GUIDE

A Guide to Building a Mobile Compliance Strategy

Create a future-focused compliance strategy that adapts to evolving regulations

smarsh®

Regulators like the SEC and FINRA have made it clear they won't be letting up on their enforcement of off-channel communications violations. Thus, firms must have a mobile compliance strategy that helps mitigate risk and protect the firm against fines and reputational damage.

Structuring a strategy built to last as the regulatory landscape continues to shift is no small order. Organizations must consider multiple factors today when implementing — or enhancing — a mobile compliance strategy fit for tomorrow. Such factors include employees' and clients' use of multiple and various mobile communication channels, digital applications (such as Zoom, Microsoft Teams and Slack) and the various features within those applications.

Start by asking the right questions

When thinking about how to structure a robust mobile compliance strategy, organizations should first consider how employees and clients communicate.

Some questions to consider:

- What productivity platform (i.e., Microsoft 365, Google Workspace) does the firm use?
- Do you allow voice and text features on corporate phones or employee-owned phones?
- What do you do when your customers/clients want to communicate on mediums or mobile apps they're comfortable with but are outside approved channels?

A helpful method to use as you think through your strategy is to draw a Venn diagram to find overlap in these questions. Pinpointing that overlap will help you determine where to focus your mobile compliance strategy. While a Venn diagram exercise may sound cliche, it's a simple way to discover what makes sense, what's rational to implement, and how your organization can meet regulatory requirements.

Firms must grasp which mobile apps they use — not only for internal collaboration but also from a marketing standpoint and from the perspective of communicating and engaging with clients. From there, ensure the proper guardrails are in place by pinpointing the firm's books and records and supervisory obligations. Do not use anything you can't capture, retain and supervise.

Gather key stakeholders

Your stakeholders must be on board — and the earlier, the better. All key stakeholders should have a seat at the table early in the strategic process when structuring your mobile communications compliance strategy. Some firms call this group of stakeholders a communications governance council. We recommend including the following roles:

- ✓ Chief Privacy Officers
- ✓ Chief Information Security Officers
- ✓ Chief Information Officers
- ✓ Chief Marketing Officers
- ✓ Heads of IT
- ✓ General Counsels
- ✓ Chief Technology Officers
- ✓ Chief Compliance Officers

Don’t fall for off-channel communications myths

Any business-related communications over unapproved channels are considered “off-channel.” Unfortunately, there are a few communication myths that can put a financial services firm at risk.

Myth #1: A prohibition policy is enough

Advisers continue to rapidly adopt new ways of communicating with clients. But when these communications occur on prohibited channels, the firm risks regulatory violations and fines.

General prohibition policies are not enough. It’s imperative that firms properly capture and preserve all business-related communications. Communications platforms are far too numerous and accessible for prohibition alone.

Reasons why *prohibition alone* fails:

- Employees are pressured to engage with customers/clients/finfluencers who prefer using unapproved channels
- Employees don't like using outdated and/or clunky channels, rendering approved lists obsolete within months
- Employees prefer the convenience of using personal devices
- Personal conversations on unapproved channels can quickly and naturally evolve into business-related conversations
- Customers/clients initiate business-related conversations on an unapproved channel, leaving unrecorded and potentially risky dialogue

Steps for going beyond prohibition:

1. First, review the SEC risk alerts to see what the regulators are monitoring.
2. Review those enforcement actions and plan accordingly.
3. Senior management and the firm's compliance team should decide which communication channels the firm approves and implement a clearly defined e-communication policy and procedures and training.
4. Once the compliance controls are in place, firms should enlist a records-retention vendor or decide how the firm will monitor communications themselves.
5. Finally, firms must regularly take inventory of all the communication channels that employees and advisers use.

Myth #2: Annual training is sufficient

Annual training is not sufficient to keep pace with new communication channels and ever-evolving regulatory requirements. Given the pace of new collaboration technology adoption, it's necessary to hold refresher courses to keep employees up to date. Training should be viewed as a continual process. Employees should know the lists of approved and prohibited communication channels — and firms must update and reinforce that regularly.

Email newsletters are great for updating policies or announcing new regulations or enforcement actions resulting from violations of off-channel communications. Firms should then integrate those into employee training as well.

As part of their training, employees should know what to do in the event they inadvertently engage in off-channel communications — such as a text message from a client. In this instance, the message or conversation goes completely undocumented. Firms should prepare employees to answer questions such as, "Who do I call? How do I manage that? How do I document for that?"

One best practice is for the firm's Chief Compliance Officer (CCO) to have an open-door policy. Make sure people feel like they can come to the CCO or whoever oversees these policies and procedures should that action happen.

Employees should be required to attest or acknowledge that they understand the firm's communications policy. This could mean that if a policy violation is uncovered during a risk assessment, employees must permit the firm to look at their device to ensure there are no further off-channel communications violations.

Firms should have a handle on what disciplinary actions to take, or what escalation procedures should be in place, in the event of a policy violation. Examples include:

- Issuing a disciplinary warning
- Clawing back executive compensation or bonuses
- Terminating individuals at the center of the misconduct

Myth #3: It's impossible to reasonably monitor for off-channel communications

Policies and procedures, training and reasonable supervision to identify off-channel communications should be part of a firm's compliance framework. When monitoring for instances of off-channel communications, regulators expect firms to watch for red flags — and follow up on them.

Lexicon searches that look for keywords and phrases and potential off-channel communications in the datasets the firm is already capturing are just one way to proactively detect potential misconduct. Firms should use lexicons to their advantage.

Off-channel communications aren't always external messages. Employees often aren't capturing internal business communications taking place on approved platforms within their archiving processes.

For example, FINRA has indicated that using visual aids — such as whiteboards, or a chat or instant messaging feature during a live, unscripted online presentation — could have consequences for the firm if those aspects are not being supervised correctly. It's crucial that firms capture all those communications within their supervision framework.

How to improve your monitoring

Firms should adjust their lexicons and monitoring practices to detect channel-hopping, which occurs when conversations transition from approved channels to off-channel communications. For example, a firm could institute the lexicons "Let's take this conversation offline," or "Text me."

As new communication channels arise, it's important to keep lexicons fluid. It's also a good idea to adapt the firm's lexicon search to accurately capture communications beyond text to include emojis, GIFs, videos, and voice-to-text features that could also point to misconduct.

Another best practice is to have a review process to look for off-channel communications within permitted channels. Important details are not captured if conversations are broken up between permitted and non-permitted channels, incurring unnecessary risk to the firm.

Firms should also consider going through older communications to see if there may be compliance gaps elsewhere. For many firms, it's worth looking back and seeing how past communications will affect what the firm will do with its policies and procedures going forward. It will also let the compliance team know that remedial measures must occur.

Establish your mobile communications oversight

When structuring policies and procedures related to mobile communications oversight, one key consideration is deciding whether to allow a particular communications device, or how to enable a compliance strategy around one.

Many organizations are also starting to operationalize their governance processes around their mobile compliance strategy through multi-stakeholder discussions with their data security, data privacy, and IT teams. This holistic view allows them to see how well they understand the benefits, costs and risks of these various communication decisions.

Having a data retention policy and code of conduct is also a good idea to put policies and procedures around acceptable and prohibitive behaviors.

These policies aren't "set it and forget it." Firms will need to make sure people understand the reasoning behind policies and the real consequences for breaking those policies — whether that means suspension, fines or termination.

10 best practices for structuring a mobile compliance strategy

Enforcement sweeps have forced firms to pay more attention to their employees' mobile communication activities. As the use of mobile communications channels continues to rise and shift from trending channel to trending channel, the need for robust books and records and supervisory controls is paramount. With the need for mobility in the modern era, firms understand that these tools are critical for meeting regulatory compliance obligations and reducing the risk of an enforcement action.

Below is a summarized list of our recommended best practices for structuring a robust mobile compliance strategy.

1 Focus on tone from the top

To meet recordkeeping and supervisory obligations over employees' electronic communications, firms must first create a culture of compliance. As seen in recent SEC enforcement sweeps that found senior management and compliance teams using prohibited channels, that tone must start from the top.

Senior management and compliance teams should do more than talk the talk — they need to walk the walk. Rather than preaching about the risks of off-channel communications and taking no action, they must ensure employees follow the firm's communication policy and procedures.

Do senior executives follow the same mobile communication rules as all employees? That tone sets everything in motion regarding how effective these policies, procedures, training and technologies can be.

2 Implement policies and procedures

Policies and procedures are necessary to carry out the firm's strategy and should address what is permitted and what is prohibited. Policies should be structured in a way that's achievable for the firm based on its size, culture and business approach.

One-off situations must be considered, such as when business-related communications are received over unapproved channels. Specifically, employees should know who to call and what steps to take to ensure there are no compliance gaps.

Furthermore, policies and procedures should cover what disciplinary actions will be taken for non-compliance Be sure to document any remedial actions; regulators will want proof that policies are being enforced.

3 Define books and records

Firms should clearly understand and define what books and records to keep from a recordkeeping standpoint. Broadly, that includes:

- Client or investor communications
- Marketing communications to clients
- Communications regarding research or portfolio names
- Communications surrounding investment recommendations

4 Train and educate

Encourage people to adhere to policies and procedures concerning communications over mobile apps by educating them on the firm's reasoning. Employees should be trained on what channels they're allowed to use and what the consequences are for using unapproved channels. Compliance officers must supervise and educate, whether that's verbally during large team meetings or department gatherings or by sending out periodic emails reminding employees about the firm's mobile communication policy.

In addition to training and education, employees should attest, preferably every quarter, that they comply with the firm's electronic communication policies and procedures. These check-ins help firms stay compliant and remind employees of the seriousness of only using approved communications channels.

5 Capture emojis

An important consideration is the growing use of emojis in business communications and how to capture those from a regulatory compliance perspective. Regulators have specifically noted that the rocket ship, money bag and stock chart emojis constitute financial advice.

Essentially, regulators are saying that emojis could be used as their own language in replacement of words. While it may seem silly to focus on emojis, it's critical to understand them and their use within your business communications.

6 Monitor high-risk areas

Regulators expect organizations to have their finger on the pulse of higher risk areas. This may mean closely monitoring individuals who have violated the company's mobile compliance policy in the past.

Regulators will also be paying attention to whether there are systemic patterns of behavior, such as clients sending business communications over channels like WeChat. Regulators want to know how you are addressing that behavior across the business. They also want to know if it is operationalized so people understand what they can and cannot do with those tools.

7 Focus on the organization's use cases

Establishing oversight controls and policies and procedures around a mobile communications strategy is a complex process due to the various ways employees and clients communicate today. Focusing on the organization's specific use cases — using the Venn Diagram strategy mentioned earlier in this guide — and putting structure around those will help the organization meet its regulatory compliance objectives.

8 Don't hide or ignore compliance gaps

Keep in mind your firm might be required to self-report violations to regulators. While self-reporting a violation could still lead to a fine, you could find yourself in a more favorable situation going into an exam in the future. Regulators expect companies to mitigate that risk before they find out about a problem, so it pays to be proactive. Fixing the problem will always be a better option than ignoring it.

9 Trust, but verify

In addition to employee attestations, you should review the firm's archives at least quarterly. Look for things within the archive that may point to a violation to ensure employees are adhering to the policy from a compliance standpoint.

From a supervisory standpoint, having the correct set of lexicons in place is critical. It's also important to update those at least annually and even more frequently as new apps are introduced. Monitoring trending channels and getting a lay of the land will help firms stay on top of compliant communication practices.

Firms should conduct ongoing evaluations around mobile application channels to ensure those communications can still be captured — especially as new features are added to those applications.

For example, firms need to think about how to capture and put supervisory controls around emojis, GIFs and voice-to-text features that could signal off-channel business communications.

10 Partner with trusted vendors

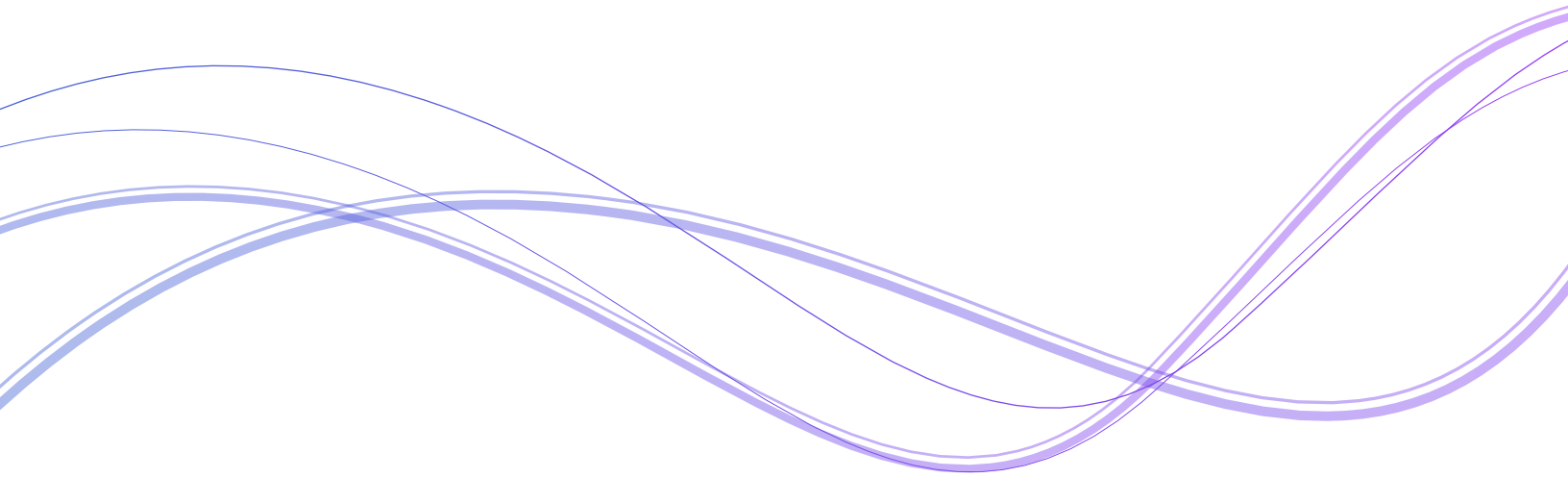
Most firms work with vendors because it's costly to build proprietary recordkeeping solutions. It's important to work with vendors that have experience in the financial services sector. Given the modernization of SEC 17a-4, firms must find partners that can handle the complexities involved with enabling the preservation and production of business records.

To maintain proper oversight and choose the right partner, ask yourself:

- Do these providers understand what my regulatory obligations are?
- Are they providing access to APIs?
- Are they making it easy for me to create and preserve a historical record?

Don’t aim for perfection

It’s impossible to stop every bad actor from engaging in off-channel communications. It’s also going to be difficult for compliance teams to keep up with the advancements in communications tools. However, by implementing robust policies and procedures, employee training and attestations, and continuously monitoring for noncompliance, firms can significantly reduce the risk of getting on the wrong side of regulators.



smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals from the most in-demand communications channels. Regulated organizations 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 advisers 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

Guide - 10/23

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