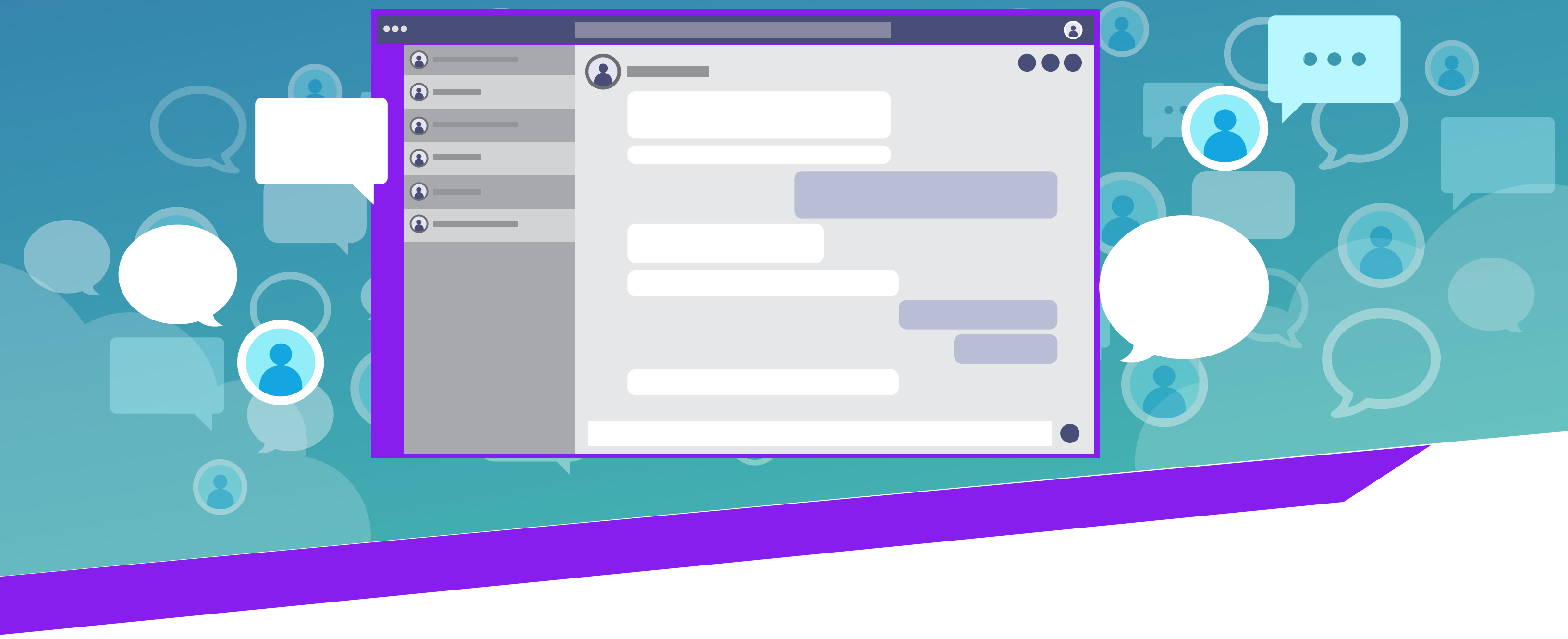
smarsh®

# How to Supervise IM & Collaboration Platforms for Compliance



The volume of electronic communications data being generated around the clock is enormous. Almost 200 million emails and 20 million texts are sent every minute, and those numbers continue to escalate.

Collaboration and instant messaging platforms like Slack and Microsoft Teams are no exception, and they are the latest tools to transform how people interact at work. Within the last five years, Slack's number of active daily users reached 12 million, and Microsoft reports that 13 million people every day are now using Teams.

Like email and text messages, collaboration platforms are producing a growing volume of data. But IM and collaboration tools pose additional, multi-faceted challenges when it comes to managing regulatory compliance. The types of rapidly generated interactive data, such as emojis, stream of chats and event information, and files have become far too complicated for traditional archiving solutions designed for a single content type, like email.

## To chat, or not to chat, that is the question

If you are reading this, then you likely know that FINRA Rule 3110 and SEC Rules 206(4)-7 require financial firms to establish and maintain a system of electronic communications storage and supervision that is supported by substantial policies and procedures. The rapid adoption of the "latest and greatest," and trending IM and collaboration apps make supervision more complicated than ever. This is what keeps compliance teams awake at night.

Some companies in regulated industries try to manage the barrage of today's communications data by prohibiting the use of IM and collaboration platforms for company business altogether. Or they significantly reconsider their mobile policies. But it's not practical or conducive to business to limit preferred modes of communication, especially when it comes to interacting with customers and attracting younger generations in the workforce.

Plus, there is inherent value in collecting data, even outside of compliance obligations. Information about how employees and customers interact can provide actionable insights for competitive organizations.

## Taking the complexity out of compliance

Managing compliance in this complicated new paradigm requires well-defined procedures, nuanced data capture, and modern tools with sophisticated search and review capabilities. All regulated firms must have strong solutions in place, or they risk having gaps in books and records reporting when regulators or legal teams come calling.

Two things can be true – employees and customers interacting across channels and platforms is essential in today's connected world, and compliance professionals have reason to be concerned about how to manage all the interactive data that's being created. To bridge that gap, having the right technology and processes in place to support capturing, archiving and supervising modern messaging will ensure a more productive, enjoyable and – compliant – workplace.

### This guide will cover:

- Benefits and drawbacks of using instant message and collaboration platforms in a regulated industry
- How to determine what your firm needs to do to build a stronger supervision program (level-setting)
- A primer on supervision policies that cut through the data noise and help you manage regulatory obligations
- Best practices for implementing, fine-tuning, and future-proofing supervision policies so the process is more efficient and effective

If you're responsible for reviewing electronic communications and/or maintaining compliance at a regulated company – **this guide is for you.**

## Collaboration platforms are a modern staple for the workforce

Firms that have adopted instant message and collaboration platforms can't do business without them now. They are critical components for rapid communication and distribution of content up and down the chain of command and across the organization.

For some companies, highly collaborative departments may find email to be limiting because the response times are slow, and inboxes are tiresome and tedious. Collaboration tools encourage instantaneous responses on mobile and desktop, making it easier to get more work done – in and outside the office. Think about it, do you respond to an email as quickly as you would a text or an IM?

Another major catalyst for the adoption of IM and collaboration tools is changing demographics. Millennials currently make up the largest segment of the workplace, and as digital natives, they are generally more tethered to mobile devices; they prefer a variety of highly responsive messaging applications, over email. Baby boomers and Gen Xers communicate more through email and in-person, which means a broad variety of ways to engage in a modern workplace.

All these modes of engagement create a trail of interactive data that is subject to regulation or litigation.

### SLACK

**32%** less email

**21%** faster response time to sales lead

**23%** fewer meetings

**86%** say it's easier to share key learnings

(Source: The Business Value of Slack, IDC Research, 2017)
Slack: 12M daily active users

### MS TEAMS

**17%** reduction in emails received per day

**18%** improvement in time-to-decision

**19%** reduction in meetings per week

**832%** ROI over 3 years

(Source: The Total Economic Impact of Teams, Forrester, 2019
Teams: 13M daily active users

## Getting real about potential risks

Allowing new tools for chat and collaboration in the workplace may invite new and various risks of misconduct. These considerations must be taken seriously and addressed regularly.

Each tool is unique, with a combination of features like chat, file sharing and collaboration, voice, video and embedded AI. They're also interactive, where files can be changed or deleted – persisting in varying states at different points in time. Conversations on IM and collaboration platforms jump quickly between desktop and mobile too, and people may enter or leave group conversations at crucial moments.

Event information, such as join/leave and edit/delete activities are typically not captured in solutions designed for monitoring email. Even if that info is captured, wrangling flattened communications data from disparate locations and trying to piece that together takes way too much valuable time away from the need to focus on monitoring problematic content in the first place.

People also communicate with a more casual tone in instant messages than they do in email. They might say things they wouldn't normally say in an email and run the risk of divulging sensitive information. Leaders may (sometimes rightly so) be skeptical that chatting is productive, and instead consider it a distraction, or that those messages are not important.

## Gaining visibility in a changing interactive landscape

Now that you've had a chance to consider the benefits and risks of new messaging tools, with regard to compliance, the next phase in optimizing your supervision program is to assess your current processes and the technology you have in place to manage the data. Here are some questions to discuss with your IT teams and compliance stakeholders:

1. Do you have an ongoing plan for capturing, archiving and supervising the data that's being created with every new messaging app used for company business?
2. Is it taking extra time to wrangle content from a bunch of places instead of from a centralized location?
3. Do you have a Bring Your Own Device plan? How are you supervising mobile messaging, particularly through IM and collaboration apps?
4. If you don't have a BYOD plan, are you depending on a phone carrier to capture chat messages for you?
5. Do you have a policy that prohibits ephemeral messaging apps like WhatsApp and WeChat?
6. Do you feel confident that you could fully-provide essential contextual data for e-discovery purposes?
7. Is there a messaging component on your company's website or mobile application? Do you capture and store those communications?

Determining the current state of your supervision procedures with relevant stakeholders will help to identify areas of risk. This is a good time to assess the technology you're using to support the process, and whether it can address your current and future needs. Massive amounts of IM and collaboration data becomes a multi-dimensional interactive trail to capture and review, which makes a compliance manager or content reviewer's job far more challenging.  It's hard to evaluate context when conversations move from private chat to a group channel, or files in various formats are attached, or people communicate only through emoji 😉.

The good news is it's possible to get a comprehensive view across multiple content types, for all employees, in native format, with metadata included. Couple that with the ability to pinpoint troublesome content and build requisite workflows within a unified platform, and you have a recipe for a highly effective supervision program.

## Policies: a primer

As we've covered in our monthly regulatory updates on the blog, electronic communications in regulated businesses are indeed under threat of scrutiny by the law, and SEC and FINRA fines are steadily increasing year over year.  The facts are well known: all electronic communications are required to be captured, stored and monitored as such. Smarsh takes care of this process from end to end.

Before we dive in, a technical clarification: at Smarsh, Supervision and Policies refer to functionality within the Professional Archive.

**Supervision:** A powerful application inside the Smarsh Pro Archive platform. The platform's policy engine is designed to speed the communications review process by automatically classifying messages as they enter a company's communications archive and highlighting keyword hits on each message, as defined by your keyword lexicon.

**Policy:** A rule that identifies and flags a specific lexicon in a message, based on a set of criteria. Policies come pre-configured and out of the box with the Pro Archive and can be customized to fit your compliance needs.

These tools are aptly named, because they are designed to support their respective functions. We'll use the terms somewhat interchangeably, but this is something to keep in mind.

Pro Archive Supervision uses Policies to expertly monitor all the communications data that businesses produce and store in an archive. This includes just about every content type you can imagine – common IM and collaboration tools like Microsoft Teams and Slack, and also text messages, social media, email, and voice apps.

Policies are rules for classifying messages as they enter a communications archive, and which flag important or problematic keywords, phrases or other criteria on qualifying messages.

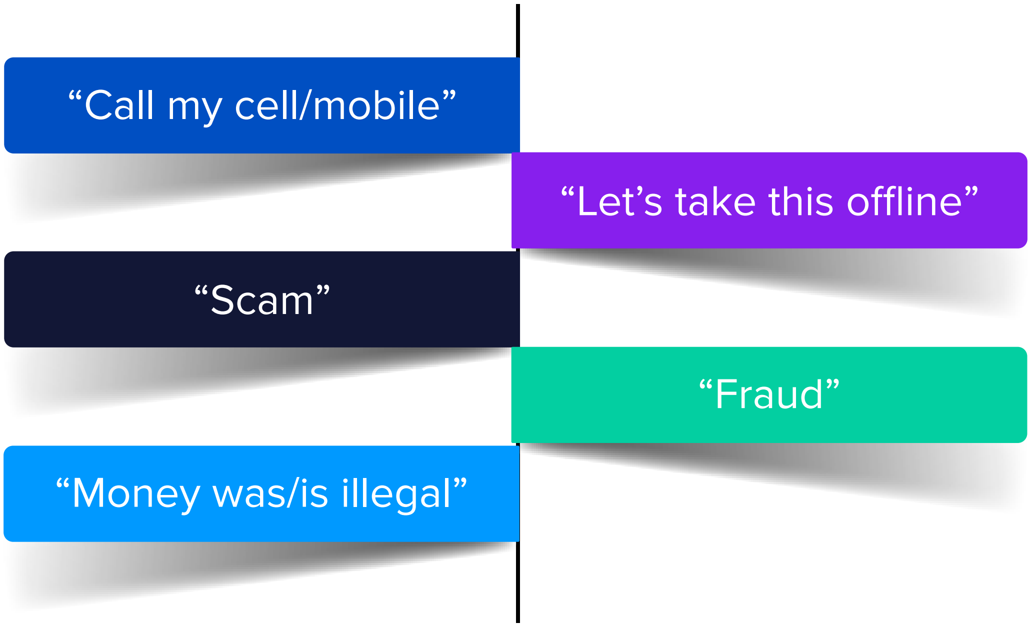
The flagged content arrives in the review queue preserved in native format, with conversational context and metadata included. There's no flattened email export of a chat log; rather, a reviewer gets a snapshot of how a conversation took place within the original platform.

Policies make the supervision and review process far less laborious and far more effective. They can be fine-tuned to drastically cut out white noise and reduce the number of messages that require review in the first place.

## A sample of policy configurations:

- **Keyword/Lexicon Policy:** Designed to scan and update messages for a defined set of words or phrases a firm considers to be “red flags”
- **Auto-Review Policy:** Designed to automatically close messages from senders that typically do not merit your review
- **Privileged Policy:** Designed to automatically close and categorize messages sent to or received from your attorney as “Privileged”
- **Retention Policy:** Designed to retain messages for a specified amount of time
- **Random Sampling:** The regular, required practice of pulling a sample of communications from various time periods to check for protected information that may have gone under the radar
- **Targeted Policy:** A required policy tactic that targets pre-determined, regulated words and phrases

So how do you decide which terms or phrases need to be monitored? You’ll have to discuss with stakeholders if there are company-specific terms that should be flagged for internal regulation, or for common issues your business faces. Here are a few examples from our master list of frequently updated terms and keywords that cause trouble in the financial services industry:



“Call my cell/mobile”

“Let’s take this offline”

“Scam”

“Fraud”

“Money was/is illegal”

## Supervision experts at your service

For additional assistance and consultation, we have a team of professional services experts that are highly attuned to the regulatory challenges that affected organizations are facing. They partner directly with firms to manage the complexity of modern compliance and give guidance on how to make the best use of technology solutions.

The Pro Services team provides a wide range of services that includes setup training, ongoing consultation, assistance developing a review process, and policy-tuning, just to name a few.

Once scalable technology has been adopted and supervision policies and procedures are in place, ongoing staff training is key to maintaining compliance – especially as new platforms emerge.

## The unified solution for comprehensive communications compliance

Interactive and dynamic conversations are fluid and the tools that people use to collaborate will keep changing, putting your supervision programs in an ongoing state of flux.

To stay ahead of the rapid adoption of new communication apps and evolving regulatory requirements, compliance managers and reviewers need the tools to react quickly to infractions and mitigate the risk of fines for non-compliance.

**Key capabilities of Smarsh Pro Archive and Supervision:**

- Review queues
- Policies & policy management
- Configurable workflows
- Reporting

Smarsh delivers a unified solution for capturing and archiving all electronic communications, with direct-from-source support for all major IM platforms and the broadest range of connected APIs to capture and control custom messaging apps. Simple onboarding and user experience make it easy to adopt. Rich policy management is available for multi-national, regional, and country-specific supervisory requirements from FINRA, SEC, IIROC, FCA, MiFID II, and more.

smarsh®

Smarsh® helps organizations get ahead – and stay ahead – of the risk within their electronic communications. With innovative capture, archiving and monitoring solutions that extend across the industry's widest breadth of channels, customers can leverage the productivity benefits of email, social media, mobile/text messaging, instant messaging/collaboration, websites and voice while efficiently strengthening their compliance and e-discovery initiatives.

A global client base, including the top 10 banks in the United States and the largest banks in Europe, Canada and Asia, manages billions of conversations each month with the Smarsh Connected Suite. Government agencies in 40 of the 50 U.S. states also rely on Smarsh to help meet their recordkeeping and e-discovery requirements.

The company is headquartered in Portland, Ore. with nine offices worldwide, including locations in Silicon Valley, New York, London and Bangalore, India. 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. *

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