COSMOS
Navigate the Compliance Universe

CEP Magazine - October 2023

Kurt Gottschall (kurt.gottschall@haynesboone.com) is a Partner at Haynes Boone in Denver, Colorado, USA.

Timothy Newman (timothy.newman@haynesboone.com) is a Partner at Haynes Boone in Dallas, Texas, USA.

Payton Roberts (payton.roberts@haynesboone.com) is an Associate at Haynes Boone in Dallas, Texas, USA.

What to do about business-related text and WhatsApp messages

By Kurt Gottschall, Timothy Newman, and Payton Roberts

Over the past year, US financial regulators have announced game-changing enforcement cases and corporate cooperation guidelines to prompt businesses to retain, review, and—if subpoenaed—produce employees' business-related text messages on both personal devices and within so-called ephemeral messaging apps such as WhatsApp, Snapchat, Telegram, Confide, and many others. The ephemeral apps are particularly ubiquitous, and many employees mistakenly believe that their messages will disappear almost magically, leaving no trace. But the technical reality is not that simple, presenting innumerable challenges for legal and compliance staff. This article highlights the recent regulatory scrutiny concerning messaging and offers practical considerations for companies of all sizes.

Recent regulatory enforcement and policy guidance

As we described in our Off-Channel Communications Client Alert,[1] in September 2022, the U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) filed 16 enforcement actions against some of the nation's largest financial firms for not preserving or reviewing text or ephemeral messages.[2] In these cases, regulators imposed more than $2 billion in penalties, required admissions, and ordered significant remedial undertakings.[3] Regulators brought these cases based upon the statutory obligations of broker–dealers, investment advisers, and commodity pool operators to preserve certain documents for inspection and review business communications as part of their routine supervision of employees.[4]

More recently, on May 11, 2023, the SEC announced settled enforcement actions against two additional broker–dealers that self-reported their failure to preserve and review off-channel communications: HSBC Securities Inc. and Scotia Capital Inc.[5] In announcing the actions, Gurbir Grewal, the director of the SEC's Division of Enforcement, encouraged other broker–dealers to self-report and noted that both firms received "reduced penalties [because of] their efforts and cooperation."[6] The SEC imposed civil penalties against HSBC and Scotia Capital of $15 million and $7.5 million, respectively—which were approximately 5%–12% of the top-tiered penalties of $125 million paid by some of the largest Wall Street firms.

Although public companies are not subject to the specific document preservation and employee supervision requirements imposed on SEC and CFTC registrants, both the U.S. Department of Justice (DOJ) and the SEC have communicated their expectations regarding messaging preservation. In 2021, Grewal noted that failing to preserve business-related text messages may "obstruct investigations, [and] raise broader accountability, integrity and spoliation issues."[7] Grewal later warned that:

> "[SEC enforcement will] consider all of our options when this sort of misconduct occurs prior to or during our investigations. For example, if we learn that, while litigation is anticipated or pending, corporations or individuals have not followed the rules and maintained required communications, have ignored subpoenas or litigation hold notices, or have deliberately used the sort of ephemeral technology that allows messages to disappear, we may well conclude that spoliation of evidence has occurred and ask the court for adverse inferences or other appropriate relief."[8]

The SEC described the "likely" impact on its enforcement investigations in bringing each of the 16 settled enforcement actions against Wall Street firms for not preserving or reviewing text or ephemeral messages as follows:

> "During the time period that Respondent failed to maintain and preserve offchannel communications its employees sent and received related to the broker-dealer's business, [Respondent] received and responded to Commission subpoenas for documents and records requests in numerous Commission investigations. As a result, [Respondent]'s recordkeeping failures likely impacted the Commission's ability to carry out its regulatory functions and investigate violations of the federal securities laws across these investigations."[9]

DOJ has communicated its focus on text messages and ephemeral communications by announcing a series of significant modifications to its published policies for evaluating corporate cooperation and compliance programs. This guidance is important because DOJ prosecutors across the country are required to consider it in evaluating any corporate settlement or declination of prosecution.

Specifically, DOJ has rolled out three recent policy announcements touching on messaging. In September 2022, Deputy Attorney General Lisa O. Monaco announced that going forward, in evaluating compliance programs, DOJ's Criminal Division would consider whether companies maintained "effective policies governing the use of personal devices and third-party messaging platforms for corporate communications."[10] DOJ further directed prosecutors to "consider whether a corporation seeking cooperation credit in connection with an investigation has instituted policies to ensure that it will be able to collect and provide to the government all non-privileged responsive documents relevant to the investigation, including work-related communications (*e.g.*, texts, e-messages, or chats), and data collected on phones, tablets or other devices that are used by its employees for business purposes." In December 2022, a speech by another senior DOJ official recognized that while there may be legitimate reasons for employees to use ephemeral messaging, these apps present significant challenges to a company's ability to both ensure that it has a well-functioning compliance program and also to access those communications when required. DOJ also announced that in some cases, the Criminal Division would require CEOs and chief compliance officers to certify that the company maintained a well-functioning compliance program and had access to required business communications.[11]

In March 2023, DOJ's Criminal Division announced even more prescriptive guidance concerning both text and

ephemeral messaging in revisions to DOJ's *Evaluation of Corporate Compliance Programs* (ECCP).[12] Under the revised ECCP, DOJ will now consider:

- Each company's specific risk profile, and whether their policies ensure that, "to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company";
- Hardware policies, including "bring your own device" programs and associated preservation policies;
- Approved electronic messaging applications for business communications, including preservation and deletion settings;
- The communication of messaging application policies to employees; and
- Whether company compensation structures include positive incentives such as career advancement or monetary rewards for developing, improving, or meeting established compliance standards, impose financial penalties for misconduct or failure to comply with corporate compliance policies, and whether such policies are enforced on a consistent basis.

In rolling out the ECCP revisions, a senior DOJ official further announced that "[d]uring the investigation, if a company has not produced communications from these third-party messaging applications, our prosecutors will not accept that at face value."[13] Instead, when a company fails to produce such communications, prosecutors will further scrutinize the company's ability to access those communications, how they are stored, and "a company's answers—or lack of answers—may very well affect the offer it receives to resolve criminal liability."