2015
Electronic Communications Compliance Survey Report
Communications compliance practices and examination expectations among compliance professionals in financial services
KEY TAKEAWAYS

The Role of Compliance Grows to Solve New Business Challenges

New FINRA and SEC guidance has raised the profile of compliance and its ability to help prevent real risk within an organization. Its role now extends into other facets of the business. For instance, collaboration with IT and other departments to implement cybersecurity measures or to process e-discovery requests.

Firms Enable Greater Social and Mobile Engagement

Advisors need access to the electronic communications channels preferred by their clients. Firms are heeding the call, and compliance is making strides – though gaps remain – in managing the subsequent retention and oversight challenges.

RISK ALERT: Electronic Message Production Puts Firms at Risk

FINRA has placed timely production of requested data under the regulatory microscope. With the volume, variety and velocity of business records on the rise, compliance departments are concerned about the ability to produce data efficiently and are looking to technology to help alleviate this burden.
Executive Summary

Now in its fifth year, the Smarsh Electronic Communications Compliance Survey sheds light on the key trends and challenges facing compliance officers around the retention and supervision of electronic communications.

This year provided perspective on not only how much the landscape has changed in just half a decade, but which areas remain frustratingly the same. As predicted in previous years, there has been significant growth in the allowance and acceptance of new communications channels. As such, advisors and marketers have more choice in how, when and on what device or channel to communicate with clients, leading to more personalized and effective communications. As a result, compliance officers have watched the scope of e-comm retention and oversight responsibilities creep. Still, for a majority, overall confidence in the ability to manage these challenges is on the rise.

Is that confidence justified? Archiving solutions demonstrate their value most discernibly when put to the test – when requests for specific content must be produced in a reasonable and specified time period. The issue of data production is under FINRA’s microscope this year, as the self-regulatory organization explicitly called out the inability to provide data in the requested time “unacceptable” in its 2015 Exams Priorities Letter. Production has become more complex, and firms manage these growing pains in different ways.

At the same time, firms rely on their compliance departments to produce more data more often, and for more purposes. The business value of the data within the archive is being leveraged in new ways to reduce risk, and compliance is playing a larger role. Compliance also has a key seat at the table in initiatives centered around the red-hot topic of cybersecurity – both FINRA and the SEC issued guidance on the subject in 2015. This industry priority is fueling collaboration with departments such as IT, furthering elevating compliance’s profile and responsibilities across the organization.

LATEST REGULATORY UPDATES

- FINRA Rules 3110, 3120, 3150 and 3170
- FCA FG 15/4 Social media and customer communications (UK)
- FFIEC – Social Media: Consumer Compliance Risk Management Guidance

Regulations Governing Electronic Communications Include:

- SEC Rules 17a3 and 17a4 of the Securities and Exchange Act of 1934
- FINRA Rule 2210 and 2212-2216
- 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, 11-39 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)
- 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, BCOSBS2, MCOB3 and ICOBS (UK)
The success of financial advisors can hinge on how effectively they communicate with clients. These conversations often take place outside the office and via channels other than email. Today’s advisors are thinking “outside the inbox” and reaching clients through LinkedIn or Twitter, among other channels, and often from a mobile device.

In the past, compliance officers approached new communications channels with trepidation. The content of the message – not the channel, the owner of the account, or the device it was delivered on – determines whether the message is a record. Each new social network or mobile device added complexity, volume and technological challenges, and oftentimes use went ignored. Or, if compliance couldn’t retain and review communication through a given channel, a customary practice was to simply not allow it. For example, in 2011, just 39 percent of respondents allowed LinkedIn compared to 72 percent today.

As a result, compliance often found itself perceived as a barrier to marketing innovation. Clearly times have changed. Compliance officers have moved away from fearing the potential threat from digital channels. For the first time in five years, new and emerging channels was cited as a concern for less than half of the respondents. The “big three” social media channels—Facebook, Twitter and LinkedIn—were all permitted for business communications at higher rates than last year, with LinkedIn experiencing the greatest increase (11.5 percent).

Part of social media’s unique value is its ability to facilitate personal relationships. Firms are not only permitting employees to conduct more social business, but empowering advisors to conduct business communication through personal social media accounts (rather than limiting deployment to “company pages” only, for instance), thus strengthening the relationship between client and advisor.

In the past, compliance officers approached new communications channels with trepidation. The content of the message – not the channel, the owner of the account, or the device it was delivered on – determines whether the message is a record. Each new social network or mobile device added complexity, volume and technological challenges, and oftentimes use went ignored. Or, if compliance couldn’t retain and review communication through a given channel, a customary practice was to simply not allow it. For example, in 2011, just 39 percent of respondents allowed LinkedIn compared to 72 percent today. As a result, compliance often found itself perceived as a barrier to marketing innovation.

Clearly times have changed. Compliance officers have moved away from fearing the potential threat from digital channels. For the first time in five years, new and emerging channels was cited as a concern for less than half of the respondents. The “big three” social media channels—Facebook, Twitter and LinkedIn—were all permitted for business communications at higher rates than last year, with LinkedIn experiencing the greatest increase (11.5 percent).

Part of social media’s unique value is its ability to facilitate personal relationships. Firms are not only permitting employees to conduct more social business, but empowering advisors to conduct business communication through personal social media accounts (rather than limiting deployment to “company pages” only, for instance), thus strengthening the relationship between client and advisor.

Firms must retain and monitor content from individual social media accounts just as they do corporate ones, and advisors must understand that their firm will be supervising their personal accounts and retaining a record of them. A compliance gap remains – an average of 32 percent of firms that allow business communication through personal social media accounts do not have a social media archiving/supervision solution in place. The gap is 13 percent larger for firms that don’t allow personal channels (but do allow corporate pages for business communication).

Among Firms That Allow the Channel, What Percentage Allow Personal Pages for Business Communication?

<table>
<thead>
<tr>
<th>Channel</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn</td>
<td>80%</td>
</tr>
<tr>
<td>Twitter</td>
<td>64%</td>
</tr>
</tbody>
</table>

OnCall Advisors is a group of physician and dentist only financial consultants who have provided trusted advice to thousands of doctors and practices from around the globe. Part of the firm’s marketing strategy includes the use of social media, including LinkedIn, Twitter, Facebook and Pinterest.

“We’ve been using LinkedIn as far back as I can remember,” said Dustin Karas, relationship manager at OnCall. “Of all the social media outlets, LinkedIn has definitely been the most successful.”

Through Karas’ LinkedIn efforts – which he manages on both his personal page and the firm’s corporate page—he has seen tangible results, such as new business leads and thought leadership opportunities.

“A large hospital once contacted us to host a seminar on financial planning for them after seeing our content and posts on LinkedIn,” Karas said. “It opened up a whole new door for our business.”

Another example of LinkedIn success comes from Heron Financial. “I want to know my clients before I ever meet them,” said David Edwards, founder and president of Heron Financial. Heron doubled its assets over the last two years by effectively utilizing LinkedIn and other forms of social media to enhance a targeted marketing effort. “Potential clients appreciate it when I educate myself about their business and personal information they make public. I want to know as much as I can about a person before I call them.”
The shift from fear to flexibility didn’t happen overnight. Since the inception of this survey in 2011, compliance officers have been steadily moving from prohibition to permission. Year over year, the path remains the same: firms institute a policy to govern usage of these channels, enable usage for business communications, and implement a retention and oversight system to enforce policy.

Since 2011, LinkedIn enjoyed the greatest increase in allowed usage, at 33 percent, closely followed by Twitter, then Facebook.

As allowance of social channels has grown, so has the percentage of firms with policies to regulate the channels’ use. In five years, policy creation has more than doubled across allowed social channels.

In 2011, only 17 percent of firms archived at least one of LinkedIn, Facebook or Twitter. The next year that grew to an average of 30 percent archiving at least one channel, and today it’s at 61 percent. While the growth in policy and enforcement technology is trending in the right direction, a compliance gap still remains. An average of 39 percent of respondents that allow social channels do not have an archiving/supervision solution in place for social media.

BRING YOUR OWN DEVICE (BYOD) AT MASS ACCEPTANCE

Social media isn’t the only place where firms are becoming more flexible around advisor needs. This year, allowance of personal devices for business communications is up 17 percent from last year, and 73 percent of respondents have a policy about BYOD, compared to 58 percent last year.

RISK ALERT:
Text Messaging Gap Still Alarms

The allowance of text messaging for business communications has yet to reach the level of acceptance of social media, but an InvestmentNews survey found that is likely to change. Eighty-five percent of investors own and use a smartphone regularly and 20 percent of surveyed investors under the age of 45 expect to be communicating with their advisors via text in five years.

Last year, survey response indicated that the usage of text messaging for business communications represented a significant compliance vulnerability. Over two-thirds of firms that allowed text messaging did not have a solution in place for retention and oversight, and unsurprisingly nearly 60 percent of those that allowed text messaging had minimal or no confidence in their ability to produce messages if requested.

This gap has narrowed, but not by a lot. This year’s survey indicates text message allowance is up by less than 2 percent, and adoption of text message oversight solutions is close to 5 percent. The compliance gap - the number of firms that allow text messaging for business communications but don’t have a system in place for retention/supervision - is still at an alarming 64 percent.

Respondents also have significantly less confidence in their ability to produce this content than any other electronic message. Client communication via text message is only going to increase, and compliance departments will want to find an effective solution to ensure they are retaining and supervising this content.
E-comm oversight is no longer just a checkbox “need to have” for compliance professionals. As electronic messaging channels have gained more prominence in business communications, firms are recognizing the value of this archived data, and the huge opportunity that message supervision presents to identify risk within an organization.

Seventy-two percent of respondents now believe message supervision is a critical tool to identify real risk in their organization, up 13 percent from last year. Eighty-one percent believe message supervision delivers valuable and actionable insights to the business, versus 65 percent last year.

Requests for data production from the archive are rising, and the reasons are growing.

Outside of a regulatory audit, litigation and e-discovery requests are the No. 1 reason digital communications data is leveraged, and 64 percent of respondents note their department is typically responsible for all noncompliance-related requests. Instances of seven or more such requests have risen by 16 percent since 2011.

Compliance leveraging the archive more often and for more reasons are not the only trends pointing to a broader narrative. The overall role for compliance in risk prevention is growing, as is compliance's impact on a business overall.

Over the past year, as FINRA and the SEC issued guidance on the need to address cybersecurity risk and preparedness, compliance continued to evolve its role in helping companies prepare for threats and develop plans to deal with an attack. In the past year, 83 percent of respondents participated in conversations about risks related to cybersecurity, and 58 percent expect their role to change as a result of managing such risks.

The list of cybersecurity concerns firms are facing – such as data encryption, detection of a breach, due diligence of third-party vendors, and data backup and retrieval – are intricately related in many cases to a comprehensive e-comm retention and supervision program.

With cybersecurity looming larger in their jobs, respondents indicated what concerned them most:

- **66%** preparing for targeted regulatory exams or regulatory scrutiny
- **53%** appropriate incident response planning and response to actual data breaches
- **50%** enforcing cybersecurity policies
The shift in compliance professionals’ top concerns shows that message supervision is moving from reactive to proactive. In 2015, as in 2011, new and changing regulations and increased scrutiny and enforcement by regulators remained among their top four concerns. But this year, balancing employee privacy considerations with oversight obligations and cybersecurity threats posed by use of electronic messaging platforms surfaced as top priorities.

**CONFIDENCE IN CYBERSECURITY PREPAREDNESS**

So how confident are respondents in their firm’s ability to meet the cybersecurity challenges? While firms still have a way to go, more than half of respondents are mostly to completely confident they are prepared to prevent and detect key cybersecurity risks.

**Top E-Comm Compliance Concerns in 2015**

- New and changing regulations
- Increased scrutiny by regulators
- Balancing employee privacy considerations with oversight obligations
- Cybersecurity threats posed by use of electronic messaging platforms

**Top E-Comm Compliance Concerns Five Years Ago**

- New and changing regulations
- Increased scrutiny by regulators
- New communications channels
- New communications devices

---

**Mostly to Completely Confident in Firm Preparedness For:**

- Malware attacks, including malicious attacks that infiltrate a network and exercise command/control with a significant impact that is hard to trace: 58%
- Traditional account takeover, including the hijacking of passwords and client user names: 62%
- General loss of client information and data, whether malicious or not: 66%
- Insider operational risks, including rogue employees penetrating business systems, or conducting illegal business operations: 66%
The production of data upon request, including e-communications, is an area of concern for regulators. FINRA recently highlighted the issue in its 2015 Regulatory Exams and Priorities Letter.

The 2015 Smarsh Electronic Communications Compliance Survey uncovered factors interfering with firms’ ability to produce e-comm data within a reasonable time period.

The No. 1 problem is the multiplicity of platforms used to retain this data. Compliance officers often deal with multiple digital channels and often multiple solutions for archiving/supervision, and this complexity is compounded by a general lack of understanding of the technology and limited staff resources.

As compliance officers look to close these gaps with electronic communications, they may want to consider those attributes in an archiving solution that have been cited as important to critically important in developing a comprehensive electronic message compliance program:

- **Interface usability**—ease of use
- **84.8%** Support for new communications channels such as social media, text messaging
- **84%** Features designed to improve review efficiency and effectiveness
- **83.2%** Single platform with which to manage and search messages from various communications channels

"Specifically, FINRA has experienced an increasing number of situations where some firms have repeatedly failed to provide timely responses to its information requests made in connection with examinations and investigations… These situations are not acceptable, as timely productions of information (as well as oral information through interviews and on-the-record testimony) are critical to FINRA achieving its investor protection and market integrity mission by identifying and shutting down bad practices and bad actors at the earliest possible time. FINRA reiterates firms’ obligation to respond to FINRA inquiries in a full and timely fashion, and cautions firms that production failures expose firms to disciplinary action."

— FINRA 2015 Regulatory Exams and Priorities Letter
The State of Regulatory Exams

According to the annual Sutherland Analysis of FINRA Sanctions, the number of overall sanctions was down year-to-year in 2014, but there was an increase in fines of 125 percent to $134 million, the most since 2005. The C-suite should also take notice that for the second year in a row, the number of people who were barred or suspended increased, this year by 15 percent.

Regulatory examinations are becoming more intensive as more types of information are being requested. The number of requested content types is up across the board, with email requests increasing by 13 percent (to 77 percent) compared to last year. Top message types requested are:

1. Email
2. Website pages (i.e. company sites, RSS feeds, blogs, wikis)
3. Instant messages (IMs)
4. Bloomberg or Reuters messages
5. Social media
6. Text/SMS messages

Supervision activity reports (proof of supervision), disaster recovery or business continuity plan (DR/BCP) and written supervisory procedures (WSP) remained the top three requested forms of related documentation. Requests for these materials are on the rise this year as well.

![Requested Related Documentation](image_url)
This year’s survey report illustrates that compliance is becoming more proactive and prominent in organizations’ overall risk mitigation efforts, including in the realm of cybersecurity.

Clearly, cybersecurity is not simply an IT or a CISO issue; it’s an area where compliance and security are converging. An overall cybersecurity strategy relies on the contributions of multiple stakeholders, aligned to tackle an unprecedented level of threat aimed at data, infrastructure and process. Compliance holds a key seat at this table.

With cybersecurity’s red-hot prominence in risk conversations, we asked respondents this year to gauge their confidence levels around preventing and detecting common cyber threats (page 7), such as:

- Traditional account takeover, including the high-jacking of passwords and client user names;
- Malware attacks, including malicious attacks that infiltrate a network and exercise command or control with a significant impact that’s hard to trace;
- Insider or operational risks, including rogue employees who penetrate business systems, or conduct illegal business operations;
- General loss of client information and data, whether malicious or not.

In each case, nearly 60 percent of respondents answered that they were mostly to completely confident in their ability to prevent and detect these threats. A word of caution, based on our experience and on how similar topics have scored over the past five years: recognize that you just don’t know what you don’t know. Confidence may not reflect reality. In many data breach cases, firms simply weren’t completely aware of all the risks. And in some instances, firms didn’t even know that a breach occurred.

Often, the gaps in security prevention and detection arise because threats evolve and change rapidly. To address this challenging environment head-on, we recommend firms undergo a third-party cybersecurity risk assessment, which can identify gaps, shine a light on threats that may be lurking and offer best practices to manage and mitigate them.

As firms work through their cybersecurity initiatives, they will undoubtedly also look to their current technology providers for guidance, assistance and assurance. We encourage firms to thoroughly review their vendors’ certifications and procedures—and digital and physical safeguards—that protect sensitive internal and public company data.

At Smarsh, our customers take great confidence from the network of security solutions deployed within our data centers and solutions. Rather than having to establish one-off relationships with a multitude of point security products or service providers on their own, Smarsh customers leverage our best-of-breed technology solutions and those of our ecosystem partners – all designed to protect their data at all times.

As compliance becomes involved in more and more conversations around mitigating cyber threats, it can also look to the archive to help strengthen these initiatives. Beyond day-to-day surveillance procedures and increased usage for e-discovery, ongoing message supervision of all content types can be a front-line defense against common cybersecurity threats including phishing attempts, confidentially breaches, employee data leaks, and the compromise of social media accounts. This utility will only continue to grow, as more content (voice files, trade data) is managed within the archive and becomes available for supervision.

The electronic communications archive is no longer simply a check-the-box technology used to fulfill regulatory requests for firm data. Instead, archiving is now playing an increasingly important role in overall cybersecurity strategy and efforts by reducing and consolidating data silos across a growing number of content channels, and identifying risky communications or activity proactively - before they become serious and potentially damaging issues.

Stephen Marsh  |  CEO, Smarsh, Inc.
The 2015 Electronic Communications Compliance Survey

SURVEY METHODOLOGY

In February and March 2015, 274 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 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
- Cybersecurity

What type of firm do you work for?

<table>
<thead>
<tr>
<th>Type of Firm</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Investment Advisor (RIA)</td>
<td>64%</td>
</tr>
<tr>
<td>Broker-Dealer (BD)</td>
<td>38%</td>
</tr>
<tr>
<td>Insurance</td>
<td>8%</td>
</tr>
<tr>
<td>Hedge Fund</td>
<td>7%</td>
</tr>
<tr>
<td>Private Equity Firm</td>
<td>4%</td>
</tr>
<tr>
<td>Bank</td>
<td>2%</td>
</tr>
<tr>
<td>Compliance Consultant</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>8%</td>
</tr>
</tbody>
</table>


Smarsh delivers cloud-based archiving solutions for the information-driven enterprise. Its centralized platform provides a unified compliance and e-discovery workflow across the entire range of digital communications, including email, public and enterprise 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, Ore, with offices in New York, Atlanta, Boston, Los Angeles and London.