SEC Enforcement Highlights the Risks of Not Preserving Text/Chat Messages—Practical Tips for Aligning Policies with Practices to Reduce Risk

December 14, 2020

At many companies, employees are increasingly using non-business communication applications ("apps") such as iMessage, WhatsApp and WeChat for business-related communications. This trend has likely accelerated in the COVID era, as work-from-home arrangements blur traditional lines between "business" and "personal" time and many conversations that were normally held in person are now done virtually. A recent SEC enforcement action highlights the risk that these communications pose for companies subject to strict record retention requirements, such as broker-dealers pursuant to Rule 17a-4 under the Securities Exchange Act, as well as FINRA Rule 3110 and related guidance, as well as and investment advisers subject to Rule 204-2 and related guidance under the Investment Advisers Act of 1940. But it also highlights the risks that these communications pose more broadly for companies, and the need to consider adopting technologies and policies that reduce these risks.

The *JonesTrading* Order. In September 2020, the SEC reached a settlement with JonesTrading, a registered broker-dealer, for its failure to maintain business-related text messages. Broker-dealers are subject to rigorous regulatory requirements under the Exchange Act and FINRA rules to maintain and surveil business-related written communications. According to the SEC's order, JonesTrading's policies prohibited business-related communications outside of firm-sponsored systems and specifically prohibited its employees from using text messaging for business purposes. To monitor compliance, the firm relied on annual employee attestations and trainings.

In connection with an enforcement investigation unrelated to the firm, the SEC staff sought records from the firm and found references to text messages discussing the firm's business. Further review revealed business-related text messages among the firm's employees and between employees and customers and other third parties. These messages were therefore subject to retention requirements for broker-dealers. Because this business-related messaging occurred outside of JonesTrading's computer systems, however, the firm could not preserve these texts and chats, and could not produce them in response to the SEC's requests. The SEC further found that senior management knew that the employees were communicating with each other and with customers through

text messages. Indeed, senior management (including some compliance personnel) were themselves using text messaging for business purposes.

Why Discourage Business Communications on Non-Company Apps? The *JonesTrading* enforcement is based on the violation of the *per se* requirement for broker-dealers to retain business-related records, but the action has broader implications for companies that are not subject to such requirements. In general, there are several compelling reasons for companies to limit business-related communications to company systems:

- **Security**: Companies lack control over the cybersecurity and privacy of employees' personal apps. Business information that is communicated using such apps may therefore be at greater risk of being compromised as compared with the company's email and other communication platforms that are part of the firm's computer systems.

- **Discovery**: Companies' servers generally do not capture employee communications sent or received though personal apps. Thus, when conducting an internal investigation, addressing a litigation document request or responding to a regulatory investigation, companies may be unable, through their normal document search processes, to identify relevant documents that were sent using employees' personal apps.

- **Monitoring and Required Regulatory Recordkeeping**: To the extent that a company is subject to regulatory recordkeeping requirements, or monitors business communications for other compliance, regulatory or cybersecurity purposes, that monitoring process is unable to review communications on personal apps.

For these reasons, many companies (especially those subject to the broker-dealer or investment adviser requirements to preserve documents) simply prohibit the use of personal apps for business communications. Some businesses are experimenting with apps that purport to be able to preserve WhatsApp and or other chat messages on the company system. And some companies that are not subject to broker-dealer or investment adviser requirements have adopted policies that discourage such communications, but also recognize that they do occur and create affirmative obligations to preserve such records. Such policies are generally structured as follows:

- **Business Records vs. Disposable Data**: These policies often distinguish business records, which must be preserved because (a) there is a legal or regulatory requirement to preserve them, or (b) they have a lasting business value to the company, from disposable data, which does not need to be preserved.

- **Primary vs. Secondary Communications**: These policies define primary communication tools as those that automatically preserve documents on the company's servers for long periods of time (like work emails and their attachments). Any communication tool that is not a primary one is defined as a secondary communication tool (e.g., voicemails, chats, instant messages).

- **Business Records and Primary Communications**: Having defined business records and primary communication tools, these policies then provide that employees should generally use only primary communication tools to transmit business records. But such policies recognize the need for exceptions and further provide that if a business record is sent or received by an employee through a secondary communication tool, the employee must take affirmative steps to preserve that document. Such measures may include ensuring that the app is set for indefinite preservation, as well as requiring that the employee promptly move the business record to a primary communication tool, for example, by taking a screenshot of the communication and sending the image to the employee's work email.

- **Other Considerations**: Some company policies also include a requirement that, once that business record is transferred to a primary communication tool, the employee should consult with the legal department about deleting the document from the personal app. Some policies also provide that if an employee creates business records on personal apps, the employee consents to allowing the company to conduct a reasonable search for those business records on the employee's device that contains that app.

The precise scope and wording of a company messaging policy will depend on several factors and will implicate a variety of legal, HR, business, IT and reputational considerations. But tailoring policies to match the behavior of employees, the applications that they use and the expectations of the regulators can reduce regulatory risk. It can also reduce conflicts with employees when their devices have to be searched for company-related communications.

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise law clerk Michael Pizzi for his contribution to this article.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Jeff Robins
jlrobins@debevoise.com

Chana Zuckier
czuckier@debevoise.com

WASHINGTON, D.C.

Julie M. Riewe
jriewe@debevoise.com