The messaging dilemma: grappling with employees' off-system communications

By Andrew M. Levine, Esq., and Chana Zuckier, Esq., Debevoise & Plimpton LLP

FEBRUARY 3, 2023

Recent years have witnessed rapid growth in employees' use of messaging applications and other off-system communications channels for business purposes. The work-from-home era accelerated this proliferation, as virtual communications became the norm and as lines between personal and business time further blurred.

Employees now may communicate routinely, both internally and externally, on platforms not captured by their firm's record-keeping systems. Firms are left vulnerable to scrutiny by regulators and others that expect comprehensive retention of business records. Amidst these challenges, enforcement authorities and industry alike have struggled to formulate an approach to employee messaging that is manageable, realistic, and promotes compliance.

Regulatory context

The Department of Justice (DOJ) first addressed off-system messaging in its 2017 Corporate Enforcement Policy, which required companies essentially to prohibit the use of ephemeral messaging platforms that "generate[d] but [did] not appropriately retain business records or communications." That policy offered little flexibility and raised the risk that DOJ would deny companies that utilized these messaging channels the presumption of a declination when resolving a DOJ investigation.

Following industry backlash, DOJ relaxed this policy in its March 2019 revision to the Corporate Enforcement Policy. DOJ offered a more nuanced approach that recognized the reality that business communications often utilize applications like WhatsApp and WeChat. The updated policy clarified that DOJ did not expect companies to prohibit employee messaging altogether, but to implement appropriate guidance and controls.

This issue receded somewhat during the pandemic but roared back to prominence with an SEC and CFTC sweep of Wall Street that already has generated close to $2 billion in fines and remains ongoing. The sweep followed an SEC and CFTC investigation into off-systems communications at J.P. Morgan, which resulted in a $200 million settlement. *In re: J.P. Morgan Securities LLC* (SEC press release, Dec. 17, 2021). In September 2022, the Securities and Exchange Commission and Commodity Futures Trading Commission announced charges against 16 other financial firms for violating related record-keeping obligations. (SEC press release, Sept. 27, 2022).

The firms involved in the resolutions to date have admitted wrongdoing as part of their settlements. The SEC and CFTC orders for many reflect not only pervasive off-system texting, but that senior executives tasked with enforcing compliance policies themselves frequently engaged in off-system business communications. Many of the orders also note firms' failure to produce messaging data in response to subpoenas or other inquiries, likely hindering government investigations, because messages were stored on employees' personal devices and not on firm systems.

According to DOJ, a "robust compliance program" should enable the collection and retention of business-related data and communications from employees' personal devices or third-party messaging applications.

This regulatory scrutiny continues. In late 2022, a number of major private equity firms disclosed related SEC inquiries.

Recent DOJ and SEC pronouncements

In September 2022, when announcing new corporate enforcement policies, Deputy Attorney General Lisa Monaco specifically addressed the issue of personal devices and third-party messaging applications. The associated Monaco Memo highlighted — consistent with DOJ's recently revised Corporate Enforcement Policy — that companies' approaches to off-system communications will impact how, in the context of an investigation, DOJ will assess compliance programs and cooperation.

More specifically, the Memo reflected that employees appropriately may utilize third-party platforms. However, according to DOJ, a "robust compliance program" should enable the collection and

retention of business-related data and communications from employees' personal devices or third-party messaging applications. A compliance program should include not only effective policies and training, but also enforcement of those policies (with fair discipline) when employees violate them.

The Memo added that additional guidance regarding off-system messaging would be released in the near future, which other DOJ leaders recently have reiterated. Expectations from DOJ, of course, extend more broadly to all companies subject to U.S. jurisdiction and not just financial services companies bound by the securities laws' record-retention requirements.

All companies should seek to ensure they appropriately preserve corporate records and implement a risk-based compliance program consistent with regulators' expectations.

Since the DAG's announcement, other DOJ and SEC officials have addressed this topic. In remarks last December at an FCPA (Foreign Corrupt Practices Act) conference just outside of Washington, D.C., Acting Principal Deputy Assistant Attorney General Nicole Argentieri acknowledged there are legitimate reasons for off-system messaging. However, she explained that companies must assess the risks and adapt their compliance programs to address them. Argentieri further acknowledged the complexities from practical, technological, and privacy perspectives.

David Last, Chief of DOJ's FCPA Unit, likewise observed at the same D.C. event and another in New York City the day before that this is a challenging area for companies trying to achieve compliance. Last noted that companies should adopt a risk-based approach that considers the nature of their business, size, jurisdictions in which they operate, and other characteristics. He stated that DOJ will consider how companies approach their messaging policies in light of other company policies, including record retention policies.

Charles Cain and Tracy Price, Chief and Deputy Chief of the SEC's FCPA Unit, who also spoke at the D.C. conference, provided additional guidance. In particular, they addressed the importance of ensuring accurate books and records, an obligation that cascades through the various elements of an effective compliance program. Cain emphasized it is insufficient to have robust policies on the books if those policies are not vigorously enforced. Price noted that the SEC will also consider the adequacy of employee training to ensure any messaging on off-system platforms is conducted lawfully and for legitimate purposes.

Compliance best practices

Companies seeking to implement best practices in managing off-system communications face a challenging landscape, particularly given that technological solutions seemingly have not advanced at the same pace as compliance expectations. Whether or not subject to the U.S. securities laws, all companies should seek to ensure they appropriately preserve corporate records and implement a risk-based compliance program consistent with regulators' expectations.

The following steps, among others, warrant serious consideration:

(1) **Conduct a risk assessment**: Start with a risk assessment that evaluates where the relevant risks lie regarding off-system communications. Consider what applications are popular among which employees, the purposes of any messaging for business purposes, and the contacts that employees most frequently interact with via messaging. The compliance steps described below should be tailored to the risk profile of each company, such as the type of business conducted in various jurisdictions.

(2) **Deploy relevant policies**: Adopt and implement policies that provide detailed guidance regarding off-system messaging platforms. To the extent a company allows these channels, its policies should review the use parameters, including permitted types of applications and the scope of permitted messaging. Policies should address also how employees must maintain business-related communications and contain provisions clearly permitting the company to collect communications from personal devices or third-party applications if necessary, appropriately navigating privacy restrictions to the extent possible.

(3) **Develop supporting procedures**: Associated procedures can prove essential, such as for responding effectively to regulatory or law enforcement investigations or litigation. Companies proactively should develop protocols for collecting business-related messages from employees' personal devices. U.S. regulators will expect companies to collect text messages and similar communications responsive to regulatory inquiries, and the failure to do so may have significant consequences.

(4) **Ensure appropriate training**: Training for employees should address off-system messaging and the relevant policies. This might include specific examples of permitted or prohibited communications and messaging applications. Trainings should educate employees about the importance of record retention and the possibility that the company may need to collect business-related communications from personal devices. Companies should consider reinforcing training by circulating relevant reminders to employees.

(5) **Display leadership by example**: Strong tone from the top is critical. Those in management positions should lead by example — messages from supervisors via unauthorized channels undercut gravely the effectiveness of off-system communications policies. Companies can underscore their commitment to compliance by having senior leadership directly send the periodic reminders described above.

(6) **Consider an annual certification**: Consider bolstering the relevant training by requiring a yearly compliance certification in which employees specifically certify to their understanding

of and compliance with their company's policies on off-system communications.

(7) **Monitor for compliance**: Based on relevant risk factors, companies should consider appropriate mechanisms for detecting violations of their off-system communications policies. For instance, if a company bans the use of certain mobile messaging applications, the company might consider surveilling company email or on-system messaging applications for references to the prohibited applications to determine if employees are inappropriately moving business conversations to unapproved platforms.

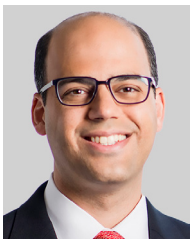
(8) **Impose fair discipline**: Discipline plays a vital role in promoting compliance. Companies may consider developing a particular disciplinary framework for off-system communications, including to help encourage compliance. Discipline imposed for violating off-system communications policies should be applied fairly and consistently and should be properly memorialized.

(9) **Explore technological solutions**: While there is currently no technological silver bullet, there are mobile applications — including Movius and Symphony WhatsApp — that can be downloaded on employees' personal devices to retain business-related SMS, WhatsApp, WeChat, or other messaging data. Companies may consider also providing corporate devices equipped with record retention applications for certain employees who have particular messaging needs due to their roles. We anticipate additional technological tools in the coming months and years, and suggest that companies remain vigilant about evaluating these options.

(10) **Prepare in advance of the anticipated guidance**: While additional DOJ guidance is reportedly imminent, companies can act immediately to improve their off-system messaging compliance by reinforcing their effective compliance program, including (as discussed above) policies, training, monitoring, discipline, and technological solutions. Companies should be ready to explain to regulators their approach to off-system messaging and how specifically they obtained comfort that their approach ensured the appropriate preservation of business records.

Undoubtedly, companies will continue grappling with employees' use of off-system messaging. There is no simple fix, and expecting all employees to avoid such communications, at least in most instances, is an unlikely strategy for success. But developing a robust compliance toolkit to address these challenges will help put companies on an appropriate (and defensible) path.

About the authors



Andrew M. Levine (L) is a litigation partner at **Debevoise & Plimpton LLP** and member of the firm's white collar and regulatory defense group. He regularly defends companies and individuals in criminal, civil, and regulatory enforcement matters, conducts internal investigations throughout the world, and advises on compliance matters, including conducting risk assessments, enhancing compliance programs, and mitigating transactional risks. He is based in New York and can be reached at amlevine@debevoise.com. **Chana Zuckier** (R) is a litigation associate at the firm, and her practice focuses on white collar and regulatory defense. She is based in New York and can be reached at czuckier@debevoise.com.

This article was first published on Reuters Legal News and Westlaw Today on February 3, 2023.