



## The SEC and Messaging Apps

Posted by William J. Stellmach, Elizabeth P. Gray and Sean Sandoloski, Willkie Farr & Gallagher LLP, on Wednesday, June 15, 2022

**Editor’s note:** William J. Stellmach and Elizabeth P. Gray are partners and Sean Sandoloski is counsel at Willkie Farr & Gallagher LLP. This post is based on a Willkie memorandum by Mr. Stellmach, Ms. Gray, Mr. Sandoloski, Amelia A. Cottrell, Randall Jackson and Michael S. Schachter.

The government’s ongoing effort to crack down on the use of ephemeral messaging platforms at financial institutions appears to have entered a new phase. According to press reports, the Securities and Exchange Commission (the “Commission” or the “SEC”) is requiring Wall Street banks to undertake an unprecedented review of dozens of their top executives’ and traders’ personal cell phones to determine the frequency with which these platforms are used to conduct bank business.

Apps like WhatsApp, Signal, and Telegram allow users to send messages using end-to-end encryption, which prohibits third parties from accessing data, allowing it to be read by no one other than the sender and recipient. Users can also send ephemeral or “self-destructing” messages that are deleted automatically after they are viewed or some set amount of time after they are sent.

These apps are very popular and in wide use, but their use to conduct securities trading-related business violates laws and regulations that require banks and broker-dealers to maintain and preserve communications—not to mention banks’ own policies. These rules enable the review of records by the Commission and other regulators (such as the Commodity Futures Trading Commission (the “CFTC”)), in the course of their examination and enforcement duties. Indeed, the Commission views these rules as “an integral part of the investor protection function of the Commission, and other securities regulators” because these “records are the primary means of monitoring compliance with applicable securities laws, including antifraud provisions and financial responsibility standards.”<sup>1</sup> This isn’t empty rhetoric. Informal messages have formed the backbone of many high-profile corporate enforcement actions over the years.<sup>2</sup> If communications are migrating to platforms where those messages are neither surveilled nor retained, it becomes materially more challenging for the government to bring all manner of cases.

The Commission, therefore, has been clear in its view that the use of “apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up” is “specifically prohibit[ed].”<sup>3</sup> The SEC’s push is

---

<sup>1</sup> Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4(f), 17 C.F.R. Part 241, Exchange Act Rel. No. 44238 (May 1, 2001).

<sup>2</sup> See, e.g., Statement of Facts, *United States v. Deutsche Bank AG*, No. 3:15-cr-61 (D. Conn.).

<sup>3</sup> <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf>.

consistent with a broader skepticism by regulators and enforcement authorities, if not outright hostility, to these platforms. DOJ for example, counsels companies to implement “appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company’s ability to appropriately retain business records or communications or otherwise comply with the company’s document retention policies or legal obligations.”<sup>4</sup>

The Commission’s recent, invasive request follows on its Fall 2021 industry-wide “sweep” investigating whether banks have adequate controls in place to monitor and collect employees’ work-related communications on their personal devices. The Fall 2021 “sweep” was born, in turn, out of the Commission’s investigation into a large financial institution’s failure to preserve these sorts of communications on its employees’ personal devices. That investigation led to a \$200 million settlement by the institution with the SEC and CFTC.<sup>5</sup>

Now the SEC appears to be trying to determine just how widespread messaging is among bankers at other financial institutions, requesting that banks search the personal phones of over 100 top traders and executives across multiple financial institutions. Press reports indicate that the German Federal Financial Supervisory Authority (“BaFin”) is conducting a materially similar investigation.

It appears that the Commission is conserving its resources—and appreciating the sensitivity of such invasive searches—by relying on banks and their outside counsel to conduct the reviews. They also appear interested only in messages related to the core business of the banks; in other words, they aren’t interested in messages complaining about one’s boss or gossiping about colleagues. What’s more, at this point, they are only interested in learning about the volume of messages sent and by whom, not the content of the messages themselves. But the popularity of these messaging apps in employees’ personal lives, the ubiquity of mobile phones, and the move away from the office to work-from-home and hybrid work models means that the Commission is likely to find that many bank employees have been using these platforms to regularly communicate with colleagues and clients alike.

Despite the broad sweep of the requests, the SEC appears to be taking a lighter touch in the course of its investigation for now. And it is unclear to what extent financial institutions will be able to corral their employees’ use of personal phones or recover information from ephemeral messaging apps. But failure to have robust procedures in place to prevent the circumvention of record-keeping rules opens the institutions up to an enforcement action themselves. Merely having policies and rules in place is not enough; we know that management’s awareness that ephemeral messaging applications are being used leaves institutions vulnerable to an enforcement action for lack of sufficient internal controls. That presents all the more reason for financial institutions to take a close look at existing policies and procedures about telecommunications and record keeping and make thoughtful decisions now—before the regulators come calling.

---

<sup>4</sup> <https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977>.

<sup>5</sup> <https://www.sec.gov/litigation/admin/2021/34-93807.pdf>; <https://www.cftc.gov/PressRoom/PressReleases/8470-21>. That the Commission secured an admission of wrongdoing is itself striking and consistent with its recently announced new policy “requiring admissions in cases where heightened accountability and acceptance of responsibility are in the public interest.” See <https://www.sec.gov/news/speech/grewal-sec-speaks-101321>.