2017

Electronic Communications Compliance Survey Report

Communications compliance practices and examination expectations among compliance professionals in financial services

Table of Contents

Key Takeaways

Firms are concerned about mobile communications, and with good reason

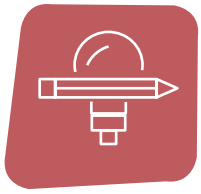
Mobile devices enable communications to happen anywhere, and compliance is failing to supervise and retain all messages sent on the go, particularly text messages.

Expanding communications options bring complexity to compliance

Employees want the flexibility to use the communications channels their clients use, so firms are allowing more channels. Unfortunately, supervision processes aren't keeping up, leaving firms vulnerable to compliance risk and widening regulatory scrutiny.

Examinations go deeper and broader

Examinations are on the rise, and regulators are honing in on electronic communications supervision. Compliance professionals are concerned about the increasingly sophisticated requests for supervision practices and different types of messages, particularly social media.



Supervision—the fine balance of resources against risks

Compliance teams are searching for the right formula to allocate their resources most efficiently. They recognize the value of electronic communications supervision beyond just fulfilling regulatory requirements, but the growing volume of messages of all types requires discipline and continuous process improvement to effectively identify risk.

Executive Summary

Against the backdrop of political shifts in Washington and growing popular distrust of "big finance," the seventh annual Smarsh survey of compliance professionals in the financial services industry reveals that the electronic communications compliance landscape has become broader, more complex and more scrutinized.

More firms are finding that gaps in retention and supervision programs have consequences. Examinations have become more comprehensive, with regulators focusing in particular on supervision processes. **FINRA reported 99 books and records cases in 2016, resulting in $22.5 million in fines. Compared to 2015, that represents a 423% increase in fines.**[1]

In conjunction, compliance professionals' concerns have expanded. One significant area of concern is the growing number of non-email communications options, particularly mobile communications.

Top Three

Concerns related to electronic message compliance

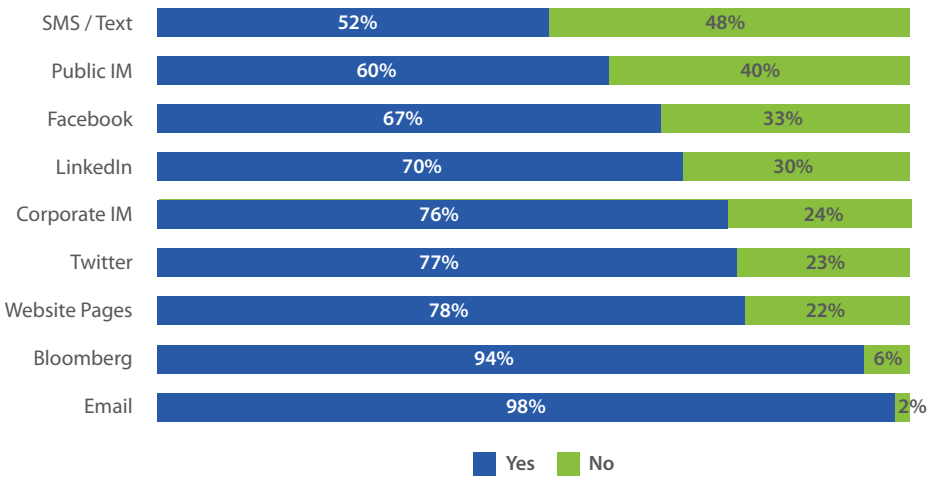
1. Non-email communications channels (e.g., social media, text messaging)
2. (tied) Mobile communications devices (e.g., smartphones, tablets)
2. (tied) Understanding new and changing regulations

Many of the archiving and supervision compliance gaps identified in previous years have narrowed. That said, a significant number of firms are still vulnerable because they have not taken action to appropriately supervise their employees' business communications, particularly mobile, social and instant messaging.

A comparison of 2016 vs. 2017 data illustrates that firms are moving to implement archiving/supervision solutions. Year-over-year, notable compliance gaps have decreased: LinkedIn (-35%), Corporate IM (-35%), SMS/text messaging (-28%) and Facebook (-26%).

Compliance gaps narrow, but remain significant

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



Even when supervision is happening, compliance teams must decide where and how to best allocate their finite resources to efficiently and effectively identify and address non-compliant communications and other actions that pose risks to their firms.

Key BD/RIA Regulations Governing Electronic Communications Include:

- SEC Rules 17a3 and 17a4 of the Securities and Exchange Act of 1934
- SEC Rules 204-2 and 206(4)-7 of the Investment Advisers Act of 1940
- SEC Guidance Update – Guidance of the Testimonial Rule and Social Media (March 2014)
- FINRA Rules 2210 and 2212-2216
- FINRA Rules 3110, 3120, 3150, and 3170
- FINRA 4511
- FINRA 4513
- FINRA Regulatory Notices 03-33, 05-49, 07-59, 10-06, 10-59, 11-39, 12-29, and 17-18
- CFTC – Clarification of NFA Compliance Rule 2-10(a) and CFTC Regulations 1.31
- FFIEC Social Media: Consumer Compliance Risk Management Guidance
- Federal Rules of Civil Procedure (FRCP)
- Gramm-Leach-Bliley Act
- SEC Regulation S-P
- U.S. State Data Protection Laws

Firms are concerned about mobile communications, and with good reason

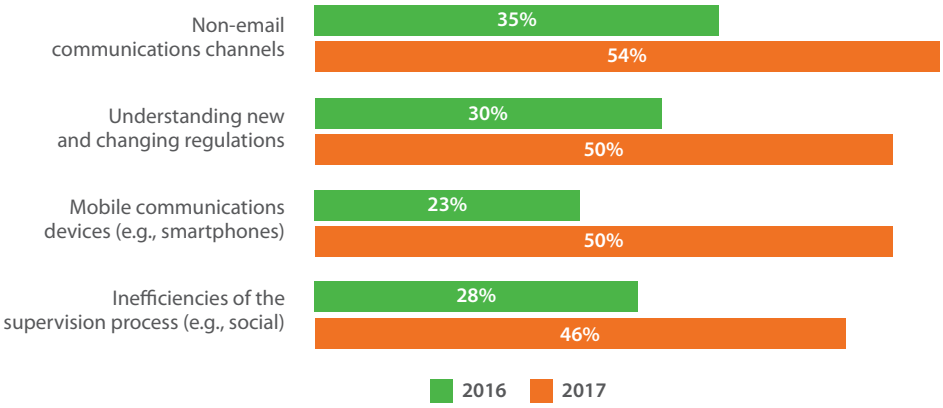
With a mobile device in nearly every hand, mobile communications are clearly top of mind with compliance professionals. FINRA Regulatory Notice 17-18 (Social Media and Digital Communications) cites an April 2015 Pew Research Center report contending that 64 percent of American adults own a smart phone of some kind, and 97 percent of smartphone owners used text messaging at least once during the study period, making it the most widely used basic feature or application.[2]

Forty-two percent of respondents report that employees have requested to use text/SMS messaging for business purposes. It is the most requested channel for business use by employees, up from 2016 when only 21 percent reported such requests.

Mobile communications devices and non-email communications channels such as text messaging account for two of respondents' top three overall e-comm compliance concerns. Not only were each of these concerns identified by at least half of survey respondents, but the percentages jumped significantly from 2016.

Nearly one-third of firms (32 percent) allow their employees to use text/SMS messaging for business.

Top electronic message compliance concerns



Furthermore, more than half of respondents (52 percent) identified text/SMS messaging as the type of non-email content that poses the greatest compliance risk to their organization, ahead of instant messaging, social media and website content.

These concerns are validated by gaps in both compliance practices and confidence when it comes to mobile communications. Among the firms that allow text/SMS messaging, more than one-third (36 percent) do not have a written policy governing its use and almost half (48 percent) do not have an archiving solution in place.

Even firms that prohibit usage of text/SMS messaging are concerned. More than one-third (35 percent) of those respondents have no or minimal confidence that they could prove that their prohibition is working; this is the lowest confidence level among prohibited channels.

How do firms justify not archiving text/SMS messaging when they allow it for business?

42% No one at my firm actually uses this channel for business communication

33% We can handle our retention / oversight needs for this channel without additional technology

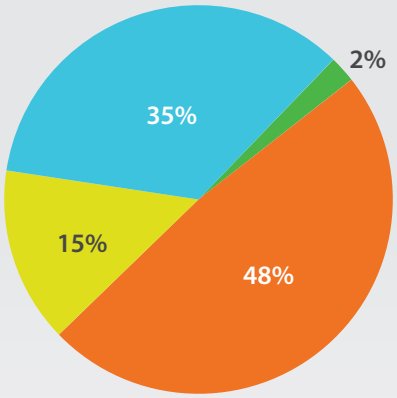
25% Waiting for regulators to enforce regulatory guidance before we archive it

Not supervising mobile? Expect to be fined.

It's no longer realistic for a firm to believe that its employees don't use text messaging to communicate with clients. Text messaging continues to surface on FINRA's enforcement radar.

- In March 2017, FINRA fined and suspended a Texas broker for one month for unapproved securities-related communications with two customers via text message, violating the firm's Written Supervisory Procedures (WSPs). The firm did not capture, review or retain the broker's text communications.[3]
- In December 2016, a New York advisor was fined and temporarily suspended for using a mobile phone to communicate with customers via text message without the firm's knowledge. The firm did not review or retain any of the text messages.[4]
- In November 2016, a New York advisor was fined and given a 60-day suspension for using text messaging on a non-firm-issued smartphone to exchange business related messages with a customer, in violation of the firm's policies. The advisor also provided the customer with a personal email address and instructed the customer to use that email address for a business-prospecting project, also in violation of the firm's WSP. This use of text messages and a non-firm-issued email address caused the firm to fail to retain those communications and undermined the firm's ability to supervise the advisor's communications with a customer.[5]

How does your firm manage the use of mobile devices for business communications?



- Personal and corporate-issued devices are allowed
- Only corporate-issued devices are allowed
- Our company does not issue mobile devices. Employees use their own
- I don't know

Who needs a computer when you've got a phone?

Mobile communications encompass more than just text/SMS messaging and Apple iMessage; they include any communication sent over a mobile device, including email, instant messages, social media updates and other business and enterprise application posts. With more than eighty percent (83 percent) of firms allowing employees to use personal devices for business communications, the supervision ramifications of bring-your-own-device (BYOD) are a reality for most compliance professionals. Regulators have made clear that the message content determines its status as a business record, even if it originates on a BYOD device.

Almost one-quarter of respondents (23 percent) have no or minimal confidence that their firm is capturing and archiving all business messages sent via mobile devices.

Mobile communications devices were identified as a concern by half (50 percent) of respondents in this year's survey, tying it as the No. 2 overall concern. This is a significant jump from 2016, when mobile devices were a concern for only 23 percent of respondents, ranking it 14th out of 16 concerns.

Apple devices are ubiquitous: 92 percent of firms allow Apple iOS devices.

Mobile Strategy: Device Ownership Scenarios

Before capturing and archiving business communications sent via mobile devices, firms must first define permitted mobile device ownership and business communications use. The ownership and billing model has a significant impact on how the firm implements its mobile archiving and compliance plan. Options include:

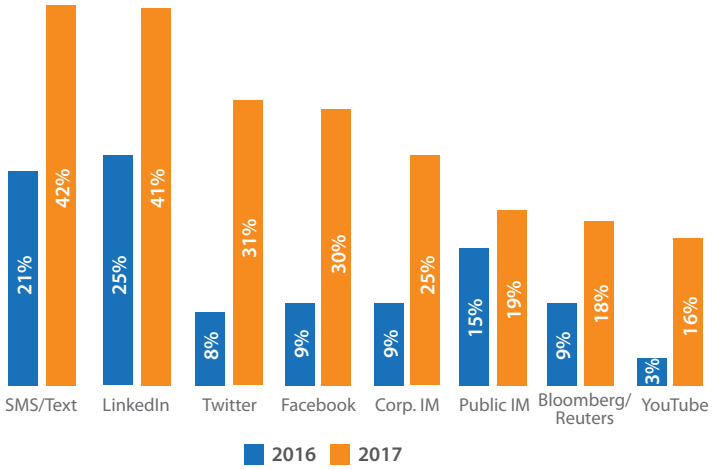
- Bring Your Own Device (BYOD)
- Choose Your Own Device (CYOD)
- Corporate-Owned Personally Enabled (COPE)

A firm may also choose to use a combination of these scenarios to fit its specific business needs, objectives, and capabilities/preferences of employees within the firm. For more information, read *5 Steps to Eradicate Text Messaging Risk*, available at www.smarsh.com/whitepapers/5-steps-eradicate-text-message-risk.

Expanding communications options bring complexity to compliance

Employee demands to use different communications channels extend beyond text/SMS messaging. This year's survey data showed increases in requests across all channels, with LinkedIn leading the way, followed by Twitter and Facebook.

Most requested communications channels, 2016-2017

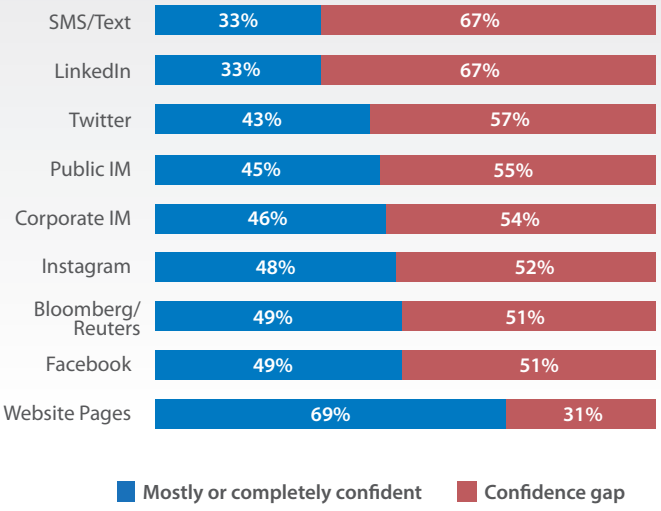


The percentage of firms allowing popular social media, instant messaging and other electronic communications channels has remained consistent year over year, with Twitter as one notable exception. More than half of firms (51 percent) now allow use of Twitter, up from 39 percent in 2016. Gaps in compliance practices —both written policies and archiving/supervision programs— remain sizable.

Prohibition doesn't work

Prohibiting the use of a communications channel is not an effective strategy for firms, either. Confidence in the effectiveness of prohibition policies is low. This confidence gap is reported by more than half of respondents for each of the top social media channels: LinkedIn (67 percent), Twitter (57 percent), Facebook (51 percent) and Instagram (52 percent).

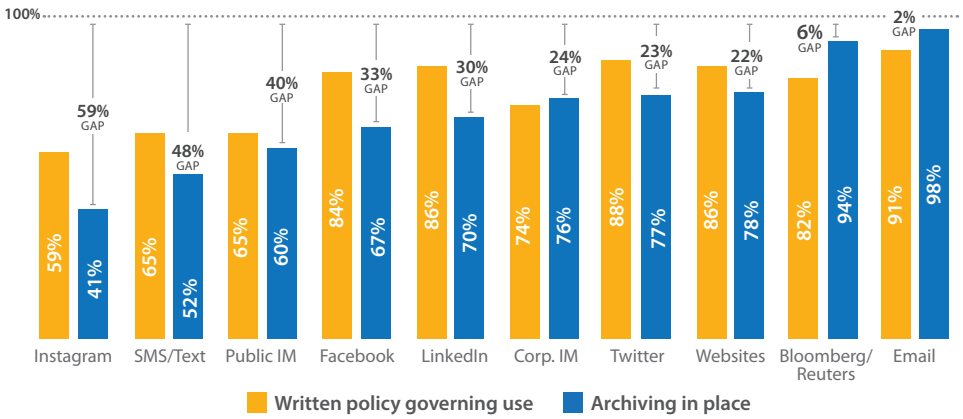
How confident are you that you could prove that your prohibition of the following channels is working?*



*Among firms that prohibit the channel

Whether their firms allow or prohibit a specific content type, *enforcing governance policies* was identified as a concern by more than one-third of respondents (39 percent).

Policy and archiving/supervision gaps*



*Among firms that allow the channel

In December 2016, FINRA censured and fined a Georgia firm $1.5 million, in part, for failure to retain approximately one million text messages sent using firm-issued devices. The firm had a policy of prohibition, which certain employees violated. Regardless of the policy, FINRA found the firm in violation of its requirement to preserve all business communications.[6]

Examinations go deeper and broader

Examinations on the rise

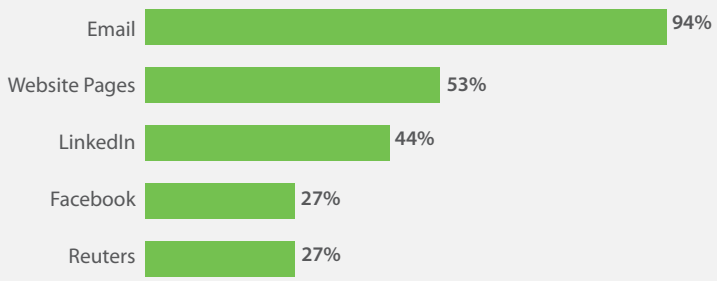
The incidents of firms being examined is on the rise with 47 percent of this year's respondents reporting being examined in the previous 12 months.

Firms examined in the past 12 months

27% 2015 **42%** 2016 **47%** 2017

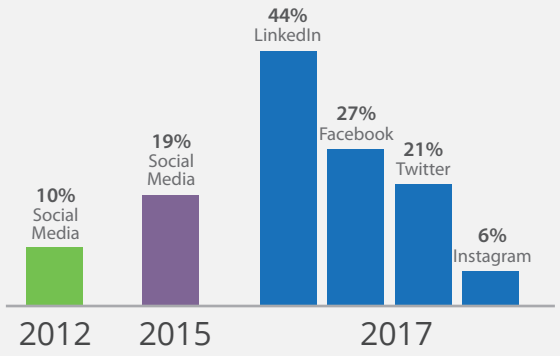
These respondents reported being asked to produce multiple types of communications content beyond email. More than half (53 percent) were requested to provide website pages and almost half (44 percent) had to provide LinkedIn content.

Top message types requested during examination*

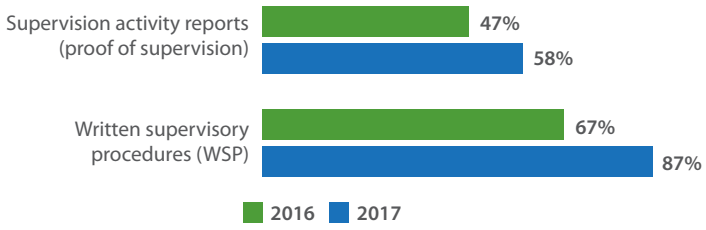


*Among firms examined in the previous 12 months

Exam requests for social media are on the rise



Documentation requested during examination*



*Among firms examined in the previous 12 months

Examiners are also honing in on supervision practices during exams. Respondents reported a 30 percent increase year-over-year in requests for written supervisory procedures and a 25 percent increase in requests for supervision activity reports.

Examiners want to know how firms are addressing mobile communications. 21 percent of respondents examined in the past year had to provide their mobile device communications policy.

Given the growing breadth, depth and frequency of exams, it is unsurprising that increased scrutiny/enforcement by regulators is a concern for 44 percent of respondents.

"These disciplinary actions are a result of FINRA's focus on ensuring that firms maintain accurate, complete and adequately protected electronic records. Ensuring the integrity of these records is critical to the investor protection function because they are a primary means by which regulators examine for misconduct in the securities industry."
-- Brad Bennett, FINRA Executive Vice President and Chief of Enforcement[7]

The February 2017 Risk Alert issued by the SEC Office of Compliance Inspections and Examinations (OCIE) identified the Books and Records Rule as one of the top five most frequent compliance topics cited in deficiency letters sent to SEC-registered investment advisers during the last two years. Typical deficiencies include:

- Not maintaining all required records
- Inaccurate or outdated books and records
- Inconsistent recordkeeping[8]

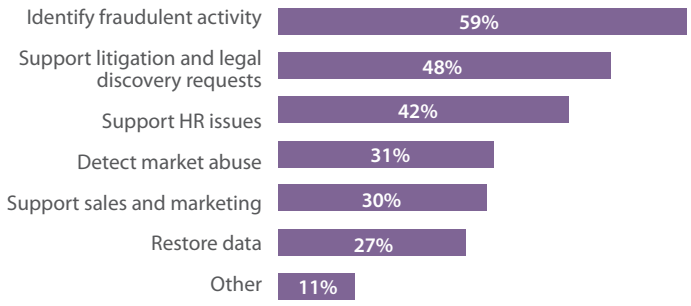
Supervision—the fine balance of resources against risks

While regulatory requirements are often the primary driver for archiving and supervision, 88 percent of respondents recognize that electronic communications data can also help identify risks to the organization. More than half of respondents (59 percent) confirm that their organization uses this data to identify fraudulent activity, among other purposes, such as supporting e-discovery and HR issues, and detecting market abuse.

22%
of respondents

report using or providing data from their archiving system(s) for other purposes (outside of a regulatory audit) **ten or more times per year.**

How electronic communications data is used outside of a regulatory audit



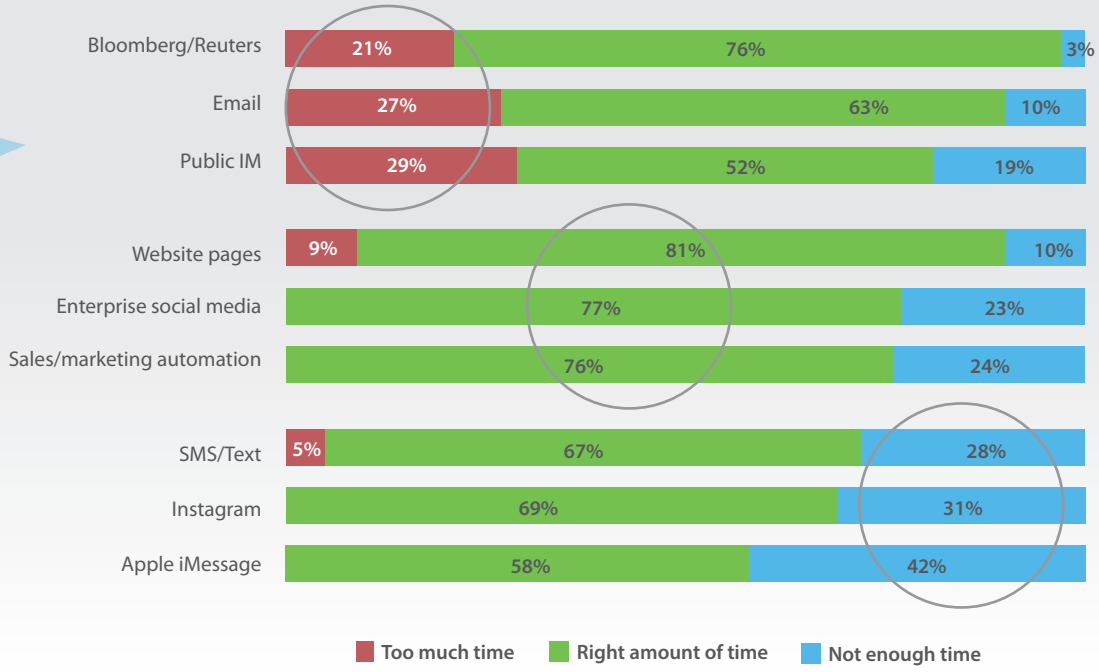
Compliance teams are devoting more resources to these purposes; more than half of respondents (53 percent) report that the time and/or money spent by their organization for electronic message compliance has increased over the past 12 months, and 54 percent expect those resources to further increase in the next 12 months.

Despite the growth in resources, many compliance professionals are still concerned about inefficiencies in the supervision process (46 percent) and how to fine-tune supervision processes to find real risk (38 percent).

With the growth in the number of allowed channels and the sheer volume of messages, compliance is struggling to separate the wheat from the chaff. Survey respondents reported challenges allocating resources across the multiple communications channels their employees use. They believe too much time is spent reviewing some channels, including email, while other channels, such as SMS/text messaging do not get enough time.

How would you rate the amount of time spent supervising messages from different allowed communications channels?

Traditional content types like Email are still getting too much time and attention relative to the risks they pose, while others like text messages that pose the greatest risk aren't getting enough.



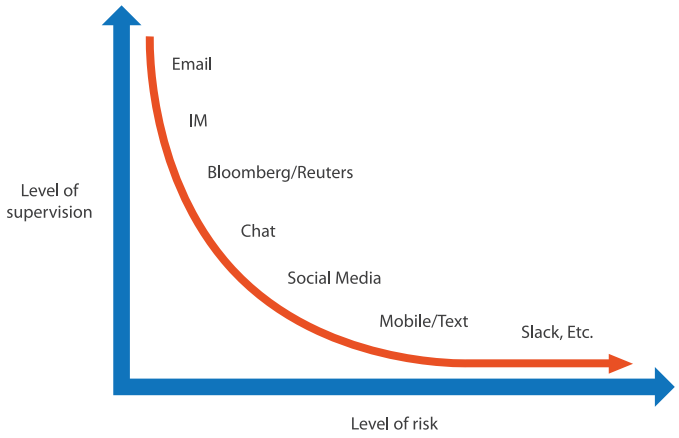
From the Desk of the CEO

Rebalancing the electronic communications risk portfolio

Electronic business communications pose a major risk to financial services firms. Scrutiny is on the rise, and more sophisticated than ever. At the same time, they're an essential part of how the business operates. They foster collaboration and knowledge-sharing among employees, grow relationships with clients and attract new business and talent. It's impossible to imagine a firm functioning without electronic communications. Email is a no-brainer, but many firms struggle with how to manage other channels such as text messaging or social media.

This year's survey reinforces that policies of prohibition are a barrier to growing business and workforce productivity. They do not deliver compliance confidence, and they simply don't work. Early 2017 examples of text-related firm penalties all have one thing in common: all prohibited its use for business communication. More than two thirds (67 percent) of respondents have no or minimal confidence that they could prove their prohibition of text messaging is actually working.

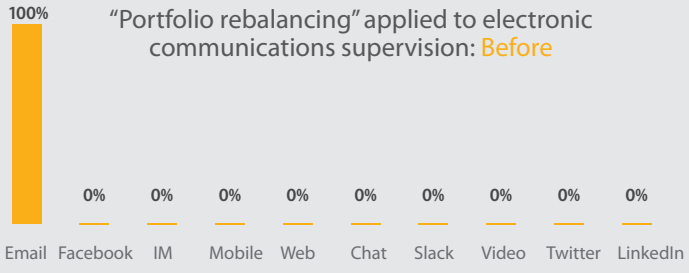
More allowed channels and messages to supervise pose a challenge to compliance teams that must focus their efforts on the areas of greatest risk. Email will always merit scrutiny because of sheer volume, but our survey indicates that it might be getting too much attention to the detriment of other channels. Compliance professionals are spending too much time looking for risk in email, and not enough time in mobile, IM and social media. We know that conversations today roam across multiple channels – what starts in an email thread may move over to IM then on to texts. Compliance must follow the conversation, not just review one channel in isolation.

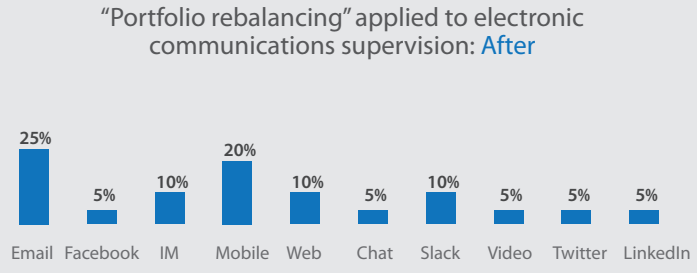


THE ELECTRONIC COMMUNICATIONS COMPLIANCE SUPERVISION RISK CURVE

One survey respondent commented: "The more channels for business communications, the more oversight is required. Although electronic archiving presents efficiencies in the oversight process, there is still a need for human oversight and the more channels the more human review is required. Human resources become the limitation." This is a common and intuitive observation, but I don't believe that it has to be the case.

It's encouraging to see that many organizations are dedicating more resources to electronic message compliance, but they must be strategically applied. It is an ongoing re-balancing act to allocate supervision resources. Technology can help compliance teams search across multiple content types, easily adapt policies and automate supervision.

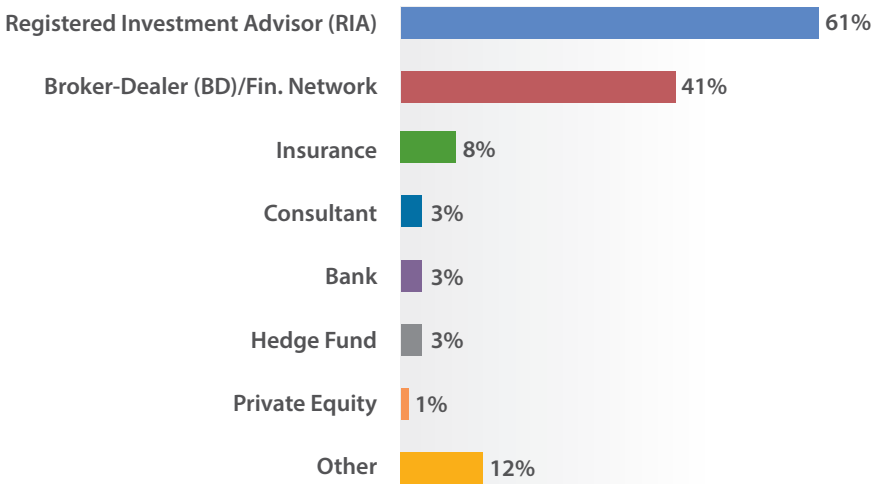




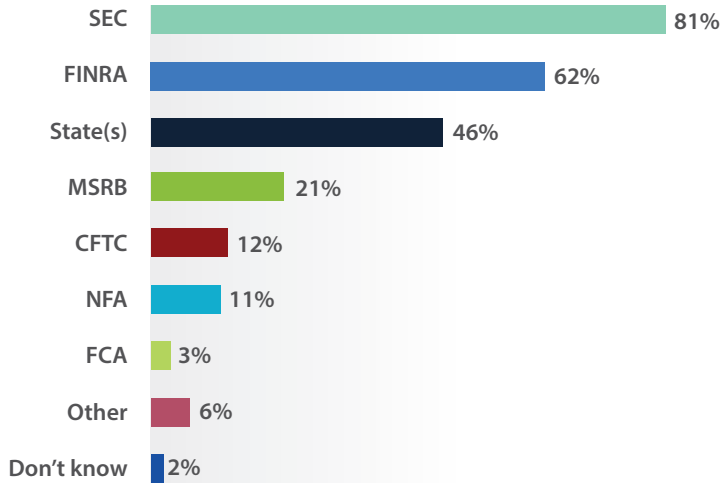
On their own, however, neither resources nor technology will erase compliance concerns. That will only come with clear policies that employees understand, comprehensive archiving that captures messages across all channels from whatever device they're sent, and supervision that effectively combines technology and automation with human insights and strategy. While archiving gaps are shrinking, there is still a long way to go—especially as regulators have become more sophisticated in their requests.

Stephen Marsh | CEO, Smarsh, Inc.

What type of firm do you work for?



What regulatory agencies oversee your firm?



1 https://us.eversheds-sutherland.com/NewsCommentary/Press-Releases/197511/Annual-Eversheds-Sutherland-Analysis-of-FINRA-Cases-Shows-Record-Breaking-2016

2 http://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-17-18.pdf Aaron Smith, Pew Research Center, Internet, Science & Tech, U.S. Smartphone Use in 2015 (April 1, 2015).

3 https://www.finra.org/sites/default/files/publication_file/March_2017_Disciplinary_Actions.pdf

4 https://brokercheck.finra.org/individual/summary/2800349

5 https://brokercheck.finra.org/individual/summary/4926890

6 http://www.finra.org/sites/default/files/SunTrust_AWC_122116.pdf

7 http://www.finra.org/newsroom/2016/finra-fines-12-firms-total-144-million-failing-protect-records-alteration

8 https://www.sec.gov/ocie/Article/risk-alert-5-most-frequent-ia-compliance-topics.pdf

Survey Methodology

In February and March 2017, 119 individuals in financial services with direct compliance supervision responsibilities participated in a 31-question survey designed to identify current trends and to share insight on policies and practices about the usage, retention and supervision of electronic business communications.

Respondents were drawn from a wide range of firm sizes and job titles, from C-level management and chief compliance officers to compliance department staff.

Smarsh offered an incentive to respondents in the form of a charitable donation via Smarsh Full Circle (www.smarsh.com/fullcircle), its community service initiative. Questions were answered through an online survey, and the responses were collected by a third party.

Topics included:

- Confidence in compliance policies and enforcement
- Policies and use of different communication types
- Policies and use of different communication devices
- Examination incidence and expectations
- Supervision and archiving practices
- Confidence in message supervision

Smarsh
851 SW 6th Ave, Suite 800
Portland, OR 97204

1-866-SMARSH-1
www.smarsh.com

LinkedIn: Companies/Smarsh
Facebook: Smarshinc
Twitter: @SmarshInc

Smarsh® delivers a comprehensive and integrated stack of cloud-based information archiving applications and services that help companies protect themselves and manage risk. Its centralized platform provides a unified compliance and e-discovery workflow across the entire range of digital communications, including email, social media, websites, instant messaging and mobile messaging. Founded in 2001, Smarsh helps more than 20,000 organizations meet regulatory compliance, e-discovery and record retention requirements. The company is headquartered in Portland, Oregon, with offices in New York City, Boston, Raleigh, N.C., and London.