STRADLEY RONON

June 28, 2023

Client Alert

White-Collar Defense and Securities Litigation & Enforcement

Off-Platform & Ephemeral Messaging – Prepare Now for More Scrutiny

For financial services industry participants and registrants in particular, the focus by various U.S. federal government agencies on "off-platform" and ephemeral messaging has become unmistakable. Below, we discuss the risks associated with the use of messaging for business communications and offer several practical steps companies can take to limit the resulting regulatory and legal exposure.

Background

Over the last decade, we have seen instant messaging grow as a communication method, and migrate from personal use to a tool for business communications as well. For regulated entities, communications using instant messaging create risks that business communications are not preserved pursuant to the books and records provisions applicable to the financial services industry. These unpreserved messages have been given the name "off-platform," or at times, "off-channel" communications, because they occur outside the company's electronic business platform where communications are otherwise preserved. The use of these off-platform communications has been augmented in recent years by the growth of ephemeral messaging applications (apps), such as Signal. Ephemeral messaging is a form of digital communication defined by two characteristics: (1) the automated and timed deletion of a message's content for both sender and recipient; and (2) end-to-end encryption, which prevents third-party access. In addition to these security advantages, popular ephemeral messaging apps such as Signal, Telegram and WhatsApp are highly intuitive modes of communication and allow for the effective exchange of information without the need for significant IT infrastructure.

As a result of these advantages, the use of ephemeral messaging is becoming more common, even in highly regulated industries. Given the risk of enforcement actions or even criminal liability as described more fully below, now is a good time for every organization, particularly those in the financial services industry, to revisit its policies and procedures and its implementation of those policies and procedures as to off-platform and ephemeral messaging apps in order to ensure compliance with the applicable regulatory requirements.

Recent Enforcement Actions by the SEC and CFTC

Despite the rising popularity of these apps, the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have made clear that the use of off-platform and ephemeral messaging is unacceptable in the context of securities trading where rules require regulated entities to maintain and preserve all written business communications. Making plain its view, the SEC published guidance stating that compliance with the "Books and Records Rule" necessitates

"[s]pecifically prohibiting business 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."[1] [2]

Violations of these Books and Records requirements resulted in significant fines for regulated entities over the last two years, and this trend is sure to continue. In 2021, approximately 11 banking institutions were fined approximately $1.8 billion by the SEC and CFTC for the pervasive use of off-platform communications using messaging apps like iMessage and WhatsApp by company personnel that were not properly retained. A new wave of fines was meted out in 2022 when additional institutions were punished when broker-dealer personnel used these types of apps for business communications, but the business communications were not properly and securely preserved. In 2023, new cases were settled by large financial institutions with the SEC and the CFTC over their failures properly to store business communications on employees' personal devices.[3] While the focus to date of the federal agencies has been on the largest financial institutions, regulators typically work their way down the list from the largest institutions to smaller ones. It is also likely that state regulators and self-regulatory organizations, such as the Financial Industry Regulatory Authority (FINRA), will be entering into this enforcement cycle and expand the focus to smaller firms.

Potential Criminal Liability

Beyond civil penalties, employees' use of ephemeral messaging apps can also lead to potential criminal consequences for employers. Even where an unregulated entity has limited books and records responsibilities, law enforcement officials consider the use of ephemeral messaging in business as a potential tool to facilitate criminal conduct by automatically destroying the records of business communications. More recently, the U.S. Department of Justice (DOJ) has weighed in on this issue. In March 2023, Assistant Attorney General Kenneth Polite, Jr., emphasized during his keynote address at the American Bar Association's Annual National Institute on White Collar Crime that the DOJ wants companies to halt the proliferation of ephemeral messaging as a business tool. "In today's day and age, the use of these services is ubiquitous," AAG Polite stated, and "[j]ust as we expect corporations to adapt to the realities of modern life and update their policies and practices, accordingly, so too does the department."[4]

Specifically, AAG Polite advised that companies should implement policies and procedures governing the use of ephemeral messaging that are "tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate, business-related electronic data and communications can be preserved and accessed. Our prosecutors will also consider how companies communicate the policies to employees, and whether they enforce them on a consistent basis." [5] A company's ability to explain the creation and enforcement of ephemeral messaging policies – in addition to producing communications from all third-party messaging apps – will be a critical consideration for how the DOJ will treat a company in assessing potential corporate liability in the context of a criminal investigation.

---

[1] OCIE Risk Alert, Observations from Investment Adviser Examinations Relating to Electronic Messaging (December 14, 2018), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf (last visited April 14, 2023).

[2] Nevertheless, some argue that there is no intellectually honest distinction between ephemeral messaging and telephone calls: since securities laws and regulations do not require firms to record all oral communications that take place either in person or on the telephone, the same should apply to ephemeral messages from a policy standpoint.

[3] *See*, *e.g.*, 17 C.F.R. §§ 240.17a-3 & 17a-4. *See also*, 17 C.F.R. § 275.204-2.

[4] Kenneth A. Polite, Jr., United States Assistant Attorney General for the Criminal Division, Keynote Address at the American Bar Association's 38th Annual National Institute on White Collar Crime (Mar. 3, 2023) (remarks available at https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-keynote-aba-s-38th-annual-national).

[5] *Id.*

As AAG Polite's remarks illustrate in no uncertain terms, a "company's answers – or lack of answers – may very well affect the offer it receives to resolve criminal liability."[6]

While the DOJ continues to criticize the use of ephemeral messaging, some organizations have argued that there may be legitimate business purposes for using those tools. In the face of criticism, the DOJ has conceded that organizations may legitimately use ephemeral messaging, but only if they have appropriate safeguards in place that ensure communications and other documents are retained pursuant to a corporate information retention policy or applicable legal requirements.[7] But absent such safeguards, use of ephemeral messaging apps may appear to the DOJ as either evidence that the entity is a bad actor or as a basis to bring charges for obstruction of justice if the lack of corporate records impedes a criminal investigation.

Where a company knows that its conduct falls within the purview of an ongoing investigation, the continued use of tools that destroy communications could be viewed by prosecutors as a new crime: obstruction of justice.[8] Even if innocent of the issues motivating the initial investigation, the destruction of communications could provide a separate basis for liability.

What This Means to You

For regulated entities, enforcing a total prohibition on the use of off-platform communications and ephemeral messaging is no simple feat, especially with many employees using their own phones or other devices for business purposes. A first step is implementing a compliance policy that either prohibits their use or clearly identifies any messaging apps that are permitted and sets out guidelines for use that comply with applicable recordkeeping and supervision requirements. Additional proactive measures for monitoring any action that potentially circumvents the prohibited apps and, therefore, the recordkeeping rules will put institutions in the best possible posture to avoid an enforcement action. A company's failure to take these steps may come at a hefty price. While an SEC investigation into senior banking personnel's use of WhatsApp to conduct securities business recently led to a $200 million settlement, fines may escalate as this industry sweep continues for firms that do not heed these early warnings by taking proactive internal action. Even for companies outside the SEC and CFTC's regulatory purview, allowing business communications to take place over ephemeral messaging apps carries with it the risk that government authorities will view the entity as a bad actor.

Furthermore, given the enforcement actions over the past two years by the SEC and the CFTC, we expect that off-platform communications and use of ephemeral apps for business communications are now on the agendas of all regulators in the financial services industry. Regulated entities should expect to see inquiries into how they limit the use of off-platform communications from all relevant regulators and interested organizations – the SEC, CFTC, state regulators, SROs such as FINRA, and law enforcement officials. This topic will be included on the checklist of inquiries propounded by regulators' exam staff. Officials will inquire about the existence of policies banning these practices and steps each organization has taken to implement these policies. What training have employees received? How does an organization monitor whether employees are complying with the polices? How has an organization tested the efficacy of its policies?

---

[6] *Id.*

[7] *See* Justice Manual § 9-47.120(5)(c), Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy.

[8] *See* 18 U.S.C. § 1512(c).

Additionally, prior to taking on-the-record testimony (OTR) of witnesses, regulators are now routinely including questions in pre-OTR questionnaires as to the methods of communication, apps and social media a witness uses to communicate. During the OTR, the regulator will regularly ask the witness under oath whether they use any of these methods to communicate regarding business, and if they say yes, the regulator may issue additional document requests as to the off-platform messaging. These inquiries may also ultimately lead to an enforcement action against the firm.

As a result, ***now*** is the right time for companies to consider both policies for future employee conduct and whether past conduct requires remediation.

Practical Steps for Your Organization to Respond

Below are some practical steps that organizations should consider to manage their employees' use of off-platform and ephemeral messaging applications:

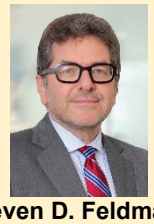
- Implement an appropriate program that addresses the remediation of any past violations of books and records policies through the historical use of off-platform communications and ephemeral messaging.
- If the historical conduct was pervasive and records cannot be recovered, FINRA members should consider whether there is an obligation to self-report to FINRA pursuant to Rule 4530.
- Design policies that clearly define the role that off-platform and ephemeral messaging may play, if any, in the corporate communications environment, and that comply with applicable recordkeeping and supervision requirements.[9]
- Update Annual Compliance Questionnaires to confirm the employees' compliance with the policies on off-platform and ephemeral messaging apps.
- Update training to include firm policies on the use of off-platform communications and ephemeral messaging apps and provide regular reminders regarding prohibited digital communications.
- Provide resources to assist employees in complying with the policies and procedures, such as tools to log and journal any instant messages received in violation of company policy.
- Integrate monitoring and internal disciplinary policies to include off-platform communications and ephemeral messaging.

[9] For example, consider "blacklisting" potentially problematic apps by clearly informing employees of apps which cannot be installed on devices used for business purposes.

Conclusion

The popularity of instant messaging and ephemeral messaging, especially among younger members of the workforce, demonstrates that this form of communication will remain in use. As such, organizations will need to ensure that they are adequately addressing off-platform and ephemeral messaging in their policies and procedures and directing their employees to compliant forms of communication. With all emerging technologies, proactive corporate governance provides the best defense. Smaller firms cannot wait on the sidelines to act until this industry sweep reaches their front doors. By then, it will be too late to avoid fines and reputational harm. Even unregulated entities need to consider the DOJ's directive that business communications using ephemeral messaging do not generally comport with the conduct of good corporate citizens.

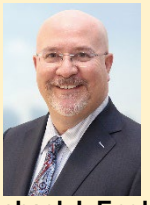
Our team is ready to assist in modifying policies, implementing new procedures and remediation of past conduct, as well as to work through the other considerations outlined above. Please don't hesitate to contact us.



Steven D. Feldman
Partner & Co-Chair,
White-Collar Defense,
Internal Investigations &
Corporate Compliance
212.404.0659
sfeldman@stradley.com

Frederic M. Krieger
Senior Counsel,
Investment Management
and Securities Litigation
& Enforcement
212.540.4568
fkrieger@stradley.com

Amy E. Sparrow
Partner,
Securities Litigation
& Enforcement
215.564.8155
asparrow@stradley.com



Michael J. Engle
Partner & Co-Chair,
White-Collar Defense,
Internal Investigations &
Corporate Compliance
215.564.8737
mengle@stradley.com