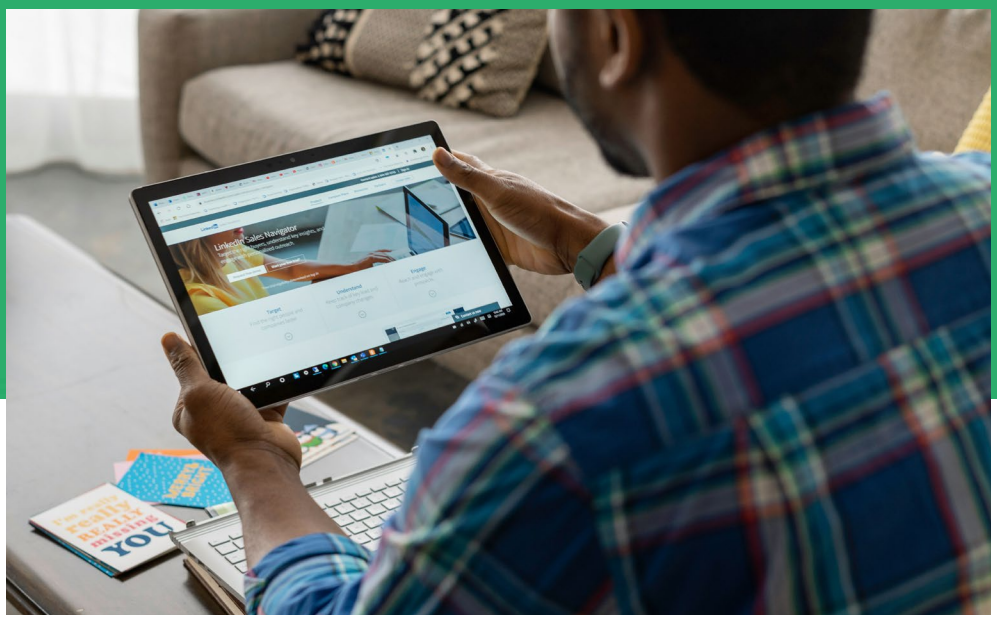


COMPLIANCE CONSIDERATIONS BYOD VERSUS CORPORATE DEVICES

THETALAKE

CONFIDENTIAL

SUBJECT

This brief sets out the compliance considerations for financial services firms that allow employees to use personal devices for business purposes, specifically in relation to the capture, retention, and supervision of electronic communications. Also known as Bring Your Own Device or 'BYOD' programs, these technologies enable staff to use corporate-managed applications on personal mobile phones, tablets or laptops, instead of a corporate device, to communicate and collaborate for work purposes.

This brief describes the capabilities of BYOD, explains how personal devices are used in practice and outlines the applicable regulations in the US, UK and Canada for capturing and supervising communications made through them. Finally, we analyze a few use cases for BYOD and how regulatory compliance mandates apply to those scenarios.

HOW BYOD IS USED

Bring Your Own Device or 'BYOD' refers to an employee using corporate-managed applications on their personal devices for work purposes. This is in contrast to using a corporate device which is owned and provided by a company for employees to use exclusively for work. Personal devices can include laptops, mobile phones, tablets, and other personal devices depending on the firm's guidelines.

Employees are able to connect to their employer's communications platforms and tools through apps installed by the organization. These include apps for Unified Communication and Collaboration tools such as Zoom, Microsoft Teams, Cisco Webex and RingCentral. Some organizations install mobile device-based compliance apps which provide employees with a second phone number, separating personal and business communications on one device.

BYOD gives employees the convenience of using the devices they are familiar with for both personal and work communications, and eliminates the need to carry two separate phones. There are financial benefits for organizations through saving on hardware costs where employees provide their own devices.

To illustrate, what follows are three real-world examples of how BYOD devices 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:

Organising a charity event - non-regulated

The HR team members in a US bank use their personal devices to coordinate their participation in a charity run. Employees communicate with each other via their personal WhatsApp to share details on location, logistics and sponsorship successes.

EXAMPLE B:

Client and personal calls - regulated and non-regulated

A UK-based financial adviser allows its staff to use their own mobile device for work-related communications under its BYOD policy. This includes making voice calls to clients to make recommendations and give advice. The policy gives staff the flexibility to also use their phone for personal calls and other communications such as SMS, without needing to carry or switch between two separate phones.

EXAMPLE C:

Investment banking - regulated

A US investment bank allows employees to use their own devices for work purposes. The investment bankers join Microsoft Teams meetings with other market participants via their phones when travelling between offices, and regularly continue the in-meeting chats post meeting to share updates about market developments.

THE KEY CAPABILITIES AND RISKS OF BYOD

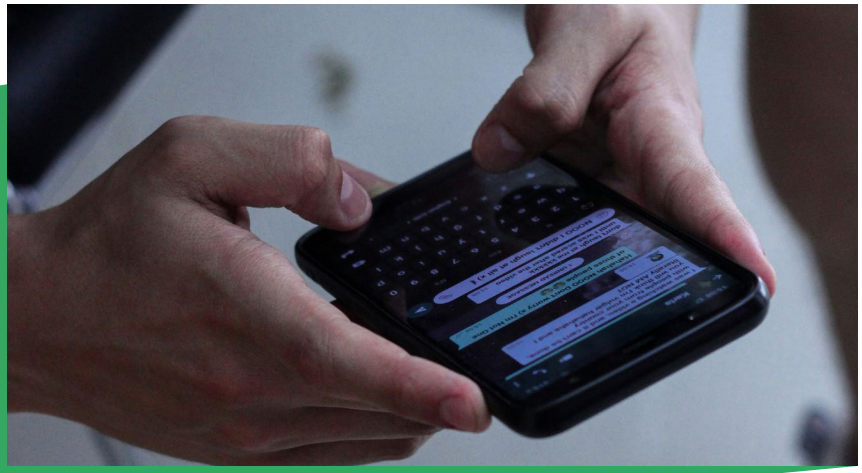
Understanding the scope of electronic written, audio and visual communications available when using personal devices for business is critical for firms to be able to capture and supervise them in accordance with regulatory obligations.

BYOD allows employees to use their personal devices for business communications across audio, written and visual and video channels. To facilitate this, organizations provide approved corporate-managed apps for UCC platforms like Zoom, Microsoft Teams, Ring Central and Cisco Webex. Organizations may install mobile device-based compliance apps which provide a separate business line for mobile phone calls, SMS and consumer messaging platforms like WhatsApp.

The range of digital communications available to employees using BYOD includes chats, calls, screen sharing, video, emojis, reactions, attachments and file sharing. This requires firms to be able to capture and supervise a broader scope and context of communications in addition to traditional channels like email.

The ongoing regulatory scrutiny and heightened enforcement activity for off-channel communications, as detailed in section 4, are key drivers for firms considering a BYOD policy. Allowing employees to use approved, feature rich communications apps helps mitigate the risk of off-channel communications. When features and tools are not available, employees may turn to unapproved channels and personal devices in order to work more efficiently, engage with clients on their preferred platforms, or avoid carrying a second corporate device.

However, BYOD does not eliminate the risk of off-channel communications. Even where there are clearly defined guidelines about what digital communication channels, tools and features are permissible and prohibited, there is a risk that personal applications on personal devices are inadvertently or deliberately used for business purposes.



KEY REGULATIONS THAT APPLY TO THE CAPTURE & SUPERVISION OF COMMUNICATIONS ON PERSONAL DEVICES

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).

Recordkeeping

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 states 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." FINRA's 2025 Annual Regulatory Oversight Report featured multiple findings of personal accounts being used to communicate with customers for firm business. The regulatory expectations are reflected in the rules and enforcement examples 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 the communication determines what must be retained".

An example of a FINRA violation can be seen where a registered representative used an unapproved communication method, his personal cell phone, to communicate via text message with firm customers regarding firm-related business. One of many firm's violations of SEC rules sets out how "Using their personal devices, these employees communicated both internally and externally by personal text messages or other text messaging platforms…"

Similar violations under CFTC Regulations 23.202 and 1.35.are evident in several orders where each firm failed to stop its employees from communicating "using unapproved communication methods, including messages sent via personal text, WhatsApp or Signal". Where employees communicated using unapproved methods on their personal devices, often in contravention of the firms' policies, these were generally not monitored, subject to review, or archived.

In the UK, violations of rules extend to the PRA's Record keeping rule 2.1 where enforcement against a bank included "not having any policies and procedures regarding the retention of such business-related messages on mobile devices (whether Firm issued or personally owned)". Similarly, 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 MiFID II requirements.

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 on personal devices "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 violations, the failure " to maintain hundreds if not thousands of business-related communications" on personal devices and channels, meant firms "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:

Organising a charity event - non-regulated

In the first example the HR team members are using their personal devices to coordinate their participation in a charity run via a dedicated WhatsApp group which is distinct from other business communications. 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."

However it is important to note that there is a risk that the communications between employees on personal channels could change to business communications. Training and awareness will be important to remind employees of the firm's and regulatory expectations.

EXAMPLE B:

Client and personal calls - regulated and non-regulated

In scenario B the regulated financial advisers are using their own mobile devices for work-related communications under the firm's BYOD policy. The calls they make to clients using the Zoom app where advisers make recommendations and give advice, need to be retained and supervised in accordance with FCA SYSC rules 10A.1.6 and 6.1.

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

Providing employees with training and awareness of the firm's policy on only using firm-approved apps and channels will be important to help mitigate the risk of employees using personal channels for business communications on the single device.

EXAMPLE C:

Investment banking - regulated

In example C, the US based investment bankers are using their personal phones to join Microsoft Teams meetings with other market participants when travelling between offices, and regularly continue the in-meeting chat conversations after the meeting to share updates.

In accordance with SEC's Exchange Act Rule 17a-4, and FINRA Rule 4511, the firm must retain records of communications related to its "business as such", which includes the written in-meeting and post-meeting chat messages, along with file links, images and reactions like emojis which provide contextual meaning to the written communications, for at least 3 years.

Learn More	Visit: **ThetaLake.com**