# Social Media Guide for Financial Institutions

March 2016 Update

Chapman and Cutler LLP

Attorneys at Law · Focused on Finance®

# SOCIAL MEDIA GUIDE FOR FINANCIAL INSTITUTIONS

March 2016 Update

Heather L. Hansche
Lindsay S. Henry

# Table of Contents


SECTION PAGE

Overview ..... 1

Business Use of Social Media ..... 3

Brand Awareness and Image ..... 3

Marketing and Market Intelligence ..... 3

Customer Experience ..... 4

Risks from Social Media Use ..... 4

Reputation Risk, Brand Damage, and Brand Identity Theft ..... 4
Confidential Business Information ..... 5
Privacy and Use of Customer Information ..... 5
Disparaging Comments, Defamation, Harassment, and Intentional Infliction of Emotional Harm ..... 5
Compliance with Applicable Laws, Regulations, and Terms of Use ..... 5
Third-party Risk ..... 6
Operational Risk ..... 6

Social Media Risk Assessment ..... 7

Social Media Network Participation ..... 7

Terms of Use and Privacy Policies ..... 7

Social Media Sites ..... 7
Financial Institution Sites ..... 8

Third-party Arrangements ..... 8

Social Media Guidelines and Policies ..... 8

Crisis Response Policy ..... 9

Privacy Policy ..... 9

Training ..... 9

Legal and Regulatory Considerations ..... 11

FFIEC Guidance ..... 11

Compliance and Legal Risk ..... 13

Deposit and Lending Products ..... 13
Truth in Savings Act (TISA) ..... 13
Fair Lending Laws ..... 13
Fair Credit Reporting Act (FCRA) ..... 13

Truth in Lending Act (TILA) ..... 14
Real Estate Settlement Procedures Act (RESPA) ..... 14
Fair Debt Collection Practices Act (FDCPA) ..... 15
Unfair, Deceptive, or Abusive Acts or Practices ..... 15
Deposit Insurance or Share Insurance ..... 15
Advertising and Notice of FDIC Membership ..... 15
Advertising and Notice of NCUA Share Insurance ..... 15
Interagency Statement on Sales of Nondeposit Investment Products (Interagency Statement) ..... 15

Payment Systems ..... 16
Electronic Fund Transfer Act (EFTA) ..... 16
Check-based Transactions ..... 16

Bank Secrecy Act/Anti-Money Laundering Program ..... 16

Community Reinvestment Act ..... 16

Privacy ..... 16
Gramm-Leach-Bliley Act (GLBA) Privacy Rules and Data Security Guidelines ..... 16
CAN-SPAM Act and Telephone Consumer Protection Act (TCPA) ..... 17
Children's Online Privacy Protection Act (COPPA) ..... 17
Reputation Risk ..... 18
Operational Risk ..... 18

Federal Trade Commission ..... 18

.com Disclosures: How to Make Effective Disclosures in Digital Advertising ..... 19
Operation Full Disclosure ..... 20
Guides Concerning the Use of Endorsements and Testimonials in Advertising ..... 20
The FTC's Endorsement Guides: What People Are Asking ..... 20
Native Advertising ..... 21
FTC Native Advertising Workshop ..... 21
Self-regulatory Advertising Principles ..... 22
Search Engine Advertising Guidance ..... 22

National Labor Relations Act and State Employee Social Media Laws ..... 22

National Labor Relations Act ..... 23
State Laws — Access to Employee Social Media ..... 24

Employee Social Media Policies ..... 25

Conclusion ..... 27

More Information ..... 28

# Overview

In 2011 the term "social media" was added to the *Merriam-Webster's Collegiate Dictionary*. The dictionary indicates that the phrase was first used in 2004 and provides this definition: "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)." Wikipedia — uniquely positioned to supply a definition of social media as the online encyclopedia created by collaborative efforts of an online community — offers this definition of social media: "computer-mediated tools that allow people to create, share or exchange information, ideas, and pictures/videos in virtual communities and networks."

Social media is extremely popular. Among adults in the United States who use the Internet, 74% are on a social media network: 71% use Facebook; 23% use Twitter; 26% use Instagram; 28% use Pinterest; and 28% use LinkedIn.[1] Further, now more than half of online adults use multiple social media sites, which represents a significant increase in just the past two years. The forms of social media change rapidly and currently include social networking sites, microblogging, social news sites, consumer review sites, photo sharing, video sharing, virtual worlds, and gaming. The pace of change is illustrated by the Federal Financial Institutions Examination Counsel ("FFIEC") Social Media: Consumer Compliance Risk Management Guidance (the "FFIEC Guidance") issued in December 2013, which includes these examples of social media: Facebook, Google+, MySpace, Twitter, Yelp, Flickr, YouTube, LinkedIn, Second Life, FarmVille, and CityVille. Notably missing from the FFIEC's list are these fast-growing channels: Instagram, Pinterest, Tumblr, Vine, and Snapchat.

Social media is an important consideration for financial institutions because their regulators have issued formal guidance on the topic, requiring financial institutions to incorporate the guidance in their risk management programs. The FFIEC Guidance was initially proposed in January 2013 and became effective in December 2013. It applies to all financial institutions regulated by the federal banking agencies, the Consumer Financial Protection Bureau ("CFPB"), and the National Credit Union Administration ("NCUA"), and when it was published the FFIEC encouraged state banking regulators to adopt the guidance for the financial institutions they supervise. To date, the Conference on State Bank Supervisors, the trade association for bank regulators that develops and coordinates supervision policies for banks, has not provided guidance on social media activities for banks. In addition, the Illinois Department of Financial and Professional Regulation, Division of Banking, has not acted on this issue for Illinois banks. Aside from regulatory concerns, social media is also an important consideration for all financial institutions because, as these statistics demonstrate, financial institution customers and employees are involved in social media. Customers' involvement and willingness to share information about themselves allow financial institutions to interact with customers, promote products and services, and obtain information about customers for market analysis purposes — compelling reasons for a financial institution to become involved on an enterprise-wide basis.

Each of these undertakings is limited by law, regulations, and guidance, such as the FFIEC Guidance that directs financial institutions to implement risk management policies and procedures to manage the use of social media. This Guide discusses these topics and provides a framework for financial institutions to identify

---

1 Maeve Duggan, Nicole B. Ellison, Cliff Lampe, Amanda Lenhart, and Mary Madden, Pew Research Center, *Social Media Update 2014* (January 9, 2015), http://www.pewinternet.org/2015/01/09/social-media-update-2014.

and evaluate their involvement in social media and steps to maximize benefits and mitigate business and legal risks.

# Business Use of Social Media

### Brand Awareness and Image

Brand awareness and image are the most obvious motivations for a company's engagement in social media. Social networking channels such as LinkedIn, participation on microblogs such as Twitter, Google+, and Facebook, and sponsorship of blogs can be used to connect with customers. Such social media participation can enhance a brand name in many ways, such as by providing consumer education and positioning a business as a source of expertise, providing information about the company's community involvement, including informing consumers of philanthropic efforts, and providing updates on locations, including weather-related closings and changes in hours that impact a customer's use of a business's services.

As would be expected, retail and consumer goods businesses are the most active on social media. Facebook lists the following brands with the most fans: McDonalds, Disney, MTV, Red Bull, Samsung Mobile, FIFA World Cup 2010, KFC, Converse, and National Geographic.[2] While no financial institutions are listed in the Facebook fans' top ten, of those financial institutions with a Facebook company page, Capital One, Chase, and Bank of America have the largest number of fans,[3] while CitiBank, Bank of America, Goldman Sachs, and Chase have the largest number of Twitter followers.[4]

Several banks including Citibank, Bank of America, and Wells Fargo have multiple social media accounts on single social media channels, and Chase and Wells Fargo have "social media command centers" that monitor the mention of their companies on social networks and respond to customer comments.[5] Social media engagement is not limited to large banks — the Independent Community Bankers Association of America began issuing an annual list of its Top Community Bank Leaders in Social Media in 2013 as part of its initiative to assist its members in their social media engagement.[6] The 2015 list includes four Illinois banks — MB Financial, Busey Bank, Bank of Springfield, and First American Bank — as banks that use social media as an integral part of their marketing and communications strategies.[7]

### Marketing and Market Intelligence

Other benefits of corporate participation in social media networks are product marketing and promotion and driving customers to the company's website. McDonalds, one of Facebook's top ten, reports

---

2 http://fanpagelist.com/category/corporate_brands.

3 http://thefinancialbrand.com/52752/power-100-2015-q2-facebook-banks.

4 http://thefinancialbrand.com/52757/power-100-2015-q2-twitter-banks/.

5 Mark Calvey, *Wells Fargo's listening: Bank unveils 'social media command center' in San Francisco*, http://www.bizjournals.com/sanfrancisco/blog/2014/03/wells-fargo-social-media-twitter-facebook-linkedin.html; Rachel Louise Ensign, *Social Media Transform Bank-Customer Interplay* (March 13, 2014), http://online.wsj.com/news/articles/SB10001424052702303546204579437692833009398.

6 http://www.icba.org/smleaders/index2.cfm.

7 *Id.*

$292 million in product spending by Facebook fans as compared to $188 million for non-Facebook fans, underlining the powerful effect of its social media presence.[8] A business can expand its reach by combining traditional marketing tools with social media, for example, posting its television advertisements on channels such as Facebook, Twitter, and YouTube.

Because social media is interactive, a company can gather information on the public's perception of the company, its products, and its services. Various monitoring and analytic tools are available that listen to customers, competitors, and critics, providing information that can be used in developing customer service initiatives and in product design. Social media networks can also be used to gain information on customers that the company can use to deliver customized messaging, promotions, and online behavioral advertising.

### Customer Experience

Customer review sites as well as social media channels where a company has an account allow companies to communicate directly with customers faster and outside the typical call center environment to address specific customer concerns and demonstrate excellent customer service for others who have viewed the negative comment. For example, Bank of America invites customers seeking assistance to contact it through Twitter and Facebook. These sites can also be used to send a single company message about a topic of general concern to multiple followers instantly, such as information regarding weather-related location closings or a change in hours.

### Risks from Social Media Use

There are both business and legal risks associated with the use of social media. The extent to which the risks apply to each organization will vary based on the degree of an institution's and its employees' participation in social media. The FFIEC Guidance points out, however, that even financial institutions that do not actively engage in social media will have risks that must be assessed, monitored, and addressed in their social media policies.[9] The following identifies categories of business and legal risks and provides examples of each.

#### I. Reputation Risk, Brand Damage, and Brand Identity Theft

- Comments made by social media users (including employees) and phishing and fraudsters masquerading as the financial institution may not be identified quickly or responded to appropriately.

- Terms of use of the social media channel may license the financial institution's intellectual property, allowing it to be used without the permission or control of the financial institution.

- Customers may perceive the actions of the third-party channel as actions by the financial institution using the site.

---

8 *The Value of a Facebook Fan 2013: Revisiting Consumer Brand Currency in Social Media* (April 2013), http://www.syncapse.com/wp-content/uploads/2014/11/Syncapse_Value-of-a-Fan-Report_2013-FINAL.pdf.

9 *Social Media: Consumer Compliance Risk Management Guidance* Federal Financial Institutions Examination Council, (December 11, 2013), https://www.ffiec.gov/press/PDF/2013_Dec%20Final%20SMG%20attached%20to%2011Dec13%20press%20release.pdf.

- Out-of-date or incorrect information or responses may result in negative public opinion.

### II. Confidential Business Information

- Release of confidential information of the financial institution, including products, business plans, or payroll, may occur.

### III. Privacy and Use of Customer Information

- Release of private customer information in a manner that violates applicable law or is inconsistent with the financial institution's privacy policy may occur when the financial institution responds to consumer concerns or in connection with promotions, including endorsements.

- Users may post confidential information about themselves or others on a financial institution's social media page or website even if this conduct is prohibited under the terms of use.

- Children under age 13 may post personal information about themselves even if this conduct is prohibited under the terms of use. This may be of greater concern if the financial institution's social media page or website includes activities directed toward children.

- The financial institution may not adequately disclose the types of customer information obtained by it during its monitoring and analyzing of customer behavior on social media channels. These activities may violate applicable law or the financial institution's privacy policy and terms of use.

- Customers concerned about their privacy may adversely view a financial institution's use of this information for behavioral marketing even if such use is allowed under applicable law and the financial institution's privacy policy and terms of use.

### IV. Disparaging Comments, Defamation, Harassment, and Intentional Infliction of Emotional Harm

- Disparaging comments or misrepresentations about a customer may be posted by an employee on the financial institution's social media page or website or on the employee's personal pages in response to a customer concern or otherwise.

- An employee or former employee may post disparaging comments about a coworker.

### V. Compliance with Applicable Laws, Regulations, and Terms of Use

- Social media posts may contain sufficient terms to be deemed advertising under various federal consumer financial protection laws without otherwise adhering to applicable legal requirements.

- Posts may contain endorsements subject to the Federal Trade Commission ("FTC") Endorsement Guides without complying with the disclosure requirements.

- Posts may be viewed as an unfair, deceptive, or abusive act or practice.

- Financial institution regulators may monitor social media networks to identify possible compliance issues.

- Each social media channel requires users to agree to its terms of use, which may limit the promotion of financial services and related content; for example, Facebook prohibits paid "likes" and Twitter allows promoted posts of certain financial services and related content only if approved by Twitter.

### VI. Third-party Risk

- A financial institution may choose to use a third party to provide services related to its social media activities, for example, to monitor its social media presence and to help with engagement within social media networks (posting and replies). As with all third-party service providers, the financial institution is responsible for the activities delegated to the third party.

- Participation as a user on a social media network exposes the financial institution to reputation and operational risk related to the conduct of the network.

- The financial institution is responsible for its compliance with the social media channel's terms of use, which can be unilaterally changed without notice.

### VII. Operational Risk

- Information technology risks including failed systems or processes apply to a financial institution's use of social media.

- There is a risk of takeover of the financial institution's social media pages or website.

- There is a risk of the introduction of malware when financial institution-owned devices are used to access social networking sites.

- Socially engineered risks to obtain login credentials of employees and customers accessing social media sites exist.

# Social Media Risk Assessment

Under the FFIEC Guidance, each financial institution is required to perform a social media risk assessment and update it periodically.[10] The risk assessment will be used to identify and measure the financial institution's existing controls to mitigate those risks and, as appropriate, enhance its policies and procedures to address its social media vulnerabilities. Identified below are issues for a financial institution to consider when conducting its social media risk assessment.

### Social Media Network Participation

The first step to performing a risk assessment is to identify all current social media activity and any future social media activity under consideration for the financial institution. This includes identifying the social media networks where the financial institution is a user and has employees participating on behalf of the financial institution.

Since employee personal use of social media may expose the financial institution to risk, the financial institution may also wish to informally survey its employees, perhaps as part of its social media training, to determine what social media activities they participate in personally. The number of employees using a particular social media network may help the financial institution prioritize its risks and risk mitigation activities; provided, however, all such survey activities must be consistent with applicable law, including the National Labor Relations Act and state laws.

The financial institution should review its existing policies to determine whether they adequately address social media and consider whether it has an adequate social media monitoring program including the necessary technology to manage these activities. For example, does the information security policy address social media activities including links between social media channels and the financial institution's website?

### Terms of Use and Privacy Policies

#### I. Social Media Sites

As part of its risk assessment, the financial institution should identify all social media network terms of use and privacy policies that currently apply to it as a user of social media networks and then review them to determine whether they are acceptable. These terms of use may include objectionable provisions such as grants of a sub-licensable, transferable, royalty-free, worldwide license to a user's intellectual property posted on the network; indemnification of the network by the user with no limitations on liability; and the right to change terms of use at any time. The financial institution may choose to limit its use of a social media platform based on the content of its terms of use and privacy policy, for example, by limiting what can be posted to the site.

10 *Id.* at 5.

Terms of use may also prohibit certain practices. For example, Facebook prohibits businesses from incentivizing people to use social plug-ins or to "like" a page. These terms of use change frequently and must be reviewed prior to launching any marketing initiative. In addition, the FTC views such posts as an endorsement, subject to its Endorsement Guides requiring additional disclosures.

### II. Financial Institution Sites

The financial institution should also review its terms of use for employee and public use of social media platforms and determine whether they are adequate to protect the financial institution. In addition to the federally mandated Privacy Notice for financial institutions, the terms of use typically incorporate a website privacy policy. The website privacy policy must correctly describe how the institution obtains information, including through social media channels, tracking, and cookies, and how such information is used by the financial institution. Financial institutions should become familiar with the *Self Regulatory Principles for Online Behavioral Advertising* adopted by the Digital Advertising Alliance and enforced by the Better Business Bureau and the Direct Marketing Association.[11] Financial institutions that engage in behavioral advertising should add disclosures of their data collection practices in the website privacy policy and provide a clear, prominent notice on the page(s) where data is collected that links the consumer to additional information concerning the data collection and the consumer's ability to opt out of targeted online behavioral advertising.

#### Third-party Arrangements

Financial institutions must conduct an evaluation and perform due diligence appropriate to the risks of each third-party service provider they engage and must monitor the service provider's performance consistent with the financial institution's obligations under applicable regulatory guidance, including CFPB Bulletin 2012-03, *Third Party Service Provider Risk Management Policy*; OCC Bulletin 2013-29, *Third-Party Relationships*; FDIC FIL 44-2008, *Guidance for Managing Third Party Risk*; and FRB SR 13-19, *Guidance on Managing Outsourcing Risk.*

To evaluate its compliance with these requirements, the financial institution must obtain due diligence-type information about any service provider it uses related to its social media engagement, including technology companies, companies that monitor and respond to consumer comments, and each social media network of which it is a user. It must also review and revise, as appropriate, all applicable contracts and put in place a system to measure and monitor the service provider's performance.

#### Social Media Guidelines and Policies

All of a financial institution's guidelines and policies that apply to employees and that may govern employee personal use of social media must be reviewed. This review will not be limited to social media-specific policies and should include a review of general policies related to use of institution-owned technology and employee technology for business purposes and confidentiality of business and customer information.

All policies and procedures related to the financial institution's sanctioned social media activities by employees should be identified and reviewed to ensure that these activities have appropriate approval

11 www.aboutads.info/principles.

authorities. Employees should be directed to protect the confidentiality of financial institution proprietary information, and the policy should clarify ownership of the financial institution's social media accounts where sanctioned employees participate on behalf of the financial institution. In addition, the policy should specify whether use of these social media accounts is permitted during working hours and should prohibit discrimination and harassment of individuals as well as defamation and denigration of competitors. Policies should describe the FTC Endorsement Guides and provide disclosures of the employment relationship and require their inclusion in covered posts by employees. The financial institution should also develop practices to monitor these social media activities. Finally, the consequences of violations of the social media policy should be specified and enforced.

These policies should be reviewed and revised, as appropriate, to determine whether they are adequate both to protect the financial institution and to comply with legal requirements that apply to the financial institution as an employer.

### Crisis Response Policy

A financial institution should confirm whether its general crisis response policy has a social media component and, if so, whether it is adequate to address social media events that may quickly have a detrimental effect on the financial institution's reputation. In an era where responses are expected immediately, this expectation is even higher for users of social media. An open response or non-response to questions on a financial institution's social media page can quickly lead to the proliferation of false or misleading information.

### Privacy Policy

A financial institution should review both its website privacy policy and its federally mandated Privacy Notice to see whether they accurately disclose how information regarding customers will be obtained through social media channels and used by the financial institution. To the extent that the privacy policy and notice provide customers a right to opt out of information sharing, such as online behavioral advertising or non-affiliate sharing, the financial institution must ensure that a customer's name is added to the opt-out list promptly and that the list is checked prior to engaging in these activities.

### Training

Financial institutions must provide guidance and training for their employees on the employees' use of social media to control those communications made on behalf of the financial institution as well as personal communications that could be interpreted as having been made on behalf of the financial institution. This includes policies for employee business use (i.e., use of internal company platforms and employees authorized to post on public platforms on the financial institution's behalf) and employee personal, non-work-related use of social media.

The individuals at a financial institution in charge of conducting the social media risk assessment should obtain the employee social media training materials and the financial institution's schedule for social media training, if any. If there are training materials, the financial institution should confirm whether the training materials address the various ways in which the financial institution is engaged in social media. If

there are no training materials, they should be created and a training program should be implemented as part of the institution's new employee or ongoing employee training.

# Legal and Regulatory Considerations

No single body of law governs the use of social media. There are both federal and state laws, agency guidance, and self-regulatory requirements that must be reviewed for applicability to social media activity — some are specific to social media and others are existing laws that apply to certain activities wherever they occur, including on social media. There is also no single definition of social media among the laws that specifically govern social media activity, which means care must be taken when analyzing the application of laws, rules, and guidance to various financial institution activities. In addition, social media platforms generally include terms of use and privacy policies that apply when the platform is accessed and used by a financial institution.

Following is a summary of those laws, rules, and regulatory guidance that apply to a financial institution as a regulated entity promoting its business through social media, including how it may limit its employees' social media conduct. Other employment laws that may be applicable to a financial institution as an employer, such as limitations on screening candidates via social networking sites and intellectual property law, are beyond the scope of this Guide.

### FFIEC Guidance

On December 11, 2013, the FFIEC issued final guidance for financial institutions and non-financial institutions supervised by the CFPB relating to their use of social media. The FFIEC Guidance primarily adopted the terms of the proposed guidance issued in January 2013 and was made effective immediately. The FFIEC Guidance defines social media as "a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video."[12] Messages sent via traditional email or text message are not social media; however, messages sent through social media channels are social media.[13]

Financial institutions are expected to maintain a risk management program that identifies, measures, monitors, and controls risks related to their involvement in social media.[14] A financial institution should obtain input from specialists in compliance, technology, information security, legal, human resources, and marketing to develop its risk management program.[15] The size and complexity of the entity's risk management program should be tailored to the scope of its involvement in social media; however, even a financial institution that does not actively use social media must address risks such as negative comments on social media channels and must establish policies and guidance for employee personal use of social media.[16]

12 *FFIEC Guidance*, at 6.

13 *Id.*

14 *Id.*

15 *Id.* at 7.

16 *Id.* at 6-7.

The financial institution's risk management program can be addressed in existing policies and procedures or in policies and procedures developed specifically for social media activities, and should include at least the following seven elements:

- *Governance Structure*: establish clear roles and responsibilities allowing the board of directors and senior management to direct how social media will be used to further the strategic goals of the institution and assess the risks presented by social media activities on an ongoing basis;

- *Policies and Procedures*: address the use and monitoring of social media and the financial institution's compliance with all applicable consumer protection laws, regulations, and guidance. This should include how social media will, or will not, be used in evaluating loan and deposit relationships. Such policies and procedures should incorporate methodologies to address risks from online postings, edits, replies, and retention;

- *Third-party Relationships*: implement a due diligence process for selecting and managing third-party relationships in connection with social media, including vendors and social media channels on which the institution participates as a user;

- *Training*: establish an employee training program that incorporates the institution's policies and procedures for official, work-related use of social media, and potentially for other uses of social media, including defining impermissible activities;

- *Oversight*: provide for the monitoring of information posted to proprietary social media sites;

- *Audit and Compliance*: verify that both functions have systems in place sufficient to ensure ongoing compliance with internal policies and all applicable laws, regulations, and guidance; and

- *Reporting*: ensure appropriate reporting to the board of directors or senior management that enables periodic evaluation of the effectiveness of the institution's social media program.[17]

The FFIEC Guidance identifies three broad categories of risks related to a financial institution's use of social media: (1) compliance and legal risk; (2) reputation risk; and (3) operational risk.[18]

The majority of the FFIEC Guidance addresses compliance and legal risk, in particular the risk of compliance with consumer protection laws.[19] It provides a list of the various legal and regulatory requirements applicable to marketing and advertising, account origination, and document retention for deposit and lending products, payment system services, and financial institution products and services generally. The FFIEC provides the following specific examples regarding how these requirements apply to activities conducted using social media channels, and cautions financial institutions that the lists are not all-inclusive. The FFIEC warns financial institutions that they must remain aware of legal developments and evaluate how they may apply to the financial institution's social media activities.[20]

17 *Id.* at 7.

18 *Id.*

19 *Id.* at 8-16.

20 *Id.* at 8.

I. Compliance and Legal Risk

***Deposit and Lending Products***

*Truth in Savings Act (TISA)*. TISA imposes disclosure requirements designed to enable consumers to make informed decisions about deposit accounts and prohibits deposit accounts from being advertised in a way that is misleading or inaccurate or that misrepresents the institution's deposit contract.[21] If an advertisement is contained on social media and includes a triggering term, additional terms are required to be disclosed and can be disclosed using a link.

*Fair Lending Laws*. Social media activities must not violate the Equal Credit Opportunity Act ("ECOA") or the Fair Housing Act.[22] The FFIEC Guidance focuses on the ECOA prohibitions against discouraging applicants, timeframes for notifying applicants of adverse action and the reasons for the decision (including whether the reason comes from social media or other sources), the requirement to preserve prescreened solicitations sent through social media, and the prohibition on requesting certain information (age, race, sex, color, religion, or national origin) from an applicant. The Guidance notes that certain social media platforms may maintain such prohibited information about users and cautions financial institutions not to improperly collect the information, use the information, or give the appearance that it uses such information. The Guidance also states that the Fair Housing Act prohibitions on discrimination apply and reminds financial institutions that mortgage lenders who maintain a Facebook page must display the Equal Housing Opportunity logo.

*Fair Credit Reporting Act (FCRA)*. The FCRA contains restrictions and requirements related to prescreened solicitations for credit, responding to disputes, and collecting medical information in connection with loan eligibility. The FCRA also requires financial institutions to provide a notice of adverse action when they rely on information contained in a consumer credit report (similar to the requirement in the ECOA) and to notify a consumer when they rely on information obtained from a third party if such information reflects upon the credit standing, capacity, character, general reputation, personal characteristics, or mode of living of the applicant.

In 2011 and 2012, the FTC determined that companies that market profiles of consumers gathered from online and offline sources for employee background screening are credit reporting agencies subject to the FCRA rules.[23] If a financial institution engages a company to provide background reports that include information from social media for employment decisions, the financial institution must ensure that the company complies with the FCRA requirements as part of its due diligence. The company must take reasonable steps to ensure the maximum possible accuracy of information reported from social media and that such information relates to the correct person. The company also must agree to provide copies of the background reports to consumers and have a process in place if consumers dispute the reports. In addition, the company must notify employers of their responsibility under the FCRA and receive a certification from

21 *Id.* at 8-9.

22 *Id.* at 9-10.

23 https://www.ftc.gov/sites/default/files/documents/closing_letters/social-intelligence-corporation/110509socialintelligenceletter.pdf and https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

the financial institution regarding its use of the reports. The financial institution, as a user of consumer reports, must keep such reports secure and dispose of them properly. Finally, if the financial institution takes adverse action based on information in a report, it must provide an adverse action notice to the consumer.

Similar steps must be taken if the financial institution engages a company to provide background reports that include information from social media for credit purposes. Currently the three largest credit reporting agencies — Experian, TransUnion, and Equifax — do not use social media information in their credit scores, but FICO has indicated that it is evaluating how social media data could be incorporated into its credit scoring model in the future.[24]

Financial institutions should consider whether their employees are permitted to use information they gather from social media sites to make credit decisions. The information posted on social media sites may be incorrect or misleading. For example, a review posted on a user review site (e.g., Yelp) may be biased. Since review sites are not credit reporting agencies, users that post information on review sites are not subject to the FCRA requirements that information furnished be accurate and complete. In addition, financial institutions should consider whether social media data is predictive of the creditworthiness of an applicant. In making this determination, financial institutions should recognize that not all individuals use social media. Failure to take this into account in its underwriting policy may expose a financial institution to a claim that an applicant was treated unfairly.

A financial institution's decision to use, restrict, or prohibit the use of social media data in making credit decisions should be documented as part of its underwriting policy and employees should be trained on how such information can and cannot be used and what records must be maintained so that the financial institution can appropriately respond to requests from consumers and regulators. Finally, if social media data is used, the financial institution will be required to provide the FCRA adverse action notice disclosure for use of third-party information when adverse action is taken.

*Truth in Lending Act (TILA)*. Social media communication that includes an advertisement for a credit product must comply with the TILA and Regulation Z, including required disclosures about loan terms and costs that vary based on the type of loan (i.e., private education loans, home secured loans, and credit card accounts).[25] The Regulation Z rules that govern electronic advertisements apply to social media advertisements, allowing creditors to provide the required disclosures on a different page from the advertisement if (a) the advertisement clearly refers to the page or location where the information is located and (b) the information is provided in a clear and conspicuous manner. Further, the FFIEC Guidance cautions financial institutions that the timeframes for providing TILA disclosures apply to social media advertisements.

*Real Estate Settlement Procedures Act (RESPA)*. The Guidance identifies the RESPA prohibitions on fee splitting and accepting or giving kickbacks in exchange for referrals of settlement services business as applicable to financial institution relationships involving social media.[26] In addition, the RESPA disclosure requirements apply to applications taken electronically through social media channels.

---

24 Stephanie Armour, *Borrowers Hit Social-Media Hurdles: Regulators Have Concerns About Lenders' Use of Facebook, Other Sites* (Jan. 8, 2014), http://www.wsj.com/news/articles/SB10001424052702304773104579266423512930050.

25 *Id.* at 10.

26 *Id.* at 11.

*Fair Debt Collection Practices Act (FDCPA)*. Financial institutions must ensure that their third-party debt collectors (and themselves if they are acting as a debt collector) comply with the FDCPA when using social media to contact a delinquent customer.[27] The FDCPA restrictions on publicly disclosing that a consumer owes a debt apply to communications through social media; for example, a debt collector writing about a debt on a person's Facebook wall may violate the FDCPA. The FDCPA limits on contacting consumers, their families, or third parties in an inappropriate manner and making false or misleading representations also apply to communications made through social media.

*Unfair, Deceptive, or Abusive Acts or Practices*. The FFIEC reminds financial institutions that a practice can be unfair, deceptive, or abusive despite technical compliance with other applicable laws.[28] The agencies caution financial institutions that they should not engage in any practice or advertising through social media that could be deemed to be unfair, deceptive, or abusive. Finally, the FFIEC Guidance notes that financial institutions must take care to ensure that any social media communication is accurate, consistent with other information presented by the financial institution through electronic media, and not misleading.

*Deposit Insurance or Share Insurance*. Both the Federal Deposit Insurance Corporation ("FDIC") and the NCUA requirements apply to advertising or other activities conducted using social media.[29] These include:

> Advertising and Notice of FDIC Membership. The institution must include the official advertising statement of FDIC membership in each advertisement of FDIC-insured products. The FFIEC Guidance reminds financial institutions that the FDIC advertising statement must appear even in a message that promotes non-specific financial institution products and services if such message includes the name of an insured depository institution. However, advertisements that include only non-deposit products or hybrid products (products with both deposit and non-deposit features, such as sweep accounts) are prohibited from including the FDIC advertising statement.
>
> Advertising and Notice of NCUA Share Insurance. As applicable, the institution must include the official advertising statement of NCUA membership in each advertisement designed to attract "public attention or patronage to a product or business." The advertising statement must be clearly legible and at least as large as the smallest font size used in other portions of the advertisement to convey other information to the consumer.

*Interagency Statement on Sales of Nondeposit Investment Products ("Interagency Statement")*. The Guidance clarifies that sales activities conducted using social media are subject to the Interagency Statement, including the requirement that sales materials and presentations must clearly indicate that the product is:

- Not insured by the FDIC.
- Not a financial institution deposit, a financial institution obligation, or guaranteed by the financial institution.

---

27 *Id.*

28 *Id.*

29 *Id.* at 11-12.

- Subject to investment risk, including potential principal loss.

***Payment Systems***

*Electronic Fund Transfer Act (EFTA)*. If social media is used to engage in electronic funds transfers or remittance transfers from consumers in the United States to consumers or businesses in a foreign country, the EFTA and Regulation E will apply.[30] This will include disclosures, cancellation rights, liability for unauthorized transfers, and error resolution procedures.

*Check-based Transactions*. If social media is used as a gateway for authorizing payments in a check-based transaction, applicable industry rules (such as National Automated Clearing House Association), relevant state Uniform Commercial Code, the Expedited Funds Availability Act, and Regulation CC will apply.

***Bank Secrecy Act/Anti-Money Laundering Program***

The FFIEC Guidance summarizes the requirements of an effective BSA/AML compliance program and reminds financial institutions that their compliance programs must be commensurate with each institution's respective BSA/AML risk.[31] A financial institution should consider its social media activities as part of its BSA/AML risk assessment and determine how these activities should be addressed in its BSA/AML compliance program. The FFIEC specifically refers to emerging areas of BSA/AML risk in the "virtual world" such as digital currencies and Internet games involving virtual economies that may allow players to cash out as a way to launder money.

***Community Reinvestment Act***

In a revision to the proposed guidance, the final FFIEC Guidance determines that comments about a financial institution's performance in meeting the credit needs of its community made on social media platforms that are not run by or on behalf of the financial institution are not necessarily deemed to have been received by the institution and so are not required to be retained under the Community Reinvestment Act's two-year lookback requirements.[32] A financial institution must ensure, however, that it has procedures to address any such comments received through social media sites run by or on behalf of it.

***Privacy***

*Gramm-Leach-Bliley Act (GLBA) Privacy Rules and Data Security Guidelines*. Financial institutions must consider the extent to which the Privacy Rules and Data Security Guidelines apply to their social media activities.[33] Financial institutions may collect or otherwise have access to information from or about consumers through social media channels, for example, if a financial institution integrates social media components into its customers' online account services or allows consumers to apply for financial institution products or services using social medial channels. The FFIEC Guidance notes that when there is a

30 *Id.* at 12-13.

31 *Id.* at 13-14.

32 *Id.* at 14.

33 *Id.* at 14-16.

"consumer" or "customer" relationship triggering the Privacy Rule requirements, the financial institution must clearly disclose its privacy policies on its social media channels.

Users including those under age 13 may post confidential or sensitive information such as account numbers on an institution's social media page or website. An institution's procedures should include a process to take down such sensitive material, as appropriate, to minimize the risks associated with the personal information of users remaining in the social media space.

Social media platforms may be vulnerable to risk of account takeover and the distribution of malware.[34] In order to comply with the Data Security Guidelines and safeguard the confidentiality and security of customer information, financial institutions must ensure that they have systems in place to protect the information technology systems used in their social media platforms. A financial institution's data security breach incident response program should be reviewed and revised to address social media breaches and account takeover issues, as appropriate.

The FFIEC Guidance also cautions that even if the Privacy Rules do not apply, a financial institution will likely face reputation risk if it does not appear to be protecting the confidentiality and security of customer information or if it appears to be less than transparent about the privacy policies that apply to the social media sites it uses.

*CAN-SPAM Act and Telephone Consumer Protection Act (TCPA).* The CAN-SPAM Act applies to unsolicited communications to consumers and businesses via email and establishes certain requirements for commercial email messages. The FTC enforces the CAN-SPAM Act for commercial emails and the Federal Communications Commission ("FCC") enforces the CAN-SPAM Act for text messages. Under the CAN-SPAM Act, advertisers are prohibited from using false or misleading header information and deceptive subject lines. Each commercial email must give recipients an opt-out method and each advertiser must maintain an opt-out list.

The TCPA applies to telephone calls, including text messages, and requires the sender of marketing messages to obtain prior written consent from the consumer to send prerecorded messages or to use an automatic telephone dialing system to send text messages. TCPA opt-ins cannot be obtained in promotional rules, and where the TCPA opt-in is requested the advertiser must also provide the method to opt out and stop the texts. Financial institutions should also consider adding the message that "standard text rates may apply" to TCPA opt-in disclosures.

The financial institution should review its social media activities and determine whether any are subject to the CAN-SPAM Act and the TCPA. It should then review its policies and procedures related to the CAN-SPAM Act and the TCPA and the authorizations it obtains from customers enabling it to communicate with them using text messages and determine whether the policies and procedures and/or authorizations require revision to address its social media activities.

*Children's Online Privacy Protection Act (COPPA).* COPPA and its implementing regulations impose obligations on operators of general audience commercial websites and on online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The

34 https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks.

financial institution should review its social media activities to determine whether the activities may be subject to COPPA. A social media platform that requires users to attest that they are at least 13 may rely on such self-certification. The FFIEC Guidance cautions financial institutions that they should still, however, monitor whether they are collecting any personal information of a user under age 13 on those sites. COPPA also imposes obligations on operators of commercial websites and online services directed at children younger than 13 that collect, use, or disclose personal information from children. In maintaining its own social media site, a financial institution should ensure that it establishes, posts, and follows policies restricting access to the social media site to users 13 or older, particularly if such social media site contains any activities that may attract children under age 13, such as video games and virtual worlds.

### II. Reputation Risk

The FFIEC identifies as a principal concern reputation risk as the result of negative public opinion in connection with the financial institution's use of social media. It describes risks related to social media use that may result in injury to the financial institution's reputation and cautions financial institutions to manage these risks, which include:

- Fraud and Brand Identity Risks
- Third-party Risks
- Privacy Risk
- Customer Complaints and Inquiries
- Employee Use of Social Media

The Guidance also includes suggested steps to minimize these risks, such as implementing social media monitoring tools to identify fraudulent use of the financial institution's brand, negative comments, and complaints. Even where such communications are posted on other parties' social media sites, the financial institution may wish to review them and respond as appropriate depending on its individual risk profile.

### III. Operational Risk

The third area of risk identified by the FFIEC is the financial institution's risk of loss from inadequate or failed processes or systems related to its use of technology when it engages in social media activity. The FFIEC identifies account takeover and vulnerability to malware as particular concerns and advises that the financial institution should incorporate these events in its security incident response procedures. It also refers financial institutions to other regulatory guidance related to technology and operations risk, including the *FFIEC Information Technology Examination Handbook*.

## Federal Trade Commission

In the exercise of its authority under Section 5 of the Federal Trade Commission Act ("FTC Act"), the FTC has adopted guidelines, issued Frequently Asked Questions ("FAQs"), and engaged in initiatives to prevent business practices that are deceptive or unfair to consumers and to enhance consumer choice. Financial institutions are subject to these guidelines and initiatives under Section 8 of the Federal Deposit

Insurance Act, which authorizes prudential regulators to take action against financial institutions for violations of any law or regulation, including Section 5 of the FTC Act. As a result, financial institutions engaged in social media activities must also take FTC guidelines and initiatives into consideration when designing and implementing their social media programs.[35]

### I. .com Disclosures: How to Make Effective Disclosures in Digital Advertising

In adopting its revised .com Disclosures guidance on March 12, 2013,[36] updating the version issued in 2000, the FTC acknowledged changes to the marketplace including smartphones with small screens and the rise of social media marketing.[37] The FTC advised advertisers that consumers should be provided with clear and conspicuous information to make informed decisions, despite space constraints and limitations of social media platforms.[38] The guidance emphasizes that existing consumer protection laws apply to the Internet and other electronic media, concluding that, "if a particular platform does not provide an opportunity to make clear and conspicuous disclosures, it should not be used to disseminate advertisements that require such disclosures."[39]

The new guidance recommends that advertisers place required disclosures "as close as possible" to the relevant claim.[40] In addition, the disclosure must be prominent, other parts of the ad should not distract from the disclosure, and the disclosure may not be hidden in lengthy "terms of use."[41] Disclosures contained in pop-up windows are discouraged because consumers' browsers may automatically block pop-up windows.[42]

Hyperlinks should not be used for product cost or certain health and safety issues and, if used, hyperlinks should be placed close to the triggering claim and labeled to inform the consumer of its importance and relevance.[43] Labels such as "terms and conditions" and "disclaimer" on such hyperlink are deemed inadequate.[44]

---

35 OCC AL 2002-3; FDIC FIL 26-2004; FRB *Interagency Guidance on Unfair or Deceptive Acts or Practices by State-Chartered Banks* (March 11, 2004).

36 Federal Trade Commission, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (March 12, 2013), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

37 *Id.* at 1.

38 *Id.* at 5.

39 *Id.* at 4-7.

40 *Id.* at 8-10.

41 *Id.* at 17-19.

42 *Id.* at 14.

43 *Id.* at 10.

44 *Id.* at 12.

Finally, advertisers should ensure that their advertisements are mobile-optimized so that their disclosures will be clear and conspicuous regardless of the device on which they are displayed.[45] The .com Disclosures contain 22 mock advertisements formatted for computers, smartphones, and tweets to illustrate these points.[46]

### II. Operation Full Disclosure

In September 2014, the FTC issued more than 60 letters to print and television advertisers warning companies to review specific ads to ensure that disclosures were clear and conspicuous in compliance with federal requirements. The FTC highlighted ads where the disclosures were not conspicuous or placed in proximity to relevant claims, were not in a font that was easy to read or in a size or shade that stood out against the background, and did not disclose all conditions, terms, and limitations. In a related blog post, the FTC described the "4 Ps" it uses to evaluate the adequacy of disclosures in ads: (1) Prominence (is it big enough to read easily?); (2) Presentation (is it easy to understand?); (3) Placement (is it located where consumers are likely to look?); and (4) Proximity (is it close enough to the claim it qualifies?). While this guidance referred specifically to print and television advertisements, its requirements mimic those applied to online advertisers in .com Disclosures and can be used to evaluate the sufficiency of online disclosures.

### III. Guides Concerning the Use of Endorsements and Testimonials in Advertising

The FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising (the "Endorsement Guides") require that "material connections" between advertisers and endorsers must be clearly and conspicuously disclosed.[47] In 2009, the Endorsement Guides were revised to include examples of how the guidance applies to "consumer-generated" media, including bloggers.[48] The Endorsement Guides state that a blogger will be viewed as an endorser subject to the disclosure requirements when the blogger receives cash or in-kind payment to review a product.[49] The guidance advises that advertisers put processes in place to monitor the conduct of their bloggers to ensure that the statements made by bloggers about their products or services are truthful and can be substantiated and that the material connection is appropriately disclosed, noting that both the advertiser and the endorser are liable for false or unsubstantiated claims and failure to disclose the material connection.[50]

### IV. The FTC's Endorsement Guides: What People Are Asking

In May 2015, the FTC released its updated Frequently Asked Questions on the Endorsement Guides to help define what it would consider a deceptive practice when an advertiser uses endorsements in social media advertising.[51] The FAQs are consistent with the principles outlined in the 2009 Endorsement Guides but provide examples of the current forms of promotion, replacing the FAQs issued in 2009.

---

45 *Id.* at 17.

46 *Id.* at A1-A26.

47 16 C.F.R. § 255.5.

48 16 C.F.R. § 255.1 and 255.5.

49 16 C.F.R. §§ 255.1 and 255.5.

50 16 C.F.R. § 255.1.

51 https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking.

The new FAQs address various topics, including posting a Facebook or Instagram "like," rewarding social media posts with sweepstakes or content entries, Pinterest pins, acceptable abbreviated disclosures in Twitter tweets, complete disclosures of receipt of products in an endorsement, and disclosure of employment in an endorsement. As for disclosures by employees, the FTC has stated that an employee listing her employer on her profile is not a sufficient disclosure since not everyone will read her profile. If the employee makes an endorsement in a post, she must disclose her employment as part of her post.

The FTC has noted that it is more likely to bring an enforcement action against an advertiser than against an endorser (although both are possible) and so encourages advertisers to have an endorsement program in place to train and monitor their endorsers. The program should include permitted endorsements about products, methods to disclose the relationship between the advertiser and the endorser, monitoring of endorsers, and follow-up actions if an unacceptable endorsement is identified.

### V. Native Advertising

Financial institutions must consider whether material they provide to customers in a digital format is advertising material or editorial material based on the current FTC guidance and best practices such as those mentioned below. If the material is marketing, the financial institution must ensure that it contains a clear and conspicuous disclosure identifying it as such. All financial institutions should monitor the FTC's actions in this area, including reviewing any additional guidance and enforcement actions.

### VI. FTC Native Advertising Workshop

The FTC held a native advertising workshop titled *Blurred Lines: Advertising or Content?* on December 4, 2013, to examine the practice of blending advertisement with news, entertainment, and other content on digital media.[52] It is the FTC's view that because native advertising mimics the visual design of the site where it is placed, consumers may have difficulty distinguishing the material as a paid advertisement. The FTC noted that it had a long history of enforcement actions against marketers that "disguised" advertising in another format, thus giving the appearance of something other than advertising without clear and conspicuous disclosure that it was in fact an advertisement. The agency specifically referred to ads in a news format, direct mail that appears to be a notification to a contest winner, and infomercials as examples of such advertising that requires additional disclosures.

The FTC reminded the workshop attendees that enforcement against native advertising in digital media could be based on existing law intended to allow consumers to distinguish between marketing and other content, including its .com Disclosures and Endorsements Guides, and questioned whether new federal requirements specific to this new form of digital marketing should be developed. In addition, the FTC favorably commented on best practices on native advertising issued by the Interactive Advertising Bureau (IAB) and the American Society of Magazine Editors (ASME).

52 Federal Trade Commission, http://www.ftc.gov/news-events/events-calendar/2013/12/blurred-lines-advertising-or-content-ftc-workshop-native.

### VII. Self-regulatory Advertising Principles

The IAB, the ASME, the Digital Advertising Alliance (DAA), the Better Business Bureau's (BBB) National Advertising Division (NAD), its Online Interest Based Advertising Accountability Program (Advertising Accountability Program), and its Online Behavioral Advertising Principles (OBA Principles) all have rules and guidance on native advertising.

These groups' guidance is consistent with the guidance provided by the FTC and each requires clear and conspicuous disclosure that alerts the reader that a native advertisement is not the publisher's editorial content. Each guidance discusses how such disclosures should be made in an online environment and provides helpful practical advice.

The IAB issued its Native Advertising Playbook on the date of the FTC workshop. The IAB's Playbook describes six types of native advertising and outlines best practices for native advertising.

In December 2014, the BBB's Advertising Accountability Program issued a warning that advertisers must comply with its Online Behavioral Advertising Principles when engaged in native advertising. The BBB advised such advertisers that they must provide a real-time enhanced notice in or around the native ad and an easy-to-use opt-out to consumers when they track consumers across various websites. It also notified native advertisers that they must ensure that their website privacy notice contains a disclosure that describes their data collection and use practices in connection with such advertising.

### VIII. Search Engine Advertising Guidance

In June 2013, the FTC updated its 2002 guidance to the search engine industry regarding the need to clearly and prominently distinguish between advertisements and natural search results.[53] The guidance was updated in response to changes in the industry in which the FTC concluded that paid search results had become less distinguishable from natural search results and accordingly could be a deceptive practice prohibited under Section 5 of the FTC Act.[54] The FTC noted that consumers expect search results to be ranked based on relevance to a search query, not on payment from a third party.[55]

The FTC positioned this guidance as part of the agency's initiative to provide updated guidance to digital advertisers generally, including its .com Disclosures and Endorsement Guides. While the guidance is directed at search engines, financial institutions should become familiar with it because the guidance will affect how a financial institution as an advertiser is presented in search results.

### National Labor Relations Act and State Employee Social Media Laws

There are both federal and state laws that protect lawful off-duty conduct by employees. Some apply specifically to social media use and other laws are now being applied by agencies and the courts to social media use by employees. Financial institutions must stay informed about new laws and changes in the

53 Federal Trade Commission, http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-consumer-protection-staff-updates-agencys-guidance-search-engine-industryon-need-distinguish/130625searchenginegeneralletter.pdf.

54 *Id.* at 1.

55 *Id.*

application of existing laws to employee social media activities and review their policies and practices periodically to ensure that they are in compliance.

### I. National Labor Relations Act

Financial institutions must comply with the National Labor Relations Act ("NLRA") even if their employees are not unionized.[56] The NLRA protects the rights of employees (but not supervisory or managerial employees) to engage in "concerted activities" regarding pay, hours, and other terms and conditions of employment.[57] This protection does not apply to employees who engage in raising individual concerns but does apply to those engaging with coworkers to raise concerns. Employers are prohibited from taking adverse action against an employee based on such protected activity. In addition, employers are prohibited from taking actions that would have a "chilling effect" on employees' protected activities.

Starting in 2011, the National Labor Relations Board ("NLRB") became active in examining how the NLRA applies to social media, issuing dozens of decisions and three Operations-Management Memoranda on social media issues. The General Counsel's office investigates unfair labor practices and the Memoranda provide useful guidance on the current enforcement posture of the NLRB. The first two Memoranda focused on actions taken by employers in response to social media activity of their employees, helping to define when employees' social media activity is protected under the NLRA.[58] The third Memorandum focused on employers' social media policies.[59] The NLRB analyzed seven different employers' policies and found six to unduly restrict the rights of employees under the NLRA. Only one policy — Walmart's — was found to be lawful, and the Memorandum includes a copy of this policy for review. No financial institution policy was included in this analysis and, as a result, care should be taken in determining the application of the guidance outlined in the Memoranda to financial institutions and their employees.

Review of the decisions on social media policies included in the Memoranda recognizes as fundamental to a good social media policy examples of both prohibited and acceptable conduct. This will help ensure that the policy will not be viewed as having a "chilling effect" on employees' rights due to its ambiguity, in particular the right to communicate with other employees about working conditions and terms and conditions of employment. Limitations contained in the policy should be reviewed to determine whether they could "reasonably be interpreted as prohibiting employees from discussing and disclosing information regarding their own conditions of employment, as well as the conditions of employment of employees other than themselves," as these are activities protected under the NLRA.[60] If so, the limitation will be deemed to be overly broad. A "saving clause" providing that nothing in the policy should be construed to limit an employee's legally protected rights under the NLRA will not be sufficient to cure a policy that is overly broad.

---

56 National Labor Relations Board, *The NLRB and Social Media*, http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media.

57 *See* 29 U.S.C. § 157.

58 *Office of General Counsel of National Labor Relations Board*, Memorandum OM 11-74, *Report of the Acting General Counsel Concerning Social Media Cases* (August 17, 2011); Memorandum OM 12-31, *Report of the Acting General Counsel Concerning Social Media Cases* (January 24, 2012).

59 Memorandum OM 12-59, *Report of the Acting General Counsel Concerning Social Media Cases* (May 30, 2012).

60 *Id.* at 4.

This recent NLRB activity highlights the importance of a social media policy and disciplinary practices that are structured in accordance with the NLRA. Financial institutions should use the NLRB guidance in developing their social media policies and practices but be aware that the NLRB's rulings are subject to review by federal appellate courts and the courts may disagree.

### II. State Laws — Access to Employee Social Media

As of September 2015, 21 states have adopted laws (and many others have introduced or have legislation pending) prohibiting employers from requesting passwords and/or user IDs for employees' personal social media accounts.[61] These state laws also include definitions of social media and can be broad, like the Nevada law that includes elements such as instant messages, text messages, blogs, and emails, or narrower, such as the Illinois law that expressly excludes email.[62]

The Illinois law is part of the Right to Privacy in the Workplace Act and makes it illegal for an employer to ask potential and current employees for their social media passwords or otherwise demand access to their accounts.[63] The law does not prohibit employers from instituting workplace policies related to usage of the Internet, social networking sites, and email.[64] Employers also are not prohibited from viewing employee information on social media that is not restricted by privacy settings.[65]

Financial institutions should review the laws of each state where they have employees to determine whether those states have laws governing social media activity and, if so, which employer activities are limited. For example, in addition to prohibiting an employer from requesting an employee's password, some states prohibit employers from requiring an employee to (i) add a supervisor or administrator to the employee account's list of contacts ("friend" or a "connection"); (ii) change the employee's account privacy settings; (iii) access personal social media in the presence of the employer; (iv) waive the rights and protections of the law as a condition of applying for or receiving an offer of employment; and (v) divulge personal social media (except in connection with the investigation of allegations of misconduct). Penalties for violation of these state laws vary but may include civil, administrative, and criminal penalties. These state law restrictions must be taken into consideration in drafting an employee social media policy.[66]

---

61 National Conference of State Legislatures, *Employer Access to Social Media Usernames and Passwords* (July 9, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

62 NEV. REV. STAT. 613.135; 820 ILL. COMP. STAT. 55/10.

63 820 ILL. COMP. STAT. 55/10(a).

64 820 ILL. COMP. STAT. 55/10(b).

65 *Id.*

66 ARK. CODE § 11-2-124; CAL. LAB. CODE § 980; COLO. REV. STAT. § 8-2-127; 820 ILL. COMP. STAT. 55/10; MD. CODE ANN., LAB. & EMPL. § 3-712; MICH. COMP. LAWS § 37-271; N.J. STAT. § 34:6B-5; N.M. STAT. § 50-4-34; OR. REV. STAT. § 659A.330; UTAH CODE § 34-48-101; WASH. REV. CODE § 49.44.200.

# Employee Social Media Policies

A financial institution can mitigate certain business and legal risks of social media use by adopting a social media policy for its employees. In addition, the FFIEC Guidance recommends a financial institution adopt such a policy both for work-related use of social media by its employees, defining impermissible activities, and for non-work-related use by employees as part of the financial institution's social media governance policies and procedures.[67] Any such policy must, however, be drafted, monitored, and enforced in a manner that is compliant with state and federal law and NLRB decisions and guidance.

The goals of the policy should include reducing the risks detailed in this Guide, including risk of reputation and brand damage and disclosure of confidential customer and financial institution information. The policy should help ensure the financial institution's compliance with applicable laws and guidance governing marketing of its products and services. The financial institution should also clearly designate in the policy who may speak on behalf of the financial institution and the context in which this authority extends. Those employees engaged in personal social media should be provided guidance on how to clarify that they are not speaking on behalf of the financial institution.

In order to draft an effective policy, the financial institution must first identify how it uses social media and the related business and legal risks. If a financial institution actively participates in social media for business promotion such as using a corporate Facebook page or a Twitter account, it will have different and greater risks than a financial institution that does not participate in social media.

The financial institution that is actively engaged in social media will require an employee policy that includes detailed, job-specific rules for its employees participating in social media activities on its behalf. Its policy must ensure that the financial institution owns these social media accounts, and not the employee acting on behalf of the financial institution.

A policy for those employees authorized to engage in social media activities on behalf of the financial institution should address these issues:

- governance structure — approval authority for posts;
- training;
- use of personal electronic devices;
- use of business electronic devices;
- monitoring of use of business electronic devices;
- confidentiality of customer and business information;

67 *FFIEC Guidance*, at 7.

- disparaging comments about customers/employer/coworkers; and
- transparency — identification as employee when posting about financial institution.

If the financial institution has its own social media platforms, such as a blog, it will need a policy that addresses the use of these social media platforms by employees and terms of use that address use of the social media platforms by the public.

In addition, more general policies should be developed governing personal use of social media for employees *not* engaged in social media activities on behalf of the financial institution. Consistent with the NLRB guidance, care should be taken to ensure that the policy includes examples of both prohibited behavior and permitted behavior. Any restrictions contained in the policy should not be overly broad as to allow them to be construed as inconsistent with employees' exercise of protected rights under the NLRA.

A policy for these employees should address the following areas:

- training;
- limits on private social media for business use;
- use of business electronic devices;
- monitoring of use of business electronic devices;
- confidentiality of customer and business information;
- transparency — identification as employee if posting about financial institution;
- disparaging comments about customers/employer/coworkers; and
- employee obligation to clarify that he/she is speaking on his/her own behalf and is not authorized to speak on behalf of the financial institution.

The financial institution's policy should complement its other corporate policies, including those related to the use of the Internet and technology, confidentiality of the financial institution's customer information and business assets, and ethics, among others. The policy should reflect the extent to which the financial institution's corporate culture encourages its employees' engagement in social media. Due to the rapid changes in social media and the laws and guidance applicable to social media activities, financial institutions must frequently review and revise their policies as required.

By providing clear expectations about when social media can be used and for what purposes, a financial institution's policy should assist employees in adopting responsible use of social media, which should benefit the financial institution both as an employer and as a business enterprise providing products and services to customers.

# Conclusion

Financial institutions have been given a clear directive by the FFIEC to adopt a risk management program related to their social media activities. The extent of such a program will vary based on how the financial institution uses social media, but even those financial institutions that do not actively use social media are required to have a risk management program. Although financial institutions are not currently among the most active of corporate participants using social media, we expect that this will change as the variety of social media channels evolves and financial institutions seek to respond to their customers' desire to engage using social media.

The FFIEC emphasized that existing laws, regulations, and expectations continue to apply to activities conducted through social media channels and provided guidance on how these laws will be applied. At the same time, courts and agencies such as the FTC and NLRB are applying existing laws to social media activities. Financial institutions must also be mindful of new laws regulating their interaction with employees related to social media, such as state laws prohibiting the request for employee passwords.

As a highly regulated entity it is imperative that a financial institution take a disciplined approach to its adoption of social media to interact with customers and to promote its products and services. Consistent with the FFIEC Guidance, the financial institution should include specialists in compliance, technology, information security, legal, human resources, and marketing to review and implement social media initiatives. This practice will help ensure that the financial institution meets its goals for social media engagement, minimizes risk to the institution, and ensures that it is able to comply with the laws that apply to its social media activities, both current laws and new laws and guidance.

# More Information

If you would like further information concerning any of the matters discussed in this article, please contact any of the following attorneys, or any other Chapman and Cutler attorney with whom you regularly work:

**Heather L. Hansche, Partner**
312.845.3714
hansche@chapman.com

**Lindsay S. Henry, Associate**
312.845.3869
lhhenry@chapman.com

**Charlotte**
201 South College Street, Suite 1600
Charlotte, NC 28244-0009
980.495.7400

**Salt Lake City**
215 South State Street, Suite 800
Salt Lake City, UT 84111-2339
801.533.0066

**chapman.com**

**Chicago**
111 West Monroe Street
Chicago, IL 60603-4080
312.845.3000

**San Francisco**
595 Market Street, 26th Floor
San Francisco, CA 94105-2839
415.541.0500

**New York**
1270 Avenue of the Americas, 30th Floor
New York, NY 10020-1708
212.655.6000

**Washington, DC**
1717 Rhode Island Avenue NW
Washington, DC 20036-3026
202.478.6444