Articles + Publications | August 2, 2022

SEC Cracks Down on Encrypted Messaging

SPEAKERS

Ghillaine A. Reid | Casselle Smith | Jay A. Dubow | Aaron Hardy

While the phrase “clandestine messaging” evokes secret notes slipped under doors and written in code, its meaning in the world of securities regulation and enforcement is not nearly as romantic as the name suggests. Clandestine messaging applications use end-to-end encryption to prevent third parties from accessing data, ensuring that no one but the sender and the recipient can read the communications. With some clandestine messaging services, users can also send “ephemeral” messages — texts that essentially self-destruct and are deleted either immediately after viewing or a specified amount of time after they are sent.

While clandestine messaging apps like Signal, WhatsApp, Telegram, Threema, Viber, and Wickr are becoming ubiquitous in day-to-day life, using these apps for business-related communication places financial institutions in hot water. In December 2021 the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) settled enforcement actions with a Wall Street firm for failing to adequately monitor employee communications and circumventing record-keeping requirements. This investigation centered around the firm’s failure to monitor business-related communications on platforms like WhatsApp, and resulted in a combined settlement of $200 million in penalties.

The $125 million fine paid to the SEC was the largest ever for a breach of rules mandating the preservation of business-related communications, signaling a new interest in SEC investigations and enforcement. The SEC began doggedly investigating other financial institutions, whose employees use encrypted or unauthorized messaging applications to send and receive business-related communications in 2021, though this probe has ramped up in recent months and expanded to include other regulators.

In May 2022, Bloomberg announced that the SEC had launched a massive investigation into the use of clandestine messaging platforms by high-ranking Wall Street employees. To conduct this unprecedented probe, the SEC sent financial firms lists of key positions — including heads of investment banking teams and trading desks — and ordered personnel in these roles to hand over their personal mobile devices for examination.

The latest financial institution to face regulatory scrutiny in connection with its employees’ use of encrypted messaging apps announced in late July 2022 that it was being investigated by the SEC and CFTC. This announcement comes just one month after the financial institution agreed to pay approximately $25 million to settle fraud charges relating to a complex investment strategy, known as Yield Enhancement Strategy, though the investigations are not related.

At this stage, the SEC’s primary goal appears to be an attempt to discover how widespread the use of encrypted messaging apps is among bankers and traders. Understanding the full scope of the problem on Wall Street will likely inform who the SEC decides to punish (and to what extent) for failing to preserve business-related messages

sent over encrypted apps. As of May 2022, at least five major Wall Street firms have publicly acknowledged that they are fielding government inquiries into employee use of messaging apps.

While regulators are currently focusing on the volume of business communications sent over unauthorized apps, rather than the content of the messages, their position on the use of these apps is clear — warning that failure to adequately control employee use of clandestine messaging apps will make institutions vulnerable to liability for failure to preserve business communications. In an interview with Bloomberg, Federal Prosecutor Damian Williams stated, "If I were head of a fund, and I had folks communicating about business on encrypted channels or personal devices, I would want to know. That's where the bomb could be that blows up the whole shop."

At the federal level, Senate Republican Lindsey Graham has introduced the Lawful Access to Encrypted Data Act, which, if enacted would require technology providers to allow law enforcement to access encrypted data on clandestine messaging platforms. Commentators have speculated that this would amount to "an outright ban on end-to-end encryption." The government clearly views the use of encrypted messaging apps for business communications as suspicious in and of itself, as illustrated by a recent Department of Justice (DOJ) press release on Reality Television Star Jennifer Shah's telemarketing fraud case: "Shah undertook significant efforts to conceal her role in the Business Opportunity Scheme. For example, … [Shah] used and directed others to use encrypted messaging applications to communicate [with co-conspirators]."

State regulators are also concerned with the growing popularity of encrypted messaging applications — in 2021, the Michigan Senate voted unanimously to prohibit the use of "any app, software, or other technology that prevents [state departments and agencies] from maintaining or preserving a public record," essentially blocking state employees from using clandestine messaging apps. In Texas, encrypted or ephemeral messages sent by government employees are subject to the state's Public Information Act, and government agencies have faced challenges in ensuring that these messages are recorded as required by state law.

Financial institutions must protect themselves and their employees, not only by implementing policies forbidding the use of any unauthorized apps or messaging services for business communications, but also by taking affirmative steps to enforce these policies and monitor compliance. Merely *having* policies and rules in place is not enough — institutions may still be liable for failing to preserve business communications if management is aware that employees are communicating on unauthorized apps and fails to address the problem internally.

Luckily, this is an area in which attorneys can help: many institutions under investigation in the recent probe are arranging for outside legal counsel to help conduct reviews of business-related messaging practices. Given the invasive nature of the SEC's request for employee cellphone access, outside attorneys can serve as intermediaries and separate business-related messages from purely personal employee communications. This ensures that employees retain a degree of privacy while fully cooperating with regulatory investigations. For those institutions not already under scrutiny in the ongoing probe, now is the perfect moment to conduct internal reviews of messaging and communication retention rules and procedures, and to seek advice on how to construct and enforce these policies. Members of the Troutman Pepper team are available to assist on these developing issues.

RELATED INDUSTRIES + PRACTICES

- Securities Investigations + Enforcement
- White Collar Litigation + Investigations