be deployed to identify information and mitigate potential data leakage evidence the primacy of these new DLP controls.

Books and Records

Books and records are also discussed in the context of Firm Operations—FINRA stresses SEC Rule 17a-4 mandates to maintain records in non-rewritable, non-erasable format and attendant obligations to ensure these controls are enabled on relevant information. FINRA also outlines Rule 17a-4's documentation and notification requirements.

The implications of the migration to remote work for books and records rules have been meaningful given that technologies have been adjusted or adopted to support recordkeeping compliance regimes. Compliance officers should have books and records obligations in mind as they deploy new systems that support regulated activities from order taking and trade execution to corporate functions like finance as well as prospecting and customer interaction that rely on the collaboration tools discussed above. Selecting applications and vendors with expertise in financial services and establishing appropriate guardrails around leveraging new solutions for business records will help firms avert the problems FINRA identified during its 2020 exams.

Regulation Best Interest

Shifting to the next section of the 2021 Report, Communications and Sales, this article will first examine an issue that has been top of mind for compliance officers over the last two years: SEC's Regulation Best Interest (Reg BI). The new investment standard for broker-dealers went into effect in 2020 and the first round of examinations largely focused on the sufficiency of firms' compliance framework. FINRA's 2021 Reg BI priorities include: understanding how the obligation is applied when making investment recommendations, the controls in place for assessing if recommendations meet the best interest standards, and the contents and provision of Form CRS.

From a foundational perspective, ensuring that updated and consistent policies and procedures are in place across your firm is absolutely essential. This includes easy access to Form CRS and other required disclaimers and disclosures. Firms must focus on meaningful training to ensure that employees understand the importance of how and when to provide Form CRS and what products and services can be offered to customers and prospects to align with Reg BI mandates.

In a remote world, validating the distribution of Form CRS and oversight of compliance with the recommendations obligation are complex. For example, if conversations are conducted over collaboration platforms, supporting technologies can be used to overcome challenges of confirming when Form CRS has been distributed. In addition, the sophisticated AI capabilities of RegTech platforms can be deployed to determine if conversations over chat, phone, or collaboration apps contain references to Form CRS, or more broadly might be indicative of promissory statements or customer complaints that could trigger Reg BI compliance issues. On a related note, variable annuity products, which

FINRA calls out in the 2021 Report, pose similar compliance risks, so firms should consider how to manage the risks of these investment recommendation obligations in tandem.

Communications With the Public

Finally, the Communications with the Public section of the 2021 Report has meaningful repercussions for compliance professionals tasked with enabling remote work this year. FINRA flags the communications with the public Rule 2210, but practitioners should also take note of the extensive advertising section of the Covid-19 FAQs for further guidance.

In the related considerations section, FINRA covers a lot of ground from validating that marketing materials meet transparency obligations and do not contain false or misleading statements to specific concerns for communications related to digital assets and cash management accounts and considerations for the use of digital communications channels.

Not surprisingly, FINRA describes shortcomings related to digital asset and cash management account disclosures in its 2020 observations. FINRA also flags inadequate supervision of digital communications channels observing that firms are "[n]ot maintaining policies and procedures to reasonably identify and respond to red flags—such as customer complaints, representatives' email, OBA reviews or advertising reviews—that registered representatives used impermissible business-related digital communications methods, including texting, messaging, social media, collaboration apps or "electronic sales seminars" in chatrooms."

In an intersection between the 2021 Report sections on investment recommendations and communications with the public, FINRA explicitly includes new digital platforms that include "game like" features as an emerging area of risk for 2021. The gamification of finance will be a core focus in 2021, certainly in light of market gyrations related to Game Stop trading.

In terms of effective practices, FINRA focuses on policies, procedures, and training for the use of new communications tools. More specifically, FINRA stresses the need to monitor new tools and features stating "[m]arketing, compliance and information technology departments working closely together, as well as with third-party vendors, to monitor new communication channels, apps and features available to their associated persons and customers."

The challenges posed by the communications with the public rules are essentially twofold—first, define and monitor the creation of content related to financial services products and services, including digital assets and cash management accounts, and second, ensure that the platforms employees use to distribute these materials and communicate more generally align with FINRA's expectations for capture, retention, and supervision.

From a content creation perspective, particularly when compliance teams are being bombarded with proposed content from multiple sources, using technologies to vet draft advertising materials for appropriate disclaimers and disclosures and validating that they do not contain false or misleading information is essential. As the format of these advertising communications quickly moves to audio and video, finding purpose-built technologies to quickly and efficiently analyze this data at scale can meaningfully reduce the manual review burden on compliance teams.

As to the new and novel collaboration tools teams are using for internal and external communications, compliance teams must understand the capabilities of these applications and how they can be used consistent with FINRA's rules. RegTech tools now facilitate the capture, retention, and oversight of the rich features of collaboration tools, allowing for examination of what was spoken, shown, and shared across audio, video, and text. For example, modern RegTech applications detect risks across the visual elements of collaboration interactions like logos or documents shown over webcams; PII, advertising materials, and sensitive documents displayed through the screenshares; and the co-authored and edited content created on virtual whiteboards. A compliance strategy that ignores the dynamic feature sets of collaboration technologies will not pass muster when examinations roll around.

Conclusion

Collectively, the 2021 Report and this guidance provide crucial details that compliance officers can use to successfully identify potential risks and develop appropriate oversight methodologies from enhanced policies and procedures to sophisticated RegTech applications.

The solidification of remote work as the default mode for business operations will necessitate a rethinking of traditional approaches to compliance and supervision. New RegTech tools can help. As outlined above, RegTech applications are becoming an essential component of a compliance officer's strategic toolkit. RegTech systems can augment and improve

existing processes allowing for massive amounts of collaboration conversations, advertising material, order information, and other data to be analyzed consistently and effectively, helping compliance teams home in on potential risks. Hopefully background above coupled with practical guidance for addressing critical risks will help mitigate the new and weird challenges compliance officers will face in 2021.