2016 Electronic Communications Compliance Survey Report

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

TABLE OF CONTENTS

KEY TAKEAWAYS

A firm's culture is both an input to and product of its supervisory system.

- FINRA 2016 Regulatory and Examination Priorities Letter[1]

Communications supervision is more important than ever, but compliance resource constraints challenge its efficacy.

As firms aim to demonstrate their "culture of compliance," the role of electronic communication supervision is growing beyond the "retain and respond" checkbox. Compliance teams are taking a seat at the table to help manage overall corporate risk alongside other departments including IT, marketing and HR. With the mandate expanding and the stakes getting higher, resources are not keeping up, putting additional strain on the compliance function.

New communications channels are expanding the compliance perimeter.

From social media to text messages to instant messages, compliance is challenged to stay ahead of the rapidly expanding scope of business communications. Gaps in governance abound as policies, archiving and supervision fail to keep up, introducing still greater risk for firms.

Compliance departments are concerned about how their electronic communications supervision practices are keeping up.

Compliance professionals are concerned that current supervision approaches will not identify risks in their organization. They acknowledge the need for improvements in efficiency and effectiveness, particularly related to message review, to focus their finite resources on the areas presenting the greatest risk to their firm. However, they remain uncertain about how to achieve this vision.

Executive Summary

For the sixth consecutive year, the Smarsh Electronic Communications Compliance Survey illustrates the key trends and concerns facing compliance around the retention and oversight of electronic communications.

While many of the concerns highlighted by respondents remain consistent year-to-year, such as growing regulatory scrutiny and adapting to new communications channels, the responses also show supervision practices are not sufficiently addressing the compliance implications of these ongoing trends. Policy, enforcement and retention gaps remain high, leaving firms vulnerable to undetected fraud, errors, and regulatory enforcement penalties.

Against this backdrop, compliance officers have to align the benefits of modern communications with the need to protect their firms against compliance risks. For instance, supervision of new communications types poses a challenge, because most firms are already overwhelmed by the sheer volume of email they must retain and review. Resources to address this expanding compliance perimeter are growing slowly, if at all.

These concerns are consistent, regardless of whether a firm allows usage of these new communications channels or not, indicating that simply prohibiting employees from using a channel is not sufficient. Compliance must also ensure employees are not using channels without the firm's permission or knowledge, and communications "outside the compliance perimeter" represent a significant source of compliance vulnerability. It's no wonder compliance professionals are expressing concern that their current programs do not effectively identify risk.

Ultimately, this year's survey illustrates that while the challenges remain, the solution remains elusive to many firms. The current, linear approach of layering new content types on top of the supervision policies and processes originally designed for email is inefficient and ineffective. If procedures designed to identify risk in email are ineffective and waste time, extending those same procedures to additional content only exacerbates those results. There is a need to rethink the traditional approach to communications supervision, especially when considering finite resources and the growing strategic role of compliance in organizational risk management.

FINRA fines in electronic communications cases have **more than doubled**, from **$2.7 million** in 2008 to **$6.2 million** in 2015.[2]

Communications supervision is more important than ever, but compliance resource constraints challenge its efficacy.

The primary purpose of electronic message supervision is to fulfill regulatory requirements designed to protect investors, such as SEC rule 17a-4, which requires firms to archive electronic business communications in non-rewriteable and non-erasable (WORM) formats for at least three years. In addition to retention, firms are required to perform risk-based review of correspondence and internal communications.

The compliance function must ensure the firm is compliant with these mandates, thereby minimizing the business risks of non-compliance, such as fines, reputational damage, and loss of license to operate.

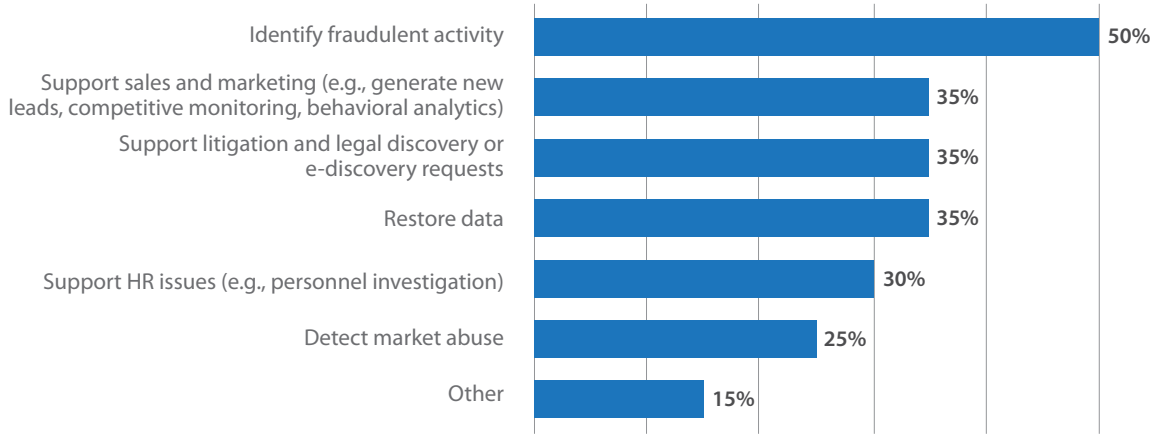
Compliance professionals certainly feel the pressure. Those responding to the survey cite increased scrutiny/enforcement by regulators as their number one concern related to electronic message compliance for the third year in a row. This is no surprise since 42 percent of respondents to this year's survey reported being examined in the past twelve months, up from 27 percent in the 2015 survey.

The value of electronic communications retention and supervision also extends beyond the regulatory checkbox. **Sixty-five percent of respondents report that the compliance function is responsible for handling requests to produce electronic communications data for e-discovery or other business purposes, bringing compliance into more aspects of business operations.**

TOP 5 Concerns Related to Electronic Communications Compliance

1. Increased scrutiny/enforcement by regulators
2. Balancing employee privacy considerations with oversight obligations
3. New communications channels (e.g., social media, text messaging)
4. Cyber security threats posed by the use of electronic messaging platforms
5. Insufficient human resources (e.g., staff or personnel)

Beyond the regulatory audit, a percentage of respondents use e-comm data for other purposes:



Resource Limitations Remain

While the importance of communications supervision is growing, resources are not. More than 87 percent of respondents expect the resources (time and/or money) dedicated to electronic message compliance will remain the same or increase only slightly in the next 12 months. Less than 1-in-10 expect to receive a significant resource increase. Unsurprisingly, this concerns compliance professionals. More than one-fourth of respondents (28 percent) cited insufficient budgets as a top concern this year, up from 22 percent last year. Likewise, 34 percent of respondents cited insufficient human resources as a top concern, up from 30 percent last year.

REGULATIONS GOVERNING ELECTRONIC COMMUNICATIONS INCLUDE:

- SEC Rules 17a3 and 17a4 of the Securities and Exchange Act of 1934
- FINRA Rules 2210 and 2212-2216
- FINRA Rules 3110, 3120, 3150, and 3170
- SEC Rules 204-2 and 206(4)-7 of the Investment Advisers Act of 1940
- FINRA 4511
- FINRA 4513
- FINRA Regulatory Notices 07-59, 10-06, 10-59, 1139 and 12-29
- January 2012 SEC National Examination Risk Alert (Social Media)
- SEC Guidance Update – Guidance of the Testimonial Rule and Social Media (March 2014)
- CFTC – Clarification of NFA Compliance Rule 2-10(a) and CFTC Regulations 1.35(a)
- 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
- IIROC Rule 29.7, IIROC Notice 11-0349, National Instrument 31-103 (Canada)
- FCA PRIN 2.1, APER 2.1a, 5, 6 & 7, SYSC 3.2 COBS 4 & 9, BCOBS2, MCOB3 and ICOBS (UK)
- FCA FG 15/4 Social Media and Customer Communications (UK)

Liability Gets Personal for Compliance Officers

In September 2015, the SEC issued a warning that compliance officers could be charged for negligently conducting their duties. Also that month, the SEC fined Securus Wealth Management's chief compliance officer $30,000 for failing to implement strong policies and procedures that would have caught stock manipulation fraud.[3]

New communications channels are expanding the compliance perimeter.

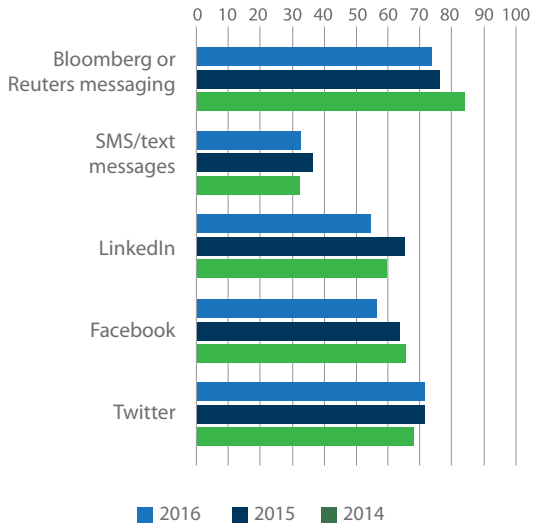
The compliance perimeter—those electronic communications channels and devices in use at an organization that require governance policies and retention/supervision solutions—is expanding, creating additional burdens on compliance teams.

Beyond the Perimeter: The Compliance Gap

It is the content of the message that determines its status as a business record. Compliance professionals need to supervise all types of business communications, even when messages reside on personal devices and social media accounts. Making this a reality, however, presents challenges, and compliance to-date has not kept up with implementing archiving and supervision systems for all the communications channels employees are allowed to use for business.

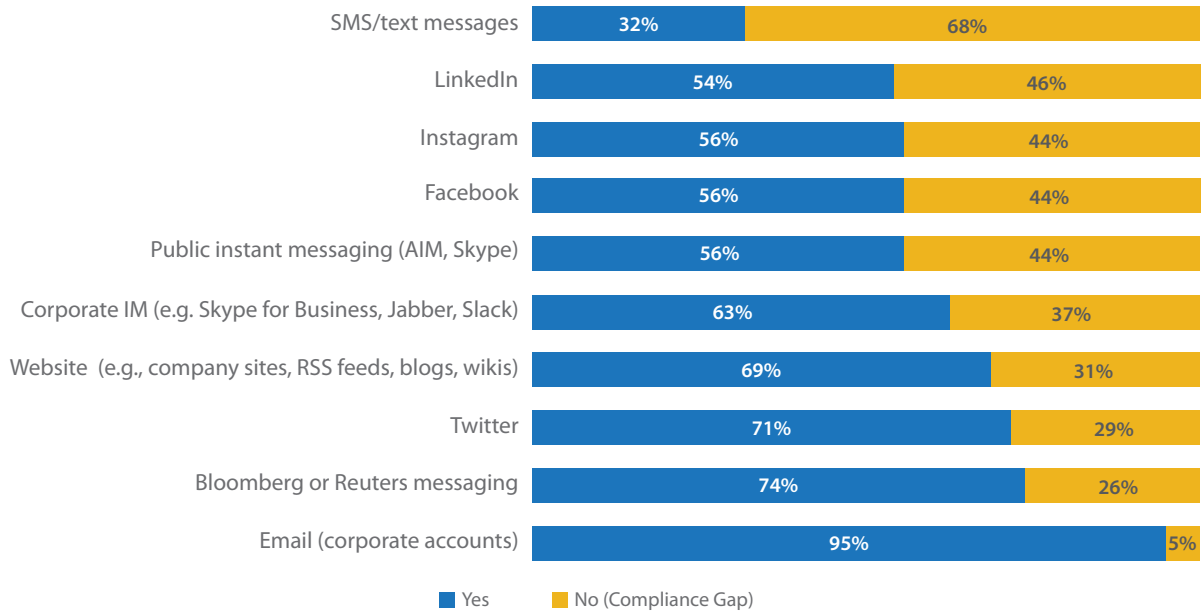
While compliance has made some progress to keep pace with these new channels – for instance, companies with policies governing the use of web conferencing platforms rose to 61 percent in 2016, up from 50 percent in 2015 – these gaps are not closing.

Three-year comparison: If allowed, archiving/supervision system in place



The percentage of firms that have archiving/supervision systems in place for new communications channels that employees are allowed to use for business has **remained stagnant**, and in some cases, gone down from 2014 to 2016.

2016 Compliance gaps: If allowed for business communications, is there an archiving/supervision solution in place?



Social Media

Almost half of respondents (48 percent) cited social media as the number one channel of perceived compliance risk. Even when a firm has banned social media channels, risks remain if employees do not adhere to the ban. In fact, the percentage of respondents who claim to have minimal or no confidence that they could prove the policy of prohibition is working ranges from 30 percent for LinkedIn to 41 percent for Facebook and 45 percent for Twitter.

Seventeen percent of respondents who allow but don't archive social media say archiving will create too much content for compliance to review. Twelve percent say they are waiting to see industry regulators enforce regulatory guidance around this channel. These approaches leave firms exposed to risk of non-compliance findings in the case of an examination.

Text Messaging/SMS

Despite the ubiquitous nature of text messaging, this communication channel presents the largest compliance gap. Similar to social media, confidence gaps abound for SMS/text messaging. Respondents report no or minimal confidence in the effectiveness of prohibition: 38 percent for SMS/text messages and 44 percent for Apple iMessage. A full 39 percent of those who allow but don't archive these messages said they are waiting for industry regulators to enforce guidance before they will begin archiving text messages.

93% **of smartphone owners use text messaging, making it the most widely used smartphone feature.**[4]

Instant Messaging

While instant messaging ranked third among the communications channels in perceived compliance risk, the survey data demonstrates that the risks are similar to the top two. Again, respondents have no or minimal confidence in the effectiveness of prohibition: 48 percent for public IM and 45 percent for corporate IM. Even when allowed, nearly half of companies (44 percent) do not have any archiving or supervision systems for public instant messaging services.

In addition, it is now difficult or impossible to archive communications from many popular consumer IM platforms, because of changes in service.

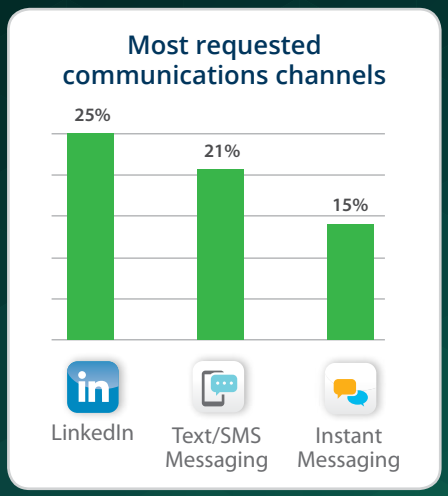
For example, Yahoo recently released a fully redesigned, web-based version of its consumer instant messaging client, Yahoo Messenger. With that release, Yahoo ended support of all prior versions of its Yahoo Messenger client. The new version of Yahoo Messenger can't be archived for retention and supervision of instant messages.

Besides email, type of content perceived as the source of the most compliance risk:

1. **Social Media**
2. **Text/SMS messaging**
3. **Instant messaging**
4. **Website content**

New Communications Channels Gaining Traction

Employees continue to request permission to use additional communications channels for business.



Email Archiving Lapses Still Widespread

While new channels are rightfully top-of-mind for compliance professionals, email is still prevalent in business communications and regulators are still paying attention to it, as demonstrated by a number of fines issued over the past year.

- A Missouri firm agreed to pay $2.6 million to settle charges of failure to retain email and other documents, including 168 million automatically generated notifications and mass marketing emails sent by third parties.
- A Pennsylvania firm was fined $20,000 for what FINRA described as an "honor system," in which brokers printed out emails for review by management. The firm, however, did not ensure compliance, and as a result, many email attachments, earlier referenced emails and personal emails were not retained.
- FINRA fined a New York firm $12,500 for not reviewing and retaining business messages sent through the personal email accounts of a registered rep and his assistant.[5]

Compliance departments are concerned about how their electronic communication supervision practices are keeping up.

Beyond the gap in retention/supervision systems, compliance risks also exist where policies are lacking or not understood, bans are not enforced, and archiving/supervision is not comprehensive or targeted to areas of true risk.

The past decade has introduced the following challenges to the traditional approach to supervision, which was originally designed for email:

- New content types
- Additional communications devices
- Exponential growth in message volume across all channels
- Further regulatory guidance
- Security and privacy concerns

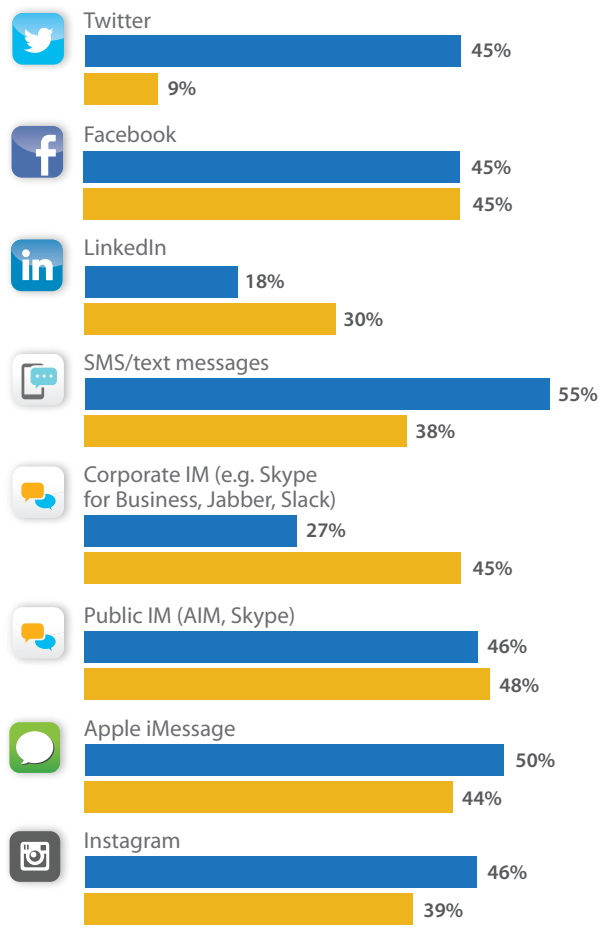
Electronic communications supervision critically affects how compliance delivers against its organizational mandate, so the supervision process must successfully incorporate solutions for these new components to fulfill its role in business risk management.

Compliance Gaps Lead to Confidence Gaps

This year's survey responses indicate compliance professionals are not optimistic that business risk is being identified. Less than half (43 percent) of respondents are mostly or completely confident their current supervision programs will effectively identify risks for their organization.

Whether new content types are allowed or not, compliance professionals report low confidence that their firm is in full compliance with regulatory requirements for these communications.

Firms lack confidence in ability to meet obligations for non-email channels



Breakdowns Across the Supervision Process

Gaps in electronic communications oversight programs threaten compliance's ability to identify and mitigate risk. Compliance professionals recognize these breakdowns, reflected in the concerns cited by respondents:

32% Inability to provide evidence of supervision

29% Policy enforcement

28% Inefficiencies of the supervision process

27% Fine-tuning supervision processes to find real risk

26% Inability to produce data upon request

21% Policy creation

> "Whilst we operate social media guidelines, sales or other staff may be using social media for work purposes outside of working hours on their own device. It's impossible to keep abreast of every business related communication."
>
> – 2016 survey respondent

Review efficiency and effectiveness is also a challenge for compliance teams. **A full 40 percent believe too many or way too many messages are flagged for review**, indicating there are either too few resources to effectively keep up with reviews, or too many false-positive search results taking up valuable compliance team time.

More Communications Formats, More Supervision Problems

The diversity of content types requiring supervision and their associated data formats also pose challenges. In addition to social media platforms such as LinkedIn and Twitter, compliance teams are faced with managing digital content in file-sharing platforms like Citrix Sharefile, from new messaging applications like Slack and from text messages.

Each new communications channel brings with it unique oversight challenges that don't correlate to existing email review processes. "Flattening" all electronic content into a standard email format – one approach – makes it harder to find specific items and understand their context. (This solution is fundamentally flawed. The conversion process alters the form of the record itself.) Compliance professionals recognize the value of maintaining messages in their native format – 50 percent of respondents stated that keeping messages in their native format is important or critically important.

Technology as Part of the Supervision Solution

Compliance professionals look to technology to help them address the challenges of the growing compliance perimeter. From efficiency and effectiveness improvements to policy and lexicon management, they recognize that many of their existing processes, especially manual ones, cannot scale for the growing volume of messages or adapt to the unique needs of each new communications channel.

Important or critically important attributes of electronic communications supervision technology, according to respondents:

65% Features designed to improve review efficiency and effectiveness

63% Single platform to manage and search messages from various communications channels (email, IM, social media, etc.)

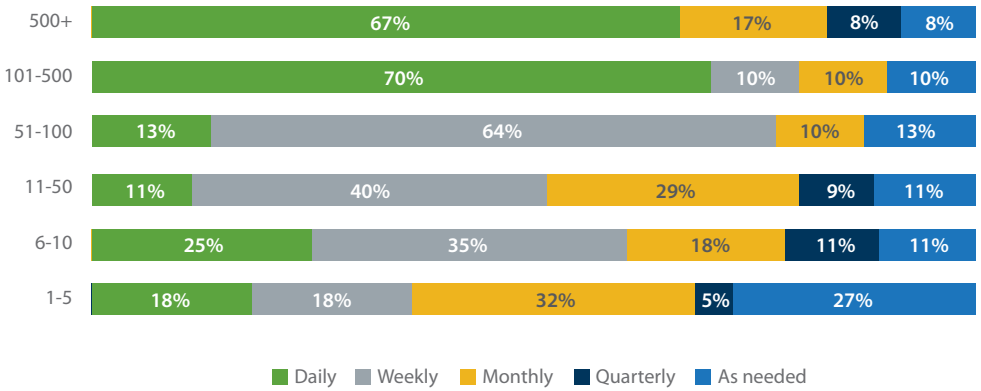
60% Support for new communications channels (such as social media, text messaging)

53% Policy/lexicon management

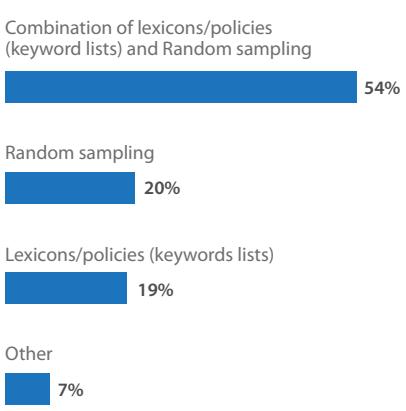
50% Keep messages in their native format

What are your peers doing for electronic communications supervision?

Frequency of message review by firm size



Supervision review models



From the Desk of the **CEO**

Smarsh has spent 15 years urging financial services firms to retain all electronic communications for compliance—regardless of the channel or the device of origin. Firms of all sizes must perform regular supervision procedures across an ever-widening set of content to make sure employees are operating within compliance boundaries.

As we analyze data from our own customer base and from the industry through projects including our annual Electronic Communications Compliance Survey, a series of conclusions surface that cause concern, individually and collectively. Set against the backdrop of increasing regulatory scrutiny, the conclusions weave a story that becomes downright troubling.

To put it bluntly, **SUPERVISION IS BROKEN.** (But, it can be fixed).

Small firms
More than a quarter of the survey respondents from the smallest firms (1-5 employees) purport to review electronic messages on an "as needed" basis. This is the classic "retain and respond" scenario, where these firms are only looking at the content in their archives with an examination or internal audit on the horizon. They're operating under the premise that simply having a repository of electronic communications is good enough.

In short, these firms are playing the odds. They're taking a calculated risk, that the time and resource cost of systematic supervision is better channeled into other activities, and worth more to the business than the threat of non-compliance.

I can't blame them. As a small business owner, I know as well as anyone that individuals must wear many hats (including compliance) and make difficult choices for the sake of the business. However, *hoping you don't get examined* is far from a sound business strategy.

Larger firms
Meanwhile, larger firms spend more time and resources—and in many cases, waste them—looking for risk in the wrong places. They have long-established surveillance procedures targeted primarily at email that are ineffective at worst and inefficient at best. Forty percent of respondents believe they have too many or way too many messages flagged for review.

The compliance perimeter
And scarier yet, while the volume of email to review only grows, the real risk that supervision is intended to reveal and mitigate is likely found elsewhere. As in what we call "outside the compliance perimeter"—in social media and text messages and other forms of electronic communications. For compliance, the supervision of new content types represents even more work. So, how are firms responding?

- **Prohibition.** There is still a large swath of registered firms that do not allow their employees to communicate via social or mobile channels. Even with a policy of prohibition, firms must still demonstrate to regulators that the policy is adhered to and enforced. This approach is ultimately unsustainable. The way today's investors want to communicate with their financial advisors is changing, and forward-thinking reps push their firms to provide them with the tools necessary to keep growing the business.
- **Head in the sand.** When regulators ask if a firm allows its employees to use social media, the response "not to my knowledge" is no longer acceptable. Our survey demonstrates there are still too many firms using new communications channels without retaining or supervising the content. This scenario is a ticking time bomb as examinations are on the rise. These firms are playing the odds, waiting for regulators to provide more guidance, or for their peers to receive penalties, before they get serious about tackling their oversight responsibilities.
- **Extend what's in place for email.** A screwdriver might be "good enough" when assembling a piece of furniture, but trying to build a house with the same screwdriver is going to be a long, arduous process. In other words, if compliance is relying on already inefficient existing procedures – random samples and lexicons that haven't been updated in years—and applying them to email PLUS new and different types of communication, they're ultimately only creating more inefficiency for more people.

So how can firms—small and large—regularly conduct systematic supervision across more content? How can they do it in a way that strengthens the ability to identify and mitigate risk while also limiting the strain on human and capital resources?

(Continued on page 11)

The path forward

Firms have been slow to modernize their approach to electronic communications supervision, caused by simple inertia, a lack of resources to support a change in policy and procedure, or not knowing that an alternative approach exists.

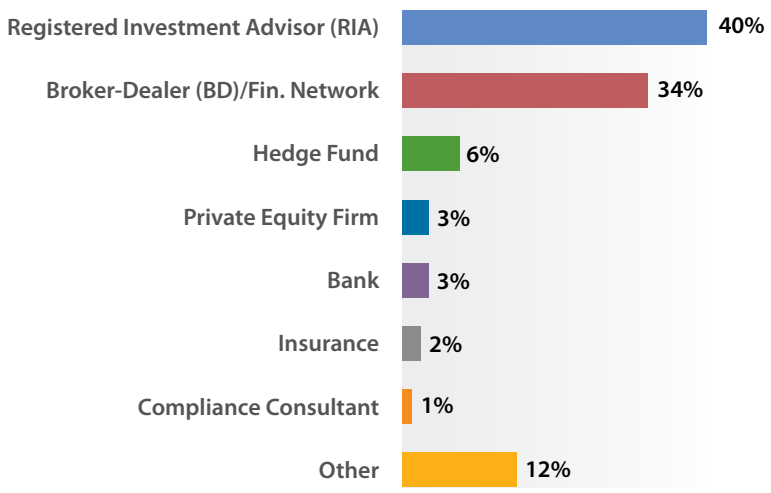
As I hear from clients and see in the survey results, compliance professionals are frustrated.

Creating a sustainable, scalable and holistic approach needed for effective electronic communications supervision today can't be done overnight, but it can be done. It requires the coordination of the right processes, technology and human capital across stakeholders from IT departments, compliance, legal and marketing units. This upfront work, however, will deliver strong ROI by reducing costs and resource needs while strengthening the effectiveness of supervision to find and address the real risk across all content types.

Those firms that recognize and invest in a future-proof supervision system will reap those rewards. The rest will continue to play the odds in the hopes that their number does not come up.

Stephen Marsh | CEO, Smarsh, Inc.

What type of firm do you work for?



1 FINRA (01/05/16) "2016 Regulatory and Examination Priorities Letter." Retrieved from https://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf

2 Sutherland Asbill & Brennan LLP (04/28/16) "FINRA's Record-breaking Fines and Sanctions of 2015." Retrieved from http://www.smarsh.com/webinars/finras-recordbreaking-fines-sanctions-2015/

3 (10/01/16) "CCO Banned from Role for Inadequate E-mail Reviews, Poor Compliance P&Ps." IAWatch.

4 InvestmentNews (07/09/14) "How advisers will communicate with clients in five years." Retrieved from http://www.investmentnews.com/article/20140709/BLOG18/140709934

5 (03/24/2016) "Cases Reveal Email Archiving Lapses, Solutions." IAWatch.

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

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

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

SURVEY METHODOLOGY

In February and March 2016, 221 individuals in financial services with direct compliance supervision responsibilities participated in a 36-question survey designed to identify current trends and to share insight on policies and practices about the retention, supervision and protection of electronic 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