New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
ALM.
FEBRUARY 24, 2021

Expert Analysis

What's Up With WhatsApp? The Retention of Work-Related Messages

By Lisa H. Bebchick, Shannon Capone Kirk, and Anne Conroy

With business travel grounded to a halt and in-person meetings nonexistent over the past year due to COVID-19, employees at financial firms have undoubtedly increased their use of electronic devices for business communications. While sending text and application-based messages may serve as an efficient means of communication in this global remote work environment, firms in regulated industries should ensure that their employees' communications are compliant with relevant regulatory obligations.

Regulatory guidance provides that if broker-dealers permit employees to use text and messaging applications (apps) for business purposes—or are aware that their employees are communicating via text or messaging apps, even if such use is proscribed—the firms must ensure that those communications are retained.

This article focuses on regulatory obligations for broker-dealers concerning record retention. In that context, we review regulatory guidance concerning the retention of communications sent by text (such as, Short Message Service (SMS)) and messaging apps (such as, WhatsApp and GroupMe) and recent enforcement activity involving these types of communications. We conclude with some practical steps that broker-dealers may consider to enhance compliance with regulatory obligations relating to text and app-based messages.

Firms may not be able to prevent every employee from utilizing unauthorized text or messaging apps for business communications; however they can take steps to demonstrate reasonable controls

Guidance on the Retention of Messages

Section 17(a) of the Exchange Act of 1934 and SEC Rules 17a-3 and 17a-4 thereunder require broker-dealers and their employees to preserve certain business-related communications. Financial Industry Regulatory Authority Rule 4511

requires member firms to preserve communications consistent with the Exchange Act and applicable Exchange Act rules. Whether a firm must retain a particular communication depends on the *content* of the communication, rather than the specific device or application used to transmit the communication. 17 CFR §240.17a-4(b)(4). Pursuant to Rule 17a-4(b)(4), firms have an obligation to retain records of communications that relate to their "business as such." *Id.*

Communications sent via text or messaging app are oftentimes viewed as more informal than other modes of communication (such as, email), and thus employees may not think of them as business communications that are required to be retained. Yet despite this perceived informality, if business-related, text and app-based communications fall within Rule 17a-4's retention requirements.

LISA BEBCHICK *is a partner at Ropes & Gray.* SHANNON CAPONE KIRK *is e-discovery counsel and* ANNE CONROY *is an associate at the firm.*

FINRA Regulatory Notice 17-18, issued in 2017, highlights a member firm's obligation to train and educate its associated persons on (i) the difference between business and non-business communications, and (ii) the measures required to ensure that business communications are retained, retrievable, and capable of being subject to supervisory review. In its 2020 Risk Monitoring and Examination Priorities Letter, FINRA commented that when reviewing a firm's use and supervision of communication channels, it would consider, among other factors, whether a member firm had maintained a reasonably-designed process to identify and respond to red flags that its registered representatives were using unapproved communication channels for business-related communications.

FINRA Regulatory Notice 20-16, which reviewed practices implemented by firms to transition to remote work due to COVID-19, outlined steps firms could take to minimize risks that associated persons would use unapproved systems and technology to conduct firm business. These steps included communicating clear guidance about firm expectations when working remotely and taking extra measures to reinforce that associated persons must use only firm-provided and approved communication systems and tools. And, most recently, in its 2021 Risk Monitoring and Examination Priorities Report, FINRA emphasized the importance of monitoring for red flags that may indicate that a registered representative is communicating through unapproved channels.

Ephemeral messaging apps (such as, Snapchat and Signal) allow for the automatic deletion of a communication after a short time period. Perhaps unsurprisingly, securities regulators either outright prohibit or strongly advise firms against sanctioning use of ephemeral messaging apps. In Regulatory Notice 11-30, FINRA issued guidance to member firms that their employees may not use a technology for business-related communication if the technology automatically erases or deletes the content of the electronic communication, as the automatic deletion of these communications would prevent a firm from complying with its retention obligations under Rule 17a-4. In 2018, the SEC Office of Compliance Inspections and Examinations issued guidance to firms that prohibiting the use of apps that allow for automatic destruction of messages was considered a best practice for maintaining compliance with the Investment Advisers Act of 1940.

SEC found that over a two-year period, several registered representatives had exchanged business related text messages with each other, customers, and other third parties but the broker-dealer failed to retain the communications. The broker-dealer was censured and ordered to pay a monetary penalty of $100,000.

While certain ephemeral messaging apps allow for opting out of the automatic destruction feature, taken together, FINRA and OCIE guidance suggests that firms should prohibit the use of any app with a setting allowing for automatic destruction of communications.

Enforcement Focuses on Retention

Regulators have focused attention on record retention in recent years given the explosive growth in the volume of data stored electronically by broker-dealers and because firms monitor employee compliance with applicable securities laws by reviewing their business-related communications.

While FINRA investigations of individual employees who improperly used text messages for business communications are not uncommon, in September 2020, the SEC reached a settlement with a broker-dealer concerning the use of text messages. *See* JonesTrading Institutional Servs. LLC, Exchange Act Release No. 89975 (Sept. 23, 2020). As part of an enforcement investigation of a third party, a broker-dealer produced certain electronic communications to the SEC, which referenced text messages between the broker-dealer's registered representatives and a customer. The broker-dealer, however, had failed to retain the text messages. This led to a separate almost year-long investigation focused on the broker-dealer. Ultimately, the SEC found that over a two-year period, several registered representatives had exchanged business-related text messages with each other, customers, and other third parties but the broker-dealer failed to retain the communications. The broker-dealer was censured and ordered to pay a monetary penalty of $100,000.

Compliance

In light of the obligation to retain business-related communications, before sanctioning the use of text and/or messaging apps, firms must evaluate whether they have the capability to retain such communications. Messaging apps, such as WhatsApp, WeChat, and Facebook Messenger, use different platforms and have different network requirements than SMS and Multimedia Messaging Service ("MMS") text messaging, which are standard features on iPhone and Android devices.

Firms that issue employees mobile devices have the advantage of acquiring text and app-based messages through direct access to the device. In contrast, firms that permit employees to use personal devices to access company applications and information—"Bring Your Own Device" (BYOD) firms—must ensure that they can retain records of communications sent and received on the employees' personal device. This retention can occur through Mobile Device Management (MDM) software installed on employees' personal devices, which is used to monitor, manage, and secure the data on the devices.

While there are several MDM software options with the capability to monitor and secure SMS and MMS data, there are currently few options that allow for remote access or collection of messaging app data. As a result, collection of messaging app data often must occur through a physical collection of mobile devices and/or by obtaining user names and passwords for collection from a cloud-based application. Thus, BYOD firms should consider requiring that personnel communicate about business matters only through firm-sanctioned messaging apps that allow for remote collection and monitoring.

Practical Takeaways

Firms may not be able to prevent every employee from utilizing unauthorized text or messaging apps for business communications; however, they can take steps to demonstrate reasonable controls, including by:

Maintaining a clear policy. The policy should provide that business-related communications must occur only on dedicated business accounts on approved devices installed with company MDM. Firms should also provide employee training to establish further awareness of and compliance with the policies. Ephemeral messaging apps should be prohibited.

Limiting use. By limiting use of text and messaging apps, firms can assert better control over such communications. Similarly, while messaging apps may be an efficient means of communication, especially when communicating across geographies, broker-dealers should use firm platforms (such as, firm email or instant messaging systems) for internal communications. Broker-dealers can also consider technological solutions to restrict employees' ability to install unapproved apps on company-issued devices.

Ensuring retention capabilities. To the extent that employees use text or messaging apps, firms should ensure that those communications are capable of being retained using MDM software or otherwise.

Segregating accounts on BYOD devices. Segregating business communications on personal devices can facilitate record retention and minimize privacy concerns regarding personal data.

Auditing use. If it is determined that employees are using text or messaging apps not authorized by the firm, the firm should take steps to rectify that noncompliance, which might include discipline and/or exploration of technological safeguards.

Staying apprised of technological developments. Technology is ever changing. Firms should stay apprised of developments to understand the ways employees may be communicating and how those communications can be retained.

Conclusion

With the increase in remote working due to the COVID-19 pandemic, the retention of communications sent by text or messaging app will surely remain a focus of regulators, such as the SEC and FINRA, in the near future. As such, broker-dealers should remain vigilant and ensure that appropriate controls are in place around the use and retention of these communications.