smarsh®

ANNUAL RISK & COMPLIANCE SURVEY REPORT

2020: The Year of Operational Disruption & Digital Transformation

Trends, challenges and opportunities driving digital communications compliance in the financial services industry

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The 2020 Smarsh Risk & Compliance Survey Report: The Year of Operational Disruption & Digital Transformation reflects feedback from executives in compliance roles and their employees, across financial services organizations.

Survey participants provided insights on how the year's unprecedented big-picture circumstances have shaped the trends, challenges and opportunities their firms face in digital communications compliance.

While this report is noteworthy given the broader pandemic-driven disruption throughout 2020, it also marks a ten-year milestone of this annual effort:

- Since 2011, we've engaged more than 1,000 participants, from junior to executive roles, representing nearly every function within compliance teams at financial services firms
- This year's participants work at broker-dealer and registered investment advisory (RIA) firms, insurance companies, hedge funds, private equity firms and banks
- The U.S.-based financial institutions and firms represented in our survey collectively encompass more than 450,000 employees and affiliated professionals, supporting more than $1.3 trillion in assets under management
- Each one of the individuals who participated in this year's survey brought a unique perspective to communications risk and compliance, and we are grateful for the valuable insights we've been able to collect, analyze and share

What is electronic communications compliance?

For the purposes of this survey, "electronic communications compliance" refers to the supervision, protection and recordkeeping of electronic communications by an organization, as mandated in regulations such as SEC Rule 17a-3 and 17a-4, SEC Rule 204-2 and 206(4)-7, FINRA 2210, 2212-2216, 3110, 4511 and 4513, and CFTC Regulation 1.31. International regulations include Markets in Financial Instruments Directive II (MiFID II), the FCA's COBS 4, BCOBS2 and MCOB3, IIROC Rule 29.7, National Instrument 31-103 (Canada), the SFC Securities and Futures Rules and UMIR Policy 7.1.

✓ We encourage you to explore the entirety of our survey analysis in the subsequent pages. Below are some of the key takeaways:

1 **The broad and rapid shift to a predominantly "work from home" model has created a surge of concern about cybersecurity risks.** Among the organizations we surveyed, 70% shifted to a primarily remote work model because of the public health crisis. Within that group, 86% have shifted more than three-quarters of their workforces to a remote model.

2 **Collaboration, video conferencing and mobile communications channels are necessary to be productive and collaborative in a remote work environment. Firms' policies and procedures covering the use of these channels are leaving them vulnerable to risk.** In 2020, collaboration and conferencing platforms (like Zoom and Microsoft Teams) instantly went from "nice to have" to critical. These platforms take the elements of instant messaging, audio/video conferencing, file sharing and social media, and bundle them into a cohesive, easy-to-use package. Survey data illustrates significant gaps between firms that have allowed these channels for business use, and the retention and oversight required to meet compliance obligations and successfully manage the subsequent risk.

3 **The pandemic has accelerated the pace of change in the use of digital communications tools. Regulators, however, remain unforgiving in penalizing financial services organizations that fail to capture, archive, monitor and produce upon request all work-related digital communications content.** The pressure to enable a wider array than ever of digital communications tools — and to do so broadly, responsibly and quickly — fell heavily on firms' compliance and IT departments. FINRA and the SEC both provided detailed pandemic guidance for firms, and did not relent in their diligence. In fact, the SEC collected more financial penalties in 2020 than in the previous fiscal year — $4 billion — mostly after March 15.[1] The regulators' message was clear: pandemic or no pandemic, firms must make it a priority to capture, preserve, protect and supervise their electronic communications. Work from home has just accentuated the critical nature of those obligations.

4 **Regardless of when the global pandemic comes to an end, the shift to a heavily remote work organization is here to stay. So is the subsequent proliferation of digital communications.** The transformative shift in where employees work exacerbated already-persistent gaps between the use of modern communication platforms and the policies and technology needed to meet compliance requirements and govern communications appropriately and securely. The pandemic accelerated the scale and urgency of these digital communications risk and compliance issues.

2020 was the year of the home office. This shift had a disruptive and significant impact on the way people interact — most likely a lasting change. Water-cooler conversations morphed into group chats. Team-building events went from after-work drinks to Zoom happy hours. Arguments about reserving conference rooms were finally settled.

Applications such as Microsoft Teams, Slack, Zoom, Webex Teams and others saw record-breaking adoption numbers. These modern communication tools are designed for mobile utility as well, so conversations can easily travel from phone to tablet to computer and back again, without interruption.

At Microsoft's quarterly earnings call in April 2020, CEO Satya Nadella noted that the company had over 200 million Microsoft Teams meeting participants in a single day, generating more than 4.1 billion meeting minutes. In a quote widely shared since then, he said, "We've seen two years' worth of digital transformation in two months."

Whatever the next twelve months bring, it is clear that the year of operational disruption and digital transformation will leave a lasting mark on how financial services firms assess and navigate communications risk and compliance in the long run.

[1] https://www.sec.gov/news/speech/clayton-sec-speaks-2020-10-08

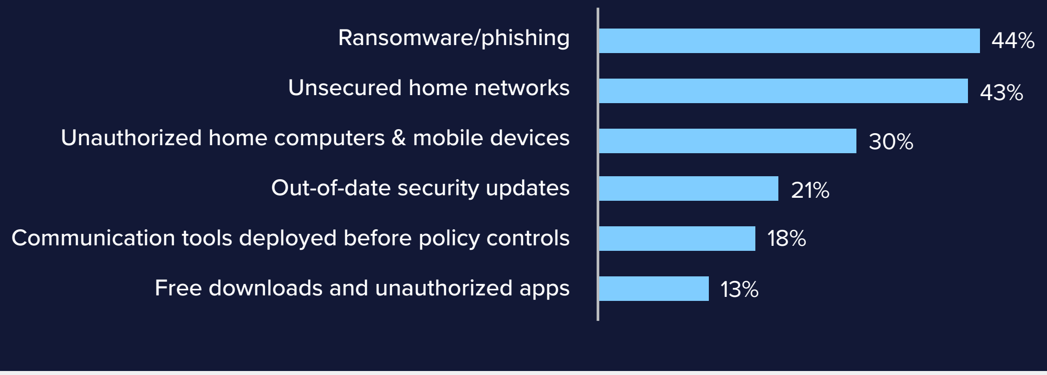
A SHIFT TO THE HOME OFFICE:

Cybersecurity is keeping compliance up at night

Trends in electronic communications and compliance have certainly evolved over the last decade, and 2020 was unlike any year that came before it. Since March 2020, when lockdowns took effect in many countries, the worldwide COVID-19 pandemic significantly changed the way businesses operate. Stay-at-home mandates and resulting dispersed workforces required all types of organizations to abruptly rethink their communications tools and oversight processes.

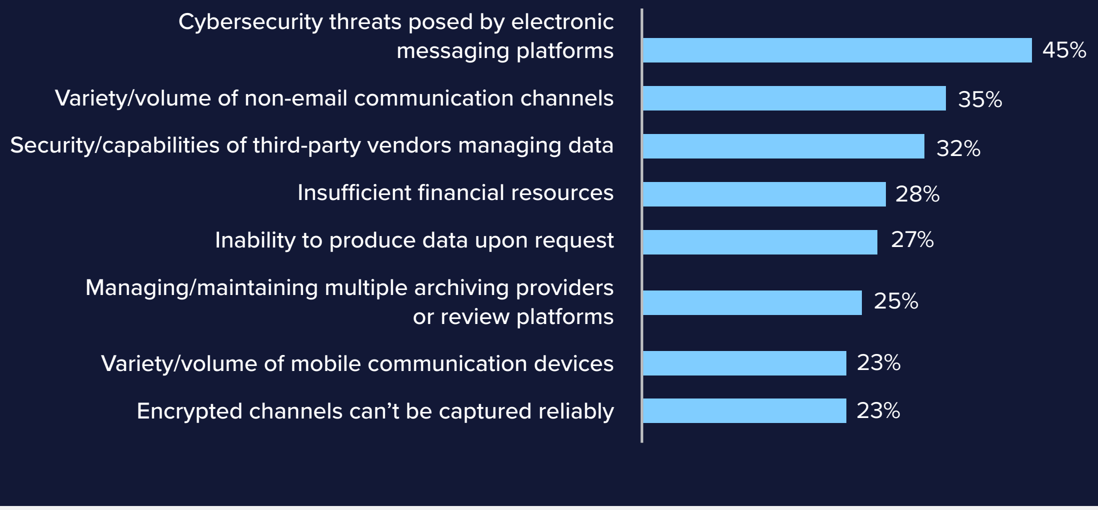
Broad shifts to remote work have introduced a range of new or enhanced risks for financial firms. Cybersecurity risks ranked highest among risks introduced by the WFH mandate for most respondents:

Top risks introduced by work-from-home mandate



Cybersecurity threats were identified as the top concern (45%) about the use of electronic messaging systems, tools and processes:

Top concerns related to electronic communications compliance systems, tools and processes



Cybersecurity risks in a remote work environment

With a distributed workforce comes an environment that is ripe for fraud, nefarious behavior and the increased likelihood of cybersecurity or compliance risks. As employees moved abruptly from their corporate offices to home offices, firms needed to move quickly to address a number of vulnerabilities. Consider:

- Employees using personal devices with no malware detection, insufficient backups or encryption
- Parents sharing devices with children who were also abruptly thrust into a remote school environment
- Connections to corporate servers and resources from unsecure (or even compromised) devices, sharing sensitive data from unsecured home wifi networks
- Files stored on unprotected drives and sensitive information on display for other people in the home

Unfortunately, many organizations are not prepared to protect their employees and their devices from cyber criminals in a remote work environment.

ASK THE EXPERT:

Sid Yenamandra, founder of the Smarsh subsidiary Entreda, the leading cybersecurity compliance provider for wealth management organizations

While some enterprises only allow the use of company-issued devices for employees, many organizations have bring-your-own-device (BYOD) policies or use a combination of both. Let's zoom in on the BYOD model. In this scenario, employees are enabled to access enterprise assets and applications using their personal devices.

In most cases, these personal devices are not managed by the enterprise, but are used to access company assets and applications. This can pose a threat to the organization's cybersecurity because there is no centralized control over the security posture of an endpoint device such as a personal laptop, tablet or phone. A BYOD user may have applications or malware on their devices that can give bad actors an access point to enterprise assets.

Most employee-owned devices are not appropriately protected. Many broker-dealers, banks, insurance companies and RIA firms have stepped up their efforts to address some of the most glaring weaknesses. But for others, cybersecurity issues are only becoming more challenging as a surge of professionals flock to video conferencing platforms to meet with clients and collaborate with colleagues.

To learn more about cybersecurity risk management, visit smarsh.com/products/entreda-unify

A SHIFT TO THE HOME OFFICE:

Electronic communications compliance gaps are putting firms at risk

Respondents are having trouble aligning their communication policies, supervisory procedures and technology with the reality of their organizations' preferences and usage. Concerns that emerged include:

- The gaps between channels that are being used and the appropriate retention and supervision measures required for each
- The pressure to balance the communication channels employees are requesting against those deemed the "riskiest"
- Lack of clarity around what channels, and modalities (feature sets) within channels, need to be retained and supervised
- Lack of confidence in ability to deliver requested communications during an examination in a manner that satisfies regulators
- Lack of confidence in ability to prove that channel or device prohibition policies — "do not use" — are being adhered to by employees

According to survey results, regulatory examinations over the last year have included requests for content generated through modern communication channels. These include IM/collaboration platforms, encrypted channels, meeting solutions, text messages, web pages, social media content and activity, Bloomberg or Reuters trading platforms, email marketing platforms, and file or document sharing. According to survey data, the top five most requested types of electronic communications in regulatory examinations were:

1. Email
2. Web pages
3. File/document sharing platforms
4. IM and collaboration platforms
5. Meeting solutions

ASK THE EXPERT:

Marianna Shafir, Smarsh Regulatory Advisor, on the current regulatory landscape

It is critical for investment advisors and broker-dealers to implement policies and procedures tailored to the COVID-19 pandemic and potential future disruptions. Regulators expect firms to adapt their oversight plans to this new normal or risk the consequences of a lax supervisory program.

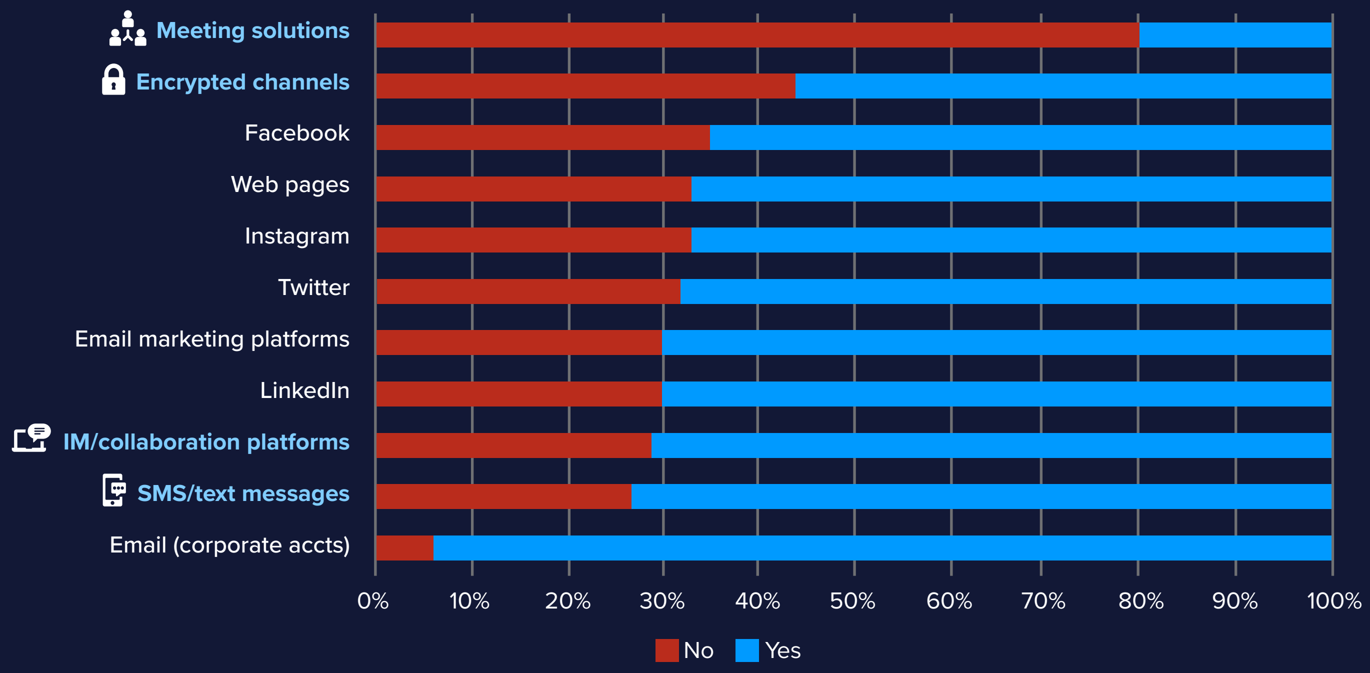
Here are a few recommendations for amending policies and procedures to reflect the business challenges brought on by the pandemic and the resulting changes in the workplace:

- Assess your firm's practices, policies and procedures to confirm they address regulatory obligations for investment advisors and broker-dealers working from home
- Provide firm personnel with additional training related to encryption and using password-protected systems
- Increase the level of oversight of supervised persons working remotely and using new and varied forms of communication to do business
- Check and double-check your systems for vulnerabilities and to ensure the communications are being captured for retention, with a particular focus on mobile devices
- Use your archiving and supervision solution to set up automated keyword and key phrase identifiers to proactively flag unauthorized communications
- Review and monitor employee emails for messages from un-archived channels. For example, automated alerts from social media to a user can flag un-monitored accounts

COMPLIANCE GAPS, BY CHANNEL

Channels with the largest compliance gaps

If allowed, is there an archiving/supervision solution in place?



What's the difference between "collaboration" and "conferencing" solutions?

While there is convergence between IM/collaboration solutions and conferencing/meeting solutions (Microsoft Teams is a key example of this), they are built to serve primarily different purposes. Smarsh used the following guidelines to define these categories within the survey.

Conferencing/meeting tools (like Zoom) are designed for hosting shared video and voice calls, virtual meetings and broadcast presentations such as webinars.

IM/collaboration tools (like Slack) are designed to help individuals or teams communicate through instant messaging, file sharing and virtual meetings, so they can accomplish a common goal or objective.

Conferencing/Meeting Solutions
(like Zoom and Webex Teams)

Key Takeaway: Do meetings that take place on conferencing/meeting solutions need to be recorded? Do they need to be archived? What about when there are chats emanating from the same platform? If company business is communicated electronically, regulated organizations need to create procedures for retaining and supervising that content — conferencing solutions included.

The widest compliance gap that emerged from the survey was around conferencing and meeting solutions such as Zoom, Webex and GoToMeeting. This is likely due to the quick and aggressive rollout and increased adoption of these tools.

Even though the vast majority of those surveyed are working remotely and allow the use of conferencing solutions (83%), only a small fraction (22%) of respondents have established archiving and supervision programs for this content.

This is an area of major concern. The foundational premise driving FINRA and SEC regulations regarding the retention and oversight of electronic communications is that the content of communications is determinative of its status as a business record. As these conferencing/meeting solutions continue to add capabilities (like chat) and firms adopt the tools for more purposes, compliance teams need to be purposeful in how they approach the oversight of the records that emerge.

Survey respondents were unclear on whether they should even record meetings that take place on conferencing solutions. In fact, **64%** say they rarely or never record meetings that take place on conferencing solutions, and almost half of those respondents (**47%**) shockingly don't see the channel as a source of risk at all.

Conferencing solutions have become essential tools for business continuity, but their potential compliance risk is evolving and perhaps not completely understood. Organizations that have increased their use of these tools or have just begun to use them (like the 51% in this survey) should step back and consider what's at stake.

Comments from respondents included:

"Did not realize there was a need until recently. We do not record face to face meetings — why would Zoom or GoToMeeting be treated differently?"

"We do not perceive much of a difference than a conference call which were never archived. Associated persons cannot use chat applications on these sites."

"This is an emerging issue for us given rapid adoption during pandemic. It has not yet been fully addressed."

More than half (**51%**) of respondents started using meeting solutions such as Zoom and WebEx — or added seats or functionality — because of work-from-home mandates.

Is inaction warranted?

ASK THE EXPERT:

Robert Cruz, Smarsh VP of Information Governance

Each collaboration or conferencing tool has its own unique set of features and modalities. For regulated firms, permitting the use of these tools can be the only available option for distributed work teams. Their use does raise a few questions, including:

- Does use by regulated users with clients or prospects create a supervisory obligation?
- Are voice, video, whiteboards and other virtual meeting features business records?
- What regulatory guidance exists and when can we expect additional clarity?

In the case of supervisory obligations such as FINRA 3110 and SEC 206(7), regulators do not differentiate one communications source from another (although it has published topic-specific notices, such as FINRA Notice 17-18 for social networking sites). Regulators do allow firms to establish their own policies for electronic communications supervision, provided they are appropriate for the firm. This includes the ability to designate an appropriate frequency of review for each message type. Regulators do not afford firms much flexibility, however, when it comes to following their own written supervisory procedures. They expect firms to be compliant with the policies they've established for business communications.

The broader question of what determines a business record also is a source of confusion, but its potential impact touches an even larger cross section of most organizations. SEC 17a-4, FINRA 4511 and similar recordkeeping rules outline the requirement to preserve communications related to its business — without specifying the form or format of the communication. The adage that most firms continue to adhere to is that "business risk and value can live everywhere," which is emphasized within FINRA's guidance on social media (FINRA Notice 11-39). The notice states that, "determining whether a communication must be retained depends on its content and not upon the type of device or technology used to transmit the communication."

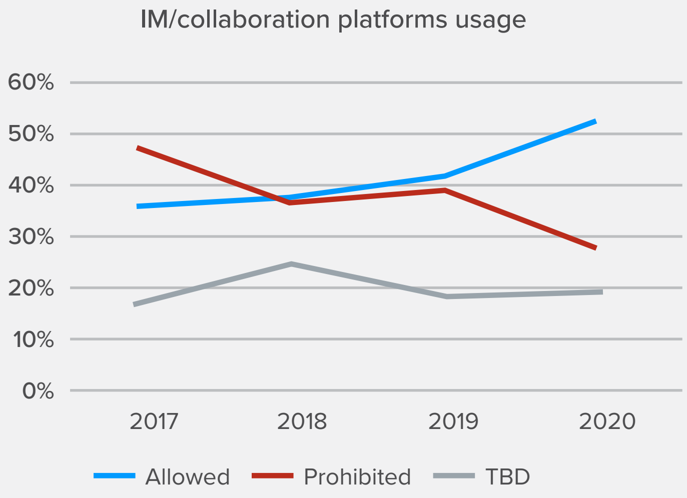
Firms tend to base supervisory and recordkeeping decisions on a risk-based calculation that weighs the benefits of supporting new tools against the potential risk mitigation strategies enabled via capture, preservation and policy controls available through each new tool. It is critical that firms have a clear understanding of which modalities are being used and for what purpose, and that they take appropriate measures to retain and supervise the business records that emerge. For its part, FINRA has provided guidance (Notice 20-16) to ensure that firms can continue to follow supervisory procedures as more employees move to a remote work environment. They've noted actions some firms have taken to ensure that unauthorized applications are not being used, as well as those applying to the Taping Rule (FINRA Rule 3170) to use voice recordings to address potential communications gaps.

The gaps between what's considered a requirement and the policies being established at regulated organizations pave the way for compliance risks. Now that remote work is an ongoing reality, virtual meetings aren't going anywhere. Regulated firms must develop policies and procedures for conferencing solutions that have been strategically considered — and then follow those guidelines.

IM/Collaboration
(like Microsoft Teams, Slack and Symphony)

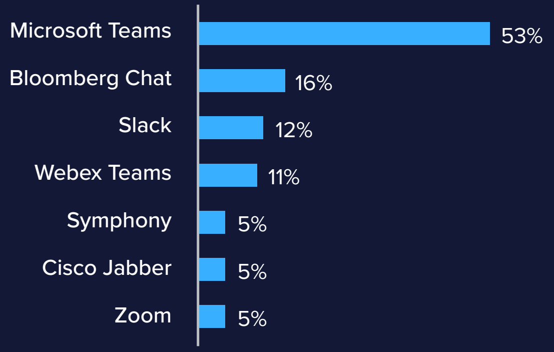
Key Takeaway: IM and collaboration platforms are incredibly useful tools for many organizations, and their use during the pandemic has been critical. However, the volume and variety of communications data they generate requires a combination of strong compliance and supervision policies, governance programs and modern technology to adequately mitigate risk.

The adoption of instant messaging and collaboration platforms has steadily increased among respondents, year-over-year.



It's worth considering that one-fifth of respondents are still determining how to even address these channels via policy, which in itself highlights a significant compliance risk.

Which of the following platforms are being used in your organization?



Respondents are using a variety of meeting and collaboration platforms. Microsoft Teams, with its Office 365 integration, is the most popular among survey respondents. Its usage increased from 44% in 2019.

These tools have become the connective tissue for many organizations that have shifted to remote work. However, IM and collaboration platforms also present unique retention and oversight challenges. With longer-term, wider adoption in mind, firms need to consider the rapidly evolving nature of these communications.

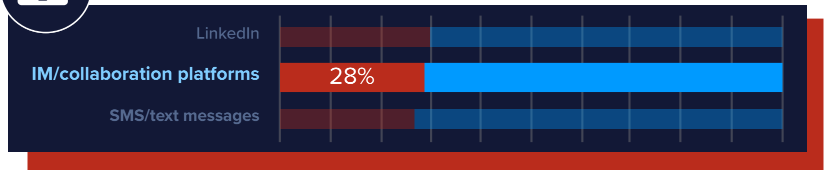
Instant messaging has been a communication tool since the 1990s, evolving along the way. Today's collaboration tools (e.g., Microsoft Teams, Slack, Symphony) are centralized platforms built around the instant message functionality. They have made it a much more dynamic experience by including persistent chats, document sharing and co-authoring features, custom emojis, video and screen sharing, and AI-enabled bots and services.

Beware of Freemium Solutions

Some organizations — especially smaller ones with limited budgets — may be tempted to use free versions of collaboration tools. It's also common for employees to start up free accounts merely for casual conversation among departments. But if work matters come up, that's a liability and a security risk for regulated organizations.

With a paid solution, messaging data can be captured through APIs and stored in an archive. On free versions, that data expires, causing trouble when an organization must quickly review and produce historical content for a legal, regulatory or internal investigation. Paid collaboration platforms also typically provide an important governance capability: prohibiting users from creating free accounts. It is crucial to plan strategically for the procurement and rollout of any IM and collaboration platform, with compliance in mind, and develop specific user guidance for employees.

RISK ALERT



Nearly one-third of respondents allow IM/collaboration platforms but do not have a system to retain and supervise the content.

These platforms also represent the second-most requested channel by employees among respondents. Despite growing adoption, **there is still nearly a 30% compliance gap with these channels.** (Nearly one-third of firms that allow IM/collaboration platforms do not have a system for the retention and oversight of the records).

Firms need to account for even more unique challenges, as these platforms are a convergence of several quickly evolving modalities of communication.

The pandemic's disruption to business has led to the widespread adoption of collaboration technologies that already existed and have now become an essential part of our everyday lives.

Microsoft Teams is the most popular IM/collaboration platform for survey respondents. In fact, it's used more than all the other IM/collaboration platforms put together. Teams use increased by almost 10% from the previous year. These are all the communication modalities that firms should consider or plan for as they build out retention and oversight strategies:

- **Data/Metadata**
  - Links
  - Comments
  - Replies
  - Edits
  - Deletes
  - Joins
  - Leaves
  - Dates
  - Time
  - Images
  - Screen shares
  - Attachments
  - Videos
  - Emojis
  - Gifs
  - Stickers
  - Hand raises
  - Questions
- **Events**
  - Group chat
  - Private chat
  - Video call
  - Voice call
  - File sharing
  - In-meeting chat

Consult with your archiving provider for prescriptive guidance on which features can and can't be captured. The right archiving solution should enable firms to leverage these capabilities.

What are the main challenges and considerations of capturing data from modern communication channels?

ASK THE EXPERT:

Steve Marsh, Smarsh Founder and Chairman

Regulated businesses have to adopt IM and collaboration tools in a compliant way. You must archive them, and you must monitor them. Historically, archiving has been single modal: it would be email or instant message. So, you're looking at a text thread. If you were looking at audio in an archive, it was probably a recorded phone call.

If you look at something like Teams or Zoom, each meeting might last 45 minutes or an hour, and people are doing this all day. In the side panel, there are often text conversations or chats that are taking place. There are files that are being transferred. There's audio throughout it all. You need to be able to see that an individual has entered a call 15 minutes late, then he dropped off the call, so some audio he will have heard and some he will not have.

And if you want to search for the point in the conversation where an employee says "iPhone," you need to be able to find that spot in the meeting, see the video, see who was sharing slides, see what was in the chat thread, who was in the room, who had been there before and to re-experience these meetings. I think that's where a lot of our product development is headed.

That's the unfortunate reality for these compliance teams. They're going to need much more sophisticated archiving and replay tools as well as the supervision and monitoring to be run on top of them.

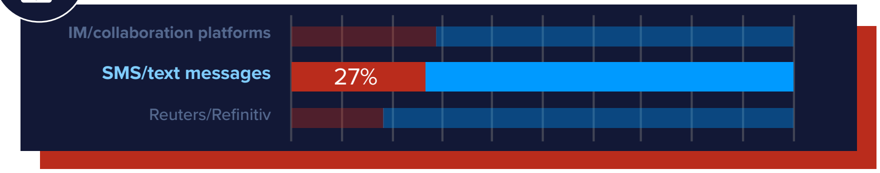
-From "Being a Leader in the Compliance Industry: An Interview with Steve Marsh"

Mobile Devices, Text Messaging and Mobile-first Apps

Key Takeaway: Every application used for business communication is being used on mobile devices. Regulated firms must consider mobile as the norm and get ahead of any compliance issues by developing explicit mobile device and communication policies for workers.

This applies specifically to two mobile-first channels — text messaging and encrypted messaging apps like WhatsApp and WeChat. Respondents indicate that both channels are in high demand, but present great risk. **Both this year and last, text messaging and encrypted channels ranked first and second, respectively, as both the most requested for business use AND the channels identified as the top sources of risk.**

RISK ALERT



More than a quarter of firms that allow employees to use text messaging for firm business do not have a retention and oversight solution in place.

Mobile devices have become essential for maintaining business continuity in our always-on world (which is even more important in our new abnormal). Of those surveyed, **40%** lack confidence in their ability to capture business communications sent and received on mobile devices. Today's work-from-home reality only exacerbates the persistent need for firms to take the right steps to implement appropriate mobile governance policies and practices.

In a 2019 survey commissioned by Avochato, 65% of respondents said they would prefer to use a financial service that communicated via text message about accounts, bills and payment reminders. Well over half (60%) said they would switch to brands that offered those services.[2]

62% of consumers report they are responding more quickly to text messages since the start of the COVID-19 pandemic.[3]

48% now prefer to receive alerts via text from businesses during an emergency, over the 45% who prefer email and 7% who prefer phone calls.[3]

[2] https://www.prnewswire.com/news-releases/study-shows-us-customers-prefer-texting-with-businesses-300974034.html
[3] https://www.zipwhip.com/blog/coronavirus-business-and-consumer-trends/

SMS/text messaging and encrypted channels merit deeper scrutiny:

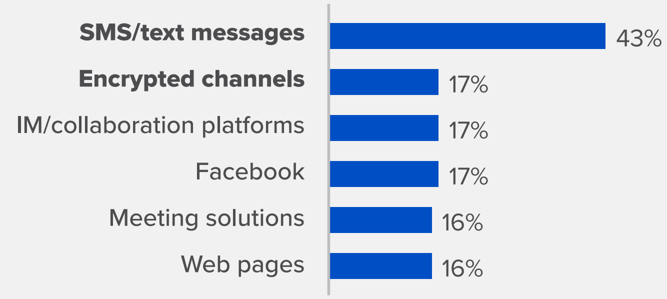
1. SMS/text messaging. Employees have been clamoring for years to be allowed to use text messages to conduct business.

More than half **(51%)** of respondents view SMS/text messaging as a top source of compliance risk, and by a large margin. However, it has consistently ranked as the most requested channel for use by employees over the years, also by a large margin.

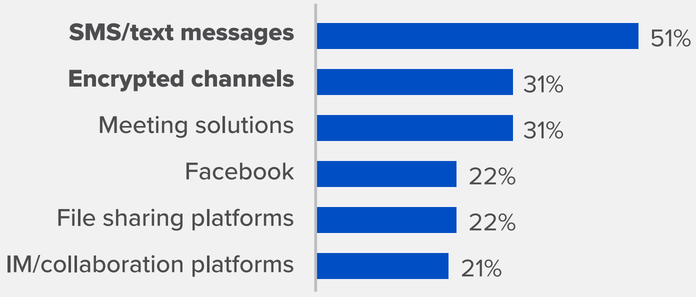
Among requested channels by employees for business use, SMS/text messaging has consistently ranked at the top by respondents.

- **2020** – Most requested
- **2019** – Most requested
- **2018** – 2nd most requested
- **2017** – Most requested
- **2016** – 2nd most requested

Communication channels requested by employees:

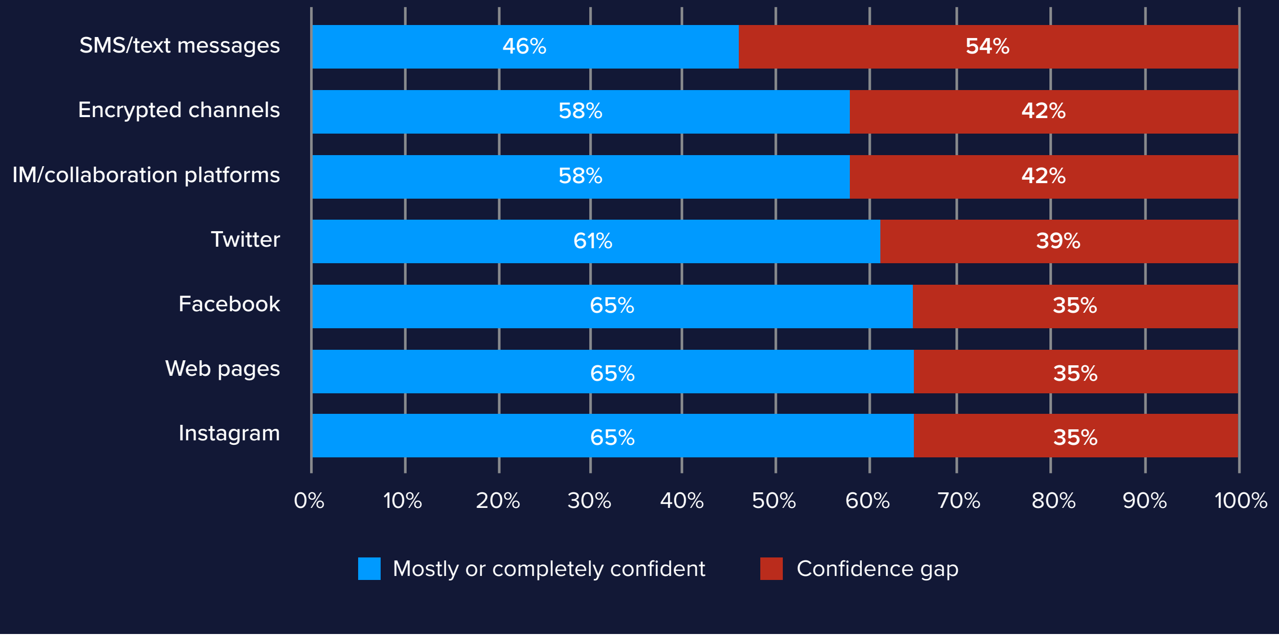


Channels perceived as top sources of compliance risk:



Firms have historically used prohibition policies to manage text message usage. Even though our mobile devices continue to become an integral part of how we do our jobs, SMS/text messaging is still overwhelmingly prohibited. Only **33%** of respondents allow it, which is only a slight increase from five years ago (2015) at **28%.** That being the case, most firms that prohibit SMS/text messaging lack confidence that these policies are being observed:

How confident are you that you could prove your prohibition of the following channels is working?



Considerations for compliant adoption of mobile text messaging

Determine your firm's device ownership scenario

- Bring your own device (BYOD): employees use their own phones, and containerization or Electronic Device Management solutions can be installed to capture only business-related communications
- Company-issued phones: employees use company-issued mobile devices specifically for conducting firm-related business
- Hybrid policy (i.e., only registered employees use company-issued devices)

Update your communications policy to account for business text messaging

- Make sure to train your employees!
- Incorporate this training into onboarding processes and require signed attestation

Determine which mobile carriers and plans your firm will use

- Your archiving technology partner should have direct-from-carrier options
- If that vendor does not, find one that does

Enable technology that can retain, supervise and produce text message data

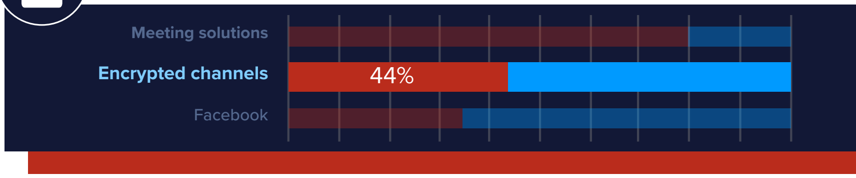
- Do away with unreliable and impractical prohibition policies
- Acknowledge the ubiquitous use of text messaging and embrace it as a preferred business tool for your employees

2. Encrypted channels like WhatsApp and WeChat

These apps are used by more people worldwide than any other tool besides email, and their rise has been meteoric. Encrypted applications were not even in the top 10 most requested by employees in 2018 or 2019 but were tied for second among the most requested channels in 2020.

Communications from these channels are intended to be ephemeral, and capture capabilities have been limited historically — although they have become materially more effective in recent years. Even so, encrypted messaging applications are the most widely prohibited among survey respondents. However, as we've seen from specific enforcement cases, and repeated experience with new communications channels, unsupervised employees and affiliated personnel may be using them anyway. This creates compliance risk for firms and may result in penalties. There is a persistent need for firms to take the right steps to implement appropriate mobile governance policies and practices.

RISK ALERT



Among the communication channels firms are allowing, encrypted channels represent the second highest compliance gap. More than four out of ten firms that allow their use do not have a retention and supervision solution in place.

In a recent FINRA case, a Florida-based broker was fined $5,000 and suspended for 30 days for using WhatsApp messenger to conduct securities-related business with customers.

According to FINRA, the broker exchanged a total of 894 WhatsApp communications between November 2017 and June 2019, many of which concerned securities-related business with three different overseas customers.

The broker primarily used a personal cell phone to communicate via WhatsApp, but occasionally used a desktop computer at the firm as well. The firm was not able to capture the communications the broker sent and received through WhatsApp.[4]

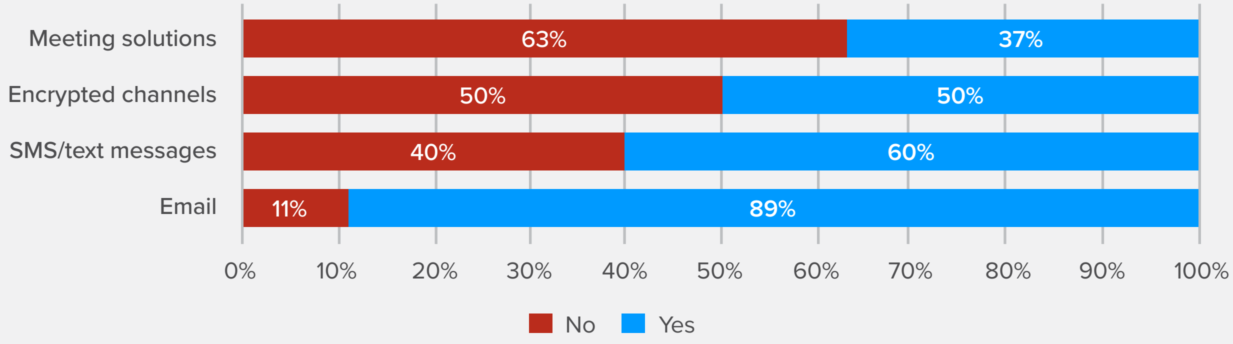
[4] https://www.smarsh.com/thought-leadership/FINRA-fines-broker-for-WhatsApp-Use/

Like collaboration platforms, mobile-first encrypted messaging apps have quickly gained popularity over the last few years. WhatsApp is the most popular messaging application in the world, with more than 2 billion daily active users, across 180 countries.

As a perceived source of risk, encrypted applications such as WhatsApp, WeChat and iMessage are the most widely prohibited at **68%**, according to survey data. However, there is a lack of confidence that workers are adhering to prohibition policies. Close to half **(42%)** of respondents have minimal confidence in their prohibition policies.

Firms also lack confidence in their ability to deliver regulator-requested content in a reasonable time frame. Compared to email, for example, this indicates a significant confidence gap and compliance liability.

Are you confident in your ability to provide communications to examiners, completely and on time?



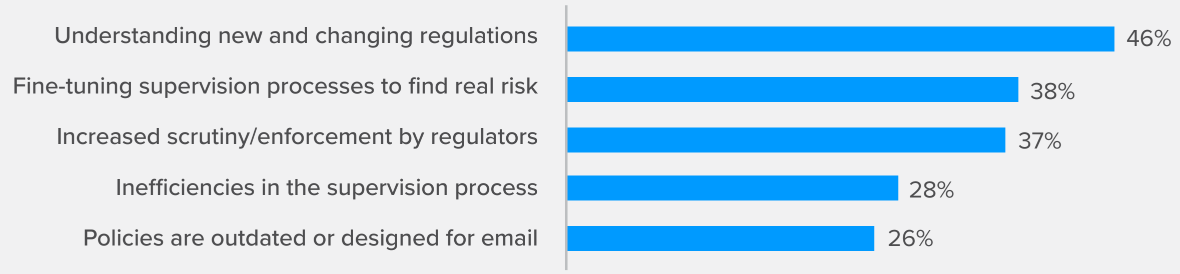
Considerations for compliant adoption of encrypted channels:

- Pull together governance stakeholders to develop a plan
- Determine which encrypted apps are being used or requested by staff
- Enable an archiving and supervision solution that is equipped to capture/preserve content from the apps your employees are using or have requested to use
- Develop communication and device policies that explicitly outline the rules for using encrypted applications
- Train employees on policies and require signed attestation

CONCLUSION

The sudden shift to remote working has not deterred regulators. In fact, factors like remote work, new devices and communication tools, and dynamic equity markets with many new novice participants are creating an environment ripe for fraud or misconduct. Consequently, regulators are on high alert, scrutinizing firms and employees, especially in the digital realms they are working today. They expect member organizations to establish and maintain reasonable compliance systems designed to monitor the activities of each associated person, no matter where their work location happens to be.

Respondents' top concerns related to electronic communications policies, regulation and enforcement



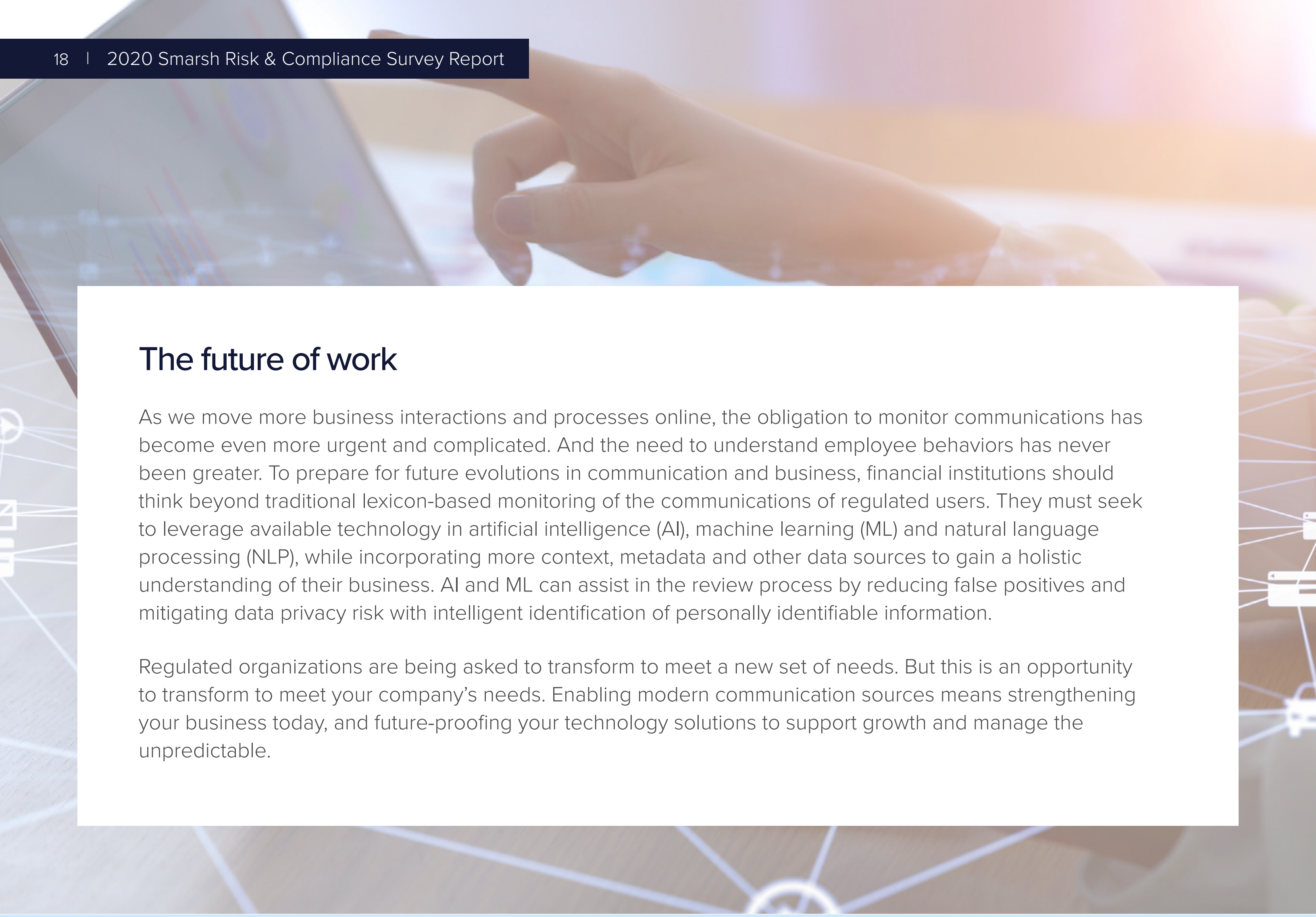
Increased scrutiny/enforcement by regulators has been a top-level concern for survey respondents every year and has been in the #3 spot for the last three years. In the #1 spot: *Understanding new and changing regulations.*

Most organizations that have shifted to a remote model will prioritize updating policies to address the changes, and many will focus on providing additional training and support for adequate capture and archiving tools from mobile devices.

Top priority investments to manage remote workforces:

- **57%** - Updating policies to address remote work
- **48%** - Additional training for remote workers
- **42%** - Support and training for conferencing or collaboration tools
- **26%** - Support for tools to capture content from mobile devices

Financial services organizations must brace themselves for any combination of regulatory developments to address new and evolving cyber threats, evolving communication preferences for digitally native workers, and technology advancements such as AI-created bots and continued development of new data sources. Fortunately, there are intelligent technology solutions that help organizations future-proof their compliance and supervisory processes and stay ready for changes in the compliance landscape.



The future of work

As we move more business interactions and processes online, the obligation to monitor communications has become even more urgent and complicated. And the need to understand employee behaviors has never been greater. To prepare for future evolutions in communication and business, financial institutions should think beyond traditional lexicon-based monitoring of the communications of regulated users. They must seek to leverage available technology in artificial intelligence (AI), machine learning (ML) and natural language processing (NLP), while incorporating more context, metadata and other data sources to gain a holistic understanding of their business. AI and ML can assist in the review process by reducing false positives and mitigating data privacy risk with intelligent identification of personally identifiable information.

Regulated organizations are being asked to transform to meet a new set of needs. But this is an opportunity to transform to meet your company's needs. Enabling modern communication sources means strengthening your business today, and future-proofing your technology solutions to support growth and manage the unpredictable.

Which technologies will play the largest role in innovating your business in the next few years?

ASK THE EXPERT:

Steve Marsh, Smarsh Founder and Chairman

Without a doubt, artificial intelligence, machine learning and natural language processing are the technologies that will drive the most innovation in our industry over the next decade, and beyond. The sheer volume and velocity of data that businesses need to process to ensure compliance is truly astounding compared to even three years ago. Businesses are struggling with their existing compliance technology to cope with this as well as the constantly evolving variety of communications data.

We recently announced our acquisition of Digital Reasoning, driven by this exact problem and where we see the industry going over the next 10 years. Harnessing the power of artificial intelligence, machine learning and natural language processing will enable us to ensure that our customers can strengthen compliance initiatives regardless of the scale of communications data they have to manage.

To us, this is the future of our industry: **Communications Intelligence**. It's a future where compliance teams can seamlessly capture human data and make sense of it at scale. This won't just mitigate risk; it will empower businesses to find insights that are critical to growth and innovation.

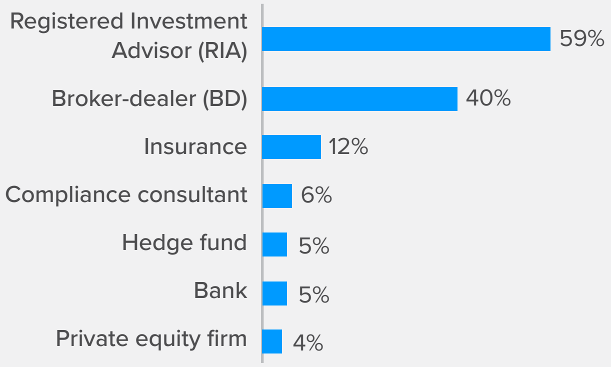
ABOUT THE SURVEY

Methodology

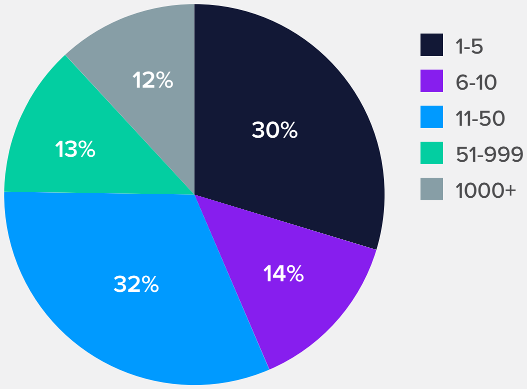
Our research methods consisted of a 33-question online survey of 111 respondents with electronic communication compliance responsibilities, conducted Sept-Oct 2020 via marketing and advertising outreach.

Organizational profile

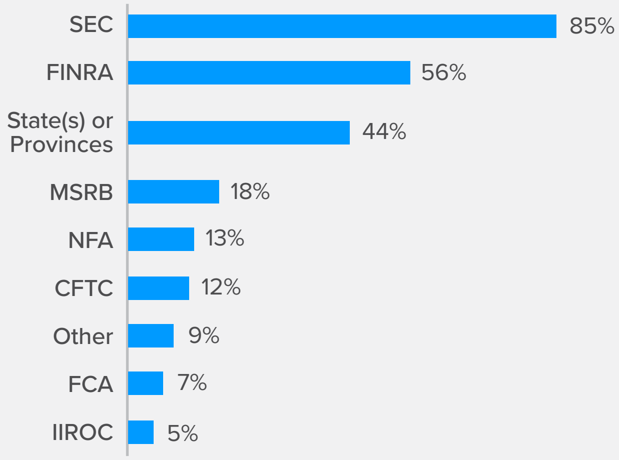
Type of firm:



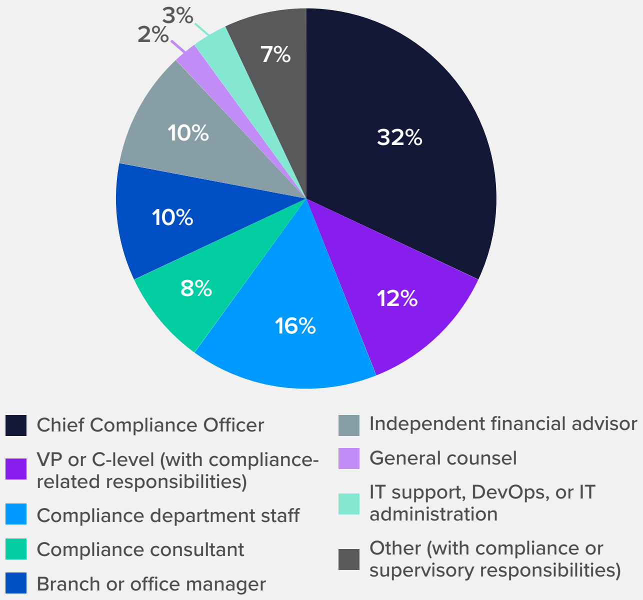
Company size by employee:



Regulating agencies represented:



Respondent profile:



ABOUT SMARSH

Smarsh is the recognized global leader in electronic communications archiving solutions for regulated organizations. The Smarsh Connected Suite provides innovative capture, archiving, e-discovery, and supervision solutions across the industry's widest breadth of communication channels.

Scalable for organizations of all sizes, the Smarsh platform provides customers with compliance built on confidence. It enables them to strategically future-proof as new communication channels are adopted, and to realize more insight and value from the data in their archive. Customers strengthen their compliance and e-discovery initiatives, and benefit from the productive use of email, social media, mobile/text messaging, instant messaging and collaboration, web, and voice channels.

Smarsh serves a global client base that spans the top banks in North America and Europe, along with leading brokerage firms, insurers, and registered investment advisors. Smarsh also enables federal and state government agencies to meet their public records and e-discovery requirements. For more information, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.