

Forward-thinking financial institutions need to be aware of social media compliance risks

By Jared C. Searls, Esq., *Bradley Arant Boult Cummings LLP*

AUGUST 16, 2019

It is easy to forget that in the not-so-distant past the phrases “follow us,” “friend us” and “use our hashtag” would have confounded many business audiences. Today, these phrases are commonplace. Indeed, social media forms the core of many companies’ marketing strategies, and financial institutions continue to explore new ways to utilize social media.

Social media is a powerful tool that can allow financial institutions to increase customer engagement, expand customer bases and provide more user-friendly and efficient services.

Social media is a powerful tool that can allow financial institutions to increase customer engagement, expand customer bases and provide more user-friendly and efficient services. However, financial services institutions must ensure they are adequately managing the unique compliance risks associated with social media.

WHAT IS SOCIAL MEDIA?

In 2013, the Federal Financial Institutions Examination Council issued guidance on the use of social media on behalf of its members, which include the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corp., the National Credit Union Administration, the Consumer Financial Protection Bureau and the State Liaison Committee.

In that guidance, the FFIEC defined “social media” as “a form of interactive online communication in which users can generate and share content through text, images, audio and/or video.”¹

The FFIEC identified the interactive nature of social media as one of its defining features and excluded traditional electronic mail or text messages from the definition.

RISKS ASSOCIATED WITH USING SOCIAL MEDIA

The FFIEC outlines three areas of risk: compliance and legal risk, reputation risk, and operational risk.² Compliance and legal risks

arise from the potential for violations of — or nonconformance with — various legal requirements, policies and procedures or ethical standards.

Reputation risks arise from negative public opinion. Operational risks are associated with inadequate or failed processes, people or systems. While this commentary focuses primarily on compliance and legal risks, it is equally important to understand all types of risks associated with the use of social media.

WHO USES SOCIAL MEDIA?

As of April 2019, there were 2.32 billion monthly active users on Facebook and one billion active monthly users on Instagram.³ According to the Pew Research Center’s 2019 survey on social media use, about 70% of U.S. adults reported that they have used social media outlets.⁴

The most popular social media platforms are YouTube and Facebook, with 73% of U.S. adults using YouTube and 69% using Facebook. Of the Facebook users, 74% reported that they visit the site daily.

After YouTube and Facebook, there is a drop-off in the number of U.S. adults using other platforms, with 37% using Instagram, 28% using Pinterest, 27% using LinkedIn, 24% using Snapchat and 22% using Twitter.⁵

Unsurprisingly, younger U.S. adults, ages 18-29, use social media at a higher percentage rate. For example, while 69% of Americans use Facebook, 79% in the 18-29 age demographic do so. The usage among age groups can differ drastically.

For example, only 37% of Americans use Instagram — much lower than the 69% using Facebook. Also, 67% of Americans ages 18-29 reported that they use Instagram, while only 23% of people ages 50-64 said they use this outlet.⁶

Social media usage also differs across gender, racial and economic groups. For example, 42% of American women reported that they use Pinterest, but only 1% of American men said they do so.

Similarly, 28% of white Americans said they use LinkedIn, while only 16% of Hispanic Americans reported that they use that platform. In addition, 49% of Americans that have an annual

income over \$75,000 said they use LinkedIn, but only 10% of Americans that have an annual income under \$30,000 reported that they use that platform.⁷

These differences can impact a financial services institution's compliance risk when posting to various social media platforms.

HOW DOES YOUR COMPANY USE SOCIAL MEDIA?

Social media, with some limited exceptions, is governed by the same laws that generally govern your financial institution (i.e., there generally are no specific laws associated with social media). Therefore, your company's social media risk is primarily defined by how your company uses social media.

For example, social media is a useful tool for debt collectors, including financial institutions, when they qualify as debt collectors under the Fair Debt Collection Practices Act, 15 U.S.C.A. § 1692. Indeed, a debt collector could use social media to gather information regarding a debtor (e.g., the debtor's location, contact information, employment status, etc.) and to contact a debtor.

Compliance and legal risks arise from the potential for violations of, or nonconformance with, various legal requirements, policies and procedures or ethical standards.

However, the debt collector must consider the risk under the FDCPA, which applies to social media. While the FDCPA does not prohibit debt collectors from using social media, the Federal Trade Commission requires them to consider the specific requirements associated with using it: making required disclosures, avoiding deceptive communications and revealing the existence of a debt to third parties.

These considerations, in action, are often obvious. At other times, however, a violation may be a bit more difficult to see at surface level. For example, an obvious violation of the FDCPA would occur if a debt collector wrote on a debtor's Facebook wall. The same can be seen by third parties and, clearly, the debt collector would have violated the FDCPA by posting.

One less obvious example that the FTC has specifically referenced is that requesting to join a debtor's social media network (e.g., "friending" the debtor on Facebook), violates the FDCPA if the debt collector does not make the disclosures required by Section 807(11) of the FDCPA. That section requires debt collectors to disclose clearly, in all communications made to collect a debt or to obtain information about a consumer, that they are attempting to

collect a debt and that any information obtained will be used for that purpose.

Therefore, it is important to look not only at a surface level, but to also develop a robust risk analysis for any social media engagement.

YOUR COMPANY'S PLATFORMS

While social media platforms share some common features, individual platforms vary greatly in their structure, features, user demographics, etc. The differences between platforms can significantly alter your company's risk.

For example, some social media platforms require users to attest that they are at least 13 years of age. The presence or absence of this type of assertion can impact how your company approaches compliance with the Children's Online Privacy Protection Act, commonly called COPPA, 15 U.S.C.A. § 6501, which imposes specific obligations regarding the collection, use and disclosure of a child's personal information.

INTEGRATING SOCIAL MEDIA INTO YOUR EXISTING PLATFORM

Social media platforms are, by definition, outside of your company's normal operating systems. Therefore, many of the controls and protections that your company takes for granted when operating on its internal platforms are not present when using social media.

For example, your communications with a customer over social media may be subject to document retention requirements. While your normal operating platform likely includes automated features that ensure you retain customer communications for the appropriate amount of time, your social media platform may not incorporate these same features.

Perhaps most importantly, your normal operating system has features designed to protect your customer's private information. When your company uses social media, you are likely relying on the social media platform's security features.

ARE YOU CONSIDERING ALL THE ISSUES?

While many social media-related legal and compliance risks are easy to identify, others are more obscure. As an example, financial institutions commonly use social media for advertising. As many institutions are aware, advertising related to lending is governed by a litany of federal and state laws. We will focus on one rather narrow example of advertising that may present some not-so-obvious compliance risks.

Consider a financial institution that uses Instagram, LinkedIn and Twitter as its only social media platforms. The financial institution creates an advertisement for a special reduced

rate product that it wants to post to the three social media outlets. It considers Regulation Z's advertising disclosure requirements and drafts an advertisement that adequately discloses the annual percentage rate and other features of the product.

The financial institution, aware that some courts have found that certain forms of social media messages must comply with the Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C.A. § 7701, commonly called the CAN-SPAM Act, took appropriate steps to ensure it mitigated whatever risk it might have under that act.

Conducting a risk assessment is the first step to effectively manage the legal and compliance risk associated with social media.

The institution starts its post for Twitter only to discover that the very short character limitation eliminates half of the message, including the required disclosures. It then decides to post the advertisement to LinkedIn and Instagram, where the character limit is a non-issue. That may resolve that portion of the problem, but it may also open up new potential liability.

The Equal Credit Opportunity Act, 15 U.S.C.A. § 1691, prohibits any creditor from discriminating against any applicant with respect to any aspect of a credit transaction on the basis of race, color, religion, national origin, sex, marital status or age. One way that a creditor can violate the ECOA is via disparate impact — when a facially neutral policy or practice that has an adverse impact on a member of a protected class.

As previously mentioned, 28% of white U.S. adults use LinkedIn, but only 16% of Hispanic U.S. adults use LinkedIn. Moreover, 67% of U.S. adults ages 18-29 use Instagram, while only 23% of U.S. adults ages 50-64 and 8% of U.S. adults ages 65 and over use Instagram.

Looking to our example, the financial institution decided to run the advertisement only on LinkedIn and Instagram. It is possible that the use of only these two outlets, over time, could lead to disparate impact on the basis of both race and age because of the differences in the percentage of Americans who use each site.

In other words, a 65-year-old individual could claim that the use of Instagram to promote an exclusive offer violates the ECOA because such advertising discriminates against individuals not using the site — specifically adults over the age of 50.

Likewise, a Hispanic American could make the same argument using the exclusive offer or advertisement promoted on

LinkedIn. Thus, what the financial institution thought were good, compliant advertisements may end up violating relevant regulations simply because of the institution's failure to consider the outlet on which the advertisements were placed.

APPROPRIATE SOCIAL MEDIA COMPLIANCE PROCESSES

Conducting a risk assessment is the first step to effectively managing the legal and compliance risks associated with social media. The risk assessment should identify how your company uses social media (e.g., advertising, customer communications, complaint management, etc.), and it should identify the social media platforms used by your company and the laws implicated by your various uses of social media.

Once the risk assessment is complete, your company should ensure that its risk management program addresses identified risks. For example, if your company uses Twitter to communicate with customers, you should have a defined policy regarding the types of information you will exchange over Twitter, when you will move the conversation to your normal operating environment, etc.

You should also ensure that your company trains employees to make sure they understand your policy, regularly assesses its compliance with your policy and institutes appropriate controls to manage the risks you identified in your assessment.

Finally, you should closely monitor developing laws and regulations that might affect your social media policy and controls. As financial institutions continue to use social media in new ways, the regulatory landscape will continue to evolve. Absent a robust monitoring program, your company could quickly fall behind and fail to implement the changes necessary to implement the latest social media guidance.

NOTES

- ¹ "Social Media: Consumer Compliance Risk Management Guidance," <https://bit.ly/1ikHTJM>.
- ² *Id.*
- ³ "Most popular social networks worldwide as of April 2019, ranked by number of active users (in millions)," <https://bit.ly/2ddRJIH>.
- ⁴ See Andrew Perrin and Monica Anderson, "Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018," <https://pewrsr.ch/2WTBSky>.
- ⁵ *Id.*
- ⁶ "Use of different online platforms by demographic groups," <https://pewrsr.ch/30WgbJJ>.
- ⁷ *Id.*

This article first appeared in the August 16, 2019, edition of Westlaw Journal Bank & Lender Liability.

ABOUT THE AUTHOR



Jared C. Searls is an attorney and member of the financial services litigation team in the Birmingham, Alabama, office of **Bradley Arant Boult Cummings LLP**. He focuses his practice on assisting financial institution clients on a wide variety of litigation and regulatory compliance matters. He can be reached at jsearls@bradley.com.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.