GUIDE

smarsh®

BYOD or Corporate-owned Device: Which Policy Reigns Supreme?

The answer every financial services firm needs to hear

With contributions from: William Tolson, Tolson Communications LLC

Introduction

Mobile devices are integral to business operations. They empower employee collaboration with instant communication and allow customers to engage on their terms.

However, the use of mobile devices in regulated industries — particularly financial services — raises significant concerns related to compliance and data security. Firms must decide whether to support a bring-your-own-device (BYOD) policy or offer corporate-owned devices to support employee collaboration and customer engagement.

In this guide, you'll learn:

- **The pros and cons of each policy**
- **Insight into how you can choose the policy that best works for your firm**
- **How each policy can fit into your compliance strategy**
- **The one true answer to the BYOD vs. corporate-owned device debate**

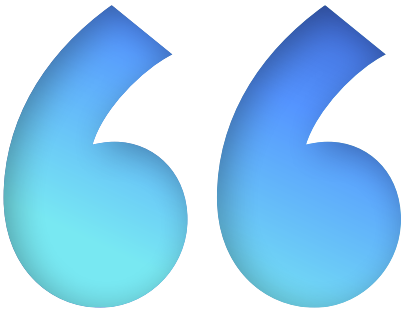
Know your firm's recordkeeping obligations

Before you choose any policy, you must know what your firm is required to do with its communications data. Your firm's mobile policy decision must be made with your firm's regulatory obligations in mind.

In the U.S., both the SEC and FINRA have recordkeeping requirements and guidelines, including:

- SEC Advisers Act Rule 204-2[1]
- SEC Rule 17a-3 and 17a-4[2]
- FINRA Rule 3110[3] and 3120[4]
- FINRA Rule 2010
- FINRA Rule 4511

Similarly, for financial services firms in Europe, Article 16(7) of MiFID II[5] states:



"... an investment firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with, sent from or received by equipment provided by the investment firm to an employee or contractor or the use of which by an employee or contractor has been accepted or permitted by the investment firm."

U.K. firms will need to comply with the Financial Conduct Authority (FCA) SYSC 9.1 and 10A.1.6[6], as well as the Conduct of Business Sourcebook (COBS) 11.8.

[1] https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf
[2] https://www.sec.gov/rule-release/34-47806
[3] https://www.finra.org/rules-guidance/rulebooks/finra-rules/3110
[4] https://www.finra.org/rules-guidance/rulebooks/finra-rules/3120
[5] https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mifid-ii
[6] https://www.handbook.fca.org.uk/handbook

How recordkeeping regulations impact your mobile policy

Ultimately, whether you choose a BYOD or corporate-owned device policy, your firm must be able to capture, archive and supervise business-related communications sent and received on a mobile device.

Compliance teams can't afford to ignore mobile communications. Mobile devices have become indispensable, with text messaging surpassing email as the most engaging communication method and colleagues and customers expecting rapid responses.

While calls and texts are important, it's equally crucial to address the use of mobile messaging apps like WhatsApp and Telegram and collaboration platforms like Microsoft Teams and Zoom. Many have become integral to daily interactions between employees and customers.

Is BYOD viable for regulated employees in financial services?

With so many regulatory requirements surrounding communications compliance, you may think that "no" may be the quick and easy answer to BYOD programs. Many in the industry believe BYOD policies expose firms and individuals to regulatory fines — and this is a valid concern and can be true.

Gartner® quick answer:[7]

BYOD programs are not appropriate for regulated employees within financial services, as they introduce significant compliance risk. To minimize risk, organizations should:

- Reduce exposure to regulatory fines by restricting BYOD program participation to those that are not subject to electronic communications regulatory requirements
- Create and sustain full awareness of regulatory requirements through frequent communications, training and employee attestations

Security risks may increase depending on how individuals use or manage their personal devices. But as we'll go over shortly, there are strategies available to firms to address this.

[7] Gartner, Quick Answer: Are Mobile BYOD Programs Still Viable for Regulated Employees in Financial Services?, Tom Cipolla, Erin Pierre, Pankil Sheth, January 20, 2023.

BYOD vs. corporate-owned devices

Each policy has its strengths, and it's important to understand which will align with your firm's communications strategy.

BYOD vs. Corporate-Owned: Pros and Cons

Set the right expectations for your business by understanding the capabilities of Bring-Your-Own-Devices vs. Corporate-Owned-Devices, and what time, training and resources are needed for both policies.

		BYOD		Corporate-Owned
Cost savings	✓	With BYOD, there's no investment in expensive hardware or software, which can be a significant cost for organizations. Costs, including upgrades, loss or damages, are the employee's responsibility.	✗	The organization must pay for all the costs of using and operating the devices: upgrades, damages, shipping, and monthly usage fees per employee. There are also ongoing administration costs (IT support, security).
Security risks	✗	Personal devices may be less secure than corporate-owned devices, increasing the risk of data breaches and unauthorized access to sensitive information.	✓	Firms can preconfigure devices with organization-controlled security measures and policies, reducing the risk of data breaches and unauthorized access.
Reduced IT support	✓	IT departments may experience reduced support requests, as employees are more likely to be familiar with the operation and troubleshooting of their own devices.	✗	Employees may be less familiar with corporate devices and require more IT support. Additionally, any device issues need to be managed by the company.
Compliance control	✗	Ensuring that personal devices comply with regulatory requirements, such as GDPR, FINRA, SEC, or HIPAA, can present more challenges than managing compliance on COD.	✓	It's easier to ensure corporate-owned devices meet regulatory requirements since the organization fully controls hardware and software configurations.
Increased productivity	✓	Employees know their own devices and can upgrade their personal devices to use the latest technology and applications, leading to greater productivity.	✗	Employees must make a transition to a new user experience and corporate devices may not be updated as frequently, which can slow down productivity.
Streamline IT management	✗	Juggling multiple devices and operating systems can complicate IT management and require additional time and resources to support tasks.	✓	Managing the same device models and operating systems simplifies IT management and support tasks.
Flexibility	✓	BYOD policies can provide flexibility regarding the devices and operating systems used, allowing employees to choose the best tools for their needs.	✗	Corporate devices may limit the types of devices and operating systems available to employees, potentially impeding their ability to choose the best tools for their needs.
Clear work-life boundaries	✗	Employees may struggle to maintain a healthy work-life balance when using their personal devices for work purposes, leading to burnout and decreased productivity.	✓	Corporate devices help employees separate work from personal life, promoting a healthier work-life balance.
Employee satisfaction	✓	Employees are familiar with their personal device, resulting in higher satisfaction.	✗	There is still a dilemma of choice regarding social and collaboration apps. Employees may prefer and default to using their own devices, increasing risk to the organization's data.

Important considerations when choosing a policy

Risk tolerance
As an organization that deals with highly sensitive and regulated data, your firm may opt for corporate-owned devices to ensure (or enforce) the security and compliance capabilities needed to meet regulatory and data privacy requirements.

Business size
Small- to medium-sized firms may want to opt for BYOD to save on costs and resource requirements. If your firm is large or complex, you should consider corporate-owned devices to streamline management, support, security and compliance.

Employee preference
It's important to remember that technologies and tools are meant to support and empower employees. If your employee base prefers using their own devices or has diverse device needs or preferences, you may consider opting for BYOD to accommodate them. Suppose your employees don't mind using a standard device or have similar device needs or preferences. In that case, you may want to opt for corporate-owned devices to simplify the enterprise environment and data compliance management.

Security Risks

8% of financial firms say security is the primary concern in their BYOD vs. corporate-owned device policy decision.*

Cost savings

20% of financial firms say cost is the primary driver in their BYOD vs. corporate-owned device policy decision.*

*According to attendees of a recent webinar, Mobile Compliance Made Easy: Optimization & Best Practices for Small Firms.

Important Note

When deciding on the best approach for your organization, whether employee- or corporate-owned — or a combination of both — it's crucial to consider the diverse ways we communicate today.

Collaboration often happens seamlessly across channels: from text to email to instant message to video call. Firms need to be able to capture, archive and supervise these business-related threaded conversations.

It doesn't have to be one or the other

BYOD and corporate-owned device policies each have merit, but that doesn't mean your firm must endure their cons. Some firms find success in having a hybrid approach. This may look like implementing a role-based policy where employees who work with sensitive data will use corporate-owned devices while the rest of the firm's workforce is allowed to use their personal devices.

Finding the right balance between convenience and the complex, ever-evolving challenges of compliantly capturing, storing and retaining these communications is essential. The significant fines recently imposed by the SEC serve as a reminder to consider the financial and reputational risks of off-channel communications.

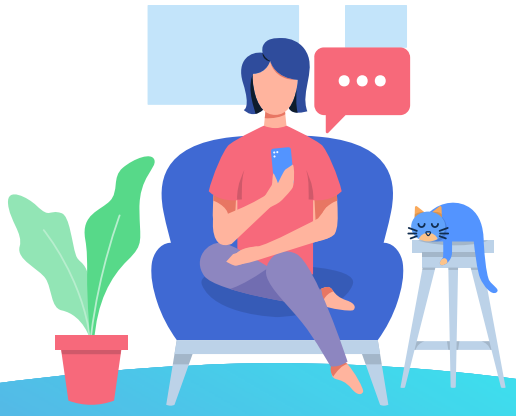
What comes next after choosing a policy

No matter which policy your firm ultimately lands on, there are implementation best practices that apply to both.

Above all, always discuss your possible strategies with your in-house legal team, outside counsel and regulatory compliance department. Each group should be able to offer insights into the appropriate regulatory requirements and legal risk challenges to consider.

You should also communicate clearly with your employees about the expectations and responsibilities of each policy. Provide them with the necessary tools and guidance to use their devices safely and effectively.

Whichever policy you choose, your organization must audit, enforce, and document the policy continuously.



Implementation best practices

- Document a well-defined device use policy and update it regularly
  - Include which applications and communications applications are off limits
  - Include data privacy (PII) safeguards
- For various devices, choose which features should be disabled
- Know your specific industry requirements for mobile devices and data retention
- Implement an annual (at minimum) employee training course
- Conduct ongoing audits of devices
- Enforce policies and discipline when necessary
- Be sure to consider e-discovery obligations
- Ensure compliance and technology infrastructure can capture, archive and supervise business communications

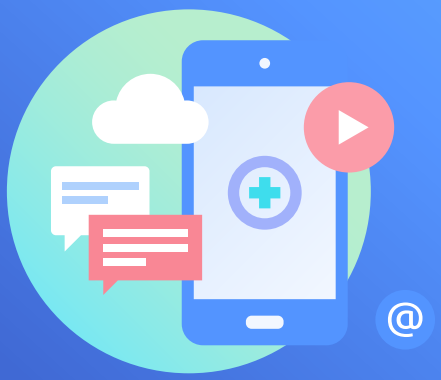
Compliance solutions for BYOD and corporate-owned devices

In the financial services sector, where compliance is of the utmost importance, firms can't risk violations — especially as fines and penalties hit all-time highs.

Mobile device management

Many firms turn to mobile device management (MDM) solutions to help bridge the gap between the organization and its employees to ensure requirements are met.

MDM is a security software used by IT departments to monitor, manage, and secure any corporate or employee-owned mobile devices that access business networks. The software is deployed across multiple carriers, plans and operating systems.



How MDMs reduce compliance concerns:

Security

- Policies for monitoring, encryption, and employee use can be created, redefined, and enforced by IT
- Containerization, or the separation of business and personal files on the same device, keeps business information secure

Risk

- Disable noncompliant or unapproved apps and prevent them from being used on the device when logged in to the business network
- Be better prepared to respond to regulatory, e-discovery, or litigation events

Compliance

- Communications such as emails, SMS/text messaging, social media, documents, and IMs can be archived directly from the device in use
- Disable the use of messaging apps that cannot be archived

An MDM solution can enable employees to use the devices that they want to use by forcing the device to abide by certain rules. This doesn't just apply to software installed across corporate-owned devices either; several MDM solutions are tailored specifically to BYOD scenarios.

Employees benefit by using the same device for work and personal use, rather than carrying separate devices — making it possible to work more efficiently. It also allows them to communicate when, where, and how their clients prefer.

It's crucial to work with a trusted vendor who can capture conversations in their native format and store and monitor the messages and contextual details — such as join/leave functionality, emojis, reactions, and more.

Containerization

Firms can limit the range of mobile communications with an access point name (APN). An APN secures communications traffic or places that traffic into a mandated container. This means employees can only message to a set group while being cut off from communicating with anyone outside of that group. This containerization is an often-used solution for narrowing communications and limiting associated risks.

Containerization programs can separate work communications from personal communications, even for firms with a BYOD program. You should always address during training what communications the business is required to capture and how they will be used. Still, it is also important to reinforce how you plan to maintain privacy for personal communications.

Which policy is a better fit for your business?

Choosing between BYOD and corporate-owned devices — or a combination of the two — depends on an organization's cost goals, resources, time and litigation profile. There's no right or wrong answer to this question. Different firms have different needs, priorities, collaboration cultures and other factors. But while policy is a choice, regulatory compliance is not.

The financial services industry's preferences and needs between BYOD and corporate-owned devices may continue to flip. But what won't change is the regulatory focus on off-channel communications. It's vital for firms to understand that no matter which policy they ultimately land on, the true answer behind this question is having a strategy that manages communications data and mitigates regulatory risk.

Related reading

- Modernizing Mobile Supervision at Enterprise Scale
- Guide to Mobile Communications Capture
- What Does the SEC 17a-4 Regulatory Recordkeeping Update Mean for You?
- Encrypted Apps & Compliance Risks - Industry Brief
- 5 Steps to Compliance in an Evolving Mobile Landscape

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in in a wide variety of digital communication channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Guide - 10/23

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh