The Department is soliciting nominations for three non-federal members from among scientists, physicians, and other health professionals and for two non-federal members of the general public who are representatives of leading research, advocacy, and service organizations for people with pain-related conditions. These candidates will be considered to fill positions opened through completion of member terms. Nominations are due by COB, January 22, 2014, and should be sent to Linda Porter, Ph.D., NINDS/NIH, 31 Center Drive, Room 8A03, Bethesda, MD 20892, ported@ninds.nih.gov by either USPS mail or email. Nominations should include contact information, and a current curriculum vitae or resume.

Dated: December 5, 2013.

Stacy C. Landis,
Director, National Institute of Neurological Disorders and Stroke, National Institutes of Health.
reputation risks raised by activities conducted via social media.

Social media has been defined in a number of ways. For purposes of the Guidance, social media is a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. Social media can take many forms, including, but not limited to, micro-blogging sites (e.g., Facebook, Google Plus, MySpace, and Twitter); forums, blogs, customer review Web sites and bulletin boards (e.g., Yelp); photo and video sites (e.g., Flickr and YouTube); sites that enable professional networking (e.g., LinkedIn); virtual worlds (e.g., Second Life); and social games (e.g., FarmVille and CityVille).

Social media can be distinguished from other online media in that the communication tends to be more interactive. For purposes of this Guidance, messages sent via email or text message, standing alone, do not constitute social media, although such communications may be subject to a number of laws and regulations discussed in this Guidance. Social media is a dynamic and constantly evolving technology and thus any definition for this technology is meant to be illustrative and not exhaustive. In addition to the examples of social media mentioned above, other forms of social media may emerge in the future that financial institutions should also consider.

Financial institutions may use social media in a variety of ways, including marketing, providing incentives, facilitating applications for new accounts, inviting feedback from the public, and engaging with existing and potential customers, for example, by receiving and responding to complaints, or providing loan pricing. Since this form of customer interaction tends to be both informal and dynamic, and may occur in a less secure environment, it can present some unique challenges to financial institutions.

II. Principal Elements of Guidance

The use of social media by a financial institution to attract and interact with customers can impact a financial institution's risk profile. The increased risks can include the risk of harm to consumers, compliance and legal risk, operational risk, and reputation risk. Increased risk can arise from a variety of directions, including poor due diligence, oversight, or control on the part of the financial institution. This Guidance is meant to help financial institutions identify potential risk areas to appropriately address, as well as to ensure institutions are aware of their responsibilities to oversee and control these risks within their overall risk management program. The Agencies and the SLC recognize that the scope of social media activities vary by financial institution. Each institution is responsible for carrying out an appropriate risk assessment and maintaining a risk management program that is appropriate and tailored to the particular institution's size, activities, and risk profile.

III. Comments Received

On January 23, 2013, the FFIEC issued proposed guidance in response to requests articulated to the Agencies by various participants in the industry for guidance regarding the application of consumer protection laws and regulations within the realm of social media. The FFIEC invited comments on any aspect of the proposal. In addition, the FFIEC specifically solicited comments in response to the following questions:

1. Are there other types of social media, or ways in which financial institutions are using social media, that are not included in the proposed guidance but that should be included?
2. Are there other consumer protection laws, regulations, policies or concerns that may be implicated by financial institutions' use of social media that are not discussed in the proposed guidance but that should be discussed?
3. Are there any technological or other impediments to financial institutions' compliance with otherwise applicable laws, regulations, and policies when using social media of which the Agencies should be aware?

The FFIEC received 81 official comments on the proposal. After consideration of all such comments, the FFIEC is issuing this final Guidance substantially as proposed, but with some changes. The changes are meant to provide further clarification of certain provisions, including those raised by commenters. For example, certain commenters expressed concerns that the proposed guidance appeared to be imposing, for all financial institutions, a single, “one-size-fits-all” approach to carrying out compliance and risk management responsibilities. The revised Guidance clarifies and points to the longstanding principle that financial institutions are expected to assess and manage the risks particular to the individual institution, taking into account factors such as the institution’s size, complexity, activities, and third party relationships.

A number of commenters also provided feedback on the appropriate definition of social media. For purposes of this final Guidance, traditional emails and text messages, standing alone, are not social media. However, messages sent through social media channels are social media. Further, the Guidance cautions financial institutions to ensure that they are aware of the laws and regulations that may apply to emails and text messages, some of which overlap with laws and regulations discussed in this Guidance as applicable to social media.

Some commenters also requested further clarification regarding the application of certain specific laws and regulations to social media activities. The Guidance contains such further discussion in a number of sections on specific laws and regulations, such as the Community Reinvestment Act. Commenters also raised issues regarding employee use of social media. The Guidance does not require a particular approach to employee personal use of social media. This final Guidance clarifies that training and guidance should be provided to employees regarding official use of social media— that is, when employees communicate officially on behalf of the financial institution.

In addition, commenters raised questions about regulators’ expectations for risk management practices regarding third parties with which a financial institution does not have a traditional vendor relationship. Such third-party relationships can still pose risks, including reputation risks, to the financial institution. The final Guidance clarifies that a financial institution should conduct an evaluation of, and perform due diligence appropriate to, the risks posed by the prospective third party prior to engaging with it.

Commenters also expressed concerns that this Guidance would require financial institutions to monitor all communications about the institution on Internet sites other than those maintained by or on behalf of the institution. This final Guidance clarifies that financial institutions are not expected to conduct such monitoring.

Finally, some commenters questioned whether the Guidance implied that financial institutions are expected to treat all negative comments about the financial institution made on its proprietary social media sites as complaints and/or inquiries and process them accordingly. The final Guidance confirms that to the extent consistent with other applicable legal requirements, a financial institution may establish one or more specified channels that customers must use for submitting communications directly to
the institution. The Guidance also clarifies that financial institutions are not expected to monitor all Internet communications for complaints and inquiries about the institution. Rather, the financial institution should take into account the results of its own risk assessment in determining the appropriate approach to take regarding monitoring of, and any response to, such communications.

IV. Paperwork Reduction Act

In accordance with the Paperwork Reduction Act (PRA), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number. The Guidance does not involve any new collections of information pursuant to the PRA. Consequently, no information was submitted to the OMB for review.

The text of the interagency Social Media: Consumer Compliance Risk Management Guidance follows:

Social Media: Consumer Compliance Risk Management Guidance

I. Purpose

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members, is issuing this Guidance. The members are the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Consumer Financial Protection Bureau (CFPB) (collectively, the Agencies), and the State Liaison Committee (SLC). The FFIEC is issuing, and the Agencies are adopting, this Guidance to address the applicability of existing federal consumer protection and compliance laws, regulations, and policies to activities conducted via social media by banks, savings associations, and credit unions, as well as by nonbank entities supervised by the CFPB (collectively, financial institutions). Various industry participants expressed a need for guidance in this area. The Agencies and SLC will use this Guidance to the extent consistent with their respective authorities.

The Guidance is intended to help financial institutions understand potential consumer compliance and legal risks, as well as related risks, such as reputation and operational risks associated with the use of social media, along with expectations for managing those risks. The Guidance provides considerations that financial institutions may find useful in conducting risk assessments and crafting and evaluating policies and procedures regarding social media. Although this Guidance does not impose any new requirements on financial institutions, as with any process or product channel, financial institutions are expected to manage potential risks associated with social media usage and access.

Financial institutions are using social media as a tool to generate new business and interact with consumers. Social media, as any new communication technology, has the potential to improve market efficiency. Social media may more broadly distribute information to users of financial services and may help users and providers find each other and match products and services to users’ needs. To manage potential risks to financial institutions and consumers, however, financial institutions should ensure their risk management programs provide oversight and controls commensurate with the risks presented by the types of social media in which the financial institution is engaged, including, but not limited to, the risks outlined within this Guidance.

II. Background

Social media has been defined in a number of ways. For purposes of this Guidance, social media is considered to be a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. Social media can take many forms, including, but not limited to, micro-blogging sites (e.g., Facebook, Google Plus, MySpace, and Twitter); forums, blogs, customer review Web sites and bulletin boards (e.g., Yelp); photo and video sites (e.g., Flickr and YouTube); sites that enable professional networking (e.g., LinkedIn); virtual worlds (e.g., Second Life); and social games (e.g., FarmVille and CityVille). Social media can be distinguished from other online media in that the communication tends to be more interactive. For purposes of this Guidance, messages sent via traditional email or text message, standing alone, do not constitute social media, although such communications may be subject to a number of laws and regulations discussed in this Guidance. However, messages sent through social media channels are social media. Social media is a dynamic and constantly evolving technology and thus any definition for this technology is meant to be illustrative and not exhaustive. In addition to the types of social media mentioned above, other forms of social media may emerge in the future that financial institutions should also consider.

Financial institutions may use social media in a variety of ways including advertising and marketing, providing incentives, facilitating applications for new accounts, inviting feedback from the public, and engaging with existing and potential customers, for example by receiving and responding to complaints, or providing loan pricing. Since this form of customer interaction tends to be both informal and dynamic, and may occur in a less secure environment, it can present some unique challenges to financial institutions.

III. Compliance Risk Management Expectations for Social Media

A financial institution should have a risk management program that allows it to identify, measure, monitor, and control the risks related to social media.

The size and complexity of the risk management program should be commensurate with the breadth of the financial institution’s involvement in this medium. For instance, a financial institution that relies heavily on social media to attract and acquire new customers should have a more detailed program than one using social media only to a very limited extent. However, in accordance with its own risk assessment, a financial institution that has chosen not to use social media should still consider the potential for negative comments or complaints that may arise within the many social media platforms described above, and, when appropriate, evaluate what, if any, action it will take to monitor for such comments and/or respond to them.

The risk management program should be designed with participation from specialists in compliance, technology, information security, legal, human resources, and marketing. Financial institutions should also provide guidance and training for employee official use of social media. Components of a risk management program should include the following:

- A governance structure with clear roles and responsibilities whereby the board of directors or senior management direct how using social media contributes to the strategic goals of the institution (for example, through increasing brand awareness, product advertising, or researching new customer bases) and establish controls and ongoing assessment of risk in social media activities;
- Policies and procedures (either stand-alone or incorporated into other policies and procedures) regarding the use and monitoring of social media and compliance with all applicable

---

4 44 U.S.C. 3501 et seq.
consumer protection laws and regulations, and incorporation of
guidance as appropriate. Further, policies and procedures should
incorporate methodologies to address
risks from online postings, edits, replies, and
retention;
• A risk management process for
selecting and managing third-party
relationships in connection with social
media;
• 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;
• An oversight process for monitoring
information posted to proprietary social
media sites administered by the
financial institution or a contracted
third-party;
• Audit and compliance functions to
ensure ongoing compliance with
internal policies and all applicable laws
and regulations, and incorporation of
guidance as appropriate; and
• Parameters for providing
appropriate reporting to the financial
institution’s board of directors or senior
management that enable periodic
evaluation of the effectiveness of the
social media program and whether the
program is achieving its stated
objectives.

IV. Risk Areas
The use of social media to attract and
interact with customers can impact a
financial institution’s risk profile,
including risk of harm to consumers,
compliance and legal risks, operational
risks, and reputation risks. Increased
risk can arise from poor due diligence,
oversight, or control on the part of the
financial institution. As noted
previously, this Guidance is meant to
help financial institutions identify
potential risks to ensure institutions are
aware of their responsibilities to address
risks within their overall risk
management program.

Compliance and Legal Risks
Compliance and legal risk arise from the
potential for violations of, or
noncomformance with, laws, rules,
regulations, prescribed practices,
internal policies and procedures, or
ethical standards. These risks also arise in
situations in which the financial
institution’s policies and procedures
governing certain products or activities
may not have kept pace with changes in the
marketplace. This concern is
particularly pertinent to an emerging
medium like social media. Further, the
potential for defamation or libel risk
exists where there is broad distribution

of information exchanges. Failure to
adequately address these risks can
expose an institution to enforcement
actions and/or civil lawsuits.

The laws and regulations discussed in
this Guidance do not contain exceptions
regarding the use of social media.
Therefore, to the extent that a financial
institution uses social media to engage in
lending, deposit services, or payment
activities, it must comply with applicable
laws and regulations as when it
engages in these activities through other
media. Financial institutions
should remain aware of developments
involving such laws and regulations.

The following laws and regulations
may be relevant to a financial
institution’s social media activities. This
list is not all-inclusive. Each financial
institution should ensure that it
periodically evaluates and controls its
use of social media to ensure
compliance with all applicable federal,
state, and local laws and regulations,
and incorporation of guidance, as
appropriate.

Deposit and Lending Products
Social media may be used to market
products and originate new accounts.
When used to do either, a financial
institution is expected to take steps to
ensure that advertising, account
origination, and document retention are
performed in compliance with
applicable consumer protection and
compliance laws and regulations. These
measures may include, but are not
limited to:
• Truth in Savings Act/Regulation DD
and Part 707.2 The Truth in Savings Act
(TISA), as implemented by Regulation DD,
and, for credit unions, by Part 707
of the NCUA Rules and Regulations,
imposes disclosure requirements
designed to enable consumers to make
informed decisions about deposit
accounts. Regulation DD and Part 707
require disclosures about fees, annual
percentage yield (APY), interest rate,
and other terms. Under Regulation DD
and Part 707, a depository institution
may not advertise deposit accounts in a
way that is misleading or inaccurate or
misrepresent the depository
institution’s deposit contract.

If an electronic advertisement
displays a triggering term, such as
“bonus” or “APY,” then Regulation DD
and Part 707 require the advertisement to
clearly state certain information, such as
the minimum balance required to
obtain the advertised APY or bonus.
For example, an electronic advertisement
can provide the required information
via a link that directly takes the
consumer to the additional information.

Fair Lending Laws: Equal Credit
Opportunity Act/Regulation B3 and Fair
Housing Act.4 A financial institution
should ensure that its use of social
media does not violate fair lending laws
and regulations.

The Equal Credit Opportunity Act,
as implemented by Regulation B,
prohibits creditors from making any oral
or written statement, in advertising or
other marketing techniques, to
applicants or prospective applicants
that would discourage a prohibited
basis a reasonable person from making
or pursuing an application. However, a
creditor may affirmatively solicit or
encourage members of traditionally
disadvantaged groups to apply for
credit, especially groups that might not
normally seek credit from that creditor.5

Creditors must observe the time
frames outlined under Regulation B for
notifying applicants of the outcome of
their applications or requesting
additional information for incomplete
applications, whether those applications
are received via social media or through
other channels.

As with all prescreened
solicitations, a creditor must preserve
prescreened solicitations disseminated
through social media, as well as the
prescreening criteria, in accordance
with Regulation B.6

When denying credit, a creditor
must provide an adverse action notice
detailing the specific reasons for the
decision or notifying the applicant of
his or her right to request the specific
reasons for the decision.7 This
requirement applies whether the
information used to deny credit comes
from social media or other sources.

It is also important to note that
creditors may not, with limited
exceptions, request certain information,
such as information about an applicant’s
race, color, religion, national origin, or
sex. Since social media platforms may
collect such information about
participants in various ways, a creditor
should ensure that it is not requesting,
collecting, or otherwise using such
information in violation of applicable
fair lending laws. Particularly if the
social media platform is maintained by
a third party that may request or require
users to provide personal information
such as age and/or sex or use data

3 15 U.S.C. 1691 et seq., 12 CFR parts 202 and
1002 and 12 CFR 701.31 (NCUA).
4 12 U.S.C. 3601 et seq., 24 CFR part 100 (HUD),
12 CFR part 128 (OCC), 12 CFR part 390 subpart
G (FDIC), 12 CFR 701.31 (NCUA).
5 12 CFR part 1002, Comment 4(b)–2.
6 12 CFR 1002.12(b)(7).
7 12 CFR 1002.9(a)(2).
mining technology to obtain such information from social media sites, the creditor should ensure that it does not itself improperly request, collect, or use such information or give the appearance of doing so.

- The Fair Housing Act (FHA), among other things, prohibits discrimination based on race, color, national origin, religion, sex, familial status, or handicap in the sale and rental of housing, in mortgage lending, and in appraisals of residential real property. In addition, the FHA makes it unlawful to advertise or make any statement that indicates a limitation or preference based on race, color, national origin, religion, sex, familial status, or handicap. This prohibition applies to all media sites. For example, if a financial institution engages in residential mortgage lending and maintains a presence on Facebook, the Equal Housing Opportunity logo must be displayed on its Facebook page, as applicable.

Truth in Lending Act/Regulation Z. Any social media communication in which a creditor advertises credit products must comply with Regulation Z’s advertising provisions. Regulation Z broadly defines advertisements as any commercial messages that promote consumer credit; and the official commentary to Regulation Z states that the regulation’s advertising rules apply to advertisements delivered electronically. In addition, Regulation Z is designed to promote the informed use of consumer credit by requiring disclosures about loan terms and costs. The disclosure requirements vary based on whether the credit is open-end or closed-end. Further, within those two broad categories, additional specific requirements apply to certain types of loans such as private education loans, home secured loans, and credit card accounts.

- Regulation Z requires that advertisements relating to credit present certain information in a clear and conspicuous manner. It includes requirements regarding the proper disclosure of the annual percentage rate and other loan features. If an advertisement for credit states specific credit terms, it must state only those terms that actually are or will be arranged or offered by the creditor.

- For electronic advertisements, such as those delivered via social media, Regulation Z permits providing the required information on a table or schedule that is located on a different page from the main advertisement if that table or schedule is clear and conspicuous and the advertisement clearly refers to the page or location.

- Regulation Z requires that, for consumer loan applications taken electronically, the financial institution must provide the consumer with all Regulation Z disclosures within the required time frames. Regulation Z does not exempt applications taken via social media.

Real Estate Settlement Procedures Act. Section 8 of the Real Estate Settlement Procedures Act (RESPA) prohibits certain activities in connection with federally related mortgage loans. These prohibitions include fee splitting, as well as giving or accepting a fee, kickback, or thing of value in exchange for referrals of settlement service business. RESPA also has specific timing requirements for certain disclosures. These requirements apply to applications taken electronically, including via social media.

Fair Debt Collection Practices Act. The Fair Debt Collection Practices Act (FDCPA) restricts how debt collectors (generally defined as third parties collecting others’ debts and entities collecting debts on their own behalf if they use a different name) may collect debts. The FDCPA generally prohibits debt collectors from publicly disclosing that a consumer owes a debt. Using social media to inappropriately contact consumers, or their families and friends, may violate the restrictions on contacting consumers imposed by the FDCPA. Communicating via social media in a manner that discloses the existence of a debt or to harass or embarrass consumers about their debts (e.g., a debt collector writing about a debt on a Facebook wall) or making false or misleading representations may violate the FDCPA.

Unfair, Deceptive, or Abusive Acts or Practices. Section 5 of the Federal Trade Commission (FTC) Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” Sections 1031 and 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act prohibit unfair, deceptive, or abusive acts or practices. An act or practice can be unfair, deceptive, or abusive despite technical compliance with other laws. A financial institution should not engage in any advertising or other practice via social media that could be deemed “unfair,” “deceptive,” or “abusive.” Of course, any determination as to whether an act or practice engaged in through social media is unfair, deceptive, or abusive, will necessarily be fact-specific. As with other forms of communication, a financial institution should ensure that information it communicates on social media sites is accurate, consistent with other information delivered through electronic media, and not misleading. A number of requirements regarding FDIC or NCUA membership and deposit insurance or share insurance apply equally to advertising and other activities conducted via social media as they do in other contexts.

Advertising and Notice of FDIC Membership. Whenever a depository institution advertises FDIC-insured products, regardless of delivery channel, the institution must include the official advertising statement of FDIC membership, usually worded, “Member FDIC.” An advertisement is defined as “a commercial message, in any medium, that is designed to attract public attention or patronage to a product or business.” The official advertisement statement must appear, even in a message that “promotes nonspecific banking products and services, if it includes the name of the insured depository institution but does not list or describe particular products or services.” Conversely, the advertising statement is not permitted if the advertisement relates solely to nondeposit products or hybrid products (products with both deposit and nondeposit features, such as sweep accounts).

Advertising and Notice of NCUA Share Insurance. Each insured credit union must include the official advertising statement of NCUA membership, usually worded, “Federally insured by NCUA” in advertisements regardless of delivery channel, unless specifically exempted. An advertisement is defined as “a commercial message, in any medium, that is designed to attract public attention or patronage to a product or business.” The official advertising statement must be in a size and print that is clearly legible and may be no smaller than the smallest font size used.
in other portions of the advertisement intended to convey information to the consumer. If the official sign is used as the official advertising statement, an insured credit union may alter the font size to ensure its legibility. Each insured credit union must display the official NCUA sign on its Internet page, if any, where it accepts deposits or opens accounts.

Nondeposit Investment Products. As described in the “Interagency Statement on Retail Sales of Nondeposit Investment Products,” when a depository institution recommends or sells nondeposit investment products to retail customers, it should ensure that customers are fully informed that the products are not insured by the FDIC or NCUA; are not deposits or other obligations of the institution and are not guaranteed by the institution; and are subject to investment risks, including possible loss of the principal invested.

Payment Systems
If social media is used to facilitate a consumer’s use of payment systems, a financial institution should keep in mind the laws, regulations, and industry rules regarding payments that may apply. Including those providing disclosure and other rights to consumers. Under existing law, no disclosure requirements apply simply because social media is involved (for instance, providing a portal through which consumers access their accounts at a financial institution). Rather, the financial institution should continue to be aware of the existing laws, regulations, guidance, and industry rules that apply to payment systems and evaluate which will apply. These may include the following:

Electronic Fund Transfer Act/Regulation E. The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E provide specific protections, including required disclosures and error resolution procedures, to individual consumers who engage in “electronic fund transfers” and “remittance transfers.”

Rules Applicable to Check Transactions. When a payment occurs via a check-based transaction rather than an EFT, the transaction will be governed by applicable industry rules and/or Article 4 of the Uniform Commercial Code of the relevant state, as well as the Expedited Funds Availability Act, as implemented by Regulation CC (regarding the availability of funds and collection of checks).

Bank Secrecy Act/Anti-Money Laundering Programs (BSA/AML)
As required by the Bank Secrecy Act (BSA) and applicable regulations, depository institutions and certain other entities must have a compliance program that incorporates training from operational staff to the board of directors. Among other elements, the compliance program must include appropriate internal controls to ensure effective risk management and compliance with recordkeeping and reporting requirements under the BSA. Internal controls are the financial institution’s policies, procedures, and processes designed to limit and control risks to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the financial institution. At a minimum, internal controls include all not limited to: implementing an effective customer identification program; implementing risk-based customer due diligence policies, procedures, and processes; understanding expected customer activity; monitoring for unusual or suspicious transactions; and maintaining records of electronic funds transfers.

An institution’s BSA/AML program must provide for the following minimum components: A system of internal controls to ensure ongoing compliance, independent testing of BSA/AML compliance, a designated BSA compliance officer responsible for managing compliance, and training for appropriate personnel. These controls should apply to all customers, products and services, including customers engaging in electronic banking (e-banking) through the use of social media, and e-banking products and services offered in the context of social media.

Financial institutions should also be aware of emerging areas of BSA/AML risk in the virtual world. For example, illicit actors are increasingly using Internet games involving virtual economies, allowing gamers to cash out, as a way to launder money. Virtual world Internet games and digital currencies present a higher risk for money laundering and terrorist financing and should be monitored accordingly.

Community Reinvestment Act
Under the regulations implementing the Community Reinvestment Act (CRA), a depository institution subject to the CRA must maintain a public file that includes, among other items, all written comments received from the public for the current year and each of the prior two calendar years that specifically relate to the institution’s performance in helping to meet its community credit needs. The institution must also include any response to those comments, as long as neither the comments nor the responses reflect adversely on the good name or reputation of any persons other than the institution, or publication of which would violate specific provisions of law.

A depository institution subject to the CRA should ensure that its policies and procedures addressing public comments take into account such comments when they are received through social media sites run by or on behalf of the institution. However, under the CRA, comments about the institution made on the Internet through sites that are not run by or on behalf of the institution are not necessarily deemed to have been received by the depository institution and would not be required to be retained. Rather, the institution should retain comments made on sites run by or on behalf of the institution that specifically relate to the institution’s performance in helping to meet community credit needs.

Privacy
Privacy rules have particular relevance to social media when, for instance, a financial institution collects, or otherwise has access to, information from or about consumers. A financial institution should take into consideration the following laws and regulations regarding the privacy of consumer information:

17 Interagency Guidance, Retail Sales of Nondeposit Investment Products (Feb. 17, 1994).
20 UCC Art. 4.
21 12 CFR part 229.
22 “Bank Secrecy Act” is the name that has come to be applied to the Currency and Foreign Transactions Reporting Act (Titles I and II of Pub. L. 91–508), its amendments, and the other statutes referring to the subject matter of that Act. These statutes are codified at 12 U.S.C. 1829b, 1951–1959; 31 U.S.C. 5311–5314, 5316–5332; and notes thereto.
23 See Bank Secrecy Act regulations are found within 31 CFR Chapter X. Also, the federal banking agencies require institutions under their supervision to establish and maintain a BSA compliance program. See 12 CFR 21.21, 163.177 (OCC); 12 CFR 208.63, 211.5(m), 211.244 (Board); 12 CFR 326.8, 390.354 (FDIC); 12 CFR 748.2 (NCUA). See also Treas. Dept’ Order 180–01 (Sept. 26, 2002).
operators of commercial Web sites and online services directed to children younger than 13 that collect, use, or disclose personal information from children, as well as on operators of general audience Web sites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. A financial institution should evaluate whether it, through its social media activities, could be covered by COPPA.

- Certain social media platforms require users to attest that they are at least 13, and a financial institution using those sites may consider relying on such policies. However, the financial institution should still take care to monitor whether it is actually collecting any personal information of a person under 13, such as when a child under 13 manages to post such information on the financial institution's site.

A financial institution maintaining its own social media site (such as a virtual world) should be especially careful to establish, post, and follow policies restricting access to the site to users 13 or older, especially when those sites could attract children under 13. This may be true, for instance, in the case of virtual worlds and any other features that resemble video games.

**Fair Credit Reporting Act.** The Fair Credit Reporting Act (FCRA) and its implementing regulations contain restrictions and requirements concerning making solicitations using eligibility information, responding to direct disputes, and collecting medical information in connection with loan eligibility. The FCRA applies when social media is used for these activities.

**Reputation Risk**

Reputation risk is the risk arising from negative public opinion. Activities that result in dissatisfied consumers and/or negative publicity could harm the reputation and standing of the financial institution, even if the financial institution has not violated any law. Privacy and transparency issues, as well as other consumer protection concerns, arise in social media environments. Therefore, a financial institution engaged in social media activities is expected to be sensitive to, and properly manage, the reputation risks that arise from those activities. Reputation risk can arise in areas including the following:

---

**Fraud and Brand Identity**

Financial institutions should be aware that protecting their brand identity in a social media context can be challenging. Risk may arise in many ways, such as through comments made by social media users, spoofs of institution communications, and activities in which fraudsters masquerade as the institution. Financial institutions should consider the use of social media monitoring tools and techniques to identify heightened risk, and respond appropriately. Financial institutions should have appropriate policies in place to monitor and address in a timely manner the fraudulent use of the financial institution’s brand, such as through phishing or spoofing attacks.

**Third Party Concerns**

Working with third parties to provide social media services can expose financial institutions to substantial reputation risk. A financial institution should regularly monitor the information it places on social media sites. This monitoring is the direct responsibility of the financial institution, as part of a sound compliance management system, even when such functions may be delegated to third parties. Even if a social media site is owned and maintained by a third party, consumers using the financial institution’s part of that site may blame the financial institution for problems that occur on that site, such as uses of their personal information they did not expect or changes to policies that are unclear. The financial institution’s ability to control content on a site owned or administered by a third party and to change policies regarding information provided through the site may vary depending on the particular site and the contractual arrangement with the third party. A financial
institution should thus weigh these issues against the benefits of using a third party to conduct social media activities.

A financial institution should conduct an evaluation and perform due diligence appropriate to the risks posed by the prospective service provider prior to engaging with the provider. To understand the risks that may arise from a relationship with a given third party, the institution should be aware of matters such as the third party’s reputation in the marketplace; the third party’s policies, including policies on collection and handling of consumer information, including the information of the institution’s customers; the process and frequency by which the third party’s policies may change; and what, if any, control the institution may have over the third party’s policies or actions.

Privacy Concerns

Even when a financial institution complies with applicable privacy laws in its social media activities, it should consider the potential reaction by the public to any use of consumer information via social media. The financial institution should have procedures to address risks from occurrences such as members of the public posting confidential or sensitive information—for example, account numbers—on the financial institution’s social media page or site.

Consumer Complaints and Inquiries

Although a financial institution can take advantage of the public nature of social media to address customer complaints and questions, reputation risks exist when the financial institution does not address consumer questions or complaints in a timely or appropriate manner. Further, the participatory nature of social media can expose a financial institution to reputation risks that may arise when users post critical or inaccurate statements. Compliance risk can also arise when a customer uses social media to communicate issues or concerns directly with a financial institution, such as an error dispute under Regulation E, a billing error under Regulation Z, or a direct dispute about information furnished to a consumer reporting agency under FCRA and its implementing regulations.

This Guidance does not require financial institutions to monitor and respond to all Internet communications; however, a financial institution is expected to take into account the results of its own risk assessments in determining the appropriate approach to take regarding monitoring of, and responding to, such communications. Appropriate steps may include, for example, establishing one or more specific channels consumers must use when submitting complaints or disputes directly to the institution for further investigation, to the extent consistent with other applicable legal requirements. However, the institution should also consider the risks, particularly the reputation risk, inherent in not responding to complaints and disputes received through other channels and tailor its policies and procedures accordingly, in a manner appropriate to the institution’s size and risk profile.

Based on its own risk assessment processes, a financial institution should also consider whether and how to respond to communications disparaging the financial institution on other parties’ social media sites. One approach to managing these risks would be to monitor question and complaint forums on social media sites to ensure that such inquiries, complaints, or comments are reviewed, and when appropriate, addressed in a timely manner.

Employee Use of Social Media Sites

Financial institutions should be aware that employees’ communications via social media may be viewed by the public as reflecting the financial institution’s official policies or may otherwise reflect poorly on the financial institution, depending on the form and content of the communications. Employee communications can also subject the financial institution to compliance risk, operational risk, as well as reputation risk. Therefore, as appropriate, financial institutions should take steps to address these risks, such as establishing policies and training to address employee participation in social media representing the financial institution. For example, if an employee is communicating with a customer regarding a loan product through an approved social media channel, policies should include steps to ensure the customer is receiving all of the required disclosures. This Guidance does not address any employment law principles that may be relevant to employee use of social media. In addition, the Guidance is not intended to impose any specific requirements for policies or procedures regarding employee personal use of social media. Each financial institution should evaluate the risks for itself and determine appropriate policies to adopt in light of those risks.

Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events. Operational risk includes the risks posed by a financial institution’s use of information technology (IT), which encompasses social media.

The identification, monitoring, and management of IT-related risks are addressed in the FFIEC Information Technology Examination Handbook, as well as other supervisory guidance issued by the FFIEC or individual agencies. A financial institution should pay particular attention to the booklets “Outsourcing Technology Services” and “Information Security” when using social media, and include social media in existing risk assessment and management programs.

Social media is one of several platforms vulnerable to account takeover and the distribution of malware. A financial institution should ensure that the controls it implements to protect its systems and safeguard customer information from malicious software adequately address social media usage. Financial institutions’ incident response protocol regarding a security event, such as a data breach or account takeover, should include social media, as appropriate.

Conclusion

As noted previously, this Guidance is intended to help financial institutions understand and successfully manage the risks associated with use of social media. Financial institutions are using social media as a tool to generate new business and provide a dynamic environment to interact with consumers. As with any product channel, financial institutions are expected to manage potential risks to the financial institution and consumers by ensuring that their risk management programs provide appropriate oversight and control to address the risk areas discussed within this Guidance.

Dated: December 12, 2013.

Footnotes:
FEDERAL RESERVE SYSTEM
Change in Bank Control Notices; Acquisitions of Shares of a Bank or Bank Holding Company

The noticants listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board’s Regulation Y (12 CFR 225.41) to acquire shares of a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received no later than January 2, 2014.

A. Federal Reserve Bank of Chicago (Colette A. Fried, Assistant Vice President) 230 South LaSalle Street, Chicago, Illinois 60690–1414:

1. The George Breckenridge Family Trust, with Maureen Breckenridge as trustee, and Maureen Breckenridge as trustee of the George Breckenridge Family Trust and the Maureen Breckenridge Trust, individually, and the George Breckenridge Family Trust, the Maureen Breckenridge Trust, and Maureen Breckenridge as trustee of the George Breckenridge Family Trust and the Maureen Breckenridge Trust, all of Yates City, Illinois, together as a group acting in concert, to retain voting shares of First Bancorp, Inc., and thereby indirectly retain voting shares of Bank of First Bancorp, Inc., and thereby acting in concert, to retain voting shares of Bank of First Bancorp, Inc., and thereby indirectly retain voting shares of First Bancorp, Inc., and thereby indirectly acquire voting shares of First Bancorp, Inc., and thereby indirectly acquire voting shares of Community First Bank, Keosauqua, Iowa, and First Iowa State Bank, Albia, Iowa.

B. Federal Reserve Bank of Kansas City (Dennis Denney, Assistant Vice President) 1 Memorial Drive, Kansas City, Missouri 64198–0001:

1. Jay R. Trofholz, Columbus, Nebraska, to retain voting shares of Valley Bank Shares, Inc., and thereby indirectly retain voting shares of First Nebraska Bank, both in Valley, Nebraska.

FEDERAL RESERVE SYSTEM
Formations of, Acquisitions by, and Mergers of Bank Holding Companies

The companies listed in this notice have applied to the Board for approval, pursuant to the Bank Holding Company Act of 1956 (12 U.S.C. 1841 et seq.) (BHC Act), Regulation Y (12 CFR Part 225), and all other applicable statutes and regulations to become a bank holding company and/or to acquire the assets or the ownership of, control of, or the power to vote shares of a bank or bank holding company and all of the banks and nonbanking companies owned by the bank holding company, including the companies listed below.

The applications listed below, as well as other related filings required by the Board, are available for immediate inspection at the Federal Reserve Bank indicated. The applications will also be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received no later than January 2, 2014.

A. Federal Reserve Bank of Chicago (Colette A. Fried, Assistant Vice President) 230 South LaSalle Street, Chicago, Illinois 60690–1414:

1. Van Buren Bancorporation ESOP, Keosauqua, Iowa; to acquire at least an additional 6 percent, for a total of 50.1 percent of the voting shares of Van Buren Bancorporation, Keosauqua, Iowa, and thereby indirectly acquire additional voting shares of Community First Bank, Keosauqua, Iowa, and First Iowa State Bank, Albia, Iowa.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Opportunity for Co-Sponsorship of the President’s Challenge Physical Activity and Fitness Awards Program

AGENCY: President’s Council on Fitness, Sports, and Nutrition, Office of the Assistant Secretary for Health, Office of the Secretary, Department of Health and Human Services.

ACTION: Notice.

SUMMARY: The President’s Council on Fitness, Sports, and Nutrition (PCFSN) announces the opportunity for non-federal public and private sector entities to co-sponsor and administer a series of financially self-sustaining activities related to the President’s Challenge Physical Activity and Fitness Awards Program (President’s Challenge). Potential co-sponsors must have a demonstrated interest in and be capable of managing the day-to-day operations associated with the program and be willing to participate substantively in the co-sponsored activity.

DATES: To receive consideration, a request to participate as a co-sponsor must be received by 5:00 p.m. EST on Friday, January 31, 2014, at the address listed. Requests will meet the deadline if they are either (1) received on or before the deadline; or (2) postmarked on or before the deadline. Private metered postmarks will not be accepted as proof of timely mailing. Hand-delivered requests must be received by 5:00 p.m. e.s.t. Requests that are received after the deadline date will be returned to the sender.

ADDRESSES: Proposals for co-sponsorship should be sent to Yesenia Diaz, Public Health Advisor, President’s Council on Fitness, Sports, and Nutrition, 1101 Wootton Parkway, Suite 550, Rockville, MD 20852; Telephone: (240) 276–9865, Fax: (240) 276–9860. Proposals may also be submitted via email to: Yesenia.diaz@hhs.gov.

FOR FURTHER INFORMATION CONTACT: Yesenia Diaz, Public Health Advisor, President’s Council on Fitness, Sports, and Nutrition, Telephone: (240) 276–9865, email: Yesenia.diaz@hhs.gov.

SUPPLEMENTARY INFORMATION: