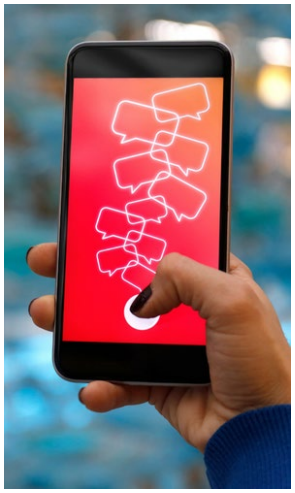
Van Ness Feldman LLP
vnf.com



Mitigating the Rising Risk from Corporate Use of Third-Party Apps

NOVEMBER 14, 2022

Michael Farber, Justin Panitchpakdi, Rachael Lipinski

Introduction

Recent federal government policy announcements and enforcement actions have shone a light on the enterprise legal risks associated with employee use of third-party messaging applications (third-party apps). The use of third-party apps to conduct company business has exploded in recent years, particularly as much of the U.S. work force became mobile during the height of the COVID pandemic. In response, many companies adopted "bring your own device" (BYOD) policies that allow for use of personal devices to conduct company business.

Encrypted instant messaging apps such as Signal, WhatsApp, Wire, and Telegram provide particular challenges to organizations seeking to manage legal risks. The use of these types of apps has grown exponentially over the last five years.

Given the increased corporate risk associated with the use of these popular third-party apps, our Litigation & Investigations team set out to outline recent federal government actions, detail some of the legal and regulatory risks associated with employee use of third-party apps and provide recommendations on how organizations can manage and limit these types of risks.

DOJ's Policy on Third-Party Messaging Platforms

In a speech delivered on September 15, 2022, Department of Justice (DOJ) Deputy Attorney General Lisa Monaco announced a revised set of DOJ Corporate Criminal Enforcement Policies. These policies were also detailed in a memorandum sent to all enforcement components within the DOJ. The "memorandum identifies additional metrics relevant to prosecutors' evaluation of a corporation's compliance program and culture." These metrics include the use of personal devices and third-party apps, stating:

> "The ubiquity of personal smartphones, tablets, laptops, and other devices poses significant corporate compliance risks, particularly as to the ability of companies to monitor the use of such devices for misconduct and to recover relevant data from them during a subsequent investigation. The rise in use of third-party messaging platforms, including the use of ephemeral and encrypted messaging applications, poses a similar challenge."

The memorandum directs prosecutors to consider whether a corporation "has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms," and provides specific guidance on how companies should approach the use of personal devices and third-party apps:

> "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. Prosecutors should also 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 contained on phones, tablets, or other devices that are used by its employees for business purposes."

The Deputy Attorney General also directed the Criminal Division to study best corporate practices on the use of personal devices and third-party apps and to incorporate those findings into the next update of DOJ's Evaluation of Corporation Compliance Programs.

Taken alongside the other metrics in the memorandum regarding individual responsibility for corporate compliance (including potential claw-back of executive salaries), this guidance sends a clear signal to company executives that there are significant risks associated with failing to properly regulate and monitor employees' use of third-party apps to "ensure that business-related electronic data and communications are preserved."

DOJ's emphasis on employee use of third party-apps is not entirely new. In 2017, DOJ began to require companies subject to Foreign Corrupt Practices Act (FCPA) enforcement to enhance third-party app messaging policies to receive cooperation credit; and that policy was modified in 2019 to allow companies some latitude in developing policies addressing third-party app usage. The Deputy Attorney General's 2022 memorandum sharpens the DOJ's policies regarding third-party apps in future enforcement cases (not just FCPA cases) and includes more specific guidance.

SEC/CFTC Settlements

On September 27, 2022, the Securities and Exchange Commission (SEC) announced civil charges against 15 broker-dealers and one affiliated investment adviser for "widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications." Those firms agreed to pay combined penalties of over $1.1 billion.

An SEC release noted:

> "From January 2018 through September 2021, the firms' employees routinely communicated about business matters using text messaging applications on their personal devices. The firms did not maintain or preserve the substantial majority of these off-channel communications, in violation of the federal securities laws. By failing to maintain and preserve required records relating to their businesses, the firms' actions likely deprived the Commission of these off-channel communications in various Commission investigations. The failings occurred across all of the 16 firms and involved employees at multiple levels of authority, including supervisors and senior executives."

Also on September 27, the Commodities Future Trading Commission (CFTC) ordered 11 financial institutions to pay a combined $710 million for recordkeeping failures associated with the use of third-party apps.

Implications and Recommendations

As explained above, there is now significant enforcement risk in industries that have specific record-keeping requirements. It is reasonable to assume that the enforcement actions pursued against financial entities will be replicated against companies in other sectors facing record-keeping requirements.

In addition to recordkeeping enforcement risk, a company's failure to address third-party app use by employees threatens to undermine any attempt to receive cooperation credit in enforcement actions taken against the company. The DOJ memorandum is clear on this point; and it is reasonable to expect that this will play out in a number of cases in the future.

What can be done address these challenges? There are a number of steps that companies can take to begin to address this growing area of regulatory/enforcement risk, including:

- ***Clear policies and training.*** Companies should implement policies clarifying that employees utilizing BYOD policies are either (1) not permitted to use third-party apps to conduct company business; or (2) have an affirmative obligation to save communications made on third-party apps that can be viewed as conducting company business. Specific company policies may vary by business component, personnel, etc. For example, some flexibility may be required for a mobile workforce. Also, with the rise of remote workspaces, companies will need to refresh training and policies to address new applications and modes of communication.

- ***Monitoring and record retention measures.*** Companies that choose to allow the use of personal devices and third-party apps should consider implementing monitoring measures to assess the

Van Ness Feldman LLP
vnf.com

level of risk associated with third-party app usage and to preserve business-related data and communications generated on those devices and apps. Monitoring solutions continue to be developed—and while perhaps viewed as intrusive—may be an important part of an enterprise risk assessment for an organization seeking to allow employee flexibility.

- ***Policies integrated into employment agreements.*** Companies may want to revise employment agreements to contain an affirmative commitment by the employee to comply with all company policies regarding mobile device and third-party app use.

- ***Signed commitments for employees utilizing BYOD policies.*** Companies with flexible BYOD policies may consider signed commitments from participating employees agreeing to not conducting business on third-party apps and/or to take steps to save all communications that are related to the company's business.

For More Information

Van Ness Feldman's Litigation and Investigations team provides strategic counsel to corporations on best practices and policies to mitigate risk in the face of evolving federal regulations. For more information on how you can ensure your company is in compliance with third party messenger apps, please contact Mike Farber, Justin Panitchpakdi, Rachael Lipinski or any other member of our Litigation and Investigations team.

Follow us on Twitter @VanNessFeldman