NEXGATE
A Division of Proofpoint

State of Social Media Infrastructure Part III

A Compliance Analysis Fortune 100 Social Media Infrastructure

Executive Summary

- ***Nexgate performed a social media compliance analysis of Fortune 100 firms.*** The analysis examined social media content posted across a range of social platforms (Facebook, Twitter, LinkedIn, etc.) to determine the extent to which regulated or otherwise sensitive information was exposed to the public.
- ***The scale of social infrastructure is overwhelming limited staff assigned to review content for compliance risk.*** The average Fortune 100 firm now has 320 social media accounts. An average of 213,539 commenters (e.g. Followers, etc.) and over 1,159 employees make over 500,000 posts to these accounts.
- ***The average firm suffered from a total of 69 unmoderated compliance incidents during our 12 month research window.*** These incidents that went virtually unnoticed by internal compliance staff since they were posted and not removed from public social pages over during our 12 month window. An unknown number of additional incidents occurred but were removed by compliance staff before our scanners evaluated each account at the end of the period.
- ***Social media compliance violations can come from both employees and commenters.*** Employees accounted for 12 incidents per firm while public Commenters accounted for 57 incidents. FINRA financial service and FDA healthcare regulations are examples of standards with specific provisions covering Commenter postings. These requirements require much larger scale compliance operations than regulations applied only to Brand posts.
- ***Nine different U.S. regulatory standards triggered incidents*** including FINRA Retail Communications, FINRA Customer Response, FFIEC / Regulation Z, FTC Sweepstakes, and SEC Regulation FD
- ***Financial Services firms accounted for the largest incident volume with over 5000 incidents (over 250 per firm).*** This result is not surprising given that financial service firms are well represented in the Fortune 100 (21 firms), have shown strong social media adoption, and are subject to the most stringent social media communication standards.
- ***FDA Adverse Drug Experience Risks represented the most common healthcare social compliance risk with 98 incidents.*** Under FDA guidelines, healthcare firms are required to notify the FDA of any report of an adverse drug experience by a consumer. Healthcare organizations must therefore monitor social channels for such reports.
- ***Best practice social media compliance controls are inconsistently enforced.*** Only 47% of Brand posts were made via Marketing and Content Publishing applications. Beyond audience engagement, publishing applications include workflow that warns employees of compliance violations and public relations mistakes prior to posting.
- ***Informal culture, pace, scale, and complexity separate the social media compliance challenge from more static public communications channels such as press, Web site, and print.*** Ignoring these differences can overwhelm compliance staff and become a barrier to social success. As social programs grow within any organization, compliance staff needs to consider more dynamic, automated compliance processes.

Contents

The Social Media Compliance Landscape

Everywhere you look, corporate investments in social media are on the rise. Wealth advisors and insurance agents are building customer relationships. Retailers are selling product. The entertainment industry promotes new movies and music. Add it all up and the average Fortune 100 firm has over 320 branded social accounts with over 200,000 followers and 1500 employee participants[1].

However, increased investment in social also comes with increased compliance risk. Regulators recognize social media as public communication channel subject existing earnings disclosure, truth in advertising, and data privacy regulations. These requirements are designed to protect consumers from being misled or defrauded. In the United States alone, the FTC, SEC, FCA, FFIEC, FINRA, FDA, ABA and others have updated existing regulations to include specific social media provisions. These updates for social essentially mirror those applied to other communications such as the email, web sites, or print.

Unfortunately, social has grown so quickly and each network has so many modes of communication that compliance practitioners are finding it difficult to simply transfer existing process to the practical realities of social. The informal culture and pace of social discussion create an environment where well-meaning employees and customers are far more likely to make mistakes than other channels. They make "misleading statements" and share data that should not be shared. In addition, scale and complexity make policy, training, supervision, and even records retention more difficult than other channels. The firm is responsible for thousands of daily posts, made to hundreds of accounts, hosted on multiple social networks (Facebook, Twitter, LinkedIn, Google+, etc.). On top of all that, the firm is not only responsible for messages posted by employees, but also for those of partners and customers.

The informal culture and pace of social discussion create an environment where well-meaning employees and customers are far more likely to make mistakes than other channels.

Goals of This Report

To understand of how well early corporate social media compliance programs are functioning in a difficult environment, we analyzed 32,000+ social media accounts of Fortune 100 firms. This paper presents the results of that analysis. In the following pages, you'll find…

- A taxonomy of the most common compliance violations and the severity of each violation
- Real-world examples of common compliance violations
- Key compliance challenges, including what makes social media different from other communication channels such as Web site, email, print advertising, etc.
- Based on these key challenges, we recommend key steps that every organization should take to better manage social media compliance risk

Methodology

The first step of our analysis was to identify the corporate social media accounts associated with Fortune 100 firms. To accomplish that task we used Nexgate's SocialDiscover technology to connect to each major social network using APIs provided by those networks and perform a search of social media account profiles for Fortune 100 brand names (e.g. "Wal-Mart", "Exxon", etc.). Social networks searched include Facebook, Twitter, LinkedIn, Google+, YouTube, Pinterest, Instagram, and Tumbler. This initial discovery process yielded over 32,000 accounts.

We then used SocialDiscover to scan public account content for compliance incidents. Incidents were identified by comparing posted content to Nexgate's compliance data classifiers. Nexgate classifiers go beyond keywords to apply natural language processing technology that analyzes content in the context that it's presented– across an entire post to the entire thread. Social account content was scanned for the 12 month period extending from July 2013 to June 2014. The scan process included over 60 million pieces of content posted by more than 110,000 employees and 200 million public commenters.

1 State of Social Media Infrastructure, Part I – Benchmarking the Social Communication Infrastructure of the Fortune 100

Third in a Three Part Series

This compliance-focused report is the third in a three part series investigating the social media infrastructure of Fortune 100 firms. The first report, titled State of Social Media Infrastructure, Part I – Benchmarking the Social Communication Infrastructure of the Fortune 100, focuses on the scope and scale of the corporate social media infrastructure itself. It describes, for example, the total number of Fortune 100 social accounts, the number of employees posting to those accounts, apps used to post, etc. The second report, titled State of Social Media Infrastructure Part II – Security Threats to the Social infrastructure of the Fortune 100, outlines the security threats impacting social media. It provides taxonomy of key threats facing enterprise social accounts, the severity of each threat, examples, and recommendations for protecting your firm.

Top-Level Compliance Incident Taxonomy

Figure 1 below breaks down the Fortune 100 compliance incidents by top-level category.

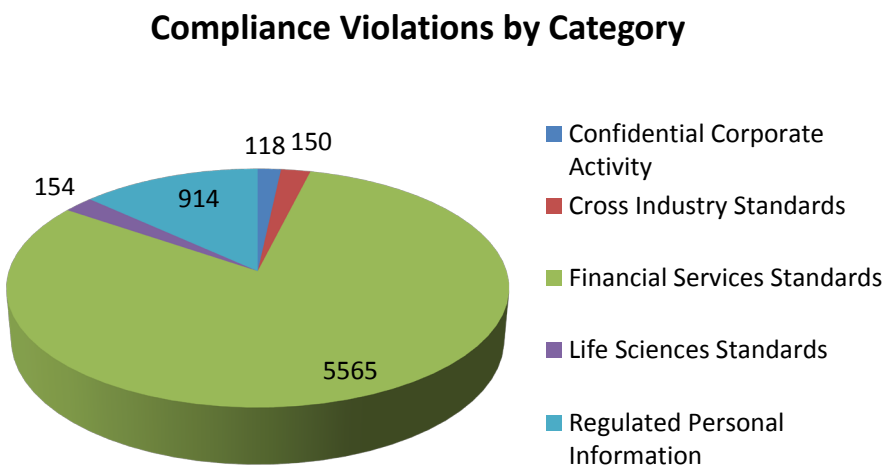

Figure 1: Top-Level Compliance Violation Categories

The total number of incidents across categories is 6907 or roughly 69 violations per firm. Not surprisingly, the largest incident volume was linked to Financial Services Standards. *Financial service firm are well represented in the Fortune 100 (21 firms), are strong social media adopters, and are subject to the most stringent social media communication standards.*

In the sections that follow, we drill down into each of these compliance categories. We describe the regulations behind top-level numbers, provide more granular data analysis, present real-world examples, and comment on social media dynamics that shape the results.

Financial Services Standards

Financial Services Standards cover regulations specific to the financial services industry. Figure 2 provides a breakdown of violations for each regulation.

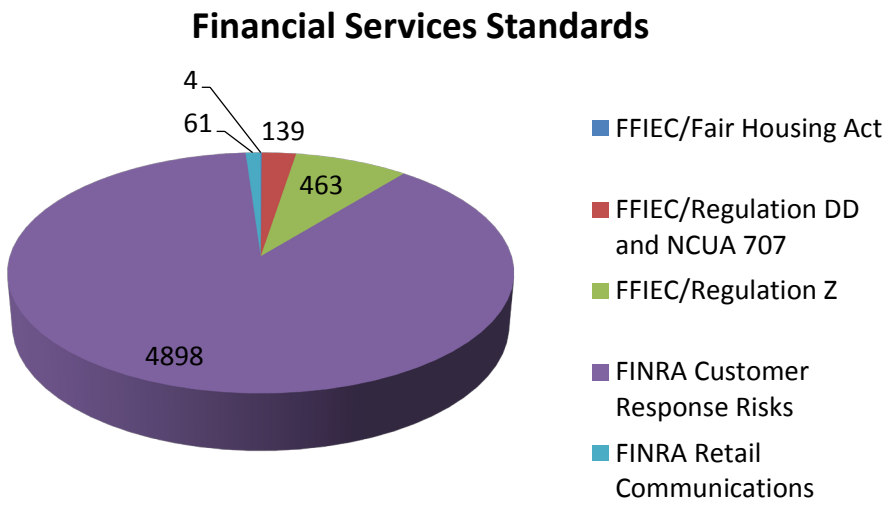

Figure 2: Financial Services Standard Incidents

FFIEC / Fair Housing Act – Governs communications relating to the housing sales, housing rentals, mortgage lending, and appraisals of residential property. Statements cannot indicate limitations or preferences based on race, color, class, nationality, religion, sex, family status, or handicap. For example, a statement that can lead to a violation would be "Families only"

FFIEC / Regulation DD and NCUA 707 – Governs communications relating to deposit accounts for personal, household or family use. Banks must clearly communicate terms and conditions regarding interest and fees according to specified guidelines. For example, the word "free" cannot be used if a minimum balance is required.

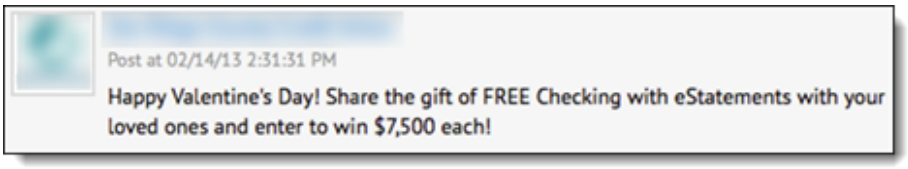

Figure 3: A Facebook FFIEC Regulation DD and NCUA 707 red flag due to lack of conditions for "free checking" (no minimum term, balance, APY, etc.). Also, the "enter to win" statement without details and instructions creates an FTC Sweepstakes risk – see Cross Industry Standards below.

FFIEC /Regulation Z (Truth in Lending) – Governs advertisements relating to consumer credit (e.g. credit card accounts, home loans, etc.). Advertisements must be clear and include disclosures of annual percentage rates (APR) and specified loan features. For example, a home loan advertisement cannot just include an APR. It must also disclose down payment requirements, repayment period, etc.

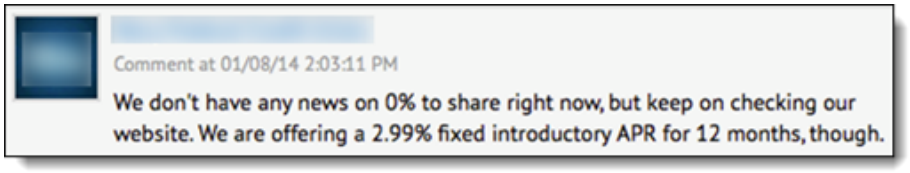

Figure 4: A Facebook FFIEC Regulation Z (Truth in Lending) incident

FINRA Retail Communications (NASD 2210) – Prohibits misleading statements in public communications and requires communications to be fair and balanced. For example, a statement by an advisor that guarantees a certain rate of return on a stock investment would be considered misleading.

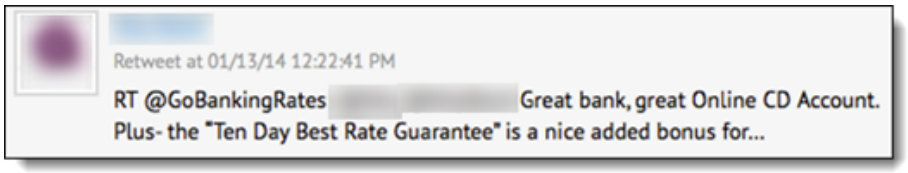

Figure 5: A Twitter FINRA Retail Communications incident

FINRA Customer Response Risks (NASD 3070) – Requires institutions to report and respond within a specified time period to any written customer complaint involving allegations of theft, misappropriations of funds, forgery, etc. For example, the bank must respond to a compliant that the bank lost a check deposit or deducted money improperly.

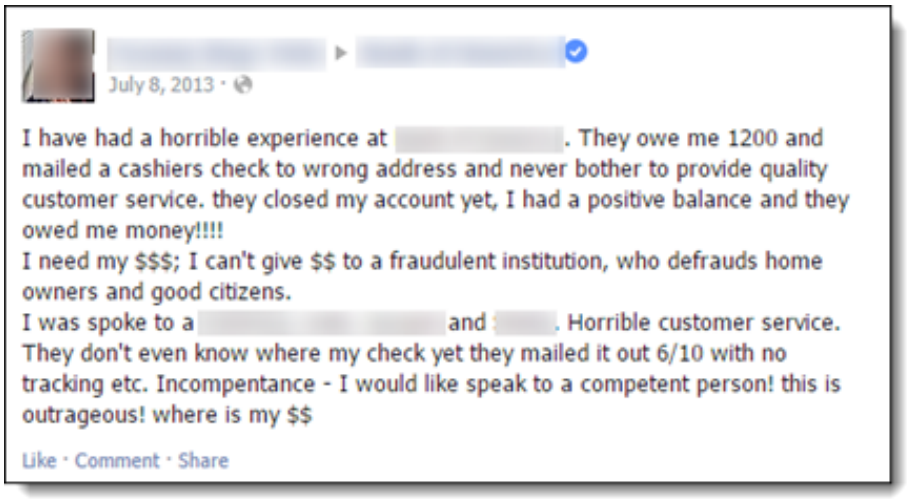

Figure 6: A Facebook FINRA Customer Response Risk incident

FINRA Customer Response Risk – A Special Incident Class

FINRA Customer Response Risk incidents dominate the financial services category. This is an expected result in that they originate from very large numbers of commenters/customers registering complaints linked to fraud, forgery, etc. All other Financial Services Standards incidents originate from a much smaller volume of brand employee commenters violating communications guidelines. If even a small percentage of commenters choose to register complaints via social media, a relatively large volume of messages require response.

FINRA Customer Response Risk highlights the fact that meeting compliance requirements for financial services firms not only requires review of employee posts, but also review of public commenter posts. There are several important considerations to consider in this respect.

- **Scale** – FINRA requires that institutions report and respond to any written customer complaint. This means that every inbound social media message must be reviewed. Spot checks or sampling do not apply. Given the already large commenter message volumes, banks are faced with a major scalability challenge as social media adoption accelerates. We know of banks with a full team dedicated to this tedious task.
- **Real-time Response Workflow** – Response to these incidents require a customer service workflow as opposed to more traditional compliance workflow. Detection needs to occur immediately and customer service teams need to be integrated into the process to handle response.
- **Brand Damage** – As examples below illustrate, customer response incidents expose serious customer complaints to the public (justified or not). If they go unaddressed, they have a negative impact on the brand (i.e. – they look bad).

FINRA Spot Checks

FINRA has been very proactive in enforcing adherence to their rules. Since June of 2013, they have instituted a "spot check" process whereby selected firms are sent a letter requesting specific documentation proving that they are taking steps to comply with FINRA guidelines. For more on FINRA spot checks and how to handle them, check out this video and FINRA's Targeted Examination Letter.

It's worth noting that FINRA Customer Response Risks are not the only compliance incidents that originate from users. As we'll discuss later (See Regulated Data), customers (unaware of the risks) often mistakenly post sensitive personal information. Credit card numbers, bank account numbers, email addresses and other personal information all end up posted publically and all create obvious liability for the institution. Bottom line – effective management of compliance, security, and brand risk requires firms to find scalable mechanisms to monitor both employee and commenter posts.

Bottom line – effective management of compliance, security, and brand risk requires firms to find scalable mechanisms to monitor both employee and commenter posts.

International Financial Services Standards

Since the Fortune 100 consists only of United States (U.S.) firms, this report focuses on U.S compliance standards. However, most Fortune 100 financial service firms maintain international operations that also make them subject to similar international standards. The United Kingdom's Financial Conduct Authority (FCA) Conduct of Business Sourcebook (COBS) 4.2 is one example. FCA COBS 4.2 requires that retail investment communications be fair, clear, and not misleading (similar to FINRA Retail Communications rules in the U.S.). For example, a financial promotion should not describe an investment product as "guaranteed", "protected" or "secure" unless those terms are justifiable and clearly explained to consumers. Maintaining compliance with regulations for each geography in which the firm operates can significantly increase operational complexity and cost.

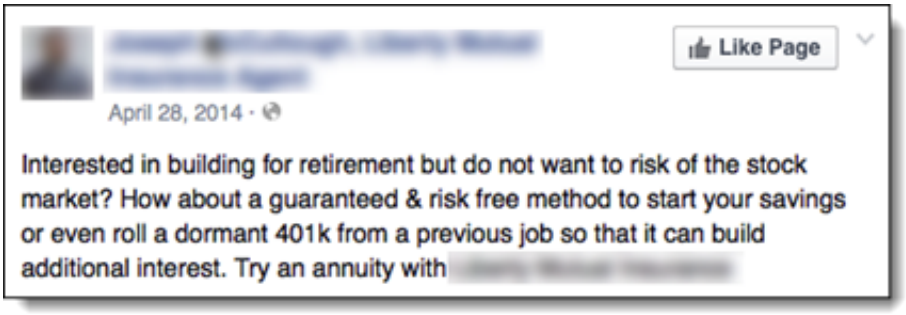

Figure 7: This Facebook post from a UK Financial Services firm promises a "guaranteed and risk free" without any clarifying detail and without any link to additional information. Such language raises FCA COBS red flags.

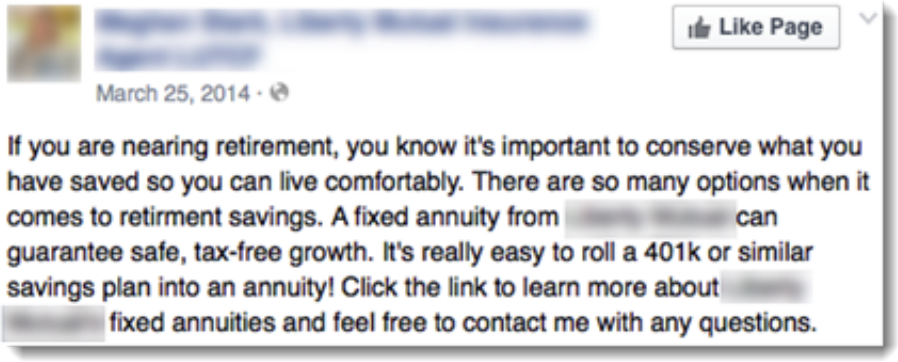

Figure 8: This Facebook post from a U.K. financial services firm uses the terms "guarantee" and "safe" raising FCA COBS red flags. However, the link to additional information may ultimately prevent an audit finding.

A Complex Challenge for Financial Services

The multiple standards listed in this section represent only a slice of the social media compliance challenge faced by Financial Service firms. Financial Services firms also need to monitor for international standards, Cross Industry Standards (SEC, FTC) General Corporate Confidentiality (mergers, layoffs, etc.), and regulated/sensitive data confidentiality (credit card numbers, account numbers, etc.). When this multiplicity of monitoring requirements is viewed in the context constantly changing social account footprint, massive message volumes, and real-time detection requirements – it's clear that Financial Service firms have their work cut out for them.

Regulated Data

Figure 7 below presents a breakdown of Regulated Data incidents. This category focuses mainly on personal identifiers (or PII) of customers and employees that require protection by a range of state, federal/national, and industry regulations.

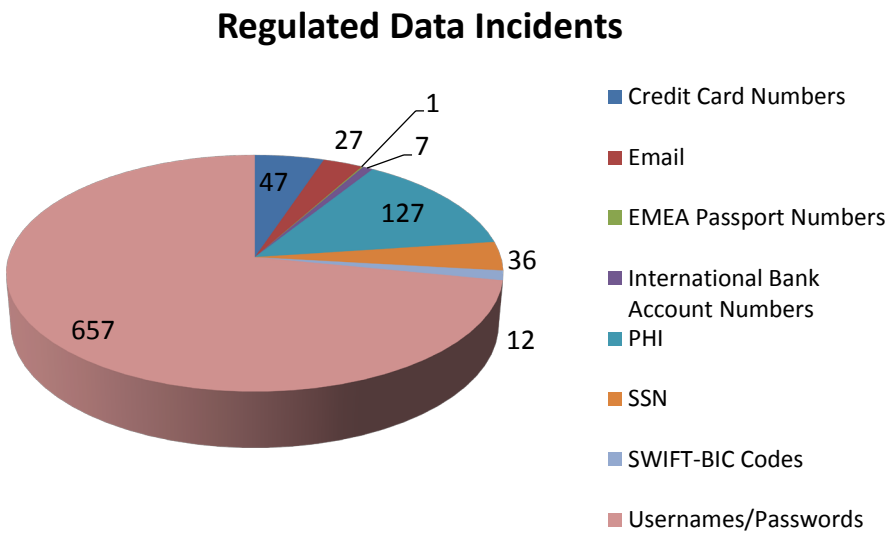

Figure 9: Regulated Personal Information

Customer Service and Regulated Data

Usernames/passwords are the most common problem in this category with 657 incidents. Like most incidents in this category, usernames/passwords are most often linked to customer service conversations (e.g "I forgot my password…." , "My credit card isn't working …" etc.). While it provides an efficient customer service medium, personal information should never be exchanged via public social posting mechanisms. If sensitive information must be shared, a private message should be employed via other (e.g. phone) channels.

Although we find that very often commenters are responsible for posting personal information, a surprising number of employees make the same mistake. Regardless of how personal information is exposed, the firm is exposed to fraud (in the case of credit card numbers, etc.) and audit risk. Therefore, like Financial Service Standards described above, managing regulated personal information risk requires monitoring of both employee and commenter posts.

Regardless of how personal information is exposed, the firm is exposed to fraud (in the case of credit card numbers, etc.) and audit risk.

Regulated Personal Information Examples

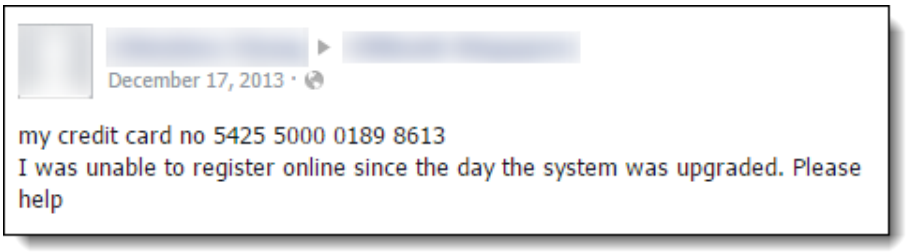

Figure 10: A Customer Shares a Credit Card Number on Facebook – Not Good

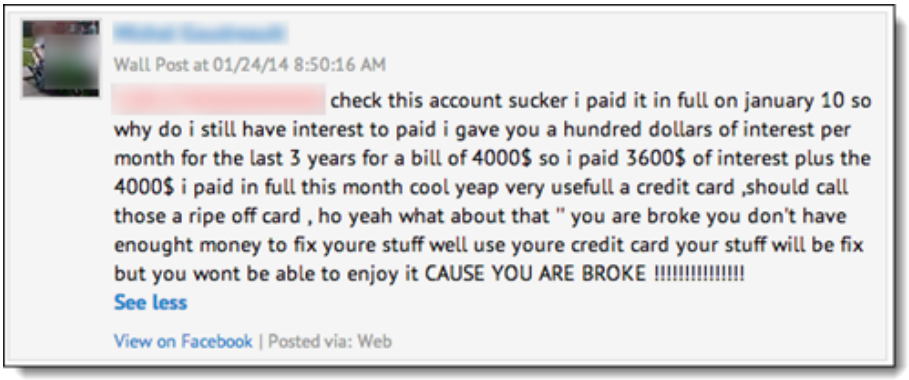

Figure 11: Another Customer Shares a Credit Card on Facebook. This post also triggers FINRA Customer Response rules.

Confidential Corporate Activity

Figure 12 below presents a breakdown of Confidential Corporate Activity incidents. This category focuses on tracking discussions of sensitive activity such as layoffs, acquisitions and merger plans.

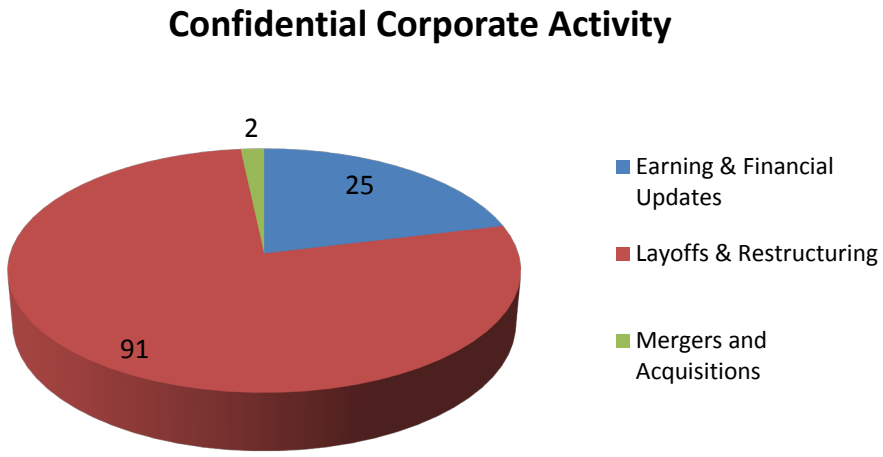

Figure 12: Confidential Corporate Activity

Understand the Technology and Use Content Publishing Workflow

A well known recent example of an incident in this area, ironically involves Twitter's Anthony Noto. Thinking that he was sending a private direct message to another executive, he made a public post exposing a recommendation to acquire another firm. Although it was certainly a post he'd like back, he fortunately did not name the specific acquisition target.

Figure 13 : Twitter CFO exposes an acquisition plan on Twitter

Mistakes like this highlight two important issues to consider for corporate social media accounts and employees who use social for business.

Understand the Technology – Make sure that employees posting to corporate accounts or representing the brand on their own accounts understand the technology. Experienced social media users may be clear on the difference between a direct message and a public post, but inexperienced users should be coached and made aware of the procedures and accounts that they should use when representing the firm in social.

Enforce Content Publishing Workflow – Every firm should consider directing employees to use an approved content publishing application (e.g. Hootsuite) to make all posts for corporate accounts and personal accounts used for business. Among the many benefits of such tools is that they can provide manual or automated compliance scanning to warn users of problems before posts are published. Manual methods make sense for relatively static conversations. Automated monitoring can be applied to interactive, fast paced conversations. It's a safety net that can prevent violations in real time – before damage can be done.

Cross Industry Standards

Figure 14 below presents Cross Industry Standards incidents. This category captures regulations that apply horizontally regardless of vertical industry. We tracked both U.S Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC) regulations. SEC incidents dominated with 149 incidents.

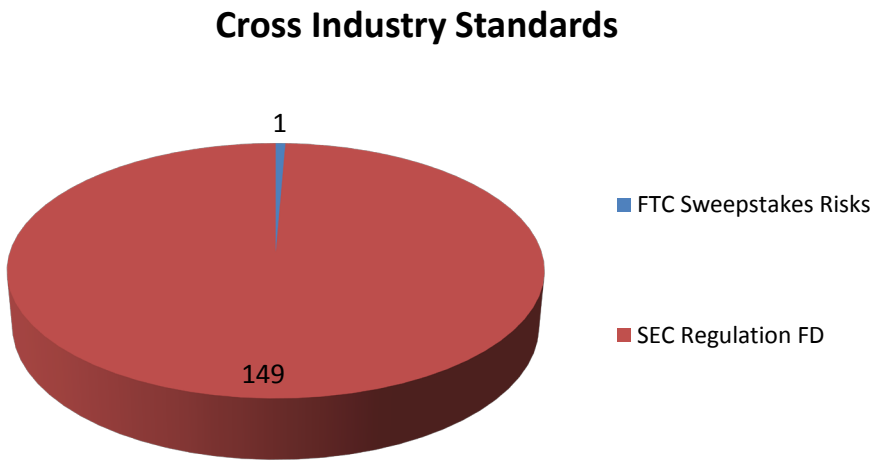

Figure 14: Cross Industry Standards

FTC Sweepstakes Risks – This requirement applies to any advertisements of a promotional sweepstakes (contest, giveaway, etc.). The promoter must make the terms of the sweepstakes absolutely clear and no sweepstakes can have cost to enter. This is a common problem on Twitter because of the character limit. If complete terms cannot be included in the message text, a link to more information may be provided. If a link is provided, the message must explicitly state that the link contains additional terms.

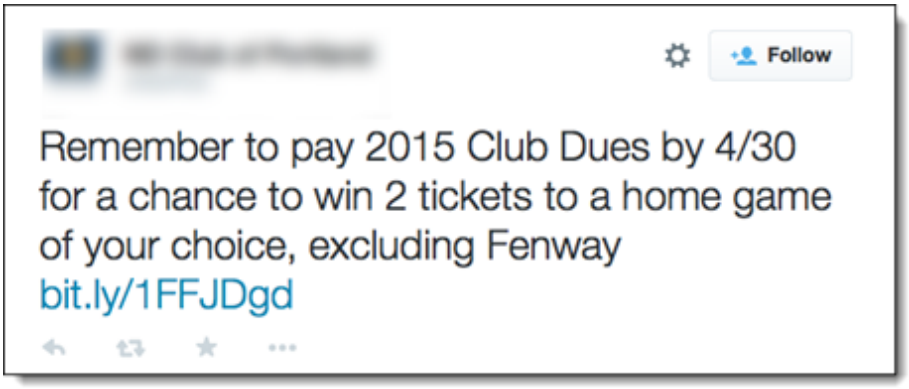

Figure 15: A Tweet containing an FTC Sweepstakes Risks incident

SEC Regulation FD – Earnings announcements or earnings impacting disclosure can only be made on specifically identified social media accounts designated as official earnings disclosure accounts. Any material earnings related disclosures made on other accounts are in violation.

Executives, Employees and SEC violations

Executives at large organizations are often charismatic public spokespeople with the potential to attract large social followings. Many of today's CEOs in particular are minor celebrities. However, as executives become more social, the likelihood of SEC disclosures increases. It's an informal environment that encourages sharing, and sometimes even trained executives overshare.

One recent public example of a probable SEC violation by an executive involved Tesla CEO Elon Musk. In the Twitter post below, Mr. Musk announced a new product plans on his personal account, which was not designated as an SEC Disclosure account. This previously private information was made available to Mr. Musk's Twitter Followers before it was made available to the general public. Was this information material to earnings? The market thought so. Within 10 minutes of the post, Tesla stock had risen by four percent adding $900 million to the company's market capitalization.

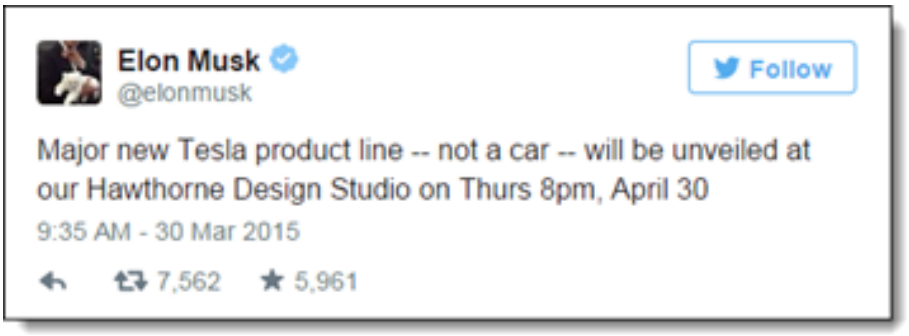

Figure 16: This Tweet added $900 million to Tesla's Market Capitalization. It's also a probable SEC violation.

Executive participation in social media can have tremendous upside for the business, but compliance professionals need to educate those executives and deploy controls to catch inevitable mistakes. As general employee populations emulate executives in social promotion of the company (e.g. social advocacy programs), we expect SEC violations to become an even greater concern across all industries.

FTC Truth in Advertising and FTC Material Connections

Beyond FTC Sweepstakes rules, corporate social media is directly subject to two additional FTC regulations – Truth in Advertising and Material Connections. Truth in Advertising rules prohibit misleading consumers with false product claims. Material Connection rules prohibit product endorsements by employees or others with material connections to the firm without disclosing their connections. Violations of these regulations result in civil fines and compensation to consumers who may have been deceived. For example, in November 2014 Sony Computer Entertainment America ran into trouble with the FTC when their advertising agency launched a Twitter endorsement campaign in which agency employees endorsed the Sony PS Vita without disclosing their connection to Sony. Cole Haan (owned by Nike) ran into similar Material Connection challenges for a Pinterest campaign. We expect FTC Material Connection incidents to grow as more organizations formally social media employee advocacy programs. It's critical that employees and partners promoting products in social disclose their connection to the corporation.

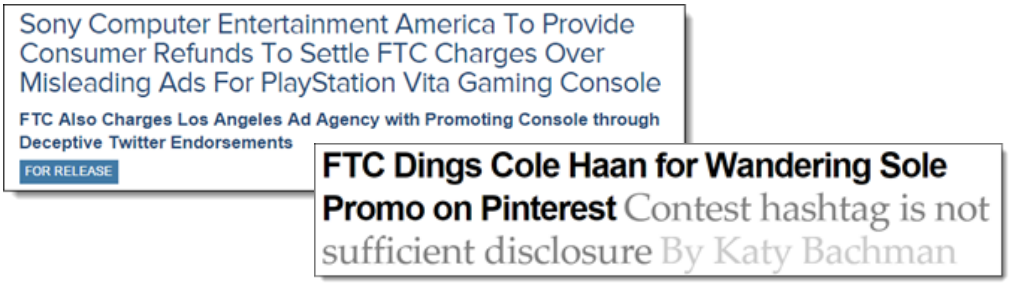

Figure 17: Sony and Cole Haan were both challenged by the FTC over Material Connection incidents in Social Media in 2014

Life Sciences Standards

Figure 17 below presents Life Sciences Standards incidents. This category covers regulations that apply to pharmaceuticals, health insurance providers, healthcare providers and other healthcare-related industries. We tracked incidents relating to both the Healthcare Information Portability and Accountability Act (HIPAA) and Food and Drug Administration (FDA) Adverse Drug Experience regulations. Both regulations triggered significant incident volumes although FDA Adverse Drug experiences were more common with 98 total incidents.

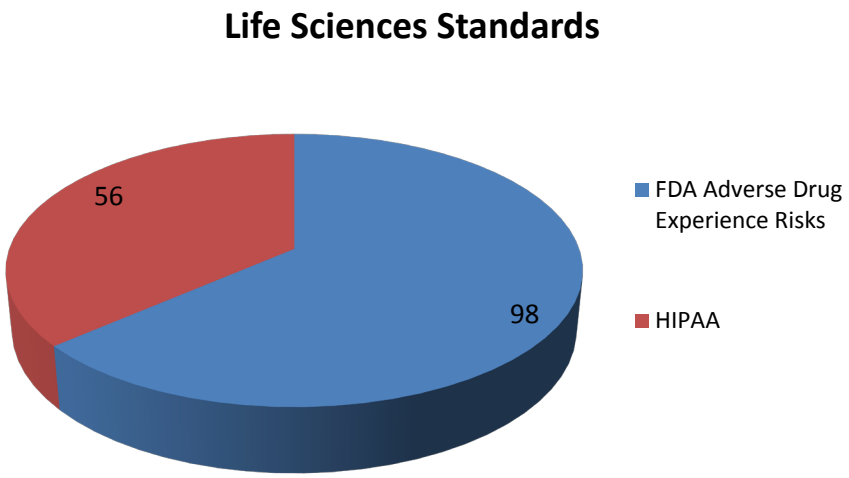

Figure 18: Life Sciences Standards Incidents

FDA Adverse Drug Experience Risks – Indicate reports of adverse side-effect of medications as defined by the FDA. For example, "I took (drug XXX) and now I've got some bad intestinal cramping. Is this expected?" Healthcare organizations are required to report these incidents to the FDA. This is another example of a social media compliance requirement that requires review of all public commenter posts.

Figure 19: A Tweet containing a FDA Adverse Drug Experience Risk incident

HIPAA – Indicates breach of patient confidentiality as defined by the Health Insurance Portability and Accountability Act (HIPAA). For example, "John Smith in C131 has influenza."

Publishing Applications – A Best Practice Indicator

Figure below presents the distribution of applications used to make social media posts by brand employees.

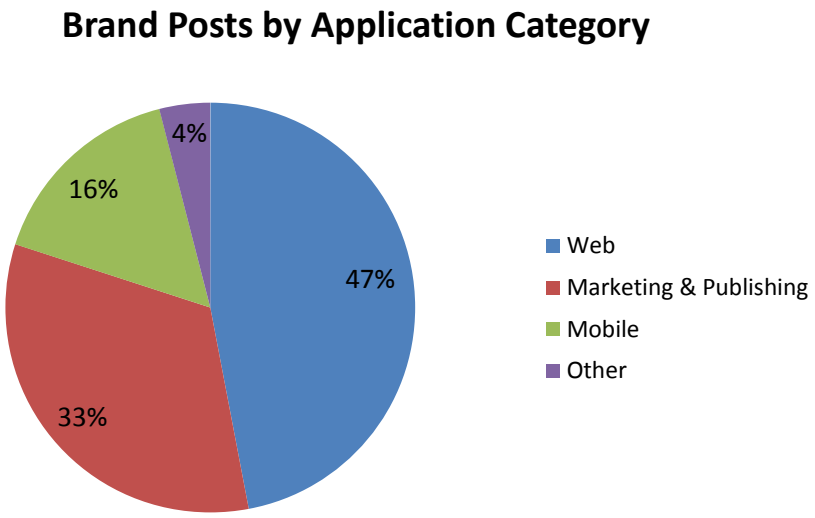

Figure 20: Distribution of Applications Used to Post by Brand Employees

The fact that only 47% of posts were made by marketing and publishing applications indicates widespread lack of social publishing best practice enforcement. In addition to helping brands engage their audiences more effectively, publishing tools can incorporate compliance moderation and even automated content scanning technology that can warn employees of compliance violations or public relations mistakes prior to making comments public. Drilling into this topic further, we found that although almost every firm uses at least one Marketing & Publishing Application, an average of 13 different applications (native Web, mobile, etc.) were actually used. The conclusion here is that although Fortune 100 organizations have invested in publishing infrastructure, employees commonly circumvent or are unaware of publishing policy. It's clear that a mix of policy training and enforcement controls are needed in this area.

An average of 13 different applications (native Web, mobile, etc.) were actually used.

Unique Social Media Compliance Challenges

A host of structural factors make social media compliance far more challenging than other more tightly controlled public communications channels such as press, Web site, print advertising, etc. Just a few of these factors include culture, pace, scale, and complexity.

Culture

Social media, almost by definition is an informal environment where people share information more freely than other mediums. A whole generation of young people is growing up with less inhibition towards protecting personal information. It's not a bad thing – it just means that as this generation becomes employees and participate in corporate social media programs, they bring a relaxed information sharing posture with them. Training individuals immersed in this culture – helping them to understand what can be shared and what can't in the context of business communications is imperative.

Pace

Corporate social communications can take place at an extremely rapid pace. Many corporate accounts support thousands of daily posts appearing 24 hours per day, 7 days per week. This speed and volume means that the likelihood of mistakes rises. Well-meaning employees engaged in a fast paced conversation (and influenced by an informal culture) make statements that violate compliance rules. Compliance moderation at this pace is major challenge. Waiting for a human moderator to review every post effectively kills the conversation. Therefore, finding ways to enable employees to engage interactively without the encumbrance of manual moderation is critical.

Scale

More than 500,000 messages, originating from 1,159 employees and 213,000 commenters were spread across over 320 accounts for the average Fortune 100 firm during our 12 month research window. Message volume alone makes manual compliance monitoring and enforcement impractical if not impossible. Assuming 1 minute of review per message, the average Fortune 100 would spend 8,333 hours per year on compliance review. To make matters worse, corporate social presence is a moving target with participants and accounts changing constantly. Just tracking which accounts need monitoring on a given day can be a major challenge.

Scalability challenges are at the heart of many of the compliance violations we find in these report.

Many organizations that we work with take a "start small" approach to social media and build initial compliance processes that work reasonably well for a handful of corporate marketing accounts. However, as social is adopted for social selling, employee advocacy, customer support, product marketing and other functions, scalability challenges emerge. Scalability challenges are at the heart of many of the compliance violations we find in these report. Bottom line – there are so many accounts and so much content that finding compliance exceptions becomes like finding the proverbial needle in a haystack.

Complexity

Multiple networks (Twitter, Facebook, LinkedIn, etc.), employee accounts, personal accounts, corporate accounts, publishing applications, and a matrix of changing regulations all interact to create a complex social media landscape that's extremely difficult to manage. Just understanding each regulation and how it translates into compliance process is a big challenge. Marketing teams that typically own social are not compliance experts and cannot be expected to build compliance process without help. Even compliance professionals find it difficult to track constantly changing regulatory language.

Recommendations

Establish Ownership

The first step in in building a successful social compliance program is establishing the core team responsible for compliance. Social media compliance requires coordination between groups. The team should include social users (marketing, support, sales, etc.), compliance, and information security team (since this committee may also be leveraged to ensure social media security.) The primary role of this cross-functional team is to assign clear roles and responsibilities within the organization for policy, training, enforcement, and audit. For help in this area, check out Nexgate's Mapping Organizational Roles and Responsibilities for Social Media.

Define Policy and Train Employees

Develop a social media security and compliance policy covering approved business use, content, and publishing workflow.

- **Approved Business Use** – Define approved social account types and business uses. Is brand representation limited to corporate marketing accounts, or is approved usage extended to executives, sales, support, and general employees? What business purpose is approved for each group (marketing, employee advocacy, prospecting, recruiting, etc.)? Which accounts are used for material earnings disclosures (if any)? Policy should also cover which social networks (Twitter, LinkedIn, etc.) are approved for each account type.
- **Content** – Define what content is allowed and not allowed to be posted for each required regulation. Policy should also extend beyond compliance to cover security-related content (e.g. malware, scams, phishing) and acceptable use (profanity, hate, intolerance, etc.). Content policy should consider both brand employee and public commenter communications. Content policy may vary for different account types (SEC disclosure accounts, etc.)
- **Publishing Workflow** – Define the publishing process employees are expected to use for corporate accounts. Policy should define which publishing tools should be used and when content should be reviewed. For example, FINRA requires that static brand content (profile data, major announcements, etc.) be reviewed before posting, while interactive conversations (social selling by brokers, etc.) may be audited after publishing.

With a policy in place, a formal training program is needed to teach employees the policy. Employees not allowed to represent the brand need to be notified of this fact and attest that they understand the policy. Corporate account owners, on the other hand, require more detailed training covering approved use, content, and publishing workflow. Ideally, training can be customized for different groups to focus on specific usage (social selling, support, etc.). Training should include examples of compliance violations, consequences, and attestation to certify that each employee understands the policy. Training programs should not be considered one-time events, but repeated annually. Online training tools can reduce costs and scale training across large, geographically diverse teams.

Social Account Discovery

Monitoring policy compliance of any social media account first requires that the business know that the account exists! In fact, one of the first requests made by social media auditors (e.g. FINRA spot checks) is a list of all corporate accounts. Unfortunately finding every account amid the sea of existing social media accounts in the world is not an easy task. The average corporation has over 300 accounts and new accounts appear on a weekly if not daily basis.

Manually searching and tracking (via spreadsheets, etc.) social accounts on an ongoing basis requires many hours to accomplish even once. Performing these searches on an ongoing basis is not only cost prohibitive, but extremely prone to errors. Automated social account discovery technology can help. These tools can not only find all branded accounts in a matter of minutes, but notify you of new accounts as they appear. Automated social account discovery tools allow you to build compliance workflow that…

1. **Classifies discovered accounts** according to approved business use. Unauthorized or fraudulent accounts can be removed, modified, or monitored as needed.
2. **Ensures training** to discovered account owners
3. **Monitors compliance** with content and publishing workflow policy

For more information on automated social account discovery, check out http://nexgate.com/products/social-discover.

Monitor and Enforce Policy

Once the inventory of brand social accounts is known, compliance with policy must be monitored and enforced. As described above, pace of communications, scale and the complexity are major barriers. Even the most mature compliance teams struggle to keep pace with growing social media deployments at many organizations. This is another area where technology can help. Social media policy monitoring technology functions 24 X 7 X 365 at virtually unlimited scale to automatically identify messages that represent security or compliance risk. Rather than manually review a message sampling – of which 99% represent no risk – automated monitroing reviews all messages and extracts those few that represent risk. Automation also alerts compliance staff in real-time so that violations than can be remediated immediately, rather than months after the fact during an audit. Finally, this technology goes beyond compliance to automatically remove security risks (malware, etc.) and inappropriate content (hate speech, pornography, etc.). In short, automated policy monitoring technology allows organizations to safely grow social media deployments without overwhelming security and compliance teams.

In short, automated policy monitoring technology allows organizations to safely grow social media deployments without overwhelming security and compliance teams.

For more information on automated security and compliance monitoring, check out http://nexgate.com/products/socialpatrol-protect-your-social-media.

Data Retention

The final consideration when building a strong social media compliance program is data retention. Multiple regulations and best practices dictate that all social media messages be retained to meet future audit and legal discovery requests. In many cases, email archiving solutions have been extended to support social media archival. When evaluating social archiving solutions, be sure to consider how well they integrate other social media compliance technologies and how easily they can be searched to identify security and compliance risks. Solutions that rely on random sampling or keyword searches on raw message are time both consuming and unreliable. To enable better supervision, an archive that integrates with an automated compliance monitoring tool is the most effective solution. This ensures that context is preserved, social data is classified for easy search, and actions enforced prior to archive are available as part of the archive supervision workflow.

For more information on integrating social media archives with automated compliance monitoring, check out http://nexgate.com/solutions/intelligent-social-content-archiving.

892 Ross Drive
Sunnyvale, CA 94089
1.408.517.4710
www.proofpoint.com