COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

Tackling off-channel communications? Don't forget ephemeral messaging

By Aaron Nicodemus | Mon, Dec 11, 2023 12:42 PM

As if creating policies and procedures to handle employee use of off-channel communications is not difficult enough, there is a subset of channels that can be even more nettlesome: ephemeral messaging.

Ephemeral messaging platforms are apps and electronic communication channels where messages are automatically deleted after a set time. Examples include WhatsApp, Telegram, Snapchat, and Signal.

Some ephemeral communications apps, like WhatsApp, also feature end-to-end encryption, which can make it difficult to recover messages in transit. Both the automatic deletion and encryption features of these apps complicate the recovery of evidence during a corporate internal investigation or when complying with a request for information or subpoena.

The Department of Justice (DOJ) has made it clear through its **Evaluation of Corporate Compliance Programs** (ECCP) guidance that it will not accept excuses when it comes to companies' policies related to off-channel communications use by employees, including use of ephemeral messaging apps.

"The DOJ does not discriminate between off-channel and on-channel communications. They are saying, 'We want all communications on the topic.'"

David Slovick, Partner, Barnes & Thornburg

Prosecutors **will evaluate** which electronic communication channels employees are allowed to use and how the firm monitors and preserves those communications; the policies and procedures the business has in place to preserve relevant business

communications; and what, if any, consequences employees face if they use off-channel communications in violation of company policy, according to the ECCP.

How well or poorly a firm monitors and retains business communications can be a mitigating or aggravating factor in the penalty phase of a DOJ criminal investigation. Done well, a firm's policies on the subject can ensure it can comply with a DOJ request for *all* relevant information.

But, if a firm's off-channel communications policy is nonexistent, weak, or loosely enforced, it could lead to gaps in its knowledge about how and where its employees are conducting company business and to whom they are talking. Such weaknesses could lead to a firm failing to comply with a request for information or subpoena from the DOJ because it simply didn't record and archive the employee communications in question.

"During the investigation, if a company has not produced communications from these third-party messaging applications, our prosecutors will not accept that at face value," said then-Assistant Attorney General Kenneth Polite Jr. in a **March speech**. "They'll ask about the company's ability to access such communications; whether they are stored on corporate devices or servers; as well as applicable privacy and local laws, among other things."

David Slovick, partner at law firm Barnes & Thornburg, said when the DOJ makes a document request, it calls for all business-related communications.

"The DOJ does not discriminate between off-channel and on-channel communications," he said. "They are saying, 'We want all communications on the topic.'"

If evidence relevant to the DOJ's investigation is discovered through other sources—say, via a whistleblower or cooperating witness or through interviews with vendors, clients, customers, and competitors—the agency might consider the fact the company did not provide that information as an aggravating factor.

Where to begin on policies

Regulated entities like broker-dealers and investment advisers have strict rules they must follow regarding off-channel communications. These firms have been put on notice by the Securities and Exchange Commission and Commodity Futures Trading Commission that **they will be heavily fined** if they fail to comply.

Other, less-regulated entities should consider implementing strong policies and procedures on off-channel communications.

One compliance executive at a major U.S. manufacturer told Compliance Week their compliance team is attempting to assess the problem of off-channel communications among employees. Using anonymous surveys, group sessions, and even one-on-one chats between line managers and employees thought to be using off-channel communications to conduct business, the company is trying to discover why employees are using such platforms and to whom they are talking.

Once that process is complete, the company will then attempt to create policies and procedures on use of off-channel communications that both comply with the DOJ’s expectations and consider how business is conducted by its employees.

Slovick recommended firms implement a strong off-channel communications policy that expressly forbids employees from conducting business on unauthorized channels. All business communications must be available to be monitored; recorded; archived; and, if necessary, produced as evidence to internal corporate investigators, an audit team, or the DOJ.

Firms should provide clear, repeated training on off-channel communications to their employees and emphasize the consequences of noncompliance. Punishment should be clear and might include withholding or clawing back compensation, fines, suspension, or even termination if employees are found to be violating the policy.

“Firms are fearful to implement a consequence management policy that includes different penalties. These are often the folks making the most money for the firm, so they may be less inclined to take action.”

Justin Muscolino, Founder, JTM Compliance Training

Remember, the DOJ has said it will consider a firm’s disciplining of employees as a mitigating factor.

Justin Muscolino, a compliance training expert and owner of JTM Compliance Training, said following through on consequences might be the most difficult part of the entire process regarding off-channel communications.

"Firms are fearful to implement a consequence management policy that includes different penalties," he said. "These are often the folks making the most money for the firm, so they may be less inclined to take action. For firms that incur the wrath of regulators, the amount of revenue derived usually exceeds the amount of fines levied by a regulator. It's the cost of doing business."

Muscolino said firms should emphasize the reasons behind policies they have implemented when training employees on how to comply.

"Every training is derived from a source or a root cause," he said. In this case, regulators are taking off-channel communications use seriously by issuing fines, and the DOJ has made it clear it will treat firms harshly that look the other way as employees continue using such platforms.

Muscolino suggested sending company-wide messages on the topic to all employees, even those not thought to be using unauthorized channels. Then, focus training on groups of employees who might be using these unauthorized channels and emphasize no one is exempt.

"The whole company has to comply, and you may have to put some employees on the spot if they are noncompliant, since it has repercussions for the entire firm," he said.

Lastly, firms should **leverage technology to monitor compliance**. This can be accomplished by an in-house team comprised of both compliance and IT employees or in collaboration with a third-party vendor.

Compliance Week's "Inside the Mind of the CCO" survey found **compliance officers are not confident** about the effectiveness of their off-channel communications monitoring processes.

MORE FROM AARON NICODEMUS

OCC offers compliance guidance to banks on 'buy now, pay later' loans

CFTC’s Pham: ‘There will likely be more’ CCOs charged with individual liability

Compliance officers share lack of faith in off-channel comms monitoring policies