COMPLIANCE CONSIDERATIONS FOR MOBILE DEVICE-BASED COMPLIANCE APPS

THETALAKE

CONFIDENTIAL

TABLE OF CONTENTS

SUBJECT

This brief sets out the compliance considerations that financial services firms need to consider when using mobile device-based compliance apps like Movius, LeapExpert, CellTrust and others, specifically in relation to the capture, retention, and supervision of electronic communications. Mobile device-based compliance apps enable users to communicate on popular consumer messaging platforms and mobile channels including WhatsApp, WeChat and iMessage and capture all communications on those platforms.

This brief describes the features and capabilities of mobile device-based compliance apps, explains how they are used in practice and outlines the applicable regulations in the US, UK and Canada for capturing and supervising the communications within them. Finally, we analyze a few use cases for mobile device-based compliance apps and how regulatory compliance mandates apply to those scenarios.

HOW MOBILE DEVICE-BASED COMPLIANCE APPS ARE USED

Mobile device-based compliance apps allow firms to use popular consumer messaging platforms and mobile channels, such as WhatsApp, WeChat, Telegram, Signal, LINE, iMessage, and SMS, while ensuring that all communications are captured and managed for recordkeeping and governance purposes. Examples of mobile device-based compliance apps include Movius, CellTrust, LeapXpert and Symphony.

Employees use the compliance app interface to send and receive messages and interact with others instead of the native messaging app interface. The compliance app interface allows users to leverage the features of consumer apps and ensure that communications are automatically captured and retained.

A key function of compliance apps is their ability to separate personal and business communications on a single device. Dual-number functionality provides employees with both personal and business lines on one phone, enabling them to manage both types of communication on one device, and avoiding the need to carry two phones. By creating a secure business layer on employees' devices, the compliance apps capture messages, texts and calls related to business without capturing personal content.

The communications captured by compliance apps integrate with archiving solutions, facilitating retrieval for audits and investigations.

To illustrate, what follows are three real-world examples of how mobile device-based compliance apps are used in financial services organizations. We will revisit these use cases in Section 5 and provide guidance about how to apply relevant regulatory requirements relating to recordkeeping and supervision.

Example A: Managing for a charity event - non-regulated

A financial services firm is using CellTrust to coordinate industry-wide participation in its charity fun run via WhatsApp. Employees communicate with industry contacts to share event details, logistics and sponsorship. Using CellTrust's dual-number functionality, employees keep all event-related communications separate from their personal communications.

Example B: Client and personal communications - regulated and non-regulated

A UK-based investment bank uses Movius to enable its regulated employees to use their own mobile device for both regulated and personal communications under its BYOD policy. Executives and employees make voice calls to discuss debt and equity underwriting and trading issues with investment banking clients, third-party advisers, and other market participants. They also use personal channels including SMS to arrange sports activities with friends in the industry without needing to switch between separate phones.

Example C: Using WhatsApp for securities business - regulated

An investment advisor deployed LeapExpert to allow its 500 registered representatives and advisers to use WhatsApp to communicate with the firm's customers about securities-related business. These communications include obtaining authorization to buy and sell stock and discussions about account performance.

THE KEY CAPABILITIES OF MOBILE DEVICE-BASED COMPLIANCE APPS

Understanding the scope of electronic written and audio communications available within mobile device-based compliance apps is critical for firms to be able to capture and supervise them in accordance with regulatory obligations. These capabilities are continuously evolving and vary by both the mobile device-based compliance apps and the features enabled by organizations.

Mobile device-based compliance apps operate by establishing a centralized, federated layer that captures interactions from platforms like WhatsApp, WeChat, LINE, Signal and more before they are sent or received. The communications, including messages, texts, calls, images, group chats, and automated messages, as well as mobile calls and SMS, are automatically captured and routed through the secure environment of the compliance app, eliminating the need for employees to install the specific communications apps such as WhatsApp.

Employees use the mobile-device based compliance app interface instead of the native messaging app, which includes a separate dialer, call and message logs. Advisors can request and record clients' consent or opt-in to send them business messages, and configure automatic out-of-office responses or custom message templates. Group messaging allows users to communicate with multiple contacts at once.

Advisors can request and record clients' consent or opt-in to send them business messages, and configure automatic out-of-office responses or custom message templates.

The mobile device-based compliance apps enable employees to separate work and personal activity on a single mobile phone by assigning them a second mobile phone number dedicated to business related messaging, calls and texts. Clients only need the business number to reach an employee, without requiring the app themselves. Personal use of mobile phones is unaffected, with the apps preserving employees' ability to use their own mobile numbers and native texting apps for private communications, which are neither accessed nor captured by the app, preserving the confidentiality of personal interactions.

The compliance apps operate on WiFi, mobile data, or cellular networks. Cloud-based recording of interactions and centralized, enterprise-level management by administrators, removes the need for employees to manually initiate capture for business communications themselves.

The compliance apps integrate with CRM and collaboration tools like Salesforce and Microsoft Teams and secure integration through SFTP, SMTP, and APIs, enables captured data to be transferred to archives and compliance management solutions.

KEY REGULATIONS THAT APPLY TO THE CAPTURE AND SUPERVISION OF COMMUNICATIONS WITHIN MOBILE DEVICE-BASED COMPLIANCE APPS

The requirements for capturing and supervising electronic communications are set out by global regulators. These include rules from the Security & Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), the Commodity Futures Trading Commission (CFTC) and the National Futures Association (NFA) in the US; the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) in the UK and the Canadian Investment Regulatory Organization (CIRO).

The preservation of communications is subject to intense regulatory scrutiny, with over $4bn in penalties levied by global regulators since 2021 where firms have failed to retain business-related communications. The 2024 FINRA Annual Regulatory Oversight Report confirms that "This risk has become a particular area of focus for regulators" noting that "Because off-channel communications occur on non-firm platforms or devices, there is an increased risk that they are not maintained and preserved as part of the firm's books and records." The regulatory expectations are reflected in the rules and example enforcement examples outlined below.

The SEC's Exchange Act Rules 17a-4, and FINRA Rule 4511 require member firms to, "among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to their "business as such." FINRA's Regulatory Notice 17-18 explains that the content of communications "made through text messaging apps and chat services" determines what must be retained.

An example of a FINRA violation can be

seen where a general securities representative communicated with customers on investment related matters through WeChat's text function but did not retain the WeChat messages. One example of an SEC violation inadvertently committed by numerous firms involves employees using their personal devices to communicate " both internally and externally by personal text messages or other text messaging platforms such as WhatsApp (off-channel communications)."

Similar violations under CFTC Regulations 23.202 and 1.35.are evident in its orders where each firm "failed to stop its employees, including those at senior levels, from communicating both internally and externally using unapproved communication methods, including messages sent via personal text, WhatsApp or Signal".

In the UK, similar violations of rules extend to the PRA's Record keeping rule 2.1 where enforcement against a bank detailed "no formal record keeping policies or procedures in place to manage or retain electronic messages such as WhatsApp messages or iMessages." In addition, the energy regulator Ofgem fined a firm under its Regulation on Wholesale Energy Market Integrity and Transparency (REMIT) Regulation 8 for not recording and retaining electronic communications "made by wholesale energy traders, on privately-owned phones via WhatsApp, which discussed energy market transactions".

Other applicable record keeping rules include NFA Compliance Rule 2-10(a), FINRA rule 2210 regarding Communications with the Public, the Investment Advisers Act Rule 204-2. The applicable FCA rules include SYSC 10A.1.6, in conjunction with the requirements for MiFID II business.

The SEC's Exchange Act Rules 17a-4, and FINRA Rule 4511 require member firms to, "among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to their "business as such."

Supervision and oversight

The supervisory obligations for electronic communications include FINRA Rule 3110(b)(4) which requires firms to have procedures for the "review of incoming and outgoing written (including electronic) correspondence and internal communications" .

Other requirements include CFTC Regulation 23.602(a) and 166.3 together with NFA Rule Supervision rule 2-9. Similarly CIRO rule 3900 and FCA's SYSC 6.1 set out broad supervisory requirements to detect risks of non-compliance with regulatory obligations.

Failures to retain records, as outlined in the cases above, directly led to supervision breaches. For example, in the SEC proceedings the failure to retain communications "led to its failure to reasonably supervise its employees within the meaning of Section 15(b)(4)(E) of the Exchange Act." In the CFTC violation, the failure " to maintain hundreds if not thousands of business-related communications", meant it "thus failed diligently to supervise its business as a CFTC registrant".

INTERPRETATIONS OF THE RULES AND APPLICATION TO THE USE CASES

To illustrate how the recordkeeping and supervision rules apply in practice we can consider the use cases outlined in section 2. These include both regulated and non-regulated business activity, and the compliance approaches and best practices therefore differ accordingly.

Example A: Managing for a charity event - non-regulated

In the first example where the financial services firm is using the CellTrust app to coordinate industry-wide participation in its charity fun run via WhatsApp, there is no regulatory requirement to retain the communications or supervise them. This is because the communications do not relate to their 'business as such" as clarified in FINRA's Regulatory Notice 17-18. Further clarification is provided in Q&A regarding the communications in scope of the rules: Using "posts information about the firm's sponsorship of a charitable event" as an example it states that "No. Whether a communication by an associated person is subject to Rule 2210 depends on whether the content relates to the products or services of the firm."

Example B: Client and personal communications - regulated and non-regulated

In scenario B regulated employees at the UK bank have installed Movius to enable them to use their own mobile device for both regulated and personal communications. The executives' and employees' business calls made through the Movius app, where they discuss debt and equity underwriting and trading issues with clients, advisers, and market participants need to be retained and supervised in accordance with FCA SYSC rules 10A.1.6 and 6.1.

The employees' personal communications arranging sports activities with friends, made through their private phone number and separate personal channels including SMS, are not captured and do not need to be retained or supervised.

Example C: Using Whatsapp for securities business - regulated

In example C, regulated registered representatives and advisers are communicating on WhatsApp with the firm's customers about securities-related business, through LeapExpert's app. In accordance with SEC's Exchange Act Rule 17a-4, and FINRA Rule 4511, the investment advisor must retain records of communications related to its "business as such", which includes the WhatsApp messages along with file links, images and reactions like emojis which provide contextual meaning to the written communications.

ABOUT THETA LAKE