U.S. regulators crack down on retention of electronic communications

By Daniel L. Stein, Esq., Michele Natal, Esq., and Lydia Ho, Esq., Mayer Brown LLP

APRIL 12, 2022

As technology continues to evolve and new modes of electronic communication are born, companies are faced with increased compliance challenges and heightened regulatory risks. With more employees working remotely due to the COVID-19 pandemic, there has been a significant rise in the use of texts, chats and online meetings to conduct business. As a result, U.S. regulators are focused on ensuring that companies are properly monitoring and retaining employee communications, including any business-related texts and chat communications on personal devices.

With the likelihood that many employees will continue to work from home for the foreseeable future, their reliance on text messaging, chat applications and videoconferencing will inevitably carry on. Accordingly, it is critical that companies evaluate their policies and procedures to ensure compliance with relevant communication monitoring and retention requirements.

Technology advances while enforcement heats up

In October 2021, Gurbir S. Grewal, Director of the Division of Enforcement at the Securities and Exchange Commission (SEC), warned that companies "need to be actively thinking about and addressing the many compliance issues raised by the increased use of personal devices, new communications channels, and other technological developments like ephemeral apps."

Shortly thereafter, news broke of the SEC's industry-wide sweep targeting Wall Street banks and their procedures for tracking and retaining employees' business-related electronic communications, making it clear that the SEC is stepping up enforcement and that record-keeping obligations are a priority.

At the end of the year, the SEC announced a $125 million settlement with J.P. Morgan Securities LLC (JPMS), a broker-dealer subsidiary of JP Morgan Chase & Co., for JPMS' alleged widespread failure to retain electronic communications from its employees' personal devices. This includes business-related text, WhatsApp messages and emails from personal accounts.

The SEC found that JPMS violated Rules 17a-4(b)(4) and 17a-4(j) (17 C.F.R. § 240.17a-4) applicable to broker-dealers, which specifies the minimum length of time records should be kept, the format in which records may be kept and that the records are subject to examination. JPMS admitted that from at least January 2018 through November 2020, contrary to its own policies and procedures, its employees communicated about business on their personal devices, and the company did not preserve any of these electronic communications. The SEC concluded that JPMS' failure to preserve these records deprived the SEC of evidence and "compromised and delayed" investigations.

U.S. regulators are focused on ensuring that companies are properly monitoring and retaining employee communications, including any business-related texts and chat communications on personal devices.

In a separate action, the Commodity Futures Trading Commission (CFTC) fined JPMorgan Chase Bank, N.A., J.P. Morgan Securities LLC and J.P. Morgan Securities plc $75 million for similar alleged violations dating back as far as 2015. The magnitude of the fines demonstrates the strict stance regulatory authorities are taking on record-keeping violations. And last month, a number of large financial institutions publicly disclosed in their annual reports that they are cooperating with investigations by the SEC and the CFTC regarding compliance with record-keeping obligations sent over unapproved electronic messaging channels.

The need for compliance reviews

The recent investigations signal that companies should anticipate similar U.S. regulatory inquiries and should preemptively consider whether they are complying with various regulatory record-keeping obligations. As SEC Director of Enforcement Grewal recommended, "[a] proactive compliance approach requires market participants to not wait for an enforcement action to put in place appropriate policies and procedures to preserve these communications."

As COVID-19 and other factors drive the use of a greater variety of electronic communications in the workforce, it is critical that

companies make an effort to keep up with advancing technology and the onslaught of new messaging and video applications.

In the past, electronic communications largely consisted of emails, but now other forms also trigger regulatory obligations, including chat systems, ephemeral messaging applications, videoconferencing platforms with collaboration features like polls, virtual whiteboards, file transfers and tools like animated gifs and reactions. Financial Industry Regulatory Authority (FINRA) has issued guidance on several topics related to electronic communications.

Companies should closely review their supervisory procedures, record retention policies and technology platforms to ensure they are compliant with applicable rules and update them as appropriate.

As an example, in the advertising-regulation FAQs section, FINRA advised that even impromptu visuals (e.g., a virtual whiteboard) presented in an online meeting will in some cases need to be retained and archived as a "communication." Whether a communication should be retained does not depend on the device or platform used but rather on the content (i.e., does it pertain to a broker-dealers' "business as such" under Rule 17a-4) and context.

Many companies have banned the use of texting, messaging, social media or collaboration applications for business-related communications. In particular, ephemeral messaging applications (e.g., Telegram, WhatsApp, Snapchat) that automatically delete messages after a certain period has passed, can prevent businesses from properly preserving the communication and lead to regulatory compliance problems.

Even if companies ban the use of such messaging applications, they cannot turn a blind eye to their employees' use of prohibited platforms. Companies are required to monitor for compliance to mitigate the risk of record-keeping violations.

Additional considerations

Given the industry-wide sweep and regulators' efforts to crack down on proper recordkeeping, we expect to see more SEC and CFTC enforcement actions on this issue in the future. Companies should closely review their supervisory procedures, record retention policies and technology platforms to ensure they are compliant with applicable rules and update them as appropriate.

Companies should also conduct employee trainings on what are approved communications platforms and the applicable restrictions on the use of personal devices outside of the company's approved systems. Refresher courses on internal policies and regulatory requirements are also recommended in the current heightened regulatory environment. It may be beneficial to periodically obtain certifications from employees attesting to the use of only company-approved electronic forms of communications to conduct business as well.

Companies should also monitor their systems for employees' use of popular email services, chat platforms and ephemeral messaging applications, and ensure they are adequately capturing and preserving business-related communications, in particular, any communications that may be occurring outside of company-approved channels. Where the company identifies a record-keeping problem, depending on the nature and significance of the issue, it may want to consider whether to self-report the issue to the relevant regulatory authorities.

As demonstrated by the recent enforcement actions, even when companies restrict employees' use of personal devices to conduct business, if they fail to enforce their policies and properly supervise their employees, they will have to deal with the regulatory consequences. To avoid regulatory risks, it is crucial that companies enforce their own policies and are proactive in curbing misuse of unauthorized communication channels.

Daniel L. Stein is a regular contributing columnist on white-collar crime defense for Reuters Legal News and Westlaw Today.

About the authors



Daniel L. Stein (L), a partner in **Mayer Brown**'s New York office, leads the firm's global Regulatory & Investigations group and is a co-leader of the White Collar Defense & Compliance group. He has extensive experience in regulatory enforcement, government and internal investigations, white-collar criminal defense and complex civil litigation. He can be reached at dstein@mayerbrown.com. **Michele Natal** (C) is counsel in the firm's New York office and a member of the Litigation & Dispute Resolution and White Collar Defense & Compliance practices. Her practice focuses on global internal investigations and enforcement matters, responding to federal and state regulators and enforcement authorities and providing proactive compliance counseling. She can be reached at mnatal@mayerbrown.com. **Lydia Ho** (R) is an associate in the firm's New York office and a member of the Litigation & Dispute Resolution practice. Her practice focuses on complex commercial litigation, government and internal investigations and international arbitrations. She can be reached at lho@mayerbrown.com.

This article was first published on Reuters Legal News and Westlaw Today on April 12, 2022.