

## Social media damage control: Why you must plan now (February 25, 2010)

If one little online video could move FDIC, why should your bank be different?

By Karen L. Garrett, partner, Stinson Morrison Hecker LLP, Kansas City, Mo. For more biographical details, see the end of this article.

**Disclaimer:** This article provides general information only. It is not intended to be a comprehensive summary of the law or to treat exhaustively the subjects covered. This information does not constitute legal advice or opinion.

The power of the internet and its ability to provide information, disinformation, and a platform for almost anyone is well known. A clear example is the video posting of a commentator on the OneWest Bank transaction with FDIC to acquire assets of IndyMac. The video was so compelling, and distributed so widely, that on Feb. 12 of this year, FDIC was forced to actually issue a press release refuting the "facts" stated in the video and providing its own fact sheet.

The power of the internet is the power behind "social media"—which today affects every financial institution. Yes, this is stated in the present tense. Every U.S. financial institution is currently affected by social media, whether or not it has embraced social media as a marketing tool.

So, what is social media? How is it affecting banks? And what do you need to know to understand and manage its risks?

### Social media—a definition

Traditional media is the use of media for one-way communication. It is a method to deliver information to a passive recipient. Examples include print advertisement, a radio or television advertisement, and even internet advertisements such as a "billboard" ad on a non-interactive website.

Social media, on the other hand, is the use of media to create two-way communication. It is intended to create and sustain ongoing conversations among participants—those participants could include customers, potential customers, bank employees, individuals, and business entities. It includes conversations from a bank to third parties and from third parties back to the bank. It also can be expected to create a conversation loop between third parties that do not communicate back to the bank.

Social media takes many forms, including social networking sites, blogs, forums, and bulletin boards. Read about common types of social media.

Social media is an exciting new tool for marketing bank products and services, and for general bank public relations purposes. It can reach thousands, possibly millions, of eyes at far less cost than traditional media. Banks that choose to participate directly in social media opportunities engage with their customers through interaction—in online "conversations" with their customers and other participants—and through the use of social media

outlets for traditional one-way marketing communications. For example, a bank may choose to maintain an interactive "blog," conversing online with participants, and permitting participants to converse with one another. A bank may also choose to simply post information through social media outlets that are designed to direct customers or potential customers to the bank's traditional or online product sources.

### Why care about social media?

Most financial institutions today have not adopted a social media marketing strategy. Many are reluctant to embrace this form of marketing—primarily because of a belief that social media is not relevant to the bank's customer base and/or because of fears of managing compliance risk in an interactive environment. The truth, however, is that even if a bank chooses not to market directly through social media, the bank's customers and employees already use social media for personal and professional purposes and they often do not distinguish between personal and business communications. Read more about the reach of social media networks. This use of social media means that discussions relating to the bank, its customer relations, its products and services, and its performance are currently being discussed in a social media forum—whether you like it or not.

The bottom line is that it does not matter whether your bank is "tweeting" or "facebooking" itself. The extensive reach of social media means that your bank is already facing certain risks which must be identified and managed.

### Social media risks

The risks presented to banks by social media are particularly troubling because they are, to some extent, unknown. Social media is in its infancy. Litigation, case law, and regulatory enforcement cannot keep pace with social media's speedy development. Legal and regulatory authority developed in the traditional media world are not helpful at this point in analyzing risk. Bank regulators have, by and large, not yet addressed social media. The numbers of persons who may see, interpret, or misinterpret a posting is almost infinite. The number of jurisdictions in which those persons reside includes virtually every jurisdiction within and without the United States. Moreover, the bank cannot control whether it is the subject of an electronic "conversation" between other outside participants.

The risks can, however, be made a bit more manageable by breaking them down. The following is a summary of some of the risks which must be. Some risks are applicable primarily to banks marketing through social media. Others are applicable to every bank—even (or especially) those with little understanding of social media.

**Traditional bank compliance.** Bank consumer compliance regulations (fair lending, Regulations E, Z and DD, and more) clearly apply to any "marketing" of bank products, including intentional marketing through social media. These compliance issues are identical regardless of whether a bank markets through traditional media or uses a Facebook page or Twitter account. As discussed below, controlling compliance risk when using social media requires the establishment of proper processes and adequate controls, taking into account the nature of the new media.

What makes compliance officers cringe and management concerned is that the compliance risk seems very different, since the bank can only control content it provides and cannot easily control what other participants in the online "conversation" may say.

The truth is that the bank can never fully control third-party content—it can manage employees, establish monitoring processes, as discussed in the risk mitigation section, and it can limit content on its own social media forums; but it cannot be responsible for what unrelated third parties communicate.

Yet lack of control over consumers is not a free pass.

E-commerce companies have faced online liability where they provided a forum that elicited specific information in violation of applicable law. For example, in the much discussed Roommates.com case, website operators lost immunity by prompting responses about roommate preferences in drop-down menu format. The questions asked triggered many consumers deciding to enter information, such as racial preferences, that violated the Fair Housing Act. Likewise, banks should be on the lookout for liability under bank regulations for prompting certain content from participants in bank-related social media discussions.

In focusing on compliance risk associated with the bank's marketing content, some bankers have focused on the difficulty of remaining in technical compliance with regulatory requirements in the environment of certain social media forms—for example, since Twitter limits each "tweet" to 140 characters, how can the bank comply with technical requirements to include "member FDIC" or the Fair Housing Lender logo?

While these are fair issues to raise (especially in light of the fact that there is no regulatory guidance as yet), such risks are regulatory in nature, generally without significant financial risk to the bank. The riskier compliance issues are those that create greater financial risk to the bank—such as failing to provide a correct APR, or misstating terms, or improperly soliciting information from participants.

The difficulty in dealing with traditional bank compliance issues in the context of social media is in controlling and educating those people posting on behalf of the bank—or even on their own behalf—so that they recognize when they are engaged in "advertising," thus triggering compliance obligations. For example, an advertisement, for Regulation Z purposes, is "a commercial message in any medium that promotes, directly or indirectly, a credit transaction." Therefore, what may appear to be "conversational" on a blog ("The money market account at ABC Bank is a great deal—no fees if you keep a small balance!") is likely to be considered advertising for compliance purposes.

Online legal risks. Any laws or regulations that affect the marketing or online delivery of products or services are potentially applicable to the bank's use of social media. For example, the bank's online privacy policy needs to be consistent with the manner in which information is collected and used on social media sites. The Children's Online Privacy Protection Act (or "COPPA") affects any online service directed to children, or any online site directed at a general audience which could collect information about children.

COPPA is one of the few laws which has specifically resulted in regulatory enforcement in the social media environment. In 2006, the Federal Trade Commission assessed a \$1 million civil penalty against Xanga.com, Inc., a social networking site that failed to comply with COPPA.

Other online risks include third-party linking from the bank's site or forum, as well as risks related to malware imported to the site by users and other fundamental data security and privacy concerns.

Defamation. Banks can be affected by claims of defamation on social networking sites as a result of official or unofficial comments made by bank employees or by third parties using the bank's hosted blog or other website. The kind of comments which could lead to claims include employees or third parties making comments about the bank, the bank's competitors, the bank's supervisors, or other employees.

False or deceptive advertising/unfair or deceptive acts and practices. The Federal Trade Commission Act requires FTC to act to prevent deceptive and unfair acts and practices. Advertisements must not mislead consumers and must not be unfair to consumers. Thus, claims made by banks or its employees in any context that could be deemed "advertising" must be accurate and must not make unsubstantiated claims. FTC publishes advisory "Guides Concerning Use of Endorsements and Testimonials." In October 2009, FTC revised the Guides to deal specifically with blogging or other online activities.

The Guides make clear that if an employee posts information promoting or endorsing the employer's products or services, the employee must clearly and conspicuously disclose his/her relationship to the employer. This includes not only a bank-initiated posting, but would also include employee product endorsements for products described on an unrelated blog or website.

**Securities laws.** A bank may run afoul of the securities laws by posting or failing to understand the powerful nature of internet postings, including postings by the bank or its employees on blogs or social networking sites. The Securities and Exchange Commission published an interpretive release with an effective date of Aug. 7, 2008 in order to guide companies on the use of company websites. Some of the guidance applies directly to blogging and other social media outlets. The release makes clear that forums on a company's website are subject to the antifraud provisions of the federal securities laws.

**Privacy and data security.** A bank-hosted blog or forum raises privacy concerns if a customer fails to understand the public nature of the forum and provides confidential information, or if an employee addresses a customer inappropriately. In addition, data security concerns are always implicated when a bank permits access to its website. For banks in particular, consumers expect banking sites to be encrypted and secure. However, the bank might also have a forum or other portion of its site not related to bank accounts that does not use encryption. Differences in the handling of data must be clearly disclosed to the site's users.

**Reputation risk.** In the social media environment, a bank faces reputation risk from a variety of directions. Some include:

- Failing to properly manage compliance and other risks, whereby the bank can find itself damaged by inadvertent violations of laws or regulations by itself or its employees.

- Hijacking of the bank's name by imposters who create a "phishing" site in order to acquire sensitive financial information.

- Risking exposure to defamation or inflammatory comments directed at the bank in a manner and in a forum that could be very harmful to the bank's reputation.

#### Risk mitigation measures

The exploding growth of social networking and other types of social media require every bank to adopt a comprehensive social media strategy—even those banks that do not now and have no intention to market through this type of media. Risk mitigation is an essential element. While risk mitigation strategy will be different for each bank, several elements should be a part of each bank's strategy.

#### Employee policies/training/controls.

Each bank should adopt an internet use policy which addresses the employee's use of social media in connection with the bank:

- Social media and banking details don't mix. Banks should prohibit employees from providing any statement on a social networking site, blog, or other internet forum concerning the availability, terms, and conditions (such as pricing or fees) of the bank's products or services, or qualification requirements for the products or services.

• Insist on disclaimers. If the employee mentions the bank's name in a posting, the employee should be required to include a disclaimer that the views expressed are personal, and not the views of the bank.

The bank may consider prohibiting the use of the bank's name at all, other than as the employee's employer. This "zero tolerance" approach might be preferable because of the difficulties associated with fully educating employees on all of the potential risks. For example, an employee posting, "I work at ABC Bank and our commercial portfolio is showing huge stress..." is creating potential reputational risk for the bank, though that employee is not addressing products or services.

• Explain the downside. Employees should be carefully trained—they need to understand the requirements of the bank's policy, and the ramifications of any failure to follow that policy. The bank should work to monitor employee use of social media to the extent the bank deems it appropriate, from a risk management standpoint. When a violation is discovered, enforcement should be clearly understood and consistently applied.

Marketing strategy. For banks that include social media in their marketing strategy, each bank should establish internal policies and procedures for prior approval of any content.

Control of content should be no less rigorous than marketing content delivered through traditional means. This means that the employees or departments charged with delivering online messages should not be chosen because of their technical expertise, but because of their understanding of the legal and regulatory issues surrounding commercial communications.

The necessity of maintaining a clear marketing strategy—including involvement of the bank's compliance and legal staff or outside advisors in the process, and using marketing personnel who understand and follow the bank's internal policies—is made more clear by the fact that the regulators will be looking at social media practices during the course of compliance examinations. (See, for example, FDIC's Compliance Information and Document Request Template, which includes a question concerning the use of social media by the bank.)

Social media marketing, and the internet in general, place an emphasis on fast and effective communication. In order for the bank to make the best use of these new tools, its review processes may need to be streamlined and the bank may need to individuals to these duties who are able to accomplish the reviews very quickly. However, while speed is essential, these communications require the same level of review as more traditional marketing. They are likely to be viewed by far more eyes than an advertisement in a local newspaper.

Terms of use. A bank that hosts blogs or participates in social networking sites should include terms of use on the sites. The bank should determine how to deliver the terms of use (in a link at the bottom of a page? A required click-through agreement?). In addition, it should include specific requirements for participation. Points that may be included in this context: age restrictions; the right of the bank to choose not to publish a comment; the bank's ownership rights, if any, in the post; a prohibition against defamation or improper use of trade names or trade secrets; prohibitions against vulgar or inflammatory language; prohibitions or limitations on uploading software to the site or providing links to external sites.

The terms of use should also include other appropriate disclaimers and education for users. For example, users should be reminded that the bank would never seek to obtain personal information on the public site. Users should be told to avoid providing any personal or confidential information on the site; instead, they should be referred to the bank's secure communication site or to a customer service number. And it should be made clear that the bank is not responsible

for posts by others on the site, or for the safety or content of any linked third- party site.

Avoid boilerplate here. The terms of use should be a carefully considered agreement, tailored to the specific type of site or social media outlet that the bank hosts or uses. Banks using social media should regularly monitor the sites for violations of the terms of use and possible misuse by the bank's own employees.

The bank should have a notice and takedown procedure for content related issues. If extensive social networking will be conducted on a bank-controlled site, the bank should consider the appointment of a Digital Millennium Copyright Act agent to ensure compliance with the DMCA to avail itself of infringement immunity for posted content. (For a U.S. Copyright Office background on the 1998 DMCA, [click here](#).)

Use and control of third-party sites. Banks need to address ownership and control of bank-related social networking tools, such as Facebook fansites and Linked-in groups. A properly drafted social networking policy will make sure that the bank, and not an employee (or former employee) controls such tools. Social networking sites such as Facebook also provide privacy controls that can be used to limit access to a bank's site.

In developing a social media strategy, banks should carefully consider using the privacy controls provided, especially permissions granted to groups. Permitting a social networking site to grant content access to members of groups may sound harmless, but many people find themselves members of very large groups, such as members of a particular city or alumni of a university.

Develop a brand management strategy. Whether or not a bank is engaged in marketing through social media, the bank should establish a strategy, through its information security policy and other means, to detect harmful or defamatory use of the bank's name or brand on social media sites. In addition, banks should consider a strategy to detect and aggressively defend the use of the bank's name in order to mitigate the risk of fraudsters impersonating the bank. Search engines and related, specialized tools can help the bank monitor use of and reference to its name online.

While social media is a new phenomenon with new technological and societal issues, the risks posed are only expanded versions of risks banks have always faced. The means to managing those risks is really the same as managing any other risk affecting the bank: assessment of how the risks affect you; developing appropriate policies and procedures; training and re-training your employees in a meaningful way; monitoring your use of social media and employee compliance; and enforcing policies when mistakes or missteps are discovered.

**Disclaimer:** This article provides general information only. It is not intended to be a comprehensive summary of the law or to treat exhaustively the subjects covered. This information does not constitute legal advice or opinion.

#### About the author

Karen Garrett, partner in the law firm of Stinson Morrison Hecker, has been engaged in a legal practice focusing on financial institution regulatory and operations matters for over 25 years, in private practice and as an in-house lawyer at a large regional bank. Garrett has significant experience working with financial institutions, trade associations, and other financial and non-financial businesses regarding operational matters and payment systems. As in-house counsel and outside counsel, Garrett has frequently worked with clients on product development, focusing on legal and compliance issues surrounding new products and services. She can be reached at [kgarrett@stinson.com](mailto:kgarrett@stinson.com), 816-691-3233.

[This article was posted on February 25, 2010, on the website of ABA Banking Journal, [www.ababj.com](http://www.ababj.com), and is copyright 2010 by the American Bankers Association.]