

Lenders Compliance Group

Tuesday, March 12, 2013

Social Media Compliance: Frequently Asked Questions

Last month, I discussed some of the [salient compliance requirements associated with using Social Media](#).^{*} Then, a few days later, I offered to you my article, entitled [Social Media and Networking Compliance](#). This month, on March 6th, I was one of three presenters who gave a webinar for [American Banker on Social Media](#), with special reference to the new rules of the Federal Financial Institutions Examination Council (FFIEC). The proposed rule, issued January 23rd, is entitled "[Social Media: Consumer Compliance Risk Management Guidance](#)."

My webinar topic: **Social Media – Employee Manual.**

The webinar was very well attended by a diverse cross-section of financial institutions. I found it quite interesting that, when polled during the webinar, by a factor of two to one these companies did not have an Employee Manual, even if about a third of them have policies and procedures relating to Social Media.

I have harped on a certain point regarding policy statements, so here it goes again: **policies and procedures are a rather abstract concept to employees; employee manuals, however, for certain rules and regulations, are the most effective means to ensure compliance.** Training is an important and an ancillary tool, but employees do not always mentally retain training information. Keep this in mind: an employee manual is a constant reminder of a company's expectations and policies.

One aspect of social media that deserves considerable attention is [trolling](#), using [anonymity](#), and general [blogging guidelines](#). Everybody knows that, for the most part, blogging is electronically available to the public. However, with regard to an individual's employment with a financial institution, what restrictions should be placed on an employee who blogs? From my own research and experience, it would seem that many employees actually have no idea of the implications, requirements, and, in some cases, the potential to easily cross over into violations of federal law or state law.

Here are the [risks at stake in social media networking and blogging](#) - though by no means less so for forms of advertising through and use of social media: financial risk, regulatory risk, sales risk, reputation risk, legal risk, strategic risk, and operational risk, such as adverse consequences to business plans, projects, Internet Technology and Information Security protections, and many core departmental functions.

In this newsletter, I will offer a high level FAQs about the use of Social Media (SM), with some additional emphasis on blogging. I will also provide bulleted guidelines to give to employees.

What is Social Media?

SM is a form of interactive online communication in which users can generate and share content through text, images, audio and/or video.

Do companies use Social Media?

HubSpot found that by November 2012 companies that blog incurred an average of 55% more visitors to their sites than companies that did not blog. Statistically, blogging companies may generate 97% more external website links and 434% more indexed pages, both of which are critical to a company's search rank. And a global survey by McKinsey of approximately 1,700 corporate executives finds that 69% of respondents claim measurable advantages from social media, including a lower cost of doing business, better access to knowledge, increased marketing effectiveness, insight for developing more innovative products and services, and higher revenues.

Does SM cover micro-blogging?

SM includes, but is not limited to, micro-blogging sites (i.e., Facebook, Google Plus, MySpace, and Twitter); forums, blogs, customer review websites and bulletin boards (i.e., Yelp); photo and video sites (i.e., Flickr and YouTube); sites that enable professional networking (i.e., LinkedIn); virtual worlds (i.e., Second Life); and social games (i.e., FarmVille and CityVille).

How do some financial institutions use SM?

[ALL ARTICLES](#)

[SUBSCRIBE](#)

[DOWNLOAD THE ARTICLE](#)

[Twitter](#) - [LinkedIn](#) - [Facebook](#)

[SUITE OF SERVICES](#)

RECENT ARTICLES



LENDERS COMPLIANCE GROUP
CFPB's Regulatory Agenda - 2013

OUR OTHER WEBSITES



BROKERS COMPLIANCE GROUP
Social Media and Networking



MORTGAGE COMPLIANCE FORUM
Action Plans to Correct Deficiencies



CFPB FORUM
CFPB's Regulatory Agenda - 2013



OCC NEWS FORUM
OCC - Correcting Foreclosure Practices



BSA NEWS FORUM
FinCEN: SAR Narrative, PowerPoint,



DODD-FRANK FORUM
CFPB's Five Year Strategic Plan



NMLS USERS FORUM
NMLS: 2011 Licensing Report



FHA FORUM
HUD: Causes of Administrative Actions



VETERANS MORTGAGE FORUM
CFPB and FTC: Warning Letters -
Misleading Advertisements

[NEWSLETTER](#)

SM has been used to receive and respond to complaints, provide loan pricing, and offer generic information about products and services.

How to manage Social Media risks?

FFIEC gives seven components to managing SM risk, specifically:

1. A governance structure
2. Policies and procedures
3. A due diligence process
4. An employee training program
5. An oversight process
6. Audit and compliance functions
7. Reports to management

What are some laws and rules affecting the use of Social Media?

For Residential Mortgage Lenders and Originators, the list should include:

- Bank Secrecy Act (BSA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
- Electronic Fund Transfer Act (Regulation E)
- Equal Credit Opportunity Act (Regulation B)
- Fair Credit Report Act (FCRA)
- Fair Debt Collection Practices Act (FDCPA)
- Gramm-Leach-Bliley Act (GLBA)
- Privacy and Data Security
- Real Estate Settlement Procedures Act (Regulation X)
- Telemarketing Sale Rule (TSR)
- Truth in Lending (Regulation Z)
- Unfair, Deceptive and Abusive Practices (UDAAP)
- Violence Against Women Act (VAWA)

What are some major risk areas?

- Brand Identity
- Consumer Complaints
- Consumer Inquiries
- Data Breach
- Fraud
- Information Security
- Libel and Harassment
- Privacy and Confidentiality
- Third Party Control of Data
- Unregulated Social Media Sites

May an employee troll or blog anonymously?

SM compliance includes regulating the employee's blog posts and even trolling activities. A person who trolls posts inflammatory, extraneous, or off-topic messages in an online community, such as a forum, chat room, or blog, with the primary intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion.

There are several types of blogs: personal blogs, microblogs, corporate blogs, organizational blogs, topic blogs, media blogs, and even reverse blogs. Web forums are community type websites where bloggers post comments and links to other forums and blogs.

In many of the aforementioned blogosphere webspaces, people can troll or post anonymously.

Outside the workplace, the employee's rights to privacy and free speech protect online activity conducted on personal social networks with a personal email address. However, an employee's posts on such personal online sites should never be attributed to the employer and should not appear to be endorsed by the employer, let alone originating from the employer's resources.

If an employee chooses to list a work affiliation on a social network, then all communication on that network should be viewed as a business-related network.

When participating in any online community, the employee should be transparent, disclose identity and affiliation with an employer, and any professional or personal interest. When posting to blogs, the employees should always use their names.

Employees of financial institutions must never create an alias and should never troll or use anonymity.

Are there restrictions to what may be posted?

Do not post any information or conduct any online activity that may violate applicable local, state or federal laws or regulations.

Never be false or misleading in online credentials.

Maintain complete accuracy in all online biographies and ensure there is no embellishment.

Use the words "expert" or "specialized" very sparingly and only when such claims can be substantiated and approved for usage by the employer.

Never use so-called "triggering terms," as set forth - or should be set forth! - in the employer's advertising policy statement or manual.

What are some guidelines to follow?

Be direct, informative and brief when using social media or networking.

Never use the employer's name, an acronym of that name, or indeed any other name associated with the employer in a blog posting, unless the employee has received written permission from the employer to do so.

Acknowledge information courteously and promptly.

Identify all copyrighted or borrowed material with citations and links.

When publishing any material online that includes another's direct or paraphrased quotes, thoughts, ideas, photos or videos, always give credit to the original material or author, where applicable.

Always evaluate the post's accuracy and truthfulness. Before posting any online material, ensure that the material is accurate, truthful and without factual error.

Spell and grammar check everything.

Should errors be corrected?

While a blog itself is not subject to the limitation on commercial speech, the content of a blog can be. The content must be informative only and nothing in the content should propose, negotiate, or arrange a residential mortgage loan transaction with a posting consumer or be for the purpose of directly gaining a residential mortgage loan transaction from a posting consumer. Federal and/or state laws govern the advertising and origination of mortgage loan products and services in all media. Indeed, discussion of a residential mortgage loan transaction or the terms and conditions relating to such a transaction should be entirely proscribed.

Corrective Actions

If an employee's blog entry contains an error or mistake, correct it.

Since transparency is a key concern in social media, admit the mistake, apologize if necessary, correct it, and move on.

Any mistake involving advertising or discussion of a residential mortgage loan transaction must be reported immediately to the employer.

Should an employee leave comments?

When posting to a blog, refrain from posting about controversial or potentially inflammatory subjects, including politics, sex, religion or any other non-business related subjects.

Keep the tone of your comments respectful and informative, never condescending or argumentative.

Use sentence case format, not capital letters.

Avoid personal attacks, online fights, and hostile communications.

If a blogger or any other poster publishes a statement with which an employee disagrees, an opinion may be posted, but do not escalate the conversation to a heated argument.

Write reasonably, factually, and with good humor.

Understand and credit the other person's point of view and avoid any communications that could result in personal, professional, or credibility attacks.

Never disclose proprietary or confidential information of the employer or any consumer

information.

Avoid forums where there is little control over what the employee knows to be confidential information.

Respect the privacy of fellow employees and associates as well as the opinions of others.

Before sharing a comment, post, picture or video about a client, other employee, or associate, through any type of social media or network, obtain that person's consent or do not post anything about that person.

Read a social media website's disclaimers and privacy policies for any rules that may violate the employer's policies regarding consumer confidential information.

How to respond to negative comments?

If a blogger or any other online participant posts an inaccurate, accusatory or negative comment about the employer or any of the employer's clients, do not engage in posting a response or exchange of posts, without prior written approval of the employer.

May a professional reference be posted?

Posting recommendations of colleagues is a tool of professional social networking sites. The recommendations and comments an employee posts about other current and former employees can have consequences, even if the employee is making the recommendations personally and not on behalf of the employer. Therefore, potential recommendations and positive references should be cleared with the employer regarding anyone who is or was (within some time frame) associated with the employer or, if the employer does not require such notification, should be polite, straightforward, and considerate.

Negative references or remarks should always be avoided.

Can trolling and anonymity be traced?

Yes. Many website owners are able to access a poster's IP address. Sometimes, that IP address may actually be associated with the employer - meaning the employee is using the employer's computer to publish an anonymous post! Not only can the website owner trace the poster's IP address but it is also possible to back trace the URL from which the poster came.

Furthermore, websites can trace which links the poster clicked on, the operating system used, the browser, the monitor's resolution and color depth, the Javascript version, entry and exit time, which web pages were visited, the time spent on the visited web pages, the geographic area, town, or city of the poster, and other information.

What are bulleted guidelines to give to an employee?

I suggest a bulleted one-page notice, made available individually as well as on the firm's corporate bulletin board. This list is surely not meant to be comprehensive. You may want to add features from the FAQs I outlined above, or revise, as needed and appropriate.

- Social Media may be used for lawful purposes only. You may not post content that is anti-competitive, obscene, otherwise objectionable, in violation of federal or state law, or that encourages conduct that could constitute a criminal offense or give rise to civil liability.
- Do not publish posts in an unlawful, threatening, or abusive manner, including, without limitation, to promote racism, bigotry, hatred or physical harm of any kind against any other poster on a website.
- You may not post content that discloses our or any other company's non-public transactions, business intentions, or other confidential information, or that discusses pricing or salaries.
- Do not troll or post anonymously, or impersonate any person or entity, or falsely state or otherwise misrepresent your affiliation with a person or entity or us.
- Do not post or transmit any material that violates our advertising policy requirements, or the rights of others, including, without limitation, privacy rights, publicity rights, copyrights, trademark rights, patent rights, contract rights, or any other right.
- You may not post content that infringes the intellectual property, privacy, or other rights of third parties.
- No material protected by copyright or other proprietary right shall be uploaded, posted, or otherwise made available on Social Media without the permission of our management and the owner of the website.
- You may not disparage, harass, abuse, threaten, or advocate violence against other participants, entities, individuals, or groups.
- You may not bash vendors, competitors, or other employees, whether by name, inference, specific description or otherwise.

- We reserve the right, as a condition of your employment, to require you to remove content immediately from any website that we determine, in our sole discretion, to be inappropriate and/or in violation of our rules.
- Do not post any messages encouraging or facilitating other posters to arrive at any agreement that either expressly or impliedly leads to price fixing, a boycott of another's business, or other conduct intended to illegally restrict free trade.
- Do not post messages that encourage or facilitate an agreement about the following subjects: pricing, discounts, loan programs, or terms or conditions of loan programs or any loan transactions; salaries; profits, profit margins, or cost data; market shares, sales territories, or markets; allocation of customers or territories; or selection, rejection, or termination of customers or suppliers.
- You may not use Social Media to solicit a client or offer products or services to any clients without our written consent.
- Don't challenge or attack others. Be courteous. Let others have their say, just as you may want to have your say.
- Don't post blatant commercial messages: any advertising of our products and services must be approved by us in advance of publication to a website.
- You may not gather for marketing purposes any email addresses or other personal information posted by other posters.
- Use caution when discussing products and services. Your comments are subject to libel, slander, and antitrust laws.
- Do not post anything that you would not want the world to see or that you would not want anyone to know came from you.
- We reserve the right to modify this Social Media Guidelines at any time without notice or liability.

Summation

Nonbanks and banks use social media as a tool to generate new business and provide a dynamic environment to interact with consumers. Financial institutions are aware that employees will not use social media exclusively for business, but it is vital that employees know certain reasonable guidelines for online behavior, most especially when participating online as representatives of their firms.

New tools on the web are introduced all the time and new challenges emerge for all of us. Networking compliance rules will evolve and require updating. Financial institutions and their employees must manage potential risks to themselves and consumers by ensuring that the institutional risk management procedures are implemented and by requiring employees to self-monitor their involvement with social media.

* Jonathan Foxx is the President & Managing Director of Lenders Compliance Group



Labels: [Consumer Financial Protection](#), [Consumer Privacy](#), [Consumer Protection](#), [ECOA](#), [EFTA](#), [Fair Lending](#), [FCRA](#), [FDCPA](#), [FFIEC](#), [FTC](#), [GLBA](#), [Networking Compliance](#), [RESPA](#), [Social Media](#), [TILA](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

[Web Toolbar by Wibiya](#)

LENDERS COMPLIANCE GROUP is the first full-service, mortgage risk management firm in the country, specializing exclusively in residential mortgage compliance and offering a full suite of services in mortgage banking for banks and nonbanks. We are pioneers in outsourcing solutions for residential mortgage compliance. We offer our clients real-world, practical solutions to mortgage compliance issues, with an emphasis focused on operational assessment and improvement, benchmarking methodologies, Best Practices, regulatory compliance, and mortgage risk management.

Information contained in this website is not intended to be and is not a source of legal advice. The views expressed are those of the contributing authors, as well as news services and websites linked hereto, and do not necessarily reflect the views or policies of Lenders Compliance Group (LCG), any governmental agency, business entity, organization, or institution. LCG makes no representation concerning and does not guarantee the source, originality, accuracy, completeness, or reliability of any statement, information, data, finding, interpretation, advice, opinion, or view presented herein.

