

An Unprecedented Era of Enforcement

How are financial services firms responding to changes in digital communications compliance?



It's tough for financial services firms to find their compliance footing in a turbulent risk landscape. It was especially tumultuous in 2023* with record-breaking fines, in-office vs. remote culture clashes, readily available generative AI technologies, growing cybersecurity and data privacy concerns, and an unprecedented volume of new, updated and expected regulatory updates.

There's simply too many questions for firms, like:

- “Should we allow the use of WhatsApp?”
- “Is our compliance strategy still good enough?”
- “What are we supposed to do when regulatory requirements evolve?”
- “How can we make our compliance controls nimble and responsive enough for further regulatory changes?”

One of the best ways to know where to go next is to know where others are.

We recently surveyed regulated firms to get a ‘lay of the land’ of the financial services sector when it comes to the retention and oversight of digital communications. The insights we’re sharing will help you and your firm build an agile and resilient communications compliance strategy for 2024 and beyond.



A quick peek inside:

- In-office vs. hybrid vs. remote collaboration
- Texting and mobile apps continue to be a struggle
- History repeats itself with new technologies
- Firms are taking risks with risk
- Actionable takeaways and next steps

* <https://www.smarsh.com/blog/thought-leadership/SEC-ramps-up-enforcement-actions-against-off-channel-communications>

The intersection of new business cultures, new technologies and new regulations

Last year saw a lot of changes in our industry.

Some firms are returning to the office full time, others remain remote-first, and many are moving forward with a hybrid approach. New technologies like generative artificial intelligence (e.g., ChatGPT) leaped onto the scene, which while promising, also create new risks and challenges for compliance teams. At the same time, firms continue to struggle to keep up with the pace of innovation and release of new features in the collaboration platforms they use every day.

As if that wasn't enough, regulators are coming down — hard — on off-channel communications and continue to emphasize their focus on addressing these violations with record-breaking fines.



Methodology

Our research methods consisted of a 15-question online survey completed by 229 respondents with communication compliance responsibilities, conducted in the fall of 2023.

What type of firm do you work for?

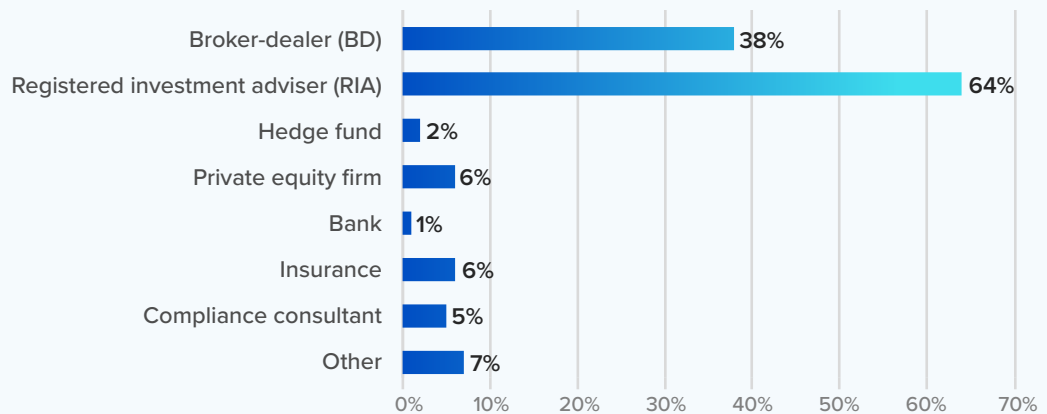


Figure 1.1

What is your primary role?

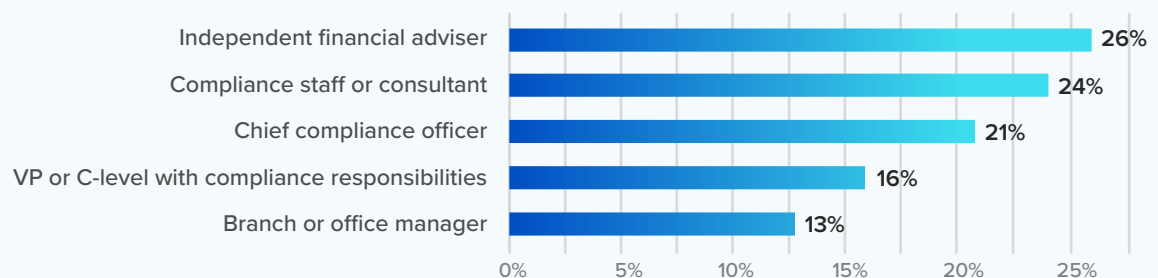


Figure 1.2

In-office vs. hybrid vs. remote-first collaboration policies

Which work policy best describes your firm?

Full-time in office Hybrid Remote-first

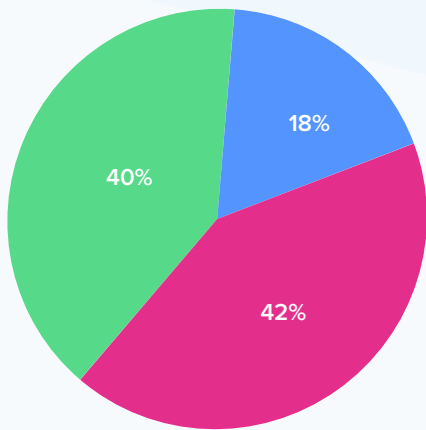


Figure 1.3

Data spotlight:

- Remote firms are more likely to enable communications channels to support business.
- Remote firms are more likely to allow the use of social media for business purposes. Is this a competitive advantage?
- Collaboration apps are most popular with hybrid firms (82%). Office-only and remote-first are at a near tie (68% and 66% respectively). So, how are remote-first firms collaborating?
- More than one in four firms don't have emerging social media apps defined in their policy. How exposed are these firms?

* Note

- Collaboration platforms examples: Slack, Microsoft Teams, Symphony
- Social media examples: Facebook, X (formerly Twitter), Instagram
- Encrypted messaging app examples: WhatsApp, WeChat, iMessage, Telegram
- Emerging social media app examples: TikTok, Lemon8, YouTube Shorts

Which digital communication channels are used by your firm's employees for business purposes?*

Full-time in office Hybrid Remote-first

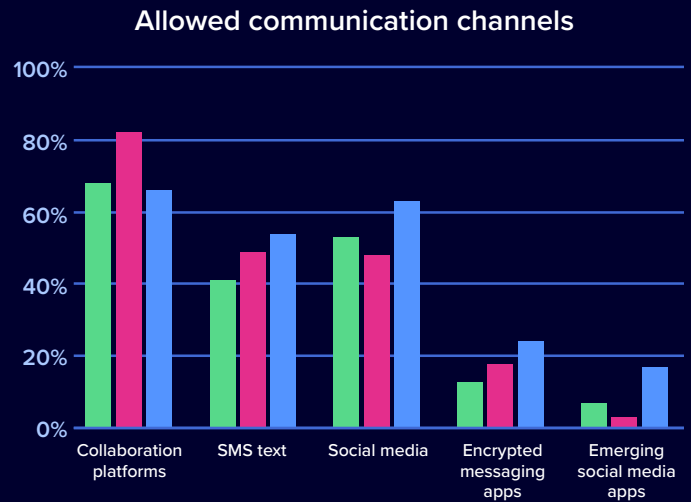


Figure 1.4

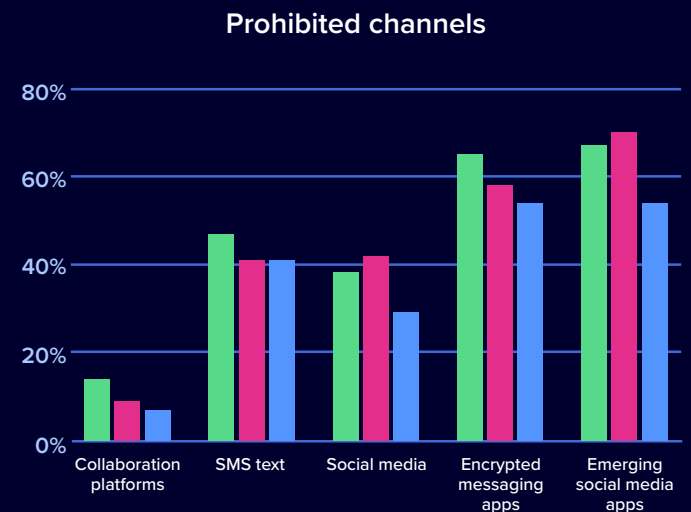


Figure 1.5

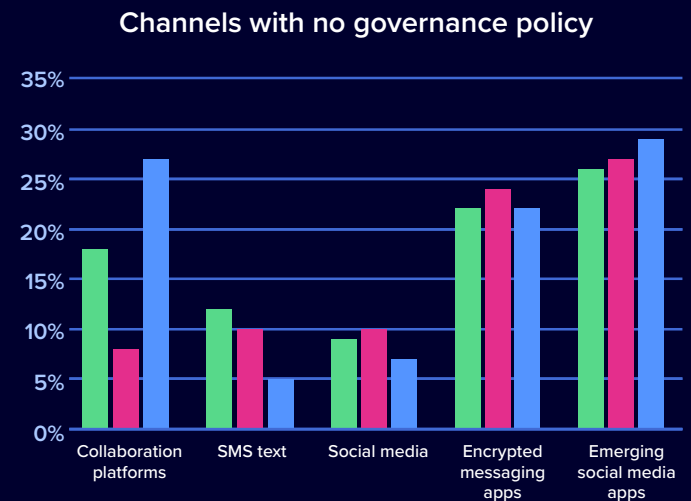


Figure 1.6

Our takeaway:

Go back to the office. Or don't. Just don't get left behind.

Running a business that's nimble, responsive and competitive means adapting to meet new changes, which may require firms to adopt new communication tools. But prior to permitting new communications channels, firms must adopt new compliance policies to ensure they can capture, store and supervise content according to regulatory requirements.

The global pandemic compromised that best practice. With governments enacting social distancing mandates overnight, firms simply didn't have the luxury of conducting due diligence before deploying new communication tools. They just needed to ensure that employees could get their jobs done.

"In 2020, one of the things that we observed was that a lot of compliance departments really tried to catch up with what was happening in their organization," says Steve Marsh, Smarsh Founder and Chairman. "Typically, they might set the rules first and then IT would roll out a new tool. During the pandemic, this happened in the reverse order."

Now, firms are in a vulnerable position where they need to ensure that controls can work uniformly, no matter if employees return to the office, work from home or split their time between the two locations.

Hybrid and remote policy drivers

Demographic changes:

By 2030, 74% of the workforce will be millennial and Gen Z workers.¹ Where predecessors may have seen software as a "nice to have," digital natives expect modern and streamlined means of communication.

Customer satisfaction:

The rise of retail investing, financial influencers ("finfluencers") and decentralized finance is changing the investor profile in financial services. The days of in-person meetings with the neighborhood financial adviser are fewer and farther between. Firms must be able to easily engage with contacts whether that's face-to-face, face-to-screen or even screen-to-screen.

Competitive advantage:

Firms that want to attract and retain Millennial and Gen Z employees - and their networks of next gen investors - will need to consider remote or hybrid work policies to remain competitive.

¹ *The Next-Gen Workforce: Five Key Tech Areas Separate Younger Workers from Older Generations*

Communication technologies supported by firms

Which digital communication channels are used by your firm's employees for business purposes?

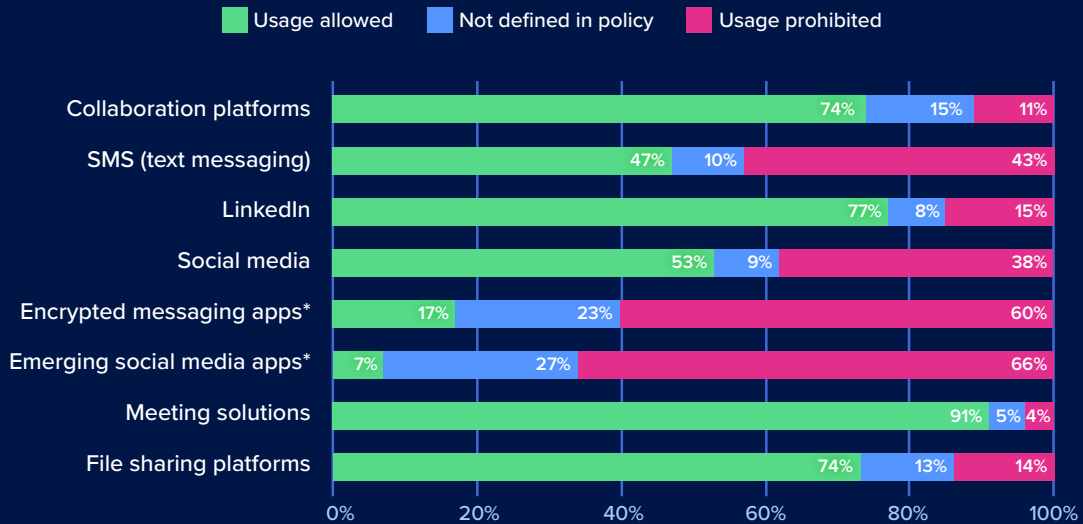


Figure 2.1 *See Note on Page 4 for examples.

Data spotlight:

- Text messaging is a near-even split of permitted (47%) and prohibited (43%).
- Only one in six firms permit encrypted apps like WhatsApp and WeChat.
- Firms are most cautious with emerging social apps. Only 7% permit the use of apps like TikTok, YouTube Shorts and Lemon8 while 66% prohibit them.

Our takeaway:

Once again, it's **another** year of (unnecessary) texting woes.

SMS text messaging continues to be a struggle. In the survey, 43% of our respondents reported their firm does not allow texting for business communications while 10% are undecided, and 65% of respondents perceive it as a top source of risk.

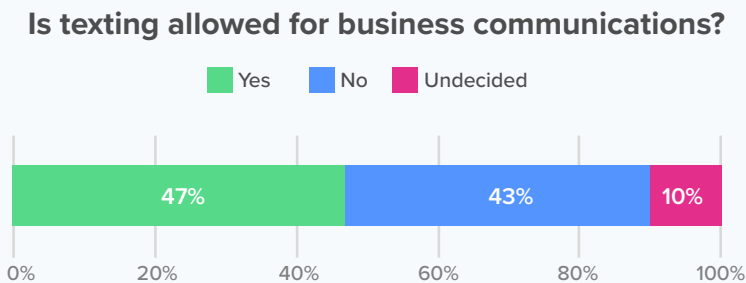


Figure 2.2

Which types of content do you perceive as the top sources of the most compliance risk?

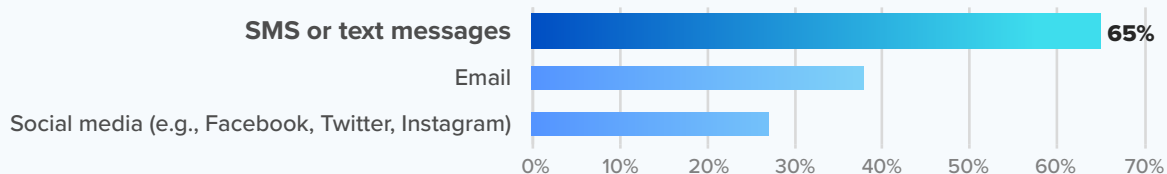


Figure 2.3

SMS text messaging as a top source of risk is up from 51% in 2019 and has consistently ranked as a leading pain point for firms for the past decade. This doesn't come as a surprise, as current enforcement actions for off-channel communications such as text messaging continue to make headlines.

"In 2016, we were highlighting this disconnect between reality and what policies were telling us," says Marsh. "Everyone was using text messaging, no one was archiving it, and at that point, the regulators weren't really enforcing the rules like they are today. So here they are many years later issuing some gigantic fines."

"Text messaging will continue to be an area of focus," continues Marsh. "If you look at the data we saw in the survey, a little bit less than half of the respondents said that they permit text messaging for business use. And that almost seems a little bit out of touch with reality when you think about just the fact that almost everyone is using text messaging for everything in their lives. It's not just their personal lives. Business communications are happening over text messaging [whether firms allow it or not]."

Biggest compliance concerns and perceived risks

Top 2023 concerns vs. same concerns in 2020

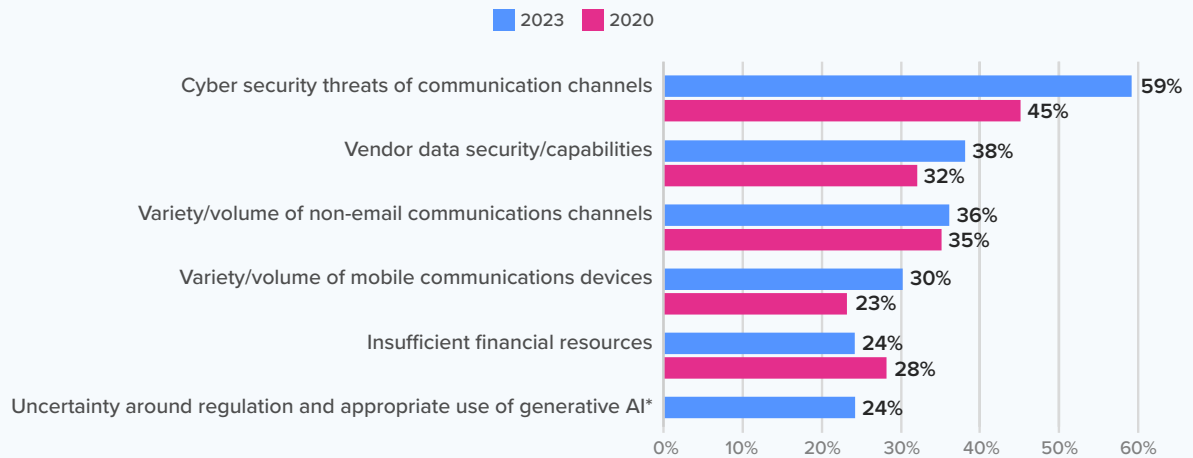


Figure 3.1 *Not a concern in 2020

Which types of content do you perceive as the top sources of the most compliance risk?

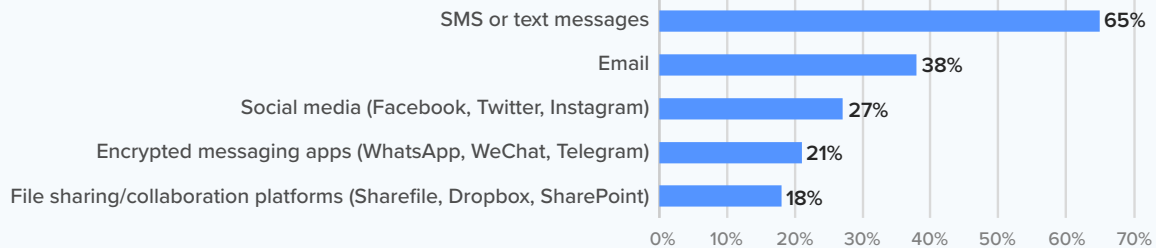


Figure 3.2

Data spotlight:

- Cybersecurity risks from new channels remain a top concern, increasing from 45% in 2020 to 59% in 2023.
- Third-party risk management concerns also saw an uptick, from 32% in 2020 to 38% in 2023.
- Mobile device concerns increased from 23% in 2020 to 30% in 2023.
- Insufficient financial resources and uncertainty around AI are tied at 24%. However, a subsequent benefit of AI solutions is addressing resource and staffing challenges.



Our takeaway: Firms are taking risks with risk

The survey shows firms are deeply aware of risk and the heavy burden of demonstrating compliance, especially when emerging communication channels are accelerating their collaboration and client engagements.

However, respondents are making tough choices based on the perceived risk to them and their firm. Cybersecurity is an obvious concern. Data leaks and ransomware attacks are major threats that must be prevented, especially when proposed rules from the SEC focus on cyber compliance. However, more firms are recognizing that communications entail a variety of risks and are moving toward a holistic view across regulatory compliance, information security, data privacy and IP protection.

Despite 65% of our respondents saying that keeping up with compliance is a top policy concern (see Figure 4.1), 29% said they are not reviewing policies following recent off-channel fines. 90% of our respondents spend less than a quarter of their time creating or adjusting policies and systems to ensure compliance with new and evolving communications regulations.

We also received many responses that indicate that smaller firms may have a perception that they're too small to receive regulatory scrutiny. This is simply not true. While big firms make the headlines, regulatory actions last year show that regulators are **not** ignoring small firms. FINRA recently expelled a firm for "abdicating its responsibility to supervise its representatives."³ Regulators are fining and barring individual advisers, compliance officers and principals for recordkeeping non-compliance.⁴

We also received responses like, "We are too small to worry about issues there," or "Only three people work here," when asked about their compliance concerns.

³ FINRA Disciplinary Action: September 2023

⁴ FINRA Disciplinary Action: October 2023

New apps, new gaps

Our survey shows 17% of firms permit encrypted apps for business communications. This can provide a competitive advantage as it allows firms to work with clients who prefer using popular apps such as WhatsApp, WeChat and Telegram.

Are encrypted messaging apps allowed for business communications?

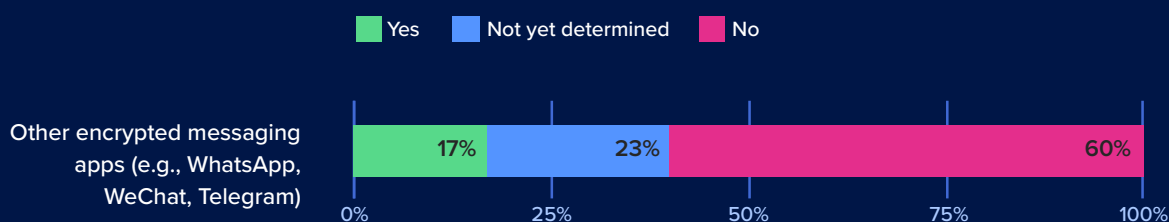


Figure 3.4

It is a common misconception that encrypted apps like WhatsApp and WeChat cannot be used compliantly. In reality, these messages can be captured and archived to enable compliant employee use with the right capture and archiving solution.

On the SEC's recent actions on off-channel communications, Elin Cherry, a compliance expert and former CEO of Elinphant says:

"The message that [the SEC] is conveying is that recordkeeping has to just be a part of [the firm's] core way of doing business. Firms need to be keeping all records — and records are defined very broadly. The SEC is making it clear in its recent actions that recordkeeping is on the top of their list for rules right now. It's important that firms are storing their records correctly, keeping them and reviewing them. It's the most important thing to the SEC right now."

Response to new regulations

Understanding new regulations is a top concern

2020 vs. 2023

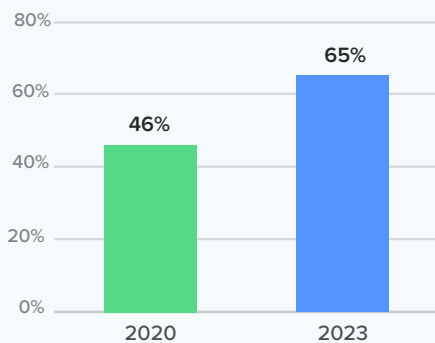


Figure 4.1

Has the recent increase in off-channel communication fines caused your firm to re-evaluate existing digital communications policies for employees?

Yes No

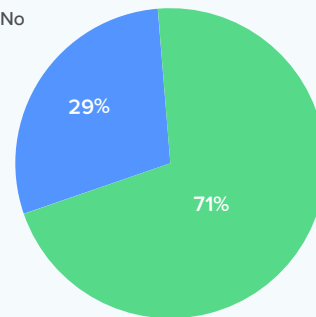


Figure 4.2

Some open responses from those not re-evaluating policies:

- “We comply and aren’t concerned with non-compliance.”
- “We believe our policies are adequate.”
- “Our team does not actively use other communication channels, so the risk is minimal compared to the cost.”
- “We’re already compliant. There’s nothing to modify.”
- “We are too small to worry about [these] issues.”
- “I believe I do as much as humanly possible to stay compliant.”

Our takeaway: History looks to be repeating itself — but why should it?

Similar to email in the early 2000s and SMS text in the 2010s, financial services firms must understand and be prepared to meet the challenges of an evolving technological and regulatory landscape. There will always be new tools (such as AI), the way we communicate will always evolve, and regulatory oversight will always adapt to meet these changes.

Compliance gaps — the difference between content being captured and archived and the communications channels that are actually used by employees — have always existed. These will continue to evolve as new tools appear in the workforce.

While smaller firms are faced with more significant resource constraints, the ability of firms to minimize the gap between policy and reality is central to their ability to identify misconduct and allow regulators to do their work. Defining the specific actions that are considered “reasonable” and “risk-based” continues to be a challenge.

Firms of all sizes should continue to view this challenge as dynamic and in need of continued policy, procedure, training and technology investments to demonstrate a proactive posture to regulators.

This isn’t the first time Marsh has witnessed the formation of compliance gaps following new technology:

“As new communication tools were introduced and adopted by firms, we found years ago that a lot of firms just continued to focus their surveillance efforts on email. We had to educate them a bit to try to incorporate some of the newer, potentially riskier communication tools into their supervision.

“We now have video conferencing tools and all of the multimodal communication that can take place within them. There’s chat. There’s audio. There’s video. There’s slide sharing and note-taking. There are a lot of different ways to communicate in these tools that we’re using day in and day out. **91%** of our respondents said that they permit [meeting solutions like Zoom] for business purposes, but there’s a lot of communication within those tools that needs to be looked at more closely.”



Intersection of evolving technology and regulatory compliance

The SEC’s marketing rule is already cracking down on registered investment advisers with “influencer” clout on social media. Regulatory actions have been levied for the use of unsupervised messages in encrypted apps. Now the industry is starting the discussion of generative AI like ChatGPT.

Firms that create or evolve their strategies to help them adapt will reduce risk and be more competitive. It’s not just about updating policies. It’s about understanding and addressing how new technologies are used and how to meet regulatory requirements. Firms that drag their heels in adopting or creating appropriate policies for new technologies are doomed to repeating history.

This doesn’t just apply to new communication tools or platforms entering the market or permitting a new channel. It also applies to new features and capabilities released on communication tools that the firm is already using.



What you can do with what we learned

Perform a gap analysis

Firms need to ensure that their policies include what communication channels, tools and platforms are permitted — and that the content is being archived. It's possible that a tool or feature that's popular with regulated employees isn't permitted in the policy. In which case, additional employee training may be required, or the compliance strategy needs to evolve to compliantly take advantage of the tool's benefits.

Understand new regulations and technology as it relates to your business

Firms will always be pressured to adopt new communication tools or features that improve collaboration or client engagement. But there needs to be a balance between being competitive and being compliant.

Before taking the leap, firms need to ask themselves, "Are we able to actually archive this? Are we able to actually monitor these things?"

Update policies for new technologies and regulations

"We're seeing that the lexicon of keywords is being updated to include other forms of communication channels, like Discord and Reddit," says Steve Boyd, Head of Miami at Optima Partners. "These types of keywords are getting put into electronic communications searches to see if people are noting these channels in their traditional communications. If employees are using these other communications, compliance needs to be aware of them. Ultimately, if it is material business that's being communicated, it will have to be archived."

Ensure training happens at all levels

Employee training is a critical component. Training employees on what communication channels they are allowed to use and how to do so in a compliant way helps mitigate risks for the company. Additionally, because technologies are continually evolving and new features are added constantly, it's important to refresh the training every year to keep pace with those changes.

Underpinning it all is a firm's culture of compliance that starts from leadership and is supported by tangible actions, which includes self-reporting and remediation.

"I think there's a lot of employee education and communication that must happen at these firms," says Boyd. "[Recent regulatory actions] said senior management was partaking in these off-channel communications. If it's embedded in your firm's culture, nobody's going to really care about it at the end of the day. The SEC will always come out with something else."

Final thought

As communication technology advances and regulations evolve, firms must keep up with and have a deep understanding of both. Not doing so means firms may develop a false sense of security in their policies, which results in communications that simply can't be captured. So, where they might think they're collaborating for success, may actually mean they're collaborating their way to hefty compliance violations, fines and other penalties.

Today, communications channels are prolific and rich in powerful features, and firms must account for their use with policies and enforcements and the right compliance solution in place.

We may not know for certain what the future holds, but one thing we do know: regulators are zeroing in on how and what firms use to communicate. Modernizing your compliance posture is critical to avoiding increasingly heavy fines and penalties.

How Smarsh can help

As the global leader in digital communications capture, archiving and oversight, we help firms simplify communications compliance. But as we all know, a prohibition policy won't save firms from fines if their regulated users are communicating with clients over prohibited channels.

That's why our solutions are designed to capture the most common (and several uncommon) communication channels. By expanding the number of channels that can be captured, Smarsh empowers your firm to allow more channels to minimize the risk of off-channel communications.



Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated agencies 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 advisors and U.S. federal, state and local government agencies. To discover more about the future of communications capture, archiving and oversight, 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.

