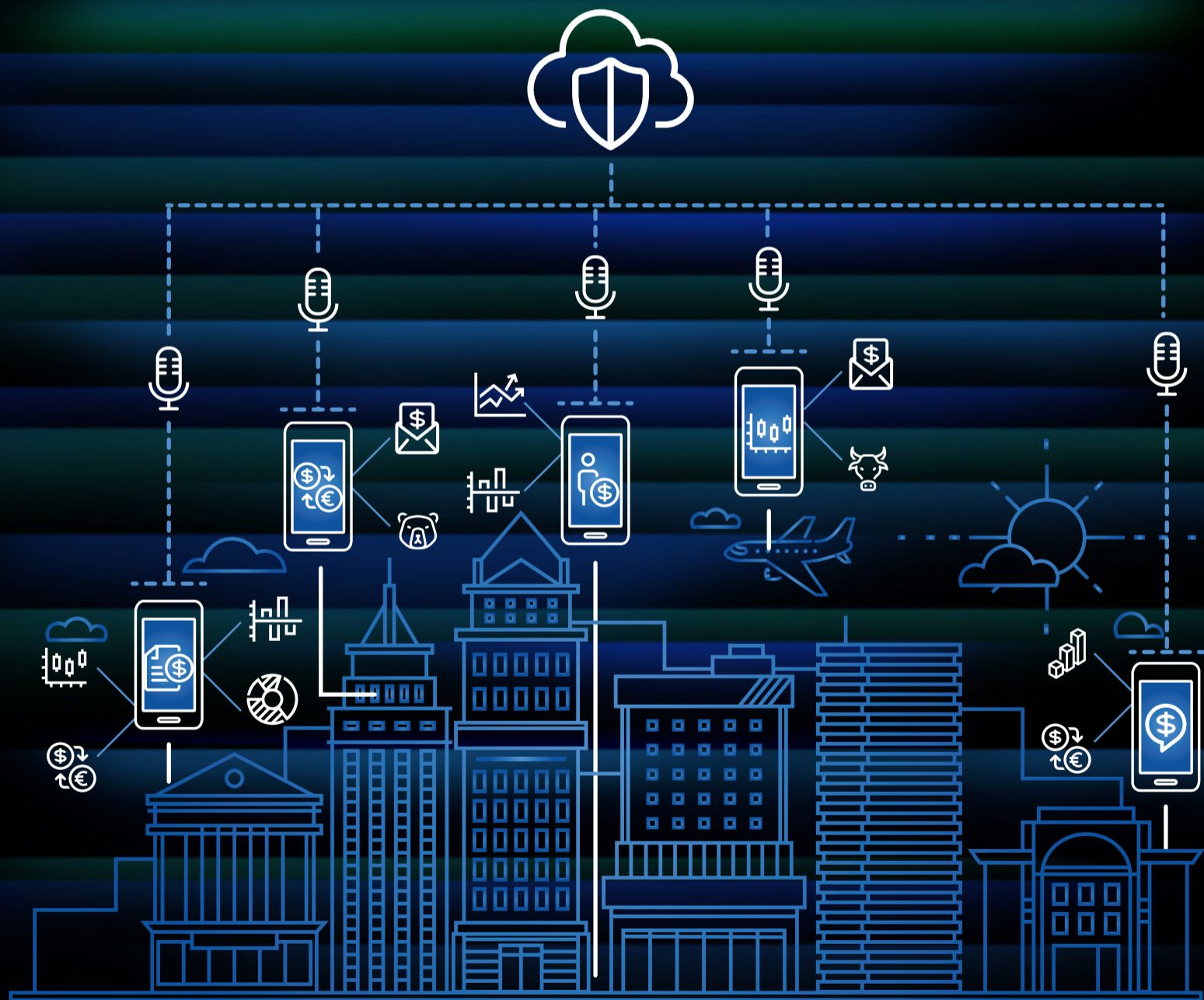


# Mobile Call Recording and Compliance

How Smart Financial Firms are Dealing with Mobile Recording Challenges to Meet Compliance and Other Needs



# Contents

---

<b>Introduction</b>	<b>3</b>
The World Requires Constant Connectivity	3
<b>State of the Industry</b>	<b>4</b>
The Move to Mobile Poses Challenges and Opportunities	4
<b>Customer Service Improves with Data Collection and Analysis</b>	<b>7</b>
Leverage Data to Deliver Customer Service	7
<b>How to Safely Enable Mobile Compliance in the 24/7 Workplace</b>	<b>8</b>
Record Everything	8
<b>What to Look for in a Provider</b>	<b>10</b>
Financial Compliance-Focused Apps	10
Cloud Integration and Flexibility	11
<b>Take Action</b>	<b>12</b>
Embrace Smartphones	12
Mobile Communications Require Rules and Regulations	13

# Introduction

## The World Requires Constant Connectivity

As the world grows increasingly global, the expectation is that financial services firms will be available to their clients 24/7 from anywhere in the world, on any network, and via any device. Financial services employees must be able to place and receive calls, emails, texts, and trades any time of day or night, to take advantage of world markets, and deliver real-time results for investors of all types and sizes.

### Mobile Devices Ensure Constant Access

Often, that means financial advisors are using their mobile devices to conduct business both outside and inside a traditional office. Doing so ensures fast response times, flexibility, and maximum returns for clients and the business, but it also shines a light on the increasing need for clear and consistent policies around all mobile communications. This is especially true in the United States, where a mix of regulations and best practices demand that financial firms record, archive, and make available for review all communications and trade data with their clients, as well as many interactions that occur within the organization among its employees, managers, and executives.

While financial services firms have been recording, logging, and archiving communications and trade data for years, they have not focused on mobile apps and devices. That presents a problem for many businesses: not only do they have to deploy and manage software that can ensure that mobile usage meets all regulatory and legal demands; many firms must also confront a culture that for years has viewed mobile phones as a way to get around compliance and regulatory concerns.

**Financial services firms have been recording landline and VoIP interactions for years—but most have ignored mobile communications. It's time for a change.**



Indeed, many traders and advisors have routinely started or moved calls to their mobile phones when the discussion in question was of a sensitive nature, or when they simply didn't want to be monitored by their superiors or regulators.

These employees aren't necessarily doing anything illegal, but they've created an environment in which they might choose to handle some communications on company-issued PCs and VoIP or landline phones, and other communications on personal or company-owned mobile devices running "off the grid." Now, that has to change.

## Challenges and Best Practices

This paper will discuss the challenges that financial institutions are facing when it comes to managing voice recordings in the United States; highlight the need to provide better security for financial professionals' mobile devices; suggest ways to simplify the process of logging, storing, managing, and retrieving mobile voice recordings in the event a regulatory body request it; show how getting the technology right can also help change the culture; and offer best practices on choosing a vendor partner to ensure compliance without risking productivity or revenue gains.

# State of the Industry

## The Move to Mobile Poses Challenges and Opportunities

The financial services industry is adapting to an increasingly mobile workplace, with more employees and customers using smart phones to gain faster access to information, increase profits, save time, provide better customer service, and compete in a global, always-on world.

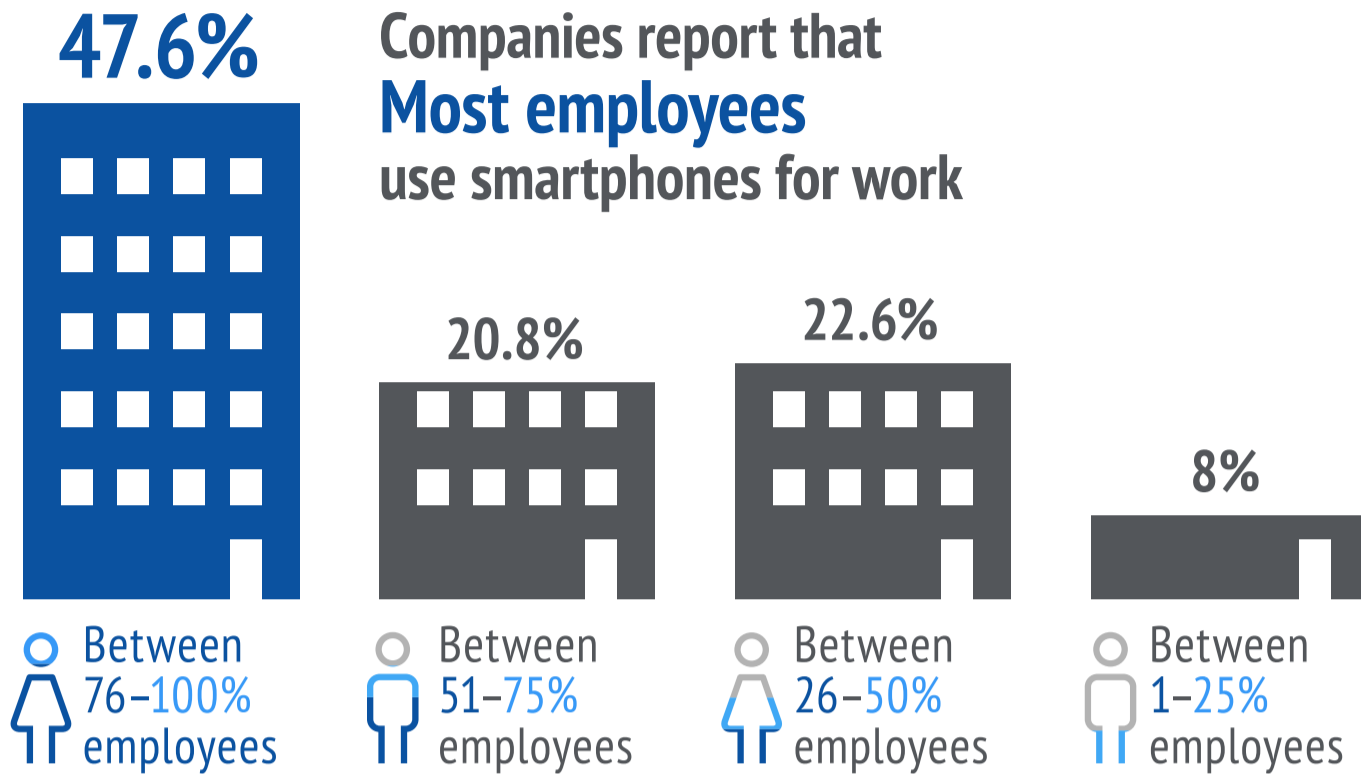
### Smartphone Usage

A recent Frost & Sullivan survey of more than 200 IT decision makers in the industry reveals that their biggest challenges for 2017 and beyond are dealing with financial information security, aligning business goals with IT, and managing new regulatory requirements. At the same time, almost all financial services firms report at least some use of mobile phones in the enterprise; in the majority of companies, more than half of all employees use smart phones for work.

### Smartphone Ownership

Smart firms are not shying away from these challenges, and are instead figuring out how to turn them into opportunities. High among them is the new mobile workplace, which is changing the way traders and advisors do business—and the ways in which their companies must support them today, and into the future.

## Employee Smartphone Usage for Work

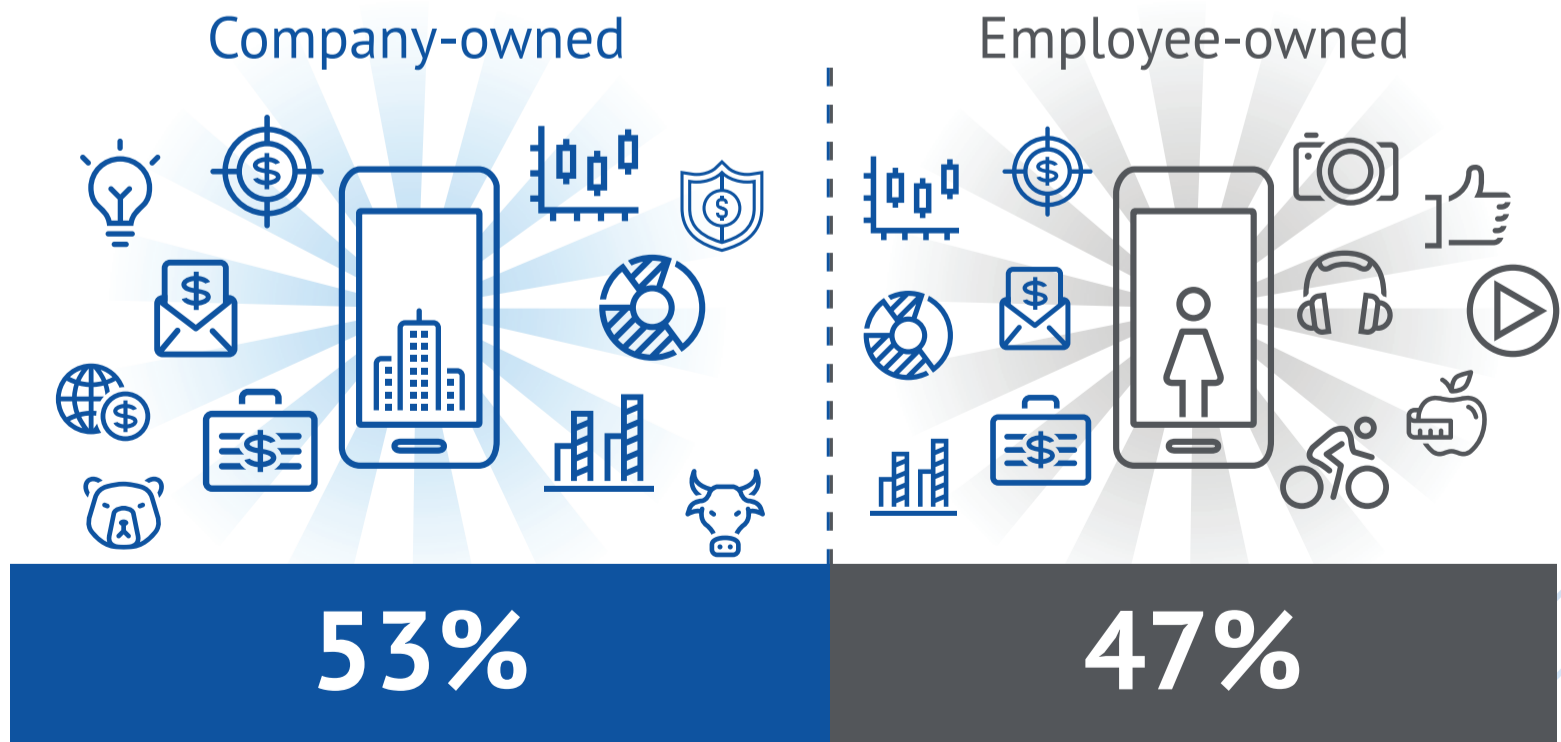


### Employees Who Use Smartphones for Work

Source: Frost & Sullivan, n = 199

The good news is, Frost & Sullivan research reveals that the mobile phones financial services employees use for business are already more likely to be owned by the company (53 percent) than by the employee (47 percent). That allows those organizations to have better control over how they are used, and to determine what gets recorded and when. Company-owned devices are also much easier to manage for security, privacy, and compliance.

## Smartphone Ownership





## The BYOD Threat is Real

But clearly, not enough financial services firms are taking the BYOD threat seriously. When traders and advisors use their personal mobile phones to conduct transactions and communicate with clients and colleagues, the firm has no visibility into those trades or discussions, no way to ensure they meet all compliance regulations and corporate policies, and no way to record and archive the exchanges for future reference and use. Given that the cost of a mobile phone—loaded with the necessary software and apps to guarantee all requirements are met—is around \$100 a month, the ROI is measured in often days or weeks.

**The costs of not changing your employees' BYOD ways can be astronomical—a single lawsuit or breach of law could run into millions of dollars in legal fees and penalties.**



Financial advisors have traditionally worked with their clients in person or on the phone—a high-touch experience was seen as a key component of business success by allowing investment professionals to make, and nurture, a deep, personal connection with their prospects and clients. But today, most customers don't expect such a high level of interaction. For one thing, consumers are increasingly mobile and digitally focused; they prefer text-based and on-the-fly communications. For another, intimate meetings are not always possible in today's global environment, where clients and prospects can be located literally anywhere in the world. To meet these expectations, financial advisors must meet their clients where they live. That means being able to use voice or text communications anytime, anywhere, without worrying about whether the contact is done on a landline phone, through Voice over IP, or on a mobile device. But those communications must be secured and recorded as needed—both to meet regulatory requirements, and to ensure the company has a record of its employees interactions for legal and customer-experience purposes.

Likewise, advisors must be able to use their own smart phones to speak with clients and respond to investor inquiries by providing financial advice and/or trade stocks on their behalf. As a result of this shift, financial services firms must enable secure and compliant mobile communications. If they don't, they are guaranteed to lose

business, as their clients switch to companies that can support their 24/7 needs, and traders and advisors leave for the same reason.

**Investors expect to have easy access to all their financial information and instantly connect with their portfolio anytime, anywhere.**



## Customer Service Improves with Data Collection and Analysis

Today's consumers expect that the companies they do business with will collect and leverage a variety of data—some personal, some global—in order to better meet their specific needs. So-called “Big Data” relies on aggregated data from a wealth of sources, including market trends, political upheavals, environmental changes, census surveys, social networks, and more, to help executives and managers set strategy and respond to opportunities. But “small data”—information specific to a particular prospect or client—can help analysts capture more business from the clients they already have by personalizing their approach at every turn.

## Leverage Data to Deliver Customer Service

Financial services firms can leverage this trend to deliver better, more personalized customer experiences. The first step: record all client data to deliver truly customized service. When companies record, archive, and analyze personal

information—such as a client’s persona, risk tolerance, portfolio allocation, long-term goals, place in the lifecycle, and so on—firms can tweak their offerings and strategies to meet each individual client’s needs, thereby increasing loyalty, conversion rates, and the bottom line.

## Deploy Secure Smartphones

The best way for financial services firms to manage this new normal is to deploy smart phones to all their traders and advisors, loaded with layers of security and software that integrates with back-end systems to ensure the company’s compliance and best practices are met. This option can seem costly up front, but it will save companies money, headaches, and possible legal trouble in the long run. It will also open up new opportunities for services and revenues as analysts leverage the information in those recordings to improve their offerings for prospects and clients.

## Ensure Rules are Followed

To ensure they see such gains, managers and executives must make it clear that absolutely no company business is to be conducted over unsecured mobile devices, and they must create policies and procedures for ensuring such behavior is followed all the time, every time. Deploying the right technology can aid those efforts, by making it easy and effective for employees to always follow the rules.

# How to Safely Enable Mobile Compliance in the 24/7 Workplace

## Record Everything

The need for financial services firms to record all voice and text communications is clear; no company should be without a mechanism for doing so. But some organizations limit their compliance efforts to the contact center and swap-trading desks, currently all that’s mandated by U.S. law. And many others have policies and procedures in place to track and archive such interactions only when they travel along the company’s internal networks. Mobile phones are typically left out of the equation.

## Don’t Leave Mobile Conversations Out

But this is a mistake. Here in the U.S., for example, the Dodd-Frank Act requires that financial services firms record all interactions in the contact center and among swap traders. Furthermore, large financial services firms have global operations and must abide by a slew of disparate international laws. So, for example, they must be aware



that Britain recently passed a law requiring that by 2018, financial services firms record all mobile communications—including voice and text—for five years, just as they do any other contact. Other countries are expected to follow, as more trading and other customer interactions are performed over mobile devices, bypassing the standard corporate voice and data networks that are already subject to strict recording and archiving regulations around the world.

## A VALUABLE SOLUTION

**Automatically record and manage all financial transaction-related communications customers make through their mobile phones. The goal is to make the experience seamless for both clients and employees.**



Companies should take three key steps to ensure their employees stay within the bounds of the law, and good corporate practices:

1. Provide smart phones to all employees;
2. Establish a company policy that forbids employees from using their own mobile devices to conduct business;
3. Implement a voice recording solution on the devices you deploy to ensure all calls and texts can be archived and searched on demand, for any reason.

The only solution for companies that want to get out in front of the issue and avoid any problems with regulators or their own lawyers in the future is to put into place policies and procedures for ensuring that all mobile communications are recorded and archived. The best way to do that is for those companies to provide their employees with a corporate-owned mobile phone that comes loaded with recording-and-archive software that the user cannot uninstall or work around; which loads all communications into a cloud-based portal or other storage system that can be easily searched and reviewed; and which integrates with the company's existing compliance systems.

## The Right Technology Can Change the Culture



For years, traders, advisors, and other employees at financial services firms have used their mobile phones to communicate with colleagues and clients off the radar of their corporate compliance rules. By using a personal device to place and receive calls, chats, texts, and even trades, these users are avoiding the recording and archiving capabilities embedded in their employers' IT infrastructure. Not all employees do so out of malice, of course; many—even most—are motivated by convenience, speed, or an understandable desire for privacy. But regardless, doing so flaunts the rules of their own organizations, as well as regulations and laws that could get them, and their employers, into serious trouble.

It is hard to stop bad actors from acting badly. But most employees are not trying to disregard the law. If companies give their employees a safe way to use their mobile devices—whether they are owned by the company or the end user—they can avoid such conflicts and stay in compliance. Software that makes it easy to stay within the letter of the law, without compromising any of the benefits that come from relying on mobile phones for communications both during and outside of normal business hours, will encourage the vast majority of employees to follow company policies and procedures.

## What to Look for in a Provider Financial Compliance-Focused Apps

Many mobile device and software vendors offer security and compliance solutions, but few have designed apps that are purpose-built for compliance in the financial services industry. The key is to deploy an application directly on the user device through a mobile device management (MDM) or enterprise mobility management (EMM) system. Ideally, once it's installed, the user won't be aware of the app—and therefore won't be able to turn it on or off. As it runs in the background, the app should automatically record on the device all voice calls or data-based communications (like text and chat); those recordings should then be uploaded

to the cloud, along with the relevant metadata, such as the location and time-stamp. Once that happens, the information can be instantly deleted from the user's device, removing the possibility that he or she can delete or otherwise change the information or recording.

## Cloud Integration and Flexibility

Once in the cloud, the voice recording and call information should be archived in the company's portal and stored for a period of time determined according to the firm's chosen parameters, made in conjunction with its compliance team. Once archived, all recordings should be searchable and retrievable on demand. Companies should have the option of using a portal that comes with the software, or integrating all logs with their existing compliance systems; and have the flexibility to choose whether to store the data in the cloud, or on their own premises.

When considering new technology specifically for this purpose, make sure it offers four key components:

1. Flexible enterprise mobility Regardless of whether the mobile device your regulated employees use is owned by you or them, your chosen software solution should make it easy to stay compliant while allowing end users the option of keeping their existing service provider, thanks to a robust MDM/EMM offering.
2. Constant compliance Voice is just one part of the equation; SMS and MMS messages should also be routinely recorded and archived via secure VPN and then stored in the cloud or on site. Look for a solution that delivers a painless user experience that is immune from tampering and requires no input or action on the part of the end user to work.
3. Seamless deployment Ensure you can get up and running quickly with a simple solution that doesn't require any changes to your existing PBX, policies, or processes.
4. End-to-end security Demand the highest levels of security accreditation and compliance available, from data center to device, including:
  - CESG IL2 2-2-4 / CESG IL3 3-3-4
  - All data handled to FIPS 140-1 and DoD 5220.22
  - Encrypted VPN (CESG accredited)
  - Portal Access using a SSL 256bit AES encryption
  - ISO 27001/ISO 27002 Information Security

# Samsung Knox



- **Defense-Grade Mobile Security Platform:** A multi-layered technology built into both the hardware and software of Samsung's latest devices. From the hardware root of trust to the Android framework, Knox constantly verifies the integrity of the device and detects any tampering, ensuring your customer's data is always secure.
- **Hardware Root of Trust:** A set of security mechanisms built into device hardware that flag any time the device's default controls have been altered. These include Secure Boot Key and Device Root Key, which perform authentication and encryption operations associated with the device.

## DATA SECURITY OPTIONS TO SUIT EVERY ORGANIZATION

- **Knox Workspace:** An on-device security offering that's secure enough to run on a government-grade network. It supports two-factor identification; powerful-but-protected apps such as Contacts, Calendar, Camera, and Email; and integration with existing MDM, VPN, and Microsoft Exchange ActiveSync.
- **Knox Customization:** A comprehensive set of tools and services that allow businesses to customize and deploy end-to-end mobile solutions. Transform Samsung devices into purpose built solutions for any industry.

Secure, manage and customize your business's mobile devices. For more information, visit [www.samsung.com/us/knox](http://www.samsung.com/us/knox)

Licensing fees apply.

## Take Action Embrace Smartphones

Financial services firms are realizing that to stay competitive in a global and increasingly dispersed workplace, they must embrace the move to mobility among their traders, advisors, and customers. Financial professionals need the flexibility to stay in touch with their clients around the clock—and that means giving them the tools and freedom they need to communicate, access information, and request trades any time of day or night, on any network or device.

# Mobile Communications Require Rules and Regulations

But enabling a mobile-first workplace takes careful thought and focus, as well as the right mix of technology and cultural change to ensure all rules and regulations are being followed. Gone are the days when financial services employees could use their mobile phones to work under the radar, conducting calls and texts and even trades in an effort to avoid being recorded by their employer or audited the regulatory agencies. Today, financial services firms must take control of those devices—and all communications and interactions that happen over them—to remain in compliance with rules that require that all transaction-related communications and trade data are recorded, saved, archived, and made searchable in the event of an issue or larger investigation.

To stay on the right side of the law, companies must deploy devices and software that automate the recording and archiving process, even without the user knowing that it's happening. By giving corporate-owned mobile phones to their employees who need them, loaded with software that will ensure compliance with all regulations, companies can mandate the use of those phones for all business purposes.

That requires a strong and reliable software solution. IT and compliance managers should look for a system that integrates with a company's existing infrastructure, is designed specifically for mobile devices, can extend to voice calls as well as any other form of communication, supports trades within the relevant software, and is so effective as to be almost unnoticeable by the end users.



WHAT NEXT?



Learn more about Samsung's  
innovative mobile workplace solutions:

[samsung.com/finance](https://samsung.com/finance)

**SAMSUNG**

White paper commissioned by Samsung Electronics America.



Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector, and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics, and emerging economies?



**Silicon Valley**

331 E. Evelyn Ave.,  
Suite 100  
Mountain View, CA 94041

Tel 650 475 4500  
Fax 650 475 1570

**San Antonio**

7550 West Interstate 10, Suite  
400  
San Antonio, TX 78229

Tel 210 348 1000  
Fax 210 348 1003

**London**

4 Grosvenor Gardens  
London SW1W 0DH

Tel +44 (0)20 7343 8383  
Fax +44 (0)20 7343 3343

877.GoFrost  
[myfrost@frost.com](mailto:myfrost@frost.com)  
[www.frost.com](http://www.frost.com)



For information regarding permission, write:

**Frost & Sullivan**  
331 E. Evelyn Ave., Suite 100  
Mountain View, CA 94041



- Auckland
- Bahrain
- Bangkok
- Beijing
- Bengaluru
- Buenos Aires
- Cape
- Chennai
- Dammam
- Delhi
- Detroit
- Dubai
- Frankfurt
- Herzliya
- Houston
- Irvine
- Iskander Malaysia/Johor Bahru
- Istanbul
- Jakarta
- Kolkata
- Kotte Colombo
- Kuala Lumpur
- London
- Manhattan
- Miami
- Milan
- Moscow
- Mountain View
- Mumbai
- Oxford
- Paris
- Pune
- Rockville Centre
- San Antonio
- São Paulo
- Seoul
- Shanghai
- Shenzhen
- Singapore
- Sydney
- Taipei
- Tokyo
- Toronto
- Town
- Valbonne
- Warsaw