WHITE PAPER

The 6 Steps to Social Media Compliance

What You Need to Know Before You Go Social

A Publication by Hootsuite and Nexgate

Hootsuite™

NEXGATE

The 6 Steps to Social Media Compliance

What You Need to Know Before You Go Social

FINRA, the SEC, FFIEC, and the FDA—each has or is in the process of creating guidelines for social media communications to regulate organizations in their respective industries.

As social media marketing continues to grow, nearly two-thirds of the Fortune 500 is actively engaging customers, partners, and prospects on YouTube (69%), Facebook (70%), and Twitter (77%) and the use of Social Relationship Platforms to expedite this engagement is increasing. How will regulators influence their activity?

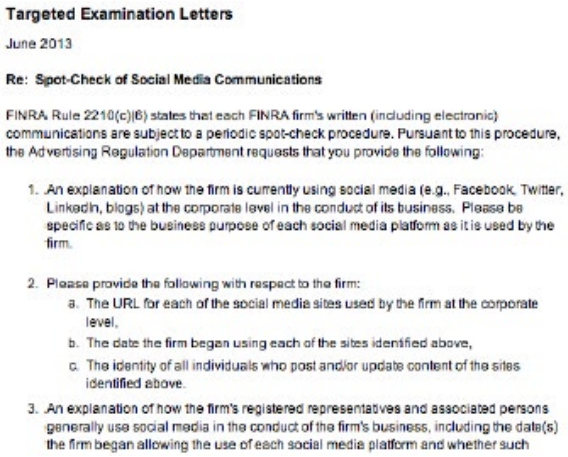
How Regulations Impact Social Organizations

Regulated industries—in particular, financial, health care, pharmaceutical, and insurance organizations—are under great pressure to leverage the power of social media to advance their business, yet fear of the ambiguity and uncertainty of emerging regulatory guidelines and requirements, as well as legal risks, can be disruptive, and violations can prove costly.

2/3 of the Fortune 500 are actively engaging customers on social channels.

For pharmaceutical organizations, for example, the FDA has two sets of guidelines governing their use of social media. Firstly, for adverse drug effect reporting, if a pharmaceutical company finds someone who is reporting adverse effects from its drugs—whether on its social media account or any other—the manufacturer must report it.

Secondly, for off-label information requests, such as a customer inquiring whether a drug will adversely react in combination with another drug or condition, the pharmaceutical company must be able to show that they saw the request and promptly responded to it with the appropriate information. Any failure to comply with either guideline may result in fines against the drug manufacturer.



Targeted Examination Letters

June 2013

Re: Spot-Check of Social Media Communications

FINRA Rule 2210(c)(6) states that each FINRA firm's written (including electronic) communications are subject to a periodic spot-check procedure. Pursuant to this procedure, the Advertising Regulation Department requests that you provide the following:

1. An explanation of how the firm is currently using social media (e.g., Facebook, Twitter, LinkedIn, blogs) at the corporate level in the conduct of its business. Please be specific as to the business purpose of each social media platform as it is used by the firm.

2. Please provide the following with respect to the firm:
   a. The URL for each of the social media sites used by the firm at the corporate level,
   b. The date the firm began using each of the sites identified above,
   c. The identity of all individuals who post and/or update content of the sites identified above.
3. An explanation of how the firm's registered representatives and associated persons generally use social media in the conduct of the firm's business, including the date(s) the firm began allowing the use of each social media platform and whether such

In another example, FINRA recently announced that it would initiate social media spot checks of its member organizations. The revelation was among the first to demonstrate how regulators would begin enforcing the application of guidelines across member organizations, and begged two questions:

1. How exactly will regulating bodies conduct such audits, and

2. How should regulated organizations explicitly enforce the stated guidelines, since most lack the requisite controls.

Despite the fear and uncertainty, many organizations are weighing the risks versus the rewards and taking the plunge. These organizations turn to Social Relationship Platforms to implement compliance controls to adhere to FINRA and other requirements.

Here are six steps to social media compliance to help bring clarity and mitigate your risk:

1. Know Your Regulations for Social Media

You and your compliance team likely have a good bearing on the regulations that impact your business, but how in tune are you with how they apply to social media?

Since it is a newer communications medium, many of today's regulations are just emerging and changing, and are somewhat vague as even the regulators grapple with the policy and its application. Many regulators, for example, realize that although they may create policy, companies need to have a way to enforce it. And in the social web, that's sometimes easier said than done. Thus, most regulations lack clarity, and most organizations lack the tools to enforce them.

Because these rules are relatively new and untested, few "best practices" have emerged for social. This means that organizations are taking it upon themselves to interpret how regulations could apply to their social media.

The more risk averse you are, the more conservative your interpretation should be.

Working together, your compliance officer and social media marketer should be able to arm one another with enough information about the guidelines and how the business is using social media and, weighing that against your tolerance to risk, define a set of policies and procedures to effectively address your compliance requirements.

2. Monitor Your Accounts

Most social media regulatory guidelines require that an organization monitor its compliance efforts. FINRA, for example, in its recently issued targeted examination letters, stated in the fifth request that member organizations provide, "an explanation of the measures that your firm has adopted to monitor compliance with the firm's social media policies."

Many organizations embrace technologies that allow for a diversified permissions set, and pre-approval before publishing to review the content disseminated on behalf of the enterprise for compliance. However, it's critical that the organization also monitor the posts and comments of its followers and fans—not just the content it distributes, as in the case of the FDA guidelines for drug manufacturers reporting on adverse effects.

What's more, what constitutes a brand-owned account can often surprise an organization. Individual employees, representatives, resellers, and partners often create social media accounts and affiliate them with the brand. The intent is typically innocent enough, but the implications are potentially risky. Imagine, for example, a drug representative making a local promotional page for her company's latest medication. It begs the questions:

1. Does the social media brand manager and/or compliance officer know this page exists?

2. Is the brand liable for claims or adverse risks reported on this page?

3. Does the brand have a means to discover this page and monitor it, even though it isn't under their control?

The last thing you as a brand owner or compliance officer want to find out is that there's an account or content you don't know about. Hence, it's critical that organizations monitor for brand-affiliated accounts and the content on them for social media regulatory compliance. A yearly social media audit by a third party organization is recommended.

It isn't helpful to use a publishing platform with compliance features if some or much of the content created completely bypasses that platform and is published directly or via another app.

3. Create Acceptable Content Use Policies

With an agreement as to how compliance regulations/guidelines impact your social media marketing, you should next create a set of Acceptable Content Use Policies (ACUP). Your ACUP (see example) should incorporate policy outlining how you and those you engage with on social media can adhere to your corporate compliance, as well as acceptable use policy for adult language, hate speech, inappropriate content, malicious links, and other risky content and activity.

Clearly documenting and displaying your ACUP puts a stake in the ground and demonstrates your conviction to create a safe and socially responsible community. Your policy isn't an instrument of censorship; rather, it's a statement describing what you will and will not stand for—an agreement, if you will, about the kind of relationship you'll have with your community.

In addition to providing public clarification around your policy, an ACUP will also provide internal guidance. Policies governing content on your accounts and channels should clearly articulate what constitutes a compliance violation, and what steps to take in the event of a violation.

As you build policies for compliance, you should consider not just the regulations that apply based on your local state or jurisdiction, but also of those states and countries where you do business. This undoubtedly complicates things, given the nature of the social web, which is inherently global. Nonetheless, from a legal and risk perspective, it's imperative to think globally when designing policy and to consider both regulated content and legal-risk content, such as personally identifiable information (PII).

4. Apply Content Controls to Enforce Your New ACUP

Policy without controls won't get you very far. As you create your ACUP, including the resultant actions you'd like to take based on the severity of a policy violation, you should also consider the mechanisms at your disposal to apply content controls.

Most organizations employ some sort of manual content moderation, whether done in-house, through a partner or service provider, or in a hybrid model. Whatever the means, manual content moderation can be expensive, exhausting, and inconsistent. Humans are fallible, and no matter how good someone is they can't be 100 percent accurate in detecting and remediating policy violations.

Many publishing tools provide workflow and built-in compliance controls, including the ability to detect (and archive) published content that may be risky to the business. Where these tools fall short, however, is the ability to detect content published to a social network outside of the publishing application. This is because the content classifiers of a publishing tool are built into the tool itself; thus, only content that passes through it is scanned, classified, and recorded.

A team consisting of personnel from IT, legal, risk, and marketing should gather on a regular basis to review policy violations, updates to regulations, and assess outcomes of your social media compliance program.

The average social enterprise has more than seven publishing tools in use, despite best practices which dictate standardizing around one. Thus, it's critical to lock your entire social media footprint into one secure platform.

5. Choose a Best-of-Breed Social Relationship Platform

Content classifiers built into publishing apps are typically limited, if available. Some of the more advanced publishing tools offer an array of classifiers, but many are relegated to detect content based solely on keywords. This leaves them prone to false positives, at the expense of significant resource requirements to build and maintain a keyword library or set of dictionaries, as well as sift through false positives and negatives. What's more, the absence of compliance-oriented content classifiers means your team will need to build multiple keyword lists for every policy you have—ACUP, security, and compliance-related.

Instead, the best approach to ensure you're accurately classifying content is to invest in a Social Relationship Platform that integrates with best-of-breed compliance technologies, enabling advanced data classifiers, including regular expressions, lexical analysis, and Natural Language Processing (NLP). These techniques provide the most accurate detection available—similar to what's used in other solutions like Data Loss Prevention (DLP), which is likely used for your existing corporate web and email infrastructure to detect confidential data that may egress your enterprise.

Each classifier should have an independent action setting in the event of a triggered policy violation, and should be template-based so you can select a policy with the check of a box, and not have to build and update them manually.

Most of the activity on an account isn't created by the account owner (i.e., you). Instead, most content is created by your fans and followers who respond to content you create and post or comment on your page. Thus, because that content—the majority of what's on your account—does not get published through your publishing tool, it doesn't get scanned for compliance.

To mitigate this risk and ensure you're reviewing all content on your page, channel, or account for compliance, it's important to have tools that analyze all content—anything you or your followers post—with data classifiers that are able to detect not only generic issues, but potential risks that are specific to your industry.

This way you can ensure that fans, followers, partners, customers, and prospects aren't mistakenly posting confidential, sensitive, or regulated data such as Personal Health Information (PHI) or Personally Identifiable Information (PII) to your account, in violation of a compliance regulation or guideline. This also addresses the issue raised in the example of pharmaceutical companies that must adhere to FDA regulations and report and respond to adverse drug effects, as well as customer inquiries.

Using technology to automate content moderation will serve several objectives. First, it'll alleviate the strain on your human resources from laboriously sifting through comments and replies, and let you instead leverage your personnel to respond to and engage with real customers, partners, and prospects. Second, it'll standardize the application of your compliance policy both within and across your social network accounts, including on Facebook, Twitter, Google+, YouTube, etc. This way you're consistently applying policy no matter the account or network, and adhering to your compliance requirements. And third, it'll ensure you're covering all content exchanged through social media communications both sent and received.

Recently, many states have started to pass laws that prohibit companies and schools from asking for passwords to social media accounts. While many have included exemptions for financial services companies, this is still a practice that causes resentment among employees, and opens the door to even more risk when those accounts (for example, Google) are linked to methods of payment. In a world where technology allows us to automate content moderation without requiring the user's password, why add another headache to an already-complicated problem?

6. Intelligently Archive Communications

One of the cornerstones of compliance is the ability to demonstrate it, and most regulating bodies require that you archive communications to do just that. Traditionally, archiving is done in the enterprise for all web, instant messaging (IM), and email communications. Enterprise archiving solutions integrate with the various communications technologies to capture, collect, and store these exchanges in the event of legal, investigative, or other inquiry. In some instances, these archives may be searched as part of an e-discovery project and used in court.

Like the web, IM, and email, social media communications for regulated organizations must also be archived. However, archiving all communications without any sort of intelligent classification system for the content would be akin to a library absent the Dewey Decimal System. How on earth would you ever find your book, or in this case, the right comment or post? Yet, this is how most social media archives work today.

Most social media archiving technologies collect and store all social communications in a dedicated social media archive. When it comes time to search and find explicit content, however, it can be quite tricky. You can have too wide or narrowly scoped searches, drive up e-discovery costs, and generally an inefficient archiving process. Without context, your archive and search process will be extremely inefficient, driving up e-discovery costs. What's more, because this archive is dedicated just to your social media, you don't get the efficiency of consolidating your archived social media communications along with all your other enterprise messaging.

Instead, the most effective and efficient course of action is to pre-classify content before archiving—again, using your advanced content classifiers—so that you can easily search for all FINRA or FFIEC content violations, for example, without having to build a list of keywords for each regulation/guidance requirement. This process should again be automated, and will save you tremendous time and costs.

Additionally, you should leverage your existing enterprise archiving solution and not a dedicated social media archive. It's more than likely your organization has already invested in an archiving solution for web, IM, and email communications, so why not leverage it versus buying and maintaining another, disparate solution just for social media?

Social media compliance is just now in its infancy. Like the many technology revolutions that have come before, it takes a while for governing bodies to fully scope out and enforce regulations detailing how organizations should comply. Nonetheless, it's critical that social media marketers, IT, and compliance officers work together to build and maintain a social compliance program now, and aggressively implement guidelines throughout the enterprise to mitigate risk and provide the best possible ROI to social media.

About Nexgate

Nexgate provides cloud-based brand protection and compliance for enterprise social media accounts. Its patent-pending technology seamlessly integrates with the leading social media platforms and applications to find and audit brand affiliated accounts, control connected applications, detect and remediate compliance risks, archive communications, and detect fraud and account hacking.

About Hootsuite Enterprise

Partner with Hootsuite to accelerate your social transformation

Hootsuite Enterprise empowers organizations to execute business strategies for the social media era. As the world's most widely used social relationship platform, Hootsuite Enterprise enables global businesses to scale social media activities across multiple teams, departments, and business units. Our versatile platform supports a thriving ecosystem of technology integrations, allowing businesses to extend social media into existing systems and programs.

We help organizations create deeper relationships with customers and draw meaningful insights from social media data. Innovating since day one, we continue to help businesses pioneer the social media landscape and accelerate their success through education and professional services.

Request a custom demo today by visiting enterprise.Hootsuite.com

Trusted by 744 of the Fortune 1000

WWF, Virgin, HBO, EUROSTAR, FOX, CBS Interactive, Allianz, IKEA, NHL, Nintendo, VICTORINOX, Mashable