shield. LEAP XPERT

2023 State of Mobile Communications Compliance

July 2023

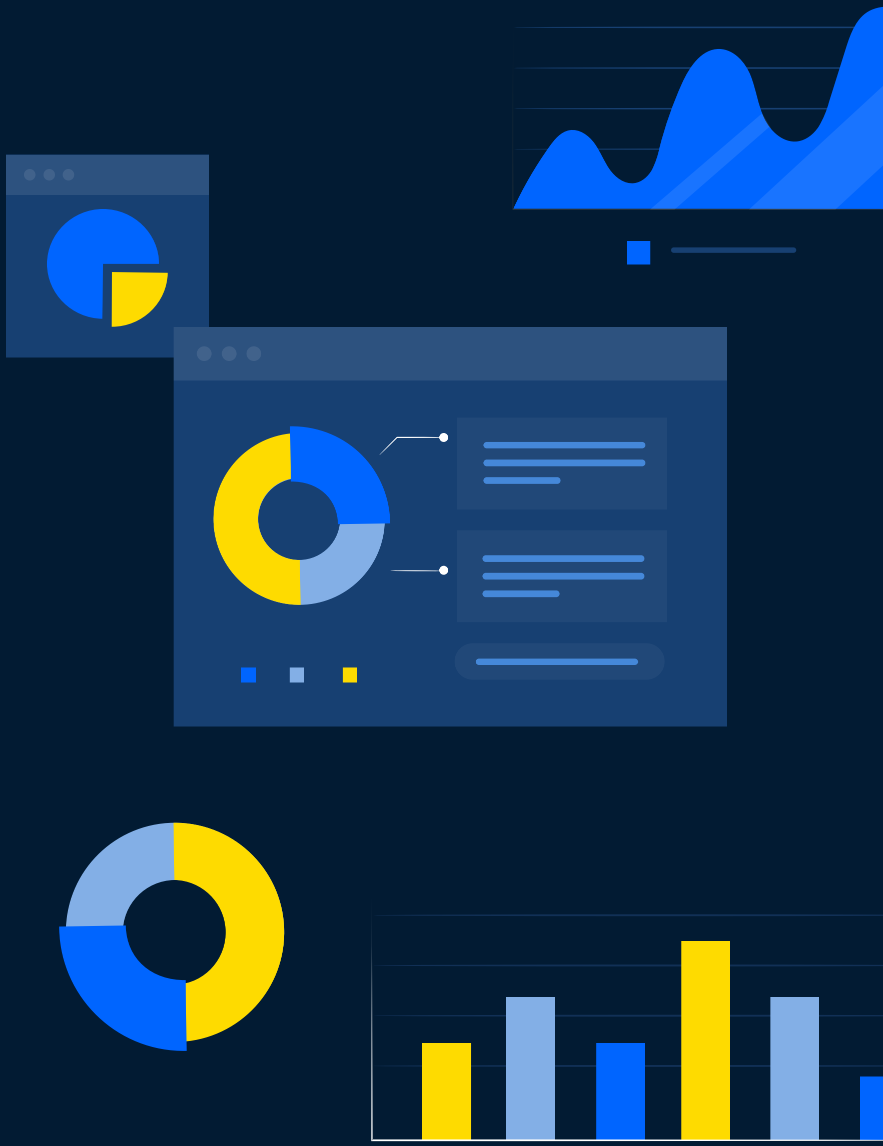


Table of Contents

Introduction and Key Findings 3

Survey Report Insights 7

Two-thirds of respondents cite clients as a key initiator of mobile messaging conversations 8

73% of financial institutions lack full confidence in unapproved communications channel bans 9

Most chat channels are either already being monitored or will be by the end of the year; WhatsApp is the top priority 10

64% of financial institutions cite regulatory audits as their top concern around mobile communications 11

Top priorities when selecting a monitoring solution for messaging channels in 2023 12

Almost half of respondents agree that user adoption of their current solution is poor 13

Half of financial institutions agree that their existing mobile communications monitoring solutions are unreliable, deliver poor user experience, and are not cost effective 14

Mobile device policy: Current vs. in 18 months 15

Demographics 16

About Shield 18

About LeapXpert 19

Introduction and Key Findings

Introduction

In today's digital-first economy, customers have become accustomed to communicating with brands and service providers using a myriad of devices, channels and mobile apps. With convenience as their top priority, they expect a fast and efficient response from their representatives.

For front office employees of financial institutions, this means communicating with clients using mobile messaging channels that veer from traditional 'approved' channels, like phone and email, to those like WhatsApp, iMessage, WeChat, SMS, and others. Archiving and monitoring these communication channels has traditionally been fraught with difficulties, exacerbated in recent years by employees using their personal devices to communicate with customers, opening the door to various security and compliance challenges. This is especially problematic for heavily regulated industries like financial services, where all communications need to be captured and archived so that they can be easily monitored by firms and regulators to ensure compliance and proper conduct.

Indeed, in the past 18 months, regulators have targeted some of the biggest banks, issuing hundreds of millions of dollars in fines (an estimated aggregate of more than $2 billion), specifically for not cracking down on employees who use WhatsApp to conduct business. This has created increased focus for financial institutions to find solutions that will ensure they are using mobile communications responsibly and are prepared for the scrutiny of regulatory audits by meeting compliance requirements.

The aim of this survey is to provide insights for compliance professionals on:

01 The main challenges facing the industry in relation to mobile messaging monitoring

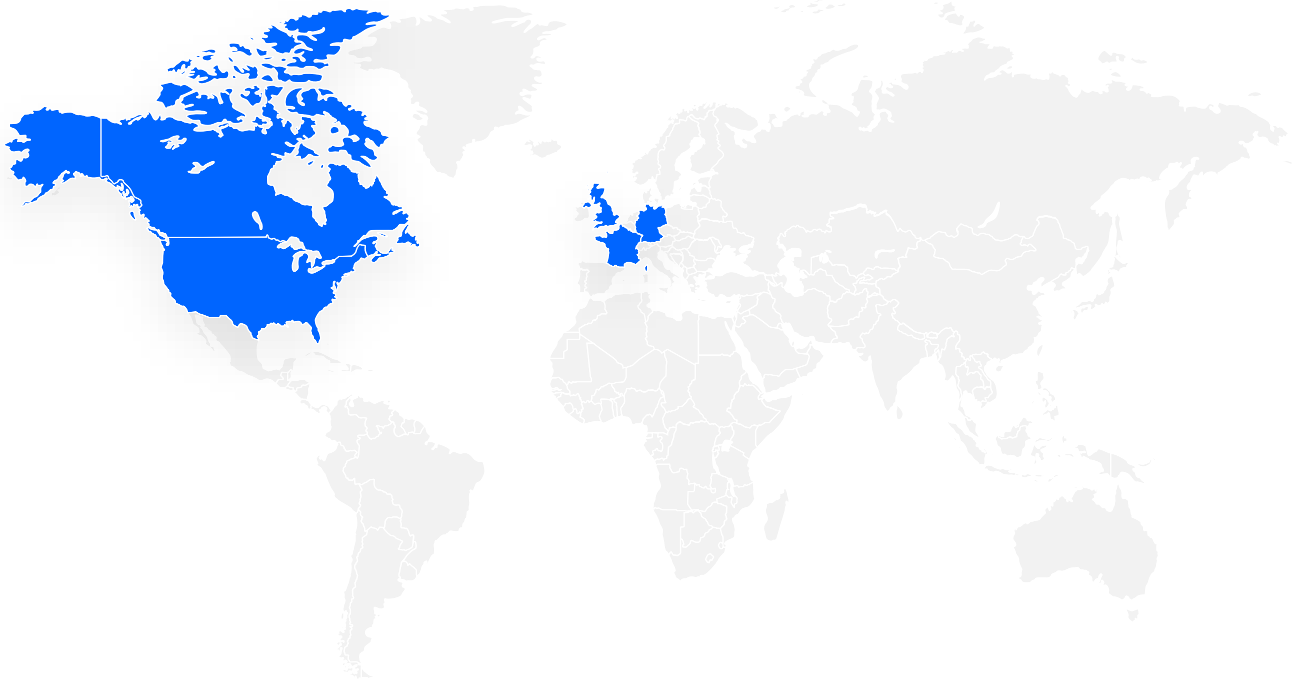
02 Effectiveness of their current solutions compared with their industry peers

03 What actions are being taken to ensure they achieve sufficient compliance as quickly as possible

Methodology

To gather insight into current priorities and pain points for financial institutions around digital communications compliance, we commissioned a survey of 200 compliance leaders from the financial services industry. The survey was administered online by Global Surveyz Research, an independent survey company.

50% of respondents were from North America and 50% from Europe (UK, France, Germany).



They included managers (and higher seniority) from companies ranging between 100 and 5K+ employees. The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during the first half of 2023.

The average amount of time spent on the survey was 7 minutes and 26 seconds. The answers to most of the non-numerical questions were randomized to prevent order bias in the answers.

Key Findings

01

73% of financial institutions lack confidence in bans on employees' use of unapproved communications channels

Almost three-quarters of financial institutions (73%) lack confidence in their ability to enforce bans of unapproved communications channels used by employees (Figure 2), suggesting those who continue to rely on 'channel banning' are potentially at risk of facing regulatory action – and hefty fines – due to non-compliance.

Given the lack of continued faith in the effectiveness of current channel banning strategies, it's unlikely this approach will remain viable moving forward, and reinforces the urgency for organizations that don't currently have a mobile communications monitoring solution in place to invest in one.

02

The top chat channel that financial institutions are already monitoring is WhatsApp (51%), with virtually every respondent planning to monitor it by the end of 2023

Financial institutions are currently investing in monitoring several chat channels, with WhatsApp (51%), SMS (45%) and iMessage (34%) being their top priorities. Virtually all respondents are planning to adopt monitoring solutions for these channels by the end of this year, as well as for channels like LINE, WeChat, Telegram and Signal, albeit to a lesser degree (Figure 4).

This commitment is a testament to the failing confidence in banning strategies and the urgency with which financial services organizations are moving to meet regulations for these channels.

03

The top concern for financial institutions (64%) is their level of preparedness for regulatory audits and potential fines

In the past year, regulators have increased exams and issued a slew of fines, specifically for not monitoring communications from mobile communications apps. This has compelled even larger financial institutions that typically have longer buying cycles to ramp up their search for communications monitoring solutions (both in the US and Europe), to withstand the scrutiny of regulators taking a closer look at their messaging channels, and to meet compliance requirements – as early as this year.

Survey Report Insights

Two-thirds of respondents cite clients as a key initiator of mobile messaging conversations

When asked who typically initiates conversations over mobile messaging, 34% of respondents said employees, 22% said the clients, and 44% said that both the clients and employees initiate them.

Despite some organizations' best efforts to prohibit employees from using mobile messaging to communicate with clients, the reality is that mobile communications are now tantamount to a key sales tool that cannot be ignored, especially with 66% of respondents citing clients as initiators of those conversations.

Simply instructing employees not to use mobile messaging ignores the reality that people use these tools as a natural way of communicating. Having a compliance solution for mobile messaging, regardless of who initiates the conversation, can reduce susceptibility to potential fines and bad press.

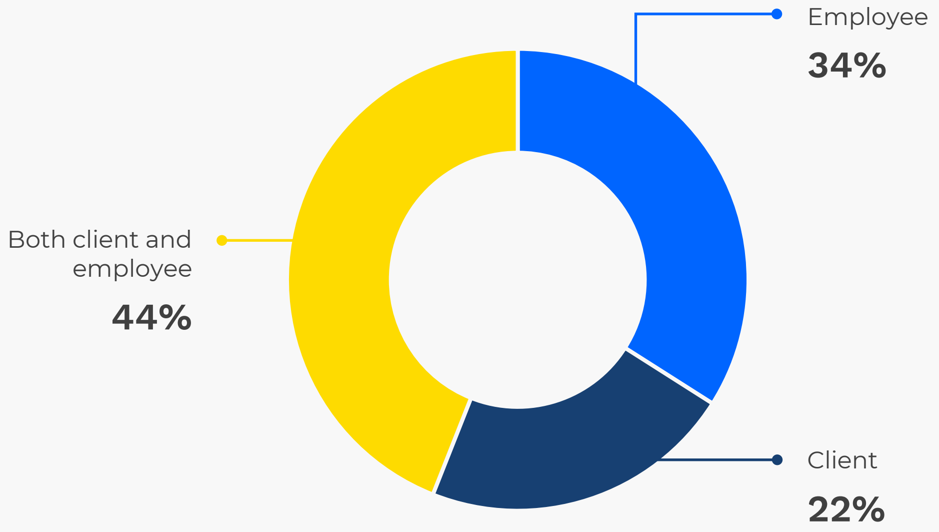


Figure 1: Initiators of Conversations Over Mobile Messaging

73% of financial institutions lack full confidence in unapproved communications channel bans

When asked how confident they are about their ability to enforce bans of unapproved communications channels used by employees, only 27% of respondents indicated they are "very confident."

Anything less than total confidence by the organization to prevent employees from using these channels could leave dangerous blind spots in coverage. **The 73% of respondents indicating they lack full confidence suggests the banning strategy is unlikely to remain viable moving forward.**

When looking more closely at respondents who indicated they lack full confidence in their organization's ability to enforce bans of unapproved communication channels by company size (Figure 3), it is apparent that firms of all sizes share this sentiment fairly equally. This confirms that the pressure to eliminate the risks associated with non-compliance is being felt across the industry, regardless of company size.

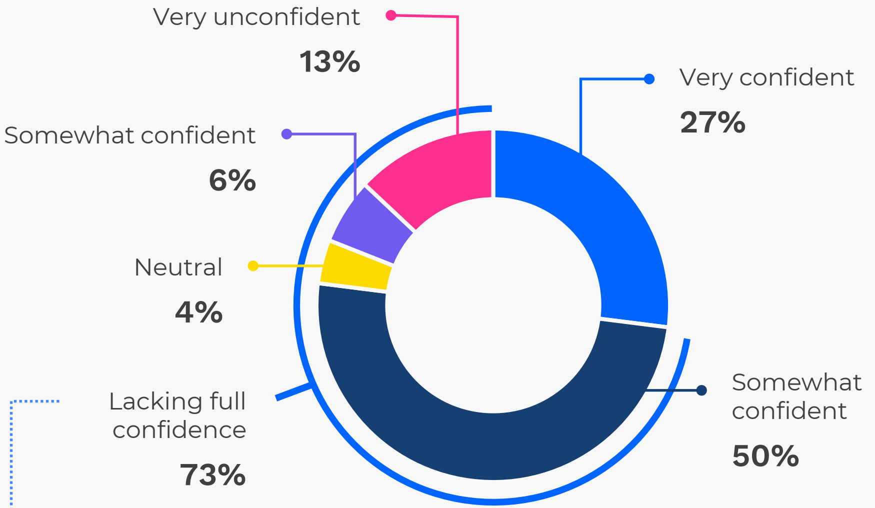


Figure 2: Confidence in Enforcement of Bans of Unapproved Communications Channels

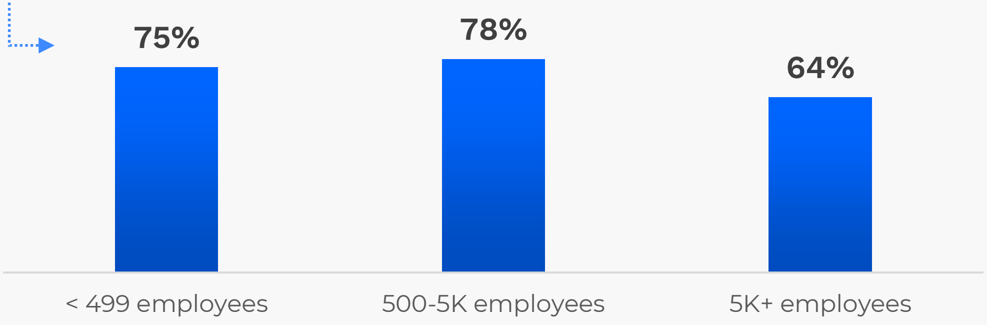


Figure 3: "Lacking full confidence", by Company size

shield. LEAP XPERT

Most chat channels are either already being monitored or will be by the end of the year; WhatsApp is the top priority

When asked when they are planning to adopt monitoring solutions for the most popular chat channels, respondents indicated that most of the channels are either already monitored or expect to be monitored by the end of this year.

The top three channels that are already being monitored are WhatsApp (50.5%), SMS (45%) and iMessage (33.5%), with virtually all of the remaining respondents planning to monitor all three channels by the end of 2023.

It makes sense that WhatsApp is a top concern, given that its usage has spiked in recent years. Our findings show that **North American companies are more advanced (57%) than their EU counterparts (44%) in relation to WhatsApp monitoring** (Figure 5). Considering the general adoption of WhatsApp is much lower in the US, this finding is especially surprising, possibly pointing to the SEC fines motivating US organizations more than their EU counterparts.

Interestingly, even the less monitored channels – WeChat (26%), Telegram (22%) and Signal (22%) – are also planned to be mostly monitored by the end of the year, which is testament to the belief that a wide range of coverage is necessary for compliance.

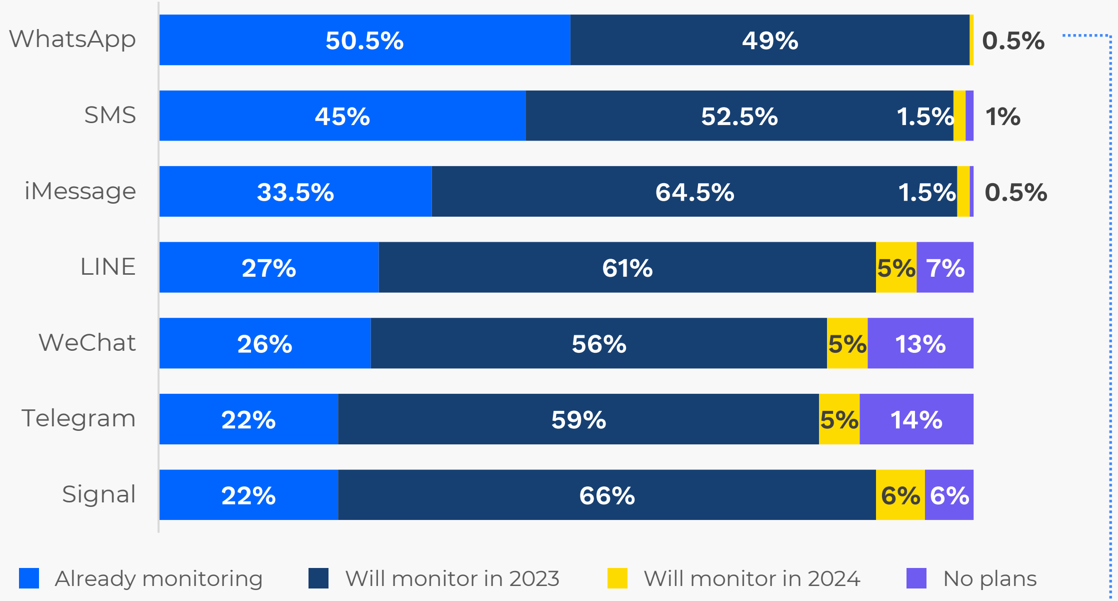


Figure 4: Monitoring Solutions Adoption Plans for Different Channels

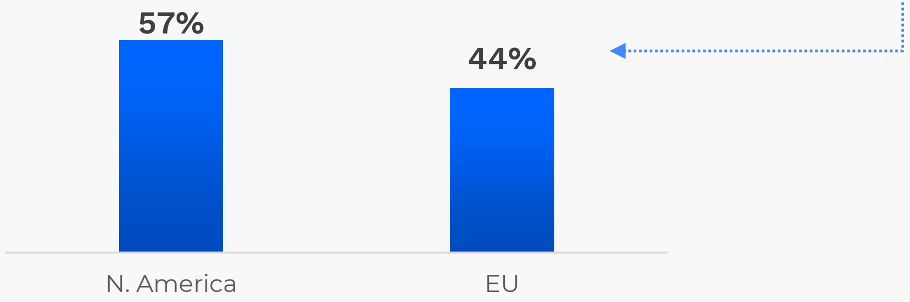


Figure 5: “Already monitoring WhatsApp”, by Region

64% of financial institutions cite regulatory audits as their top concern around mobile communications

When it comes to mobile communications, the top concern for financial institutions is their level of preparedness for the scrutiny of regulatory audits.

Of those who cited regulatory audits as a top concern (64%), 72% of compliance professionals looking to adopt a WhatsApp compliance solution in the next three months are more concerned than respondents who already have a WhatsApp solution in place (57%), indicating that monitoring solutions help to improve their peace of mind.

Given that respondents were asked to choose up to three 'top concerns', the fact that most of the remaining choices were rated fairly evenly, suggests that the rising volume of data captured through monitoring solutions is heralding a variety of new, associated problems. Concerns around costs, data overload, monitoring of this data, and analyzing it to derive actionable insights – can all be used to make a compelling business case for the urgent adoption of monitoring solutions for mobile communications channels.

Reputation is also a top overall concern for financial institutions (28%), with European respondents being more concerned (34%) about their reputation being damaged due to using unapproved communications channels (Figure 7), compared with their North American counterparts (21%).

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

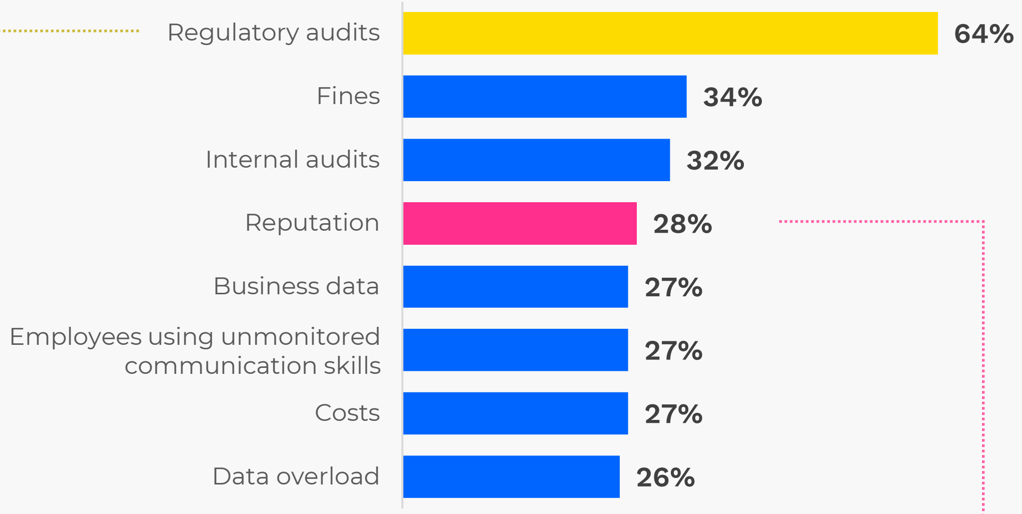


Figure 6: Top Concerns Regarding Mobile Communications

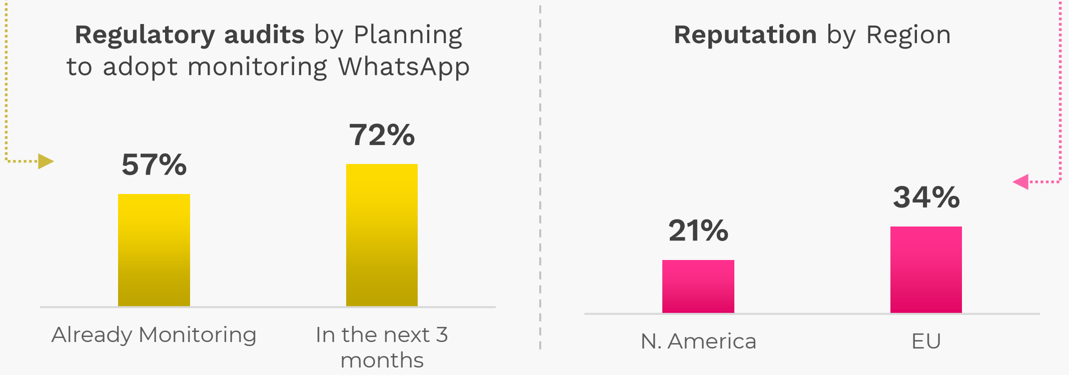


Figure 7: "Regulatory audits", by Planning to adopt monitoring WhatsApp and "Reputation", by Region

Top priorities when selecting a monitoring solution for messaging channels in 2023

We asked respondents what their most important needs are around monitoring messaging channels in 2023 (in addition to compliance). Their top responses were: integration with enterprise and business workflows such as CRMs, billing, trade systems, chat bots, etc. (54%), protecting sensitive information in the form of data loss and virus/malware prevention (44%), and reducing costs by consolidating systems for communication compliance (41%).

The fact that the 'most important need' in a solution that captures and archives messaging channels is the ability to integrate them with enterprise and business workflows makes sense, considering the insights and opportunities that capturing and integrating this data affords. Data doesn't live in a silo, so a mobile messaging compliance solution that captures messaging communications in a siloed system might check a box, but still lock firms out of valuable opportunities.

Rather, respondents have indicated they need the solution to be an enterprise-grade platform that can integrate with other IT systems, workflows, and tools such as Microsoft Teams, have the requisite controls to protect their data, and ultimately provide key insights to stakeholders throughout the organization. The benefit of a solution that can accomplish all of this would eliminate the need for financial institutions to invest in multiple, disparate systems.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

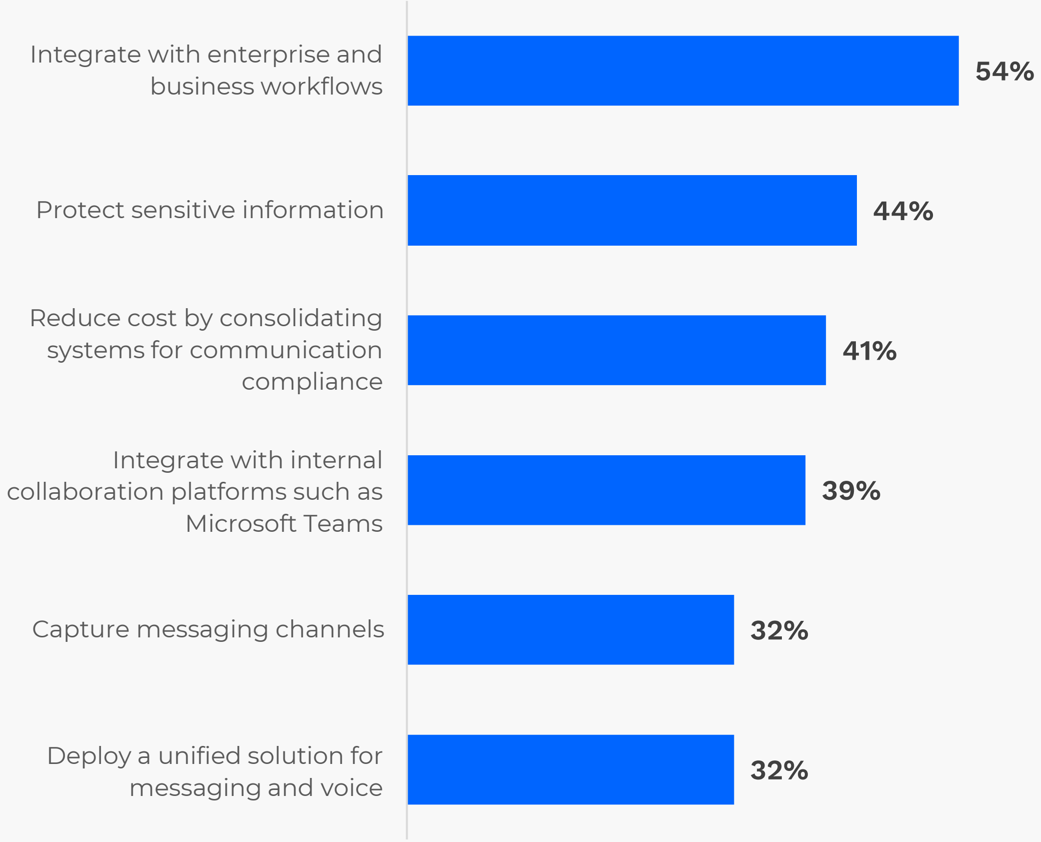


Figure 8: Most Important Needs for Messaging Channels in 2023

Almost half of respondents agree that user adoption of their current solution is poor

48% of respondents believe their current solution for mobile communications capture isn't sufficiently adopted within their organization.

When analyzing this result further, C-suite respondents agree with the statement far more (69%) than VPs (37%) and Managers and Directors (39%).

This misalignment of perceptions could highlight for managers and VPs the need to reevaluate whether the controls they have in place are effective, and push their providers to deliver a better solution.

Given that one of the key aspects keeping financial institutions from buying such solutions could be that they expect the user adoption to be poor, firms may look for a solution that facilitates user adoption more seamlessly, is intuitive, user-friendly, and doesn't disrupt employee workflows. In addition, for better adoption of the solution, it could also make sense for organizations to train their employees on the optimal use of their chosen monitoring solution.

*Percentages do not add up to 100% due to rounding up of numbers

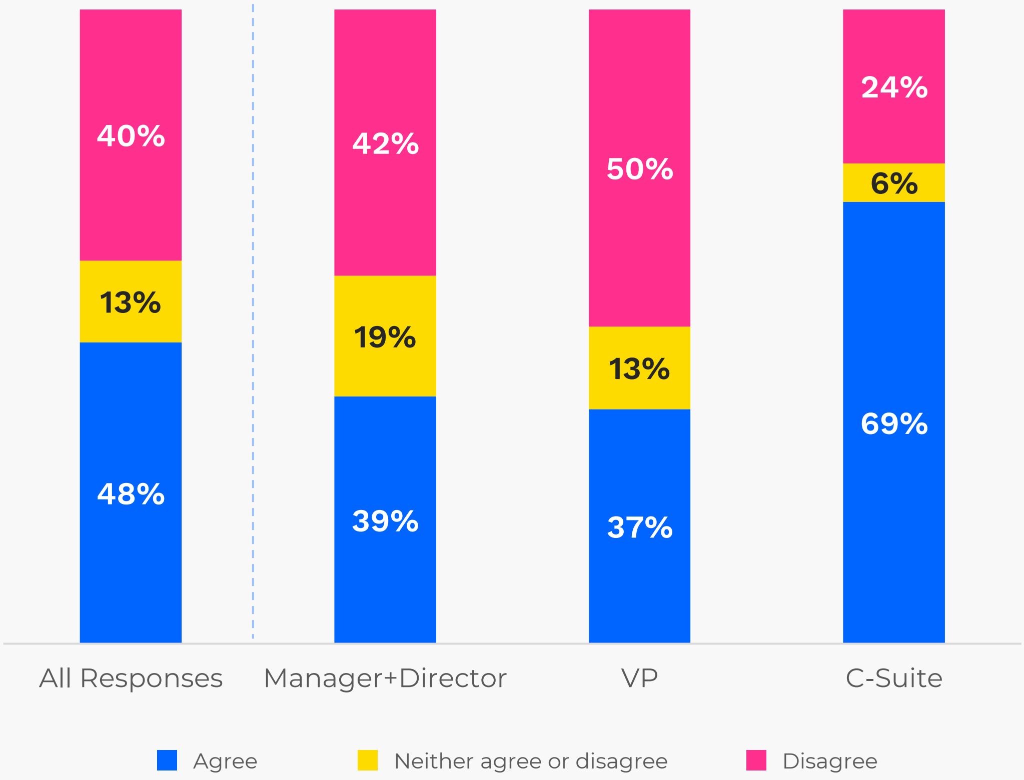


Figure 9: "User Adoption of Current Solution is Poor", by Job seniority

Half of financial institutions agree that their existing mobile communications monitoring solutions are unreliable, deliver poor user experience, and are not cost effective

50% of respondents lack faith in the reliability and cost effectiveness of their existing solutions, and in their ability to deliver a positive user experience.

When looking at the data by job seniority, there is a notable discrepancy between C-suite sentiments regarding their solution's reliability, user experience and cost effectiveness, compared with the sentiments of less senior respondents. One reason for this could be that C-suites view the platform at a high-level, whereas VPs, managers and their teams have a more hands-on experience with the platform and therefore have become accustomed to reducing their expectations.

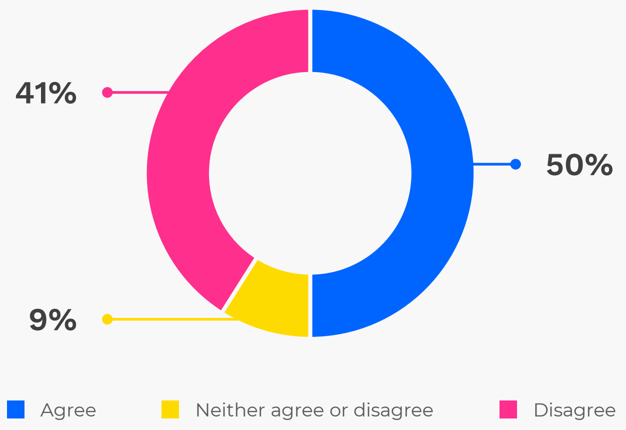


Figure 10: "My Existing Solutions are Not Reliable"

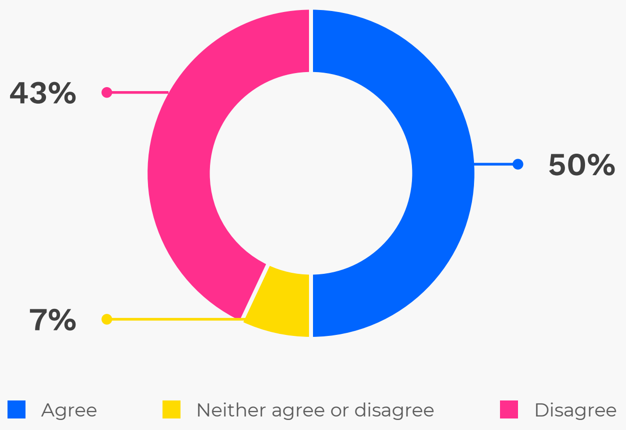


Figure 11: "My Existing Solutions Deliver Poor User Experience"

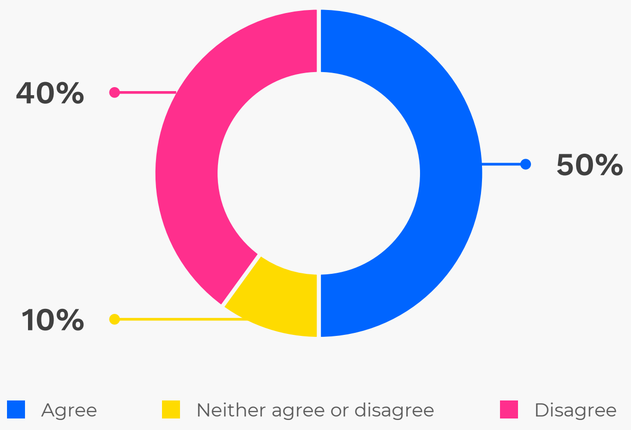


Figure 12: "My Existing Solutions are Not Cost-Effective"

Mobile device policy: Current vs. in 18 Months

We asked respondents about their current mobile device policy, and how they envisage it in 18 months. The results show that the current market is a very mixed environment, with policies divided almost equally: 53% are corporate-only and 47% are Bring Your Own Device (BYOD).

According to respondents, even within departments, there are different policies for different levels of seniority.

We are seeing a trend, however, especially in regulated industries, of an increase in corporate-issued devices, to create a more distinct division between personal and work communications. In 18 months, 66% of respondents expect to employ a corporate device only policy, or a mix of corporate-issued device with BYOD (up from 53% today). This suggests firms will soon come to rely heavily on solutions that can capture and monitor messaging apps on both corporate and personal devices.

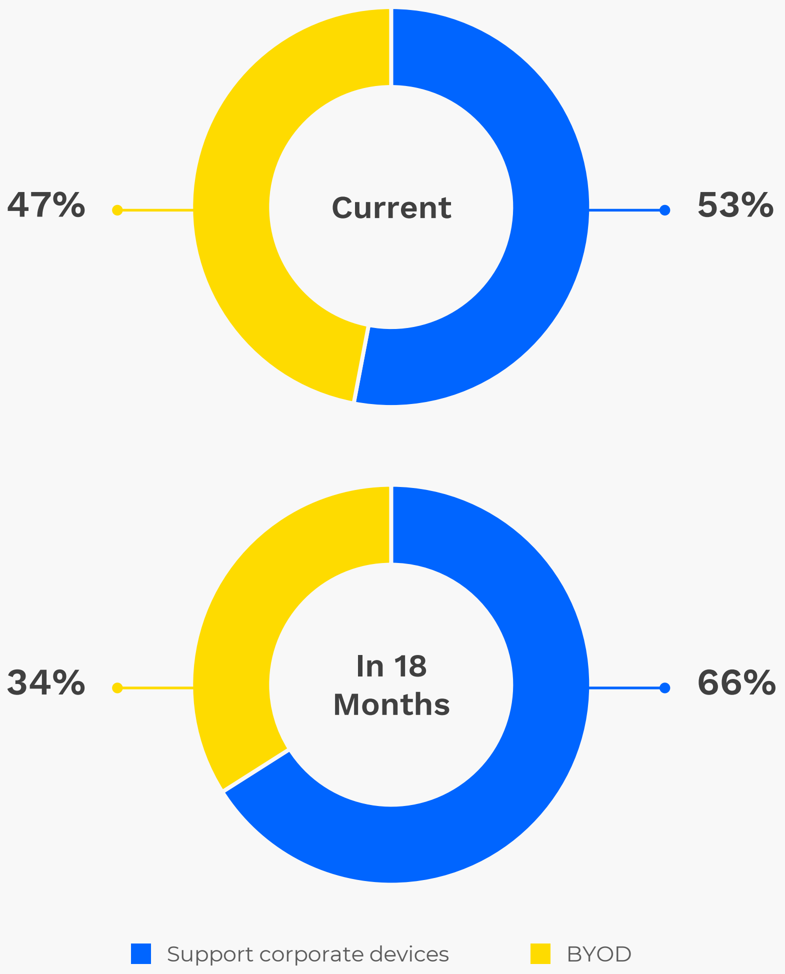


Figure 13: Mobile Device Policy, Current vs in 18 Months

Demographics

Country, industry, job seniority, company size and firm type

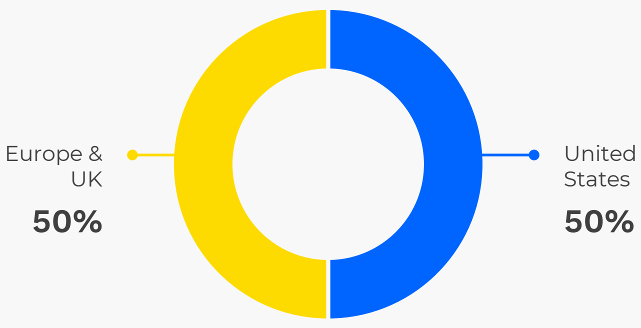


Figure 14: Country

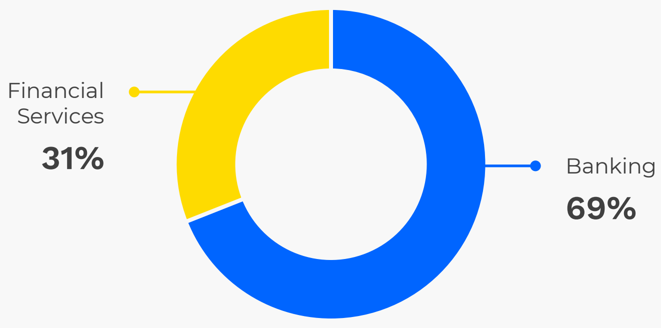


Figure 15: Industry

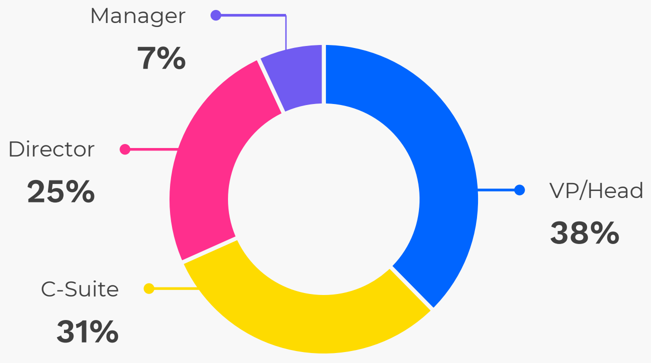


Figure 16: Job Seniority

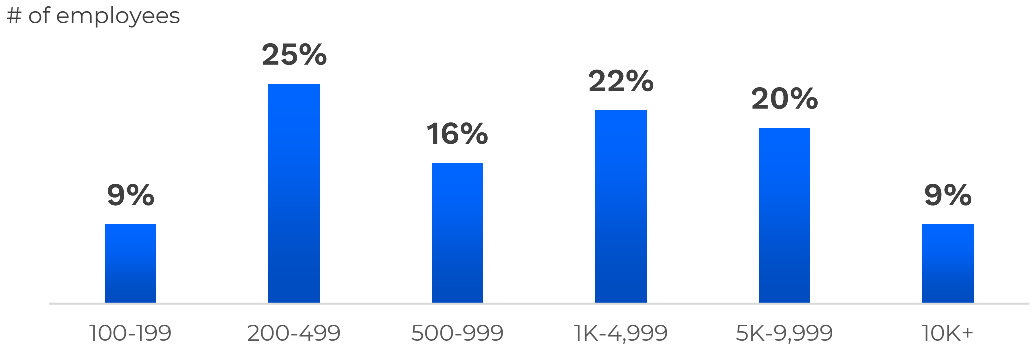


Figure 17: Company Size

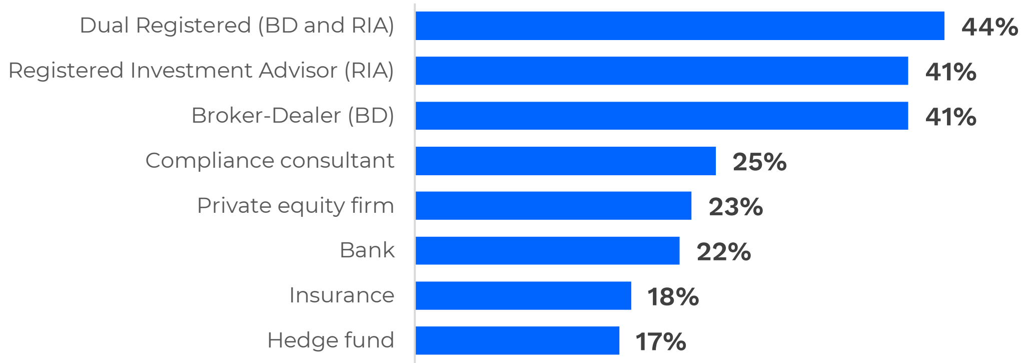


Figure 18: Firm Type

About Shield

Shield is how compliance teams in financial services and other highly regulated industries can finally read between the lines to see what their employee communications are really saying. Organizations are struggling with compliance because the insights they need to stay ahead of risk are invisible to them. Their outdated systems aren't able to keep up with all the false positives and the sheer volume of data they need to monitor.

To read between the lines and get ahead of all this, you need a way need to:

01 **See more** – with a modern, agile solution that lets you easily monitor all your channels, in a single platform.

02 **Know more** – with AI that models real human behavior to generate relevant alerts that add critical context to every decision.

03 **Solve more** – with end-to-end capabilities that eliminate data silos and let you customize workflows, policies, and procedures for greater control.

That's why large organizations prefer to partner with Shield.

Schedule a Demo with Shield >

For more information, please visit us:

Email: rbtl@shieldfc.com

About LeapXpert

LeapXpert, the responsible business communication pioneer, provides enterprises peace of mind through compliant and secure communication solutions.

The LeapXpert Communications Platform is an enterprise solution that enables employees and clients to communicate on consumer messaging applications and voice channels in a compliant, governed, and secure manner.

Founded in 2017, the award-winning company is headquartered in New York, with offices in the UK, Israel, and Asia.

Schedule a Demo with LeapXpert >

For more information, please visit us:

Email: ari.applbaum@leap.expert