PAUL HASTINGS

Stay Current

October 2022

Follow @Paul_Hastings

Ephemeral Messaging at the Office: Avoiding Pitfalls and Establishing Best Practices

By Michael Spafford, Tara Giunta & Brian Wilmot

Introduction

Users of ephemeral messaging applications may intend that their messages be—as the word "ephemeral" suggests—short lived, but the real-world consequences and legal ramifications from improper use of such apps can be anything but temporary. This has not been any more clear than now following a $1.8 billion settlement with the SEC and CFTC by 15 broker-dealers and one affiliated investment adviser for "failures by the firms and their employees to maintain and preserve electronic communications".[1] These concerns, however, are not limited to regulated financial services companies.

This article outlines the growing use of ephemeral messaging apps generally and as business tools, regulators' responses to that use (including via enforcement actions), and ways for businesses to responsibly manage employee use of ephemeral apps to conduct work. As too many companies have already learned, it is not enough to simply turn a blind eye to ephemeral messaging apps. Instead, business leaders must be responsibly and proactively engaged on the issue.

What is Ephemeral Messaging?

Ephemeral messaging applications offer users the ability to set self-destructing messages that automatically disappear from recipients' conversation histories. A classic example of an ephemeral platform is SnapChat, which quickly became the app of choice for teenagers sending photos or gossip. But, ephemeral apps have come a long way from those early days of Snapchat. Now, a wide variety of actors use ephemeral messaging apps, but largely for reasons of security and anonymity, and in some instances, to evade third-party monitoring. Some apps—such as Signal and WhatsApp—even allow users to send encrypted messages, making third-party retrieval of those messages highly difficult.

While plenty of individuals use ephemeral apps for social reasons, these apps are increasingly being used to perform business functions. For instance, some journalists use these apps to communicate with sources, and some political campaign workers may use ephemeral messaging to communicate among themselves, for fear of sensitive messages being leaked.

In many countries outside the United States, ephemeral apps such as WhatsApp have supplanted SMS messaging as a primary communication method, due largely to the fact that SMS messaging and voice calls are very expensive in those countries. Because apps such as WhatsApp require only a Wi-Fi connection, as opposed to a cellular network, communicating with family, friends, and even work colleagues and customers via WhatsApp is the norm in much of the world.

On the other side of the coin, ephemeral apps have drawn a good deal of justifiable regulatory scrutiny in recent years, given the capacity for bad actors to further illegal schemes via hidden or encrypted messages on these apps. However, due to the international popularity of ephemeral apps and their utility in providing secure platforms for sensitive, but legitimate conversations, it is neither easy nor necessarily advisable for employers to impose outright bans on their use. Employers may be wise to adopt a more nuanced approach that balances regulators' concerns with the needs of the business and its employees. As different regulators and laws govern different types of businesses, there is no one-size-fits-all approach to ephemeral messaging at the work place.

SEC/CFTC-Registrants

The U.S. Securities and Exchange Commission (SEC) requires broker-dealers to make, keep, furnish and disseminate certain records and reports, so that, among other things, the SEC, self-regulatory organizations ("SROs") and state securities regulators may conduct effective examinations of broker-dealers, as well as carry out enforcement work. Specifically, SEC Rule 17a-4(b)(4) requires that broker-dealers retain originals of all communications received and copies of all communications sent by the broker-dealer relating to its business for at least three years, the first two years in an easily accessible place. In 2018, the SEC released guidance "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." These registrants have a duty to supervise, monitor and oversee compliance with SEC rules, including monitoring and retention of business communications.

Similarly, the U.S. Commodities Future Trading Commission (CFTC) regulates entities involved in the derivatives markets, such as futures commission merchants, swap execution facilities, derivatives clearing organizations, designated contract markets, and introducing brokers. These organizations must abide the CFTC's various recordkeeping and reporting requirements, including Section 4(s)(h)(1)(B) of the Commodity Exchange Act and Regulations 166.3 and 23.602, which are more narrow that the SEC rules, but impose a broad duty of diligent supervision. If a CFTC-regulated organization's employees are conducting firm business via ephemeral messaging, away from the eyes of the entity and the CFTC, that organization may run afoul of CFTC regulations for failing to properly supervise its employees.

Enforcement

These regulations are not empty threats when it comes to ephemeral messaging—both the CFTC and the SEC have pursued numerous companies for their employees' use of apps such as WhatsApp to conduct business and evade federal investigations.

SEC/CFTC Settlement

The unprecedented $1.8 billion settlement with 15 broker-dealers and one affiliated investment adviser is the latest example of the focus by the SEC and CFTC to address long-standing books and records requirements in a technological world that has quickly changed with the explosive growth of ephemeral messaging applications for business communications. As the CFTC described the conduct, "the institutions' traders had been using unapproved communication methods on their personal devices for business-related communications" and "each firm … was aware of widespread and longstanding use by its employees of unapproved methods to engage in business-related communications." In announcing the settlement, Gurbir S. Grewal, Director of the SEC's Division of Enforcement said: "Today's actions … underscore the importance of recordkeeping requirements: they're sacrosanct. If there are allegations of wrongdoing or misconduct, we must be able to examine a firm's books and records to determine what

happened." This highlights that regulators are focused on ephemeral messages throughout the enforcement process, including their ability to investigate misconduct. Grewal further emphasized that "[o]ther broker dealers and asset managers who are subject to similar requirements under the federal securities laws would be well-served to self-report and self-remediate any deficiencies."

These settlements follow a well-publicized 2021 prior settlement with another Wall Street firm in which the combined SEC and CFTC fines totaled $200 million. The firm was cited for a failure to properly monitor and retain business communications by employees, including senior management and compliance personnel, using WhatsApp and other platforms, which circumvented federal record-keeping laws.[2] Around that same time, Grewal similarly warned registrants of the compelling need to address compliance issues associated with ephemeral messaging apps.[3]

Gorman

In February 2021, the CFTC filed an enforcement action against John Patrick Gorman III, a swaps trader at a global investment bank, for manipulating the price of USD interest rate swap spreads.[4] As part of the investigation, Gorman received a CFTC preservation request for categories of communications on his personal cellphone. Gorman deleted certain responsive communications, including those on WhatsApp, after receiving the preservation request. Gorman lied to the CFTC under oath about compliance with the preservation request, claiming that he only used WhatsApp for social conversations with coworkers. Instead, Gorman allegedly used WhatsApp to carry out manipulation, discuss the CFTC investigation, and conduct other business and/or investigation-related discussions. In its continuing civil litigation, the CFTC seeks, among other relief, civil monetary penalties, disgorgement, restitution, trading bans, and a permanent injunction against future violations of the federal commodities laws.

Jones Trading

In September of 2020, the SEC settled charges under Rule 17a-4 against an employee of the broker-dealer JonesTrading Institutional Services, LLC for failing to preserve business-related text messages with coworkers, customers, and other third parties.[5] The text messages concerned, among other things, the size of orders, the timing of trades, and the pricing of certain securities. Some of the text messages were responsive to an SEC request for records in an unrelated investigation, but, because the messages were not retained on JonesTrading systems, the firm failed to produce the responsive text messages to SEC staff. The order against JonesTrading further found that the firm's senior management were among those sending and receiving business-related texts that were not retained.

Non-Registrants

It is not just SEC and CFTC-registrants that need to be wary of misusing ephemeral messaging apps; other entities have been fined by the Department of Justice ("DOJ") and have faced civil litigation-related consequences for inadequately monitoring employees' use of these apps. For instance, in 2018, precious metals company Elemetal plead guilty in federal court to money laundering-related charges, as well as failing to "request, obtain, preserve adequately, or in some instances any[,] information regarding the content of communications between gold suppliers and [company] agents occurring on encrypted, peer-to-peer chat services, such as WhatsApp or Skype."[6] As a result of the charges, Elemetal forfeited $15 million, and former employees were ultimately sentenced to multiple years in prison.

In another matter, *FTC v. Noland*, the operators of an alleged pyramid scheme instructed employees to use encrypted messaging platforms Signal and ProtonMail, and to stop using their previous messaging platforms for work-related communications. The operators also instructed employees to turn on Signal's auto delete function, and then the employees "proceeded to exchange an untold number of messages

related to [Defendants'] business."[7] The Court issued a temporary restraining order (TRO), but the messages through Signal and ProtonMail were not turned over, and use of these platforms continued. Consequently, the Court granted the Federal Trade Commission's motion for spoliation sanctions, finding that the Defendants "acted with the intent to deprive the FTC of the information contained in the Signal and ProtonMail messages."[8] The most decisive factor to the Court in deciding to award sanctions was "the timing of the installation and use of Signal and ProtonMail." Similar misuse of ephemeral platforms has led to similar consequences in other litigation.[9]

Two broad takeaways from the enforcement actions and litigation described above is that: 1) subpoenas now typically define documents and communications broadly to capture all documents, including ephemeral communications, and 2) failure to comply with subpoenas and preserve documents creates criminal exposure, particular with a government enforcement subpoena.

Additional DOJ Guidance

The DOJ has offered companies more concrete guidance regarding the use of ephemeral messaging within the context of Foreign Corrupt Practices Act ("FCPA") enforcement. In December 2017, DOJ announced a new FCPA Corporate Enforcement Policy requiring companies to prohibit their employees from "using software that generates but does not appropriately retain business records or communications" in order to obtain full remediation credit.[10] There was serious concern raised as to the feasibility of complying with this blank ban, particularly for companies operating in jurisdictions where ephemeral messaging apps were the primary, if not sole, means of communicating.

As a result, the DOJ's stance on ephemeral messaging evolved over the following months, given its increasing recognition of the prevalence of ephemeral messaging around the world. In March 2019, DOJ revised its Corporate Enforcement Policy, moving away from strictly prohibiting the use of ephemeral messaging platforms to instead requiring companies to "implement[ ] appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms . . . to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."[11] The revised policy recognizes that prohibiting ephemeral messaging and personal communications is not necessarily enforceable, practical, or productive. The revised policy instead incentivizes companies to responsibly monitor and retain business communications issued via ephemeral apps, as the DOJ will consider such efforts when determining whether a company has cooperated with an investigation.

This month, the Deputy Attorney General issued new guidance regarding DOJ's Corporate Enforcement Policy, and highlighted again the importance of personal device use:

> How companies address the use of personal devices and third-party messaging platforms can impact a prosecutor's evaluation of the effectiveness of a corporation's compliance program, as well as the assessment of a corporation's cooperation during a criminal investigation….As part of evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential violations of law, prosecutors should consider whether the corporation has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved.

As a general rule, all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, should provide clear training to employees about such policies, and should enforce such policies when violations are identified.[12]

As the use of ephemeral messaging increases for business interactions and is often used to evade existing internal controls ensuring the preservation of important corporate communications and documents, DOJ has emphasized that companies must take steps to ensure reasonable preservation of ephemeral messaging communications.

What Companies Can Do: Emphasize Compliance

Regulators' focus on ephemeral messaging is growing alongside an increasing emphasis on corporate compliance. The most recent revisions to DOJ's Corporate Enforcement Policies increased consideration of past corporate misconduct, and placed greater scrutiny of the effectiveness of corporate compliance programs, both at the time of the misconduct and at the time of resolution. Accordingly, it would behoove companies to assess the effectiveness of their compliance programs and whether they are adequately resourced, and to ensure that their compliance programs address monitoring and retention of ephemeral communications. This is particularly true for companies that have SEC or CFTC reporting and preservation requirements, specific obligations under anti-money laundering laws, or are undergoing/expect to undergo litigation.

In addition to considering the above factors, companies assessing their current risk with regard to employee use of ephemeral messaging applications should conduct the following inquiries:

1. Existing employee use of platforms
   - Do employees currently use these platforms?
   - If so, which ones?
   - Does such use include business communications?
2. Related business policies and legal constraints
   - Is there a bring your own device ("BYOD") policy or do employees use company-provided devices?
   - Does the company have document-retention policies and procedures? Do they address ephemeral messaging, other messaging systems, and mobile device data?
   - Is the company subject to any data privacy requirements that may limit the company's ability to monitor or restrict use of ephemeral messaging?
3. Types of sensitive information
   - What information will be most sought after by litigants and regulators (sales communications, trading activities, financial transactions, etc.)?
   - Will the data be important to regulators investigating an issue and assessing individual liability (employee misconduct)?

4. Specific preservation obligations

   - Does the company have any SEC or CFTC reporting or books and records preservation requirements?
   - Is the company subject to any other potentially-relevant regulatory obligations such as money-laundering laws?
   - Is the company the subject of any ongoing regulatory investigation or enforcement action?
   - Is the company involved or expect to be involved in any litigation?

5. Existing Policies

   - What policies regarding ephemeral communications are currently in place? Are employees trained on those policies?
   - Are firm messaging systems (Microsoft Teams, Cisco Jabber, Bloomberg Chat, etc.) monitored/backed-up?
   - Does the firm have the necessary IT infrastructure/budget to implement surveillance, or to respond to regulatory/litigation requests for communications?
   - Are there policies in place regarding litigation holds/preservation notices/subpoenas?
   - When does the company collect/image mobile devices? If there is a BYOD policy, are there policies in place allowing the company to gain custody of personal devices for imaging purposes?

6. Communications and Training

   - Does the company conduct training regarding the use of ephemeral message applications and other messaging systems?
   - How does the company communicate policies regarding ephemeral messaging, mobile device usage, and business communications to employees?

7. Monitoring

   - What about ephemeral messaging platform usage—is it currently monitored via auditing or electronic surveillance?
   - How does the company monitor compliance with policies regarding the handling of ephemeral communications and mobile devices? Is this monitoring successful in identifying non-compliance?
   - How does the company handle instances of non-compliance with these policies?

The gold standard is for a company to have clear policies in place that define business communications and prohibit employees from using ephemeral messaging apps to conduct such communications, and to

have IT capabilities in place that ensure all workplace-related conversations are retained in the event of a regulatory inquiry or litigation. Those actions will best ensure that a company has minimal criminal or civil risk with regard to ephemeral communications. Companies that are unwilling or unable to prohibit employees from using ephemeral apps to conduct business should be aware of the associated regulatory and litigation risks, and should be certain that they have adequate IT safeguards in place to capture relevant communications. It is highly likely that regulators and litigants worldwide will continue to adapt their approaches to ephemeral apps, especially as these apps continue to supplant more traditional forms of communication, such as email and SMS messaging. If a company is not proactively engaged on the issue, government entities or adverse parties may force engagement via investigations and lawsuits.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington, D.C. lawyers:

Tara K. Giunta
1.202.551.1791
taragiunta@paulhastings.com

Michael L. Spafford
1.202.551.1988
michaelspafford@paulhastings.com

Brian Wilmot
1.202.551.1981
brianwilmot@paulhastings.com

[1] Press Release, SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures, SEC Release No. 2022-174(Sept. 27, 2022), https://www.sec.gov/news/press-release/2022-174; Press Release, CFTC Orders 11 Financial Institutions to Pay Over $710 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods, CFTC Release No. 8599-22 (Sept. 27, 2022), https://www.cftc.gov/PressRoom/PressReleases/8599-22

[2] Press Release, JPMorgan Admits to Widespread Recordkeeping Failures and Agrees to Pay $125 Million Penalty to Resolve SEC Charges, SEC Release No. 2021-262(Dec. 17, 2021), https://www.sec.gov/news/press-release/2021-262; Press Release, CFTC Orders JPMorgan to Pay $75 Million for Widespread Use by Employees of Unapproved Communication Methods and Related Recordkeeping and Supervision Failures, CFTC Release No. 8470-21 (Dec. 17, 2021), https://www.cftc.gov/PressRoom/PressReleases/8470-21.

[3] Speech, Gurbir S. Grewal Remarks at SEC Speaks 202 (Oct. 13, 2021), https://www.sec.gov/news/speech/grewal-sec-speaks-101321.

[4] Press Release, CFTC Charges Swaps Trader with Manipulation, Attempted Manipulation, and Making False Statements, CFTC Release No. 8359-21(Feb. 1, 2021), https://www.cftc.gov/PressRoom/PressReleases/8359-21

[5] Administrative Proceeding, SEC Charges Broker-Dealer with Failing to Preserve Required Electronic Records, SEC File No. 3-20050(Sept. 23, 2020), https://www.sec.gov/enforce/34-89975-s

[6] Press Release, U.S. Attorney's Office for the Southern District of Florida, U.S. Gold Refinery Pleads Guilty to Charge of Failure to Maintain Adequate Anti-Money Laundering Program(March 16, 2018), https://www.justice.gov/usao-sdfl/pr/us-gold-refinery-pleads-guilty-charge-failure-maintain-adequate-anti-money-laundering.

[7] *Fed. Trade Comm'n v. Noland*, No. CV-20-00047-PHX-DWL (D. Ariz. Aug. 30, 2021).

[8] *Id.*

[9] *See, e.g., Waymo LLC v. Uber Techs., Inc.*, No. C 17-00939 WHA (N.D. Cal. Jun. 8, 2017); *Weride Corp. v. Kun Huang*, Case No. 5:18-cv-07233-EJD, (N.D. Cal. Apr. 16, 2020).

[10] DOJ, U.S. Attorney's Manual § 9-47.120(3)(c) (Nov. 2017).

[11] DOJ, 9-47.120 - FCPA Corporate Enforcement Policy, https://www.justice.gov/criminal-fraud/file/838416/download.

[12] Memorandum, Dep. Att. General Lisa Monaco, Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group (Sept. 15, 2022), https://www.justice.gov/opa/speech/file/1535301/download.