Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Social media & electronic messaging:

Know your risk

An e-Book publication sponsored by proofpoint.

About us

COMPLIANCE WEEK

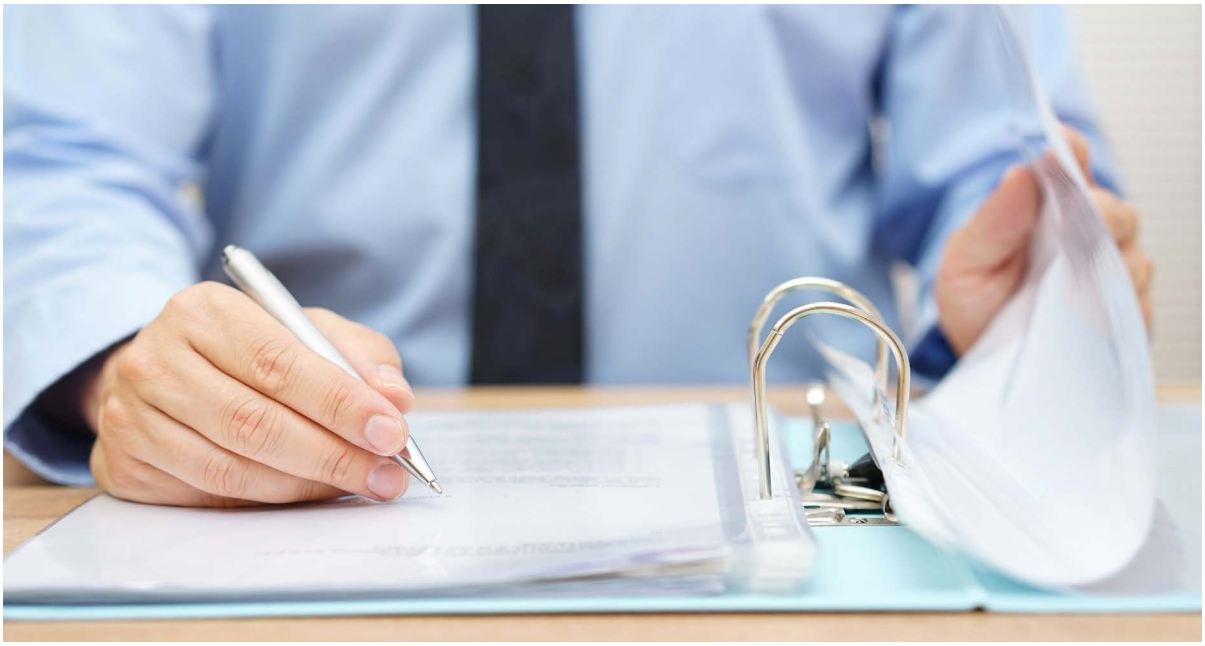
Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

proofpoint.

Proofpoint is a next-generation cybersecurity company that protects your people, data and brand against advanced threats and compliance risks. Built on the cloud and the world's most advanced intelligence platform, their solutions help you effectively detect and block targeted attacks and respond quickly to suspected compromises.

Inside this e-Book



The revised FCPA Corporate Enforcement Policy

The DOJ has made several notable revisions to its FCPA Corporate Enforcement Policy surrounding M&A, messaging apps, and much more, writes **Jaclyn Jaeger**.

The Department of Justice earlier this month made several notable revisions to its Corporate Enforcement Policy that are worth a closer look, as these changes could impact how compliance officers and general counsel choose to resolve Foreign Corrupt Practices Act matters.

On March 8, Assistant Attorney General Brian Benczkowski in remarks delivered at the ABA National Institute on White-Collar Crime Conference cryptically said the Justice Department was "currently in the process of updating the FCPA Corporate Enforcement Policy to bring it in line with current practice." It was on that same day with little fanfare that a variety of revisions were made.

The original FCPA Corporate Enforcement Policy was implemented in November 2017 to give the compliance and legal community greater transparency and consistency around how the Criminal Division's Fraud Section measures and credits voluntary self-disclosure, cooperation, and remediation efforts in criminal matters. The revised policy adds new language covering everything from self-disclosure and cooperation credit to its interactions with corporate counsel during internal investigations.

One of the more notable changes under the revised policy from a compliance standpoint pertains

to the requirement concerning retention of business records. Under the original policy, demonstrating "appropriate retention of business records" included "prohibiting employees from using software that generates but does not appropriately retain business records or communications."

This provision, which effectively put a blanket ban on the use of all messaging platforms, was immediately and widely criticized by companies and the corporate defense bar as overbroad and unrealistic, especially for multinational companies operating in countries where messaging apps—such as the widespread use of WeChat in China and WhatsApp in Brazil—are routinely used for, and are an indispensable part of, legitimate business communications.

"A lot of companies didn't have any policies addressing this," says James Koukios, former senior deputy chief of the Fraud Section at the DOJ and now a partner at law firm Morrison Foerster. For companies that did have such policies, they were essentially loose policies that wouldn't have stood up to the "very strict guidelines" that the Justice Department had outlined in the FCPA Corporate Enforcement Policy, he says.

So, it's with great relief that the revised policy softens the Justice Department's stance on this restriction by acknowledging these concerns and, instead, calls on companies to implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."

The revised policy effectively leaves it in the hands of companies to decide what communication avenues work best for their own operations. It also means, however, that compliance officers must carefully consider what policies and procedures need to be put in place to ensure the proper retention of business records to satisfy the Justice Department's expectations.

Shamoil Shipchandler, a partner at law firm Jones Day, recommends that compliance officers consider the following measures:

- Ensure the company has a specific business justification for using ephemeral messaging platforms, taking into consideration the company's legal and regulatory risks.
- Carefully craft written policies governing the use, safeguarding, and retention of ephemeral messaging, including clear guidance as to when the use of ephemeral messaging is appropriate (e.g., logistics purposes) and when it is not (e.g., substantive communications).
- If the company allows employees to use their own devices for business communications, carefully craft "Bring Your Own Device" policies that apply specifically to the use of ephemeral messaging.
- Provide regular training on the appropriate use of ephemeral messaging, and document that training.
- Periodically test and audit the use of ephemeral messaging.
- Discipline employees who violate company policies related to ephemeral messaging and record those disciplinary actions.

It's also important to keep in mind that, while the Department of Justice acknowledges there are legitimate business purposes for using messaging apps, the Securities and Exchange Commission does not provide that carveout right now. In December 2018, the SEC's Office of Compliance Inspections and Examinations issued a risk alert in which it reminded advisors "to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with applicable regulatory requirements."

To meet the record retention obligations under the books-and-records rule, the SEC recommended in that risk alert that advisers prohibit the business use of apps and other technologies that "can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up."

"The broad takeaway is that people who are registered with the Commission—like investment advisors or broker dealers—probably need to stay away from ephemeral messaging apps right now."

Shamoil Shipchandler, Partner, Jones Day

Shipchandler, a former SEC senior officer, says the warning here is that SEC-registered broker-dealers and investment advisers should continue to practice great caution concerning the use of messaging apps. "While the risk alert is not a position statement by the Commission itself, it demonstrates how line examiners are going to be evaluating policies and procedures, especially around messaging apps," he says. "The broad takeaway is that people who are registered with the Commission—like investment advisors or broker dealers—probably need to stay away from ephemeral messaging apps right now."

M&A due diligence

A second notable revision memorializes the agency's earlier position concerning cooperation credit in the context of mergers and acquisitions. While companies have always known they can engage with the Justice Department concerning potential successor liability issues, the benefits were never formally stated.

The new policy now clearly states that "there will be a presumption of a declination" where a company undertakes a merger or acquisition and uncovers misconduct "through thorough and timely due diligence or, in appropriate instances, through post-acquisition audits or compliance integration efforts, and voluntarily self-discloses the misconduct and otherwise takes action consistent with this policy (including, among other requirements, the timely implementation of an effective compliance program at the merged or acquired entity)."

In an additional footnote, the Justice Department added, "in appropriate cases, an acquiring company that discloses misconduct may be eligible for a declination, even if aggravating circumstances existed as to the acquired entity."

The policy change reflects remarks made in 2018 by Deputy Assistant Attorney General Matthew Miner, announcing the agency's intent to apply the principles contained in the FCPA Corporate Enforcement Policy to successor companies that disclose wrongdoing uncovered in connection with mergers and acquisitions. "We believe this approach provides companies and their advisors greater certainty when deciding whether to go forward with a foreign acquisition or merger, as well as in determining how to approach wrongdoing discovered subsequent to a deal," he said.

In a third change to the policy, new language has been added that now states that, to receive credit for voluntary self-disclosure in FCPA matters, a company must disclose "all relevant facts known to it, including all relevant facts about individuals substantially involved in or responsible for the violation of law." This revision was made simply to harmonize the Corporate Enforcement Policy with language that previously had been added to the Yates Memo in November 2018.

"[W]e now make clear that investigations should not be delayed merely to collect information about individuals whose involvement was not substantial, and who are not likely to be prosecuted," Deputy Attorney General Rod Rosenstein said when he first unveiled the changes in the Yates Memo.

At a high level, anytime the Department of Justice is responsive to comments and criticism from the business community and shows a willingness to refine its policies where practical and appropriate, that's always a welcome development for the legal and compliance community. ■

Handling an unpredictable CEO like Elon Musk

There are activist CEOs and rogue CEOs. Then there's Elon Musk, whose name came up quite often in a CW panel discussion about what to do when a leader goes off the rails. **Kyle Brasseur** has more.

There are activist CEOs and rogue CEOs. And then there's Tesla's Elon Musk. Musk, co-founder and CEO at the electric car maker, has repeatedly run afoul of the Securities and Exchange Commission in the last year via his personal social posts on Twitter. His "considering taking Tesla private" tweet resulted in his ousting as chairman of the company's board on top of a $20 million fine, and he egged the regulatory agency on even further in February with a production-related tweet that it felt violated a settlement previously reached between the two sides.

Throughout his lengthy standoff with the SEC, Musk remained defiant, often mocking the agency in tweets and saying he has "no respect" for it in an interview with "60 Minutes." Putting himself in the SEC's crosshairs hasn't appeared to faze Musk, though back at Tesla someone's stomach is surely turning.

"God help whomever that person is," said Carol Nolan Drake, president and CEO at board- and investor-focused firm Carlow Consulting.

Drake was part of a three-person discussion on the "Activist C-suite" session at Compliance Week's 2019 annual conference in Washington D.C. last month. The panel analyzed navigating disclosure in the age of corporate purpose, citing examples of both good and bad of senior leadership at companies taking a stand on certain issues.

Of course, it didn't take long for Musk's name to come up in a discussion of what to do when the CEO goes off the rails.

"Elon is going to do what he wants to do," said Drake. "He's such a brilliant person that there are many who will give him a pass and think that the SEC is being unreasonable, even if he's tweeting about stock prices and potential opportunities to acquire companies—the things you and I would say, 'We should never be talking about that on social media. That's insider information you shouldn't share.' "

"But is he allowed to get away with it because he is so brilliant? The answer is no."

David Dragics, senior vice president of investor relations at information technology company CACI from 1998-2018, echoed that sentiment, referring to Musk's behavior as more of an "ego thing." In that case, he says, it becomes a matter of control for the company.

"It then goes to the board, because what the CEO is doing gets back to reputation—damaging the reputation of the company by his comments," Dragics said. "As you saw in the Musk situation, the SEC came down and said the general counsel has to approve his tweets and everything like that. That's an embarrassment, and it's something you want to avoid."

Dragics continued, "Obviously, Tesla has lost a lot of market value, some of it due to Musk, but also from a production standpoint as well. If you're having production problems, what is the CEO doing going over here being rogue as opposed to paying attention to getting the business operating better? It gets back to staying in your swim lane."

Looking past Tesla and at companies in general, the losses go beyond market value and making or breaking a quarter, noted Sally Curley, CEO of investor relations and environmental, social, and governance (ESG) advisory firm CGIR.

"The other thing too—and nobody has tried to

measure this—is the impact on employees, both existing and attracting new employees," she said. "Does that turn some employees off from pursuing your organization as a place they'd like to work?

"There's a fine line between what we would define as the activist C-suite or CEO, which is a purposeful and hopefully well-thought-out statement in support of or against something, versus a CEO or CFO, or board member for that matter, going off the script and doing their own thing."

Whomever is tasked with reining in the CEO at a company, slowing down the process is key, advised Dragics. "There's the first reaction; you want to guard against making that the permanent reaction," he said. Ideally, you protect yourself from someone coming back to you and asking, "Why didn't you warn us about this?"

Meanwhile, for companies where there isn't a clear individual in this role, there's an opportunity to own it from a risk management perspective, said Curley.

Determining whose job it is becomes key when considering the relative newness to the idea of the activist CEO. "About three years ago, this would not have been a discussion," said Curley. Yet, results from the 2018 Edelman Trust Barometer, which Curley cited, indicate 84 percent of people "expect CEOs to inform conversations and policy debates on one or more pressing societal issues, including jobs, the economy, automation, regulation, and globalization." In addition, 56 percent of respondents said they have no respect for a silent CEO.

"An activist CEO could be the best thing the company has had because people know where the company stands, assuming the board and everything else is in alignment," said Drake. "With the advent of social media and other pressures on companies from competition overseas, changing dynamics of the workforce, you have people coming into the market who want to find jobs and work for companies that they admire. That could be your company, and you have an opportunity to really shape that message."

The message isn't always well received though, as Gillette learned with its #MeToo-inspired Super Bowl ad earlier this year that called on men to do better in reference to toxic masculinity. Immediate backlash on social media resulted in the shaving company pulling the ad, and many men called for a boycott of the brand.

Uber has also felt social media's wrath, revealing recently in its initial public offering (IPO) prospectus that the #DeleteUber campaign in January 2017—which was sparked by the ride-sharing company's decision to turn off surge pricing to John F. Kennedy International Airport in New York amid protests following President Trump's travel ban—resulted in "hundreds of thousands" of customers deleting the app.

"That wasn't even the CEO at the time coming out publicly—it was just an action by the company in a very politically divisive timeframe," said Curley.

Nowadays, with more accessibility to CEOs, it often falls on their lap regardless. "It emanates from the top of the organization: Investors look at the CEO, and employees look at the CEO," explained Dragics. Though only one person may be the focus, however, it takes more behind the scenes to help toe the fine line between activist and rogue.

"Everybody has to be on the same page, and if you're not, you've got to lay the issues out, getting back to what's the issue and what are the consequences," Dragics said. ■

Navigating the treacherous social media landscape

A CW Webcast presented by Proofpoint explains why firms should monitor potential social media threats. **Aly McDevitt** has more.

In today's world, social media is an inevitable reality of conducting business. It should not be feared but approached with prudence, according to a Compliance Week Webcast, "Broker-Dealers on Social Media: Understanding the Risks," presented by Proofpoint.

Businesses should take advantage of social media—but tread carefully—says Roman Tobe, former manager of product marketing at Proofpoint. The regulatory minefields around business communications on social media are both dangerous and delicate, as watchdogs like the Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), Investment Industry Regulatory Authority of Canada (IIROC), and Financial Conduct Authority (FCA) have refined their rules over recent years.

Highly regulated industries are at an even greater risk on social media, the Webcast notes. They are targeted more frequently by watchdogs and hackers alike because these industries have access to regulated data. Therefore, regulators are paying attention to them—and they are major targets for cyber-attacks. Certain employees will be targeted by hackers looking to gain access to a firm's network, and it's probably not going to be the CEO or anyone else in the C-suite.

"When you're thinking about it from an attacker's point of view, going after the top targets might be the path of most resistance," Tobe says.

Ninety-three percent of breaches are attacks targeting individuals at an organization, according to the Webcast, with e-mail being the main vehicle of phishing attacks. Ninety-six percent of breaches targeting individuals occur via an e-mail exchange, where an employee opens an attachment or link leading to malware. In recent years, malicious URLs have outnumbered attachments, Tobe says.

"Everybody [at an organization] is fair game," Tobe says. There are no barriers to entry to opening a social media account, and fake accounts will often reach out to targets and build up trust before executing on their agenda.

Is an organization responsible, from a regulatory standpoint, for accounts claiming to be associated with an organization, but that are actually not?

"If you look at the RegTech guidance, [watchdogs] are saying you need to have control systems that look at your digital assets. … If there's a really prominent fake social account out there that's phishing customers, and you're not doing anything about it, at that point it may be up to debate," Tobe warns.

Companies also need to be aware of what their own employees are posting. If an employee posts something on social media involving misleading or sensitive information, the company needs to be able to flag and remove the post as soon as possible to comply with regulatory guidelines. Organizations must have internal policies in place that will allow them to "protect employees from themselves, essentially," Tobe says.

FINRA says companies need RegTech and AI-based tools to sufficiently monitor business communications across the social media landscape. Proofpoint offers regulatory technology that automatically detects profile changes and submits them for review within minutes; it also streamlines a review process with notifications for primary and secondary levels of reviews.

There's no getting around the fact that money can be made drumming up clients on LinkedIn, Facebook, Twitter, and other social media platforms. But as regulation around social media matures, businesses' social media policies and technological tools must mature with it. ■

proofpoint.

FINANCIAL SERVICES:

10 TIPS

TO MANAGING SOCIAL MEDIA COMPLIANCE

www.proofpoint.com

INTRODUCTION

Brand trust and customer engagement have always been the lifeblood of financial institutions (FIs). Today, they're more critical than ever as FIs expand customer engagement to new digital channels like social media.

The mission of financial services firms hasn't changed. But their risks have. FIs must now comply with evolving compliance regulations and guidelines related to social media.

The average FI has more than 300 social media accounts. At the same time, most have an expanding team of advisors who want to engage in social selling. With so many corporate accounts and associated employee social accounts, corporate governance and compliance can get complex. FIs need to ensure all these activities comply with communications and retention rules from FINRA, SEC, FCA, IIROC, and others.

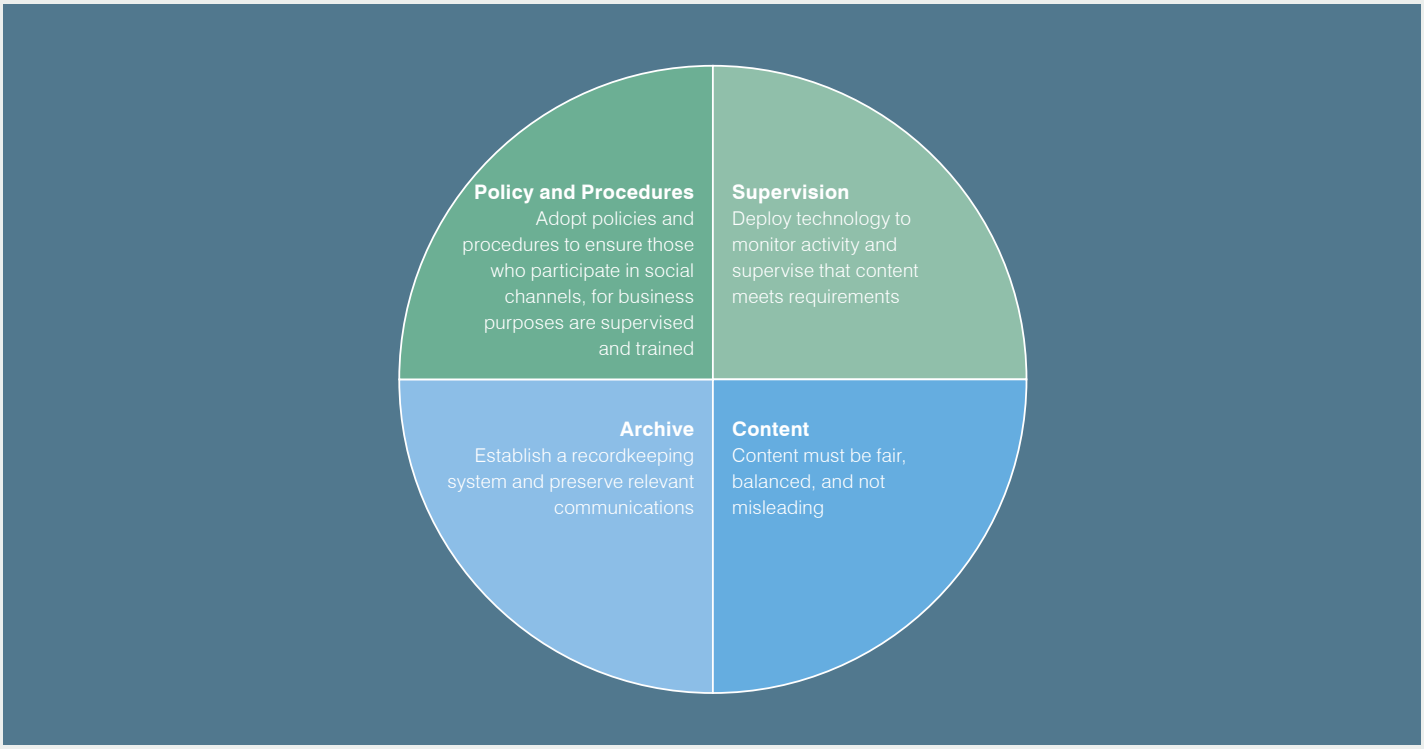
This e-book highlights key regulations and offers 10 tips for staying compliant.

SOCIAL MEDIA REGULATIONS AT A GLANCE

The primary regulations covering the financial services industry include:

- SEC
- FINRA
- FFIEC

While the language varies in each regulation, FIs need to manage social media processes across four primary categories—policies and procedures, supervision, content and archive.



10 TIPS TO STAY COMPLIANT ON SOCIAL MEDIA

You've got lots of employees and investment advisors engaging on social media.
Here are 10 steps to safely engage on social media and ensure compliance with financial services regulations:

TIP 1 KNOW YOUR SOCIAL MEDIA REGULATIONS

Social media is still a new communications medium compared to email, so some regulations are still changing.

You should acquaint yourself with the latest regulations. Your compliance officer and social media marketer should work together on the guidelines and decisions on how the business is using social media.

SPOTLIGHT

REGULATION—FINRA Rule 2210

Governs broker dealers' social media communications with the public and investors. Establishes standards for content, approvals, recordkeeping, and filing with FINRA.

TIP 2 ADOPT POLICY AND CONTROLS TO MONITOR AND SUPERVISE SOCIAL MEDIA COMMUNICATION

Most financial services regulatory guidelines require your organization to monitor its social media compliance efforts. Your corporate-owned social media accounts should be supervised (or monitored) to ensure the content and communications maintain compliance.

Other risk areas to monitor include:

- Cyber attacks
- Inadvertent sharing of personal information
- Embarrassing or inappropriate posts
- False or misleading content

SPOTLIGHT

FINRA Notices: 17-18, 11-39 and 10-06

- Monitor and supervise dynamic content that is used to engage in real-time interactive communications
- Firms can choose not to require approval prior to posting but should ensure that posts are fair, balanced, and not misleading
- Monitor and supervise third-party content

TIP 3

DEPLOY TECHNOLOGY TO CAPTURE AND RETAIN SOCIAL CONTENT

Many regulations that cover financial services (such as FFIEC, SEC, and FINRA) require you to establish a recordkeeping system for your digital communications. This includes social media.

The best approach is to classify content before archiving. This approach lets you search for all content or compliance violations without building a list of keywords for each requirement. This process should also be automated to save time and costs.

SPOTLIGHT

Securities Exchange Act Rules 17a-3 and 17a-4

Requires every member of a national securities exchange to preserve relevant communications for a period of not less than three years. For the first two years, it must be in an easily accessible place.

TIP 4 CREATE ACCEPTABLE USE POLICIES THAT ARE REINFORCED THROUGH TRAINING

Your employees and advisors want to make sure they're doing the right thing when they use social media. Build a social media acceptable-use policy that gives them guidance on compliance violations and how to avoid them.

Reinforce the policy with training. And reiterate how they should manage business communications on social media.

TIP 5 IMPLEMENT COMPLIANCE GUARDRAILS FOR YOUR SOCIAL SELLING PROGRAM

In the early days of social media, there was a firm line between personal and business use of social media. Now, financial services companies are taking steps to support their advisors in social selling without treading into an offer or promotion of securities.

Put the appropriate guardrails in place to enable your associated employees to engage in social selling. You must also regularly review and approve static content such as profiles and background images. Adopt tools that help automate your supervision and review efforts of designated social media profiles.

TIP 6

PROVIDE ACCESS TO COMPLIANT SOCIAL SELLING CONTENT

If you have plans to start a social selling program, you must ensure the social content complies with industry rules. The ideal way: provide your advisors with access to a library of pre-approved compliant content. You should also adopt review workflows to ensure new content complies with all regulations.

Articles on third-party sites can also be compelling content to share. According to FINRA, when you provide your advisors with links to third-party sites, you need to ensure it doesn't contain false or misleading content. So remember to include third-party content in your review process as well.

"CONTENT IS THE NEW CURRENCY IN SOCIAL SELLING."

Beth Wood, Vice President, Chief Marketing Officer, Individual Markets
The Guardian Life Insurance Company of America

TIP 7

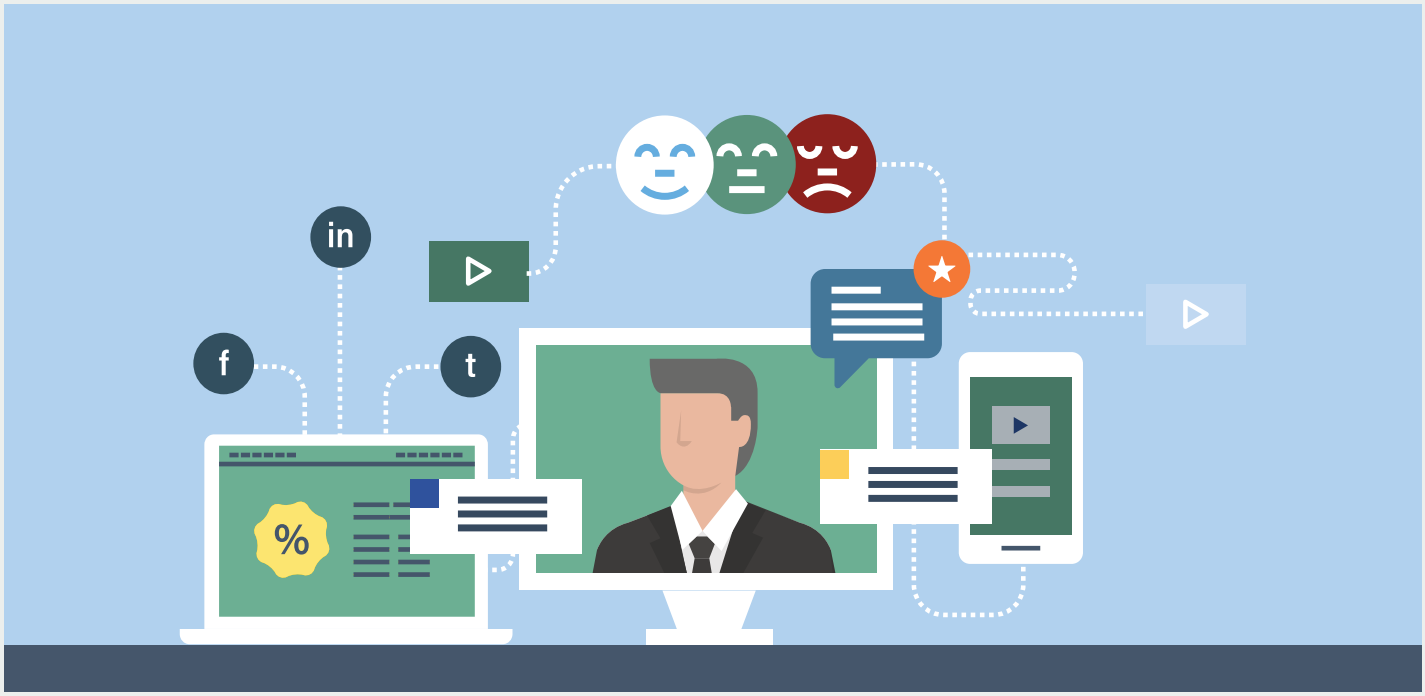
ADHERE TO FINRA'S RULES ON NATIVE ADVERTISING

Native advertising (a form of paid advertising that looks like an article) is allowed. But you must make it clear, conspicuous, and prominent that the content is an ad. The rules cover certain content standards, such as not being misleading and being upfront about paid ads.

TIP 8 ENSURE TESTIMONIALS MEET REGULATORY GUIDELINES

The use of testimonials on social media can get confusing. For advisors, SEC prohibits use of testimonials or referrals as part of social media advertisements and promotions. From FINRA's point of view, broker dealers may use customer testimonials in some specific circumstances and with proper disclosures.

Given the complexities in following two sets of rules, financial services companies tend to forbid the use of testimonials by policy. Your social media compliance tools should supervise endorsements as well.



TIP 9

ADOPT AUTOMATED CONTENT SUPERVISION TECHNOLOGY FOR YOUR STATIC AND DYNAMIC (INTERACTIVE) CONTENT

FINRA makes a distinction between static and interactive content. Static content, such as LinkedIn and Facebook profiles, require approval before being used for business. Interactive content, such as real-time posts and comments, may be supervised (or reviewed) after the fact.

Make sure you have technology that automatically supervises all content on your account for compliance. That includes anything you or your followers post as well as static content.

Financial regulation classifiers should detect issues and risks specific to your industry. This ensures your followers, partners, and customers are not mistakenly posting confidential or regulated data to your account. This approach provides the enforcement you need to avoid a violation.

TIP 10

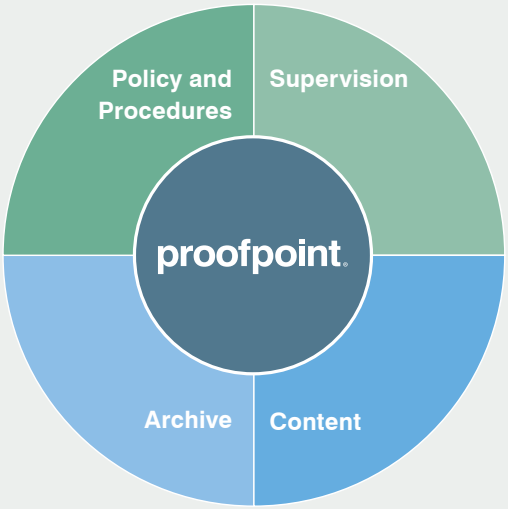
INCLUDE DATA PRIVACY, PROTECTION, AND CYBERSECURITY INTO YOUR COMPLIANCE PROCESSES

The intersection between privacy, cyber threats, and social media is very real. That's because bad actors thrive on social media as a forum to unleash brand fraud and cyber attacks. They also use social media to access your personal information based on what you post on social media.

These risks can lead to financial loss, reputational risk, and regulatory consequences. Integrate protection within your social compliance technology is a best-practices approach.

MANAGE SOCIAL MEDIA COMPLIANCE WITH PROOFPOINT

We automate financial services social media compliance supervision and record retention. With just a few clicks, pre-built financial services policy templates help you manage your social media compliance. We make it easy to manage review and approval workflows for pre- and post-published content.



Plus, all messages are automatically added to the archive—there is simply no easier way to meet social media compliance requests.

With Proofpoint Digital Compliance, you can:

- Apply policy and demonstrate compliance for FINRA, SEC, and more
- Automate compliance content scanning and enforcement across your social media properties
- Get detailed reporting for governance and compliance audits
- Capture and archive social media content, including communication between your advisors and their clients

No other solution makes it easier for FIs to safely engage on social media and stay compliant.

POLICY	SUPERVISION	CONTENT	ARCHIVE
End-to-end compliance platform that delivers social media best practice policy templates and customer success Delivers real-time monitoring to ensure policies are followed; enables firms to identify those who require additional training	Continuously monitors social accounts and identifies high-risk content; can remove it in seconds Out-of-the-box policy templates manage financial services compliance; no rule-writing or keyword lists needed Monitors RIA social profile accounts and automatically identifies testimonials in both pre- and post-published content	Provides streamlined approval workflow for stakeholders to pre-approve static content, including profiles and ads Provides immediate remediation of problematic content Provides a library of highly targeted content—both generated by internal and third-party staff	Automatically adds all messages to the archive with a single check box Captures and archives social content that constitutes advertising, sales literature, and correspondence Allows you to preserve social content for a period of at least six years per FINRA rules in SEA 17a-4 Ensures information is available for immediate access by compliance team or regulator

PROOFPOINT DIGITAL COMPLIANCE

Learn more
proofpoint.com/digital-compliance

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

OCIE: Mitigating the risks of electronic messaging

Jaclyn Jaeger explores the Office of Compliance Inspections & Examinations' insights into thwarting employee messaging risk.

Registered investment advisers will want to pay attention to some recent observations shared by the Office of Compliance Inspections and Examinations following an examination initiative it conducted that offers some key insights for firms to consider as they look to strengthen their supervisory, compliance, and risk-management practices related to the use of electronic messaging systems.

In December, the OCIE issued a Risk Alert focused on registered investment advisers to better understand the various forms of electronic messaging they use, the risks of such use, and the challenges in complying with certain provisions of the Investment Advisers Act. The OCIE conducted the examination initiative because it noticed an increasing use of various types of electronic messaging by adviser personnel for business-related communications.

"The purpose of this Risk Alert is to remind advisers of their obligations when their personnel use electronic messaging and to help advisers improve their systems, policies, and procedures by sharing the staff's observations from these examinations," the OCIE said.

Advisers Act Rule 204-2 (Books and Records Rule) requires advisers to make and keep certain books and records relating to their investment advisory

business, including typical accounting and other business records as required by the Commission. Additionally, Advisers Act Rule 206(4)-7 (Compliance Rule) requires advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act.

According to the OCIE, several changes in the way mobile and personally owned devices are used pose challenges for advisers in meeting their obligations under these two rules. "These changes include the increasing use of social media, texting, and other types of electronic messaging apps, and the pervasive use of mobile and personally owned devices for business purposes," the OCIE stated.

OCIE's examination initiative focused on whether and to what extent advisers complied with the Books and Records Rule and adopted and implemented policies and procedures as required by the Compliance Rule. During the initiative, the staff observed a range of practices with respect to electronic communications, including advisers that did not conduct any testing or monitoring to ensure compliance with firm policies and procedures.

The staff identified the following practices that it believes might assist advisers in meeting their record retention obligations under the Books and Records Rule and their implementation and design of policies and procedures under the Compliance Rule:

Policies and procedures

- Permitting only those forms of electronic communication for business purposes that the adviser determines can be used in compliance with the books and records requirements of the Advisers Act.
- Specifically prohibiting business use of apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or backup.
- In the event that an employee receives an electronic message using a form of communication prohibited by the firm for business purposes, requiring in-firm procedures that the employee move those messages to another electronic system that the adviser determines can be used in compliance with its books and records obligations, and including specific instructions to employees on how to do so.
- Where advisers permit the use of personally owned mobile devices for business purposes, adopting and implementing policies and procedures addressing such use with respect to, for example, social media, instant messaging, texting, personal e-mail, personal Websites, and information security.
- If advisers permit their personnel to use social media, personal e-mail accounts, or personal Websites for business purposes, adopting and implementing policies and procedures for the monitoring, review, and retention of such electronic communications.
- Including a statement in policies and procedures informing employees that violations may result in discipline or dismissal.

Employee training and attestations

- Requiring personnel to complete training on the adviser's policies and procedures regarding prohibitions and limitations placed on the use of electronic messaging and electronic apps and the adviser's disciplinary consequences of violating these procedures.
- Obtaining attestations from personnel at the commencement of employment with the adviser and regularly thereafter that employees (i) have completed all of the required training on electronic messaging, (ii) have complied with all such requirements, and (iii) commit to do so in the future.
- Providing regular reminders to employees of what is permitted and prohibited under the adviser's policies and procedures with respect to electronic messaging.
- Soliciting feedback from personnel as to what forms of messaging are requested by clients and service providers for the adviser to assess their

risks and how those forms of communication may be incorporated into the adviser's policies.

Supervisory review

» For advisers that permit use of social media, personal e-mail, or personal Websites for business purposes, contracting with software vendors to (i) monitor the social media posts, e-mails, or Websites, (ii) archive such business communications to ensure compliance with record retention rules, and (iii) ensure that they have the capability to identify any changes to content and compare postings to a lexicon of key words and phrases.

It "encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with their regulatory requirements.

OCIE

» Regularly reviewing popular social media sites to identify if employees are using the media in a way not permitted by the adviser's policies. Such policies included prohibitions on using personal social media for business purposes or using it outside of the vendor services the adviser uses for monitoring and record retention.
» Running regular Internet searches or setting up automated alerts to notify the adviser when an employee's name or the adviser's name appears on a Website to identify potentially unauthorized advisory business being conducted online.
» Establishing a reporting program or other confidential means by which employees can report concerns about a colleague's electronic messaging, Website, or use of social media for business communications. Particularly with respect to social media, colleagues may be "connected" or "friends" with each other and see questionable or impermissible posts before compliance staff notes them during any monitoring.

Control over devices

» Requiring employees to obtain prior approval from the adviser's information technology or compliance staff before they can access firm e-mail servers or other business applications from personally owned devices. This may help advisers understand each employee's use of mobile devices to engage in advisory activities.
» Loading certain security apps or other software on company-issued or personally owned devices prior to allowing them to be used for business communications. Software is available that enables advisers to (i) "push" mandatory cybersecurity patches to the devices to better protect the devices from hacking or malware, (ii) monitor for prohibited apps, and (iii) "wipe" the device of all locally stored information if the device were lost or stolen.
» Allowing employees to access the adviser's email servers or other business applications only by virtual private networks or other security apps to segregate remote activity to help protect the adviser's servers from hackers or malware.

In conclusion, OCIE said the key message is that it "encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with their regulatory requirements. OCIE also encourages advisers to stay abreast of evolving technology and how they are meeting their regulatory requirements while utilizing new technology." ■

proofpoint.

Intelligent Compliance is Here

Meet regulation requirements with Proofpoint Social Media Compliance

Keeping up with today's requirements for compliance and governance is a challenge. And now this includes regulation for social media. From FINRA to FCC, it's crucial that you ensure compliance as you scale your social media efforts. Bridging the gap between social media compliance and marketing practice can be a big challenge. Fortunately, Proofpoint Social Media Protection software can help.

Visit us at proofpoint.com/us/solutions/social-media-compliance to learn more.