CBA | CONSUMER BANKERS ASSOCIATION

The Voice of the Retail Banking Industry

March 25, 2013

Judith Dupre
Executive Secretary
Federal Financial Institutions Examination Council
L. William Seidman Center - Mailstop: B-7081a
3501 Fairfax Drive
Arlington, VA 22226-3550

Re: Docket Number – FFIEC 2013-0001 – Social Media Comments

Dear Ms. Dupre:

The Consumer Bankers Association (CBA)[1] appreciates the opportunity to submit comments in response to the Federal Financial Institutions Examination Council's (FFIEC's), proposed guidance titled "Social Media: Consumer Compliance Risk Management Guidance" (Guidance). Once finalized, financial institutions and others will be expected to use the Guidance in their efforts to ensure their policies and procedures provide oversight and controls commensurate with the risks posed by social media activities.

Summary of CBA's Comments

- We request the FFIEC agencies reconsider this approach of providing a brief summary of a non-inclusive list of laws and rules that may be relevant in social media and how they may apply. Instead, the Guidance should merely state that statutes and rules can apply in social media and financial institutions and others should incorporate these considerations in their compliance programs. Any substantive changes that may arise as a result of social media should be made to those specific laws and rules through the notice and comment process.
- The definition of "social media" is unclear and overbroad. We request the FFIEC agencies clarify that this definition of social media does not include emails or internal social media.
- We do not believe there should be a requirement or expectation of a separate risk management program for social media. Financial institutions should be

[1] The Consumer Bankers Association ("CBA") is the trade association for today's leaders in retail banking - banking services geared toward consumers and small businesses. The nation's largest financial institutions, as well as many regional banks, are CBA corporate members, collectively holding two-thirds of the industry's total assets. CBA's mission is to preserve and promote the retail banking industry as it strives to fulfill the financial needs of the American consumer and small business.

permitted to integrate these components and concepts into their current risk management structure.

- Financial institutions should not be required to respond to complaints not provided directly to the institution and certainly should not be expected to monitor the entirety of the Internet for complaints. They should also not be required to monitor the entirety of the Internet for purposes of monitoring fraud.
- In a number of situations, it is not practical to require the posting of privacy policies or notices on social media sites.
- The information in the Guidance with regard to the requirements of the Children's Online Privacy Protection Act (COPPA) is unclear and may contradict guidance from the Federal Trade Commission (FTC).
- The Guidance raises issues as to how to comply with the requirements in the social media context with regard to posting the FDIC advertising statement and the Equal Housing Opportunity logo, as required under the Federal Housing Act (FHA).

Discussion

General Comments

A large portion of the Guidance addresses compliance and legal risks. Here, financial institutions are expected to periodically evaluate and control their use of social media to ensure compliance with all federal, state, and local laws, rules and guidance. The Guidance provides a brief summary of the laws and rules that may be relevant to social media, which is not intended to be an inclusive list.

We request the FFIEC agencies reconsider this approach of providing a brief summary of a non-inclusive list of laws and rules that may be relevant in social media and how they may apply. Most of the statutes and rules outlined in the Guidance are very lengthy and complex, and are often accompanied by significant regulatory guidance of their own, such as official interpretations and "frequently asked questions." Examples here include the Truth in Savings Act, the Equal Credit Opportunity Act, the Truth in Lending Act, the Real Estate Settlement Procedures Act, the Electronic Fund Transfer Act, and the various federal privacy statutes and rules.

The attempt in the Guidance to describe how each of these very complex statute and rules applies to social media could result in conflicts with other interpretive guidance and lead to contradictory guidance and interpretations from examiners. Instead, the FFIEC should merely state that these statutes and rules can apply in social media, as they would in other contexts; financial institutions should carefully consider whether and how these laws apply; and financial institutions should craft appropriate compliance

programs that address social media. Any substantive changes that may arise as a result of social media should be made to those specific laws and rules through a separate notice and comment process.

One example of the potential for conflict arises in the Regulation Z definition of an "advertisement." The breadth of the definition is such that many forms of social media could be inadvertently considered advertisements subject to Regulation Z. The Consumer Financial Protection Bureau (CFPB), the agency responsible for rulemaking and interpretation under Regulation Z, should undertake the substantive analysis and obtain the necessary input to address this specific issue. Any attempt in the Guidance to venture into this area could result in further confusion.

Nevertheless, to the extent the FFIEC finalizes the Guidance with this proposed approach of providing a brief summary of a non-inclusive list of laws and rules and how they may apply to social media, we offer the following comments on how certain of these provisions should be changed or clarified.

Definition of Social Media

In the Guidance, social media is defined as "a form of interactive online communications in which users can generate and share content through text, images, audio, and/or video" and is distinguished from other online media in that this type of communication "tends to be more interactive."

This definition is unclear and overbroad. We request the FFIEC clarify that this definition of social media is not intended to include emails or internal social media. Certain financial institutions provide internal social media platforms to facilitate communications among various groups of employees. These are not accessible to non-employees and, for this reason, we believe these types of platforms should not be included within the definition of "social media." We also request all other forms of communication that are not intended to be generally available to the public be excluded, such as private message boards or email distribution lists, as financial institutions do not have the ability to access or monitor these types of communications.

Risk Management Program

As outlined in the Guidance, financial institutions should have a specific risk management program to identify, measure, monitor, and control the risks related to social media. This program should be designed with participation from specialists in compliance, technology, information security, legal, human resources, and marketing. The Guidance also lists the many components that should be included.

We do not believe there should be a requirement or expectation of a separate risk management program for social media. Financial institutions should be permitted to integrate these components and concepts into their current risk management structure, and the final Guidance should reflect this option.

Monitoring Consumer Complaints and Inquiries

The Guidance requires financial institutions and others to have procedures for monitoring consumer complaints and inquiries on social media. Specifically, financial institutions are expected to have monitoring procedures in place to address situations when users post critical or inaccurate statements on social media sites and when consumers use these sites in an effort to initiate a dispute. Institutions are also expected to consider the extent they should respond to communications that disparage them on other parties' social media sites. In these situations, the Guidance suggests institutions should consider monitoring question and complaint forums on social media sites to ensure inquiries, comments, and complaints are addressed in a timely and appropriate manner.

Although financial institutions may choose to monitor the Internet to some extent, any requirement or expectation to monitor websites and social media sites where institutions have no control is very problematic, especially since these sites continue to expand and evolve. Facebook and LinkedIn are two significant social media platforms where these problems surface. Both of these mine data from the information they receive from users, and throughout the Internet, which can be used to create sites within these platforms that provide information about specific financial institutions. It takes a considerable amount of time and effort on the part of the institutions to monitor and change the information provided on these sites, and in the end they do not have ultimate control of the information. This includes situations when unsatisfied customers and employees create sites on these platforms, or elsewhere on the Internet, that are critical of financial institutions. In some instances information may be posted on social media sites anonymously, preventing the institution from responding. These issues present serious technological and human impediments to monitoring social media and to requiring institutions to respond to "complaints" lodged through these channels.

Financial Institutions should not be required to respond to complaints not provided directly to the institution, and any expectation an institution must monitor the entirety of the Internet is not feasible. This is particularly problematic in that there are many other social media platforms outside the United States that financial institutions may not be aware of and even if they are aware, it may difficult to respond if the information is provided in different languages and where social media sites are evolving rapidly.

To the extent there remains an expectation that financial institutions monitor complaints elsewhere, we note this part of the Guidance refers to developing procedures for this type of monitoring. If this is included in the final Guidance, we request the FFIEC agencies make it clear to the industry, and to their examiners, that this should not be interpreted to mean the monitoring of the entirety of the Internet and social media sites. Instead, the expectation should be that financial institutions can tailor this monitoring to a reasonable number of such sites, perhaps based on the institution's use of social media, similar to the expectations outlined in the Guidance with regard to the compliance risk management program for social media.

Fraud and Brand Identity

Under the Guidance, financial institutions are expected to have policies and procedures to monitor and respond to such risks as phishing and spoofing attacks in which fraudsters masquerade as the institution, as well as respond to comments made by social media users. Financial institutions certainly have every incentive to identify and stop all fraudulent use of their brand. Such fraudulent use not only affects the reputation of the institution, but can lead to safety and soundness concerns to the extent this damage significantly affects the institution's financial condition.

However, similar to the concerns raised above with regard to monitoring consumer complaints and inquiries, we do not believe these provisions should be interpreted as requiring financial institutions to monitor the Internet and social media sites in their entirety as this would be excessively burdensome. The Guidance should instead clarify that each institution should have the ability to determine for itself the extent it needs to monitor the Internet and social media sites in order to protect the institution in these situations. Moreover, some social media platforms may permit users to establish "spoof" or "parody" accounts (e.g., Twitter), and financial institutions may have limited ability to prevent or remove such accounts. The final Guidance should make clear that financial institutions are liable only for their actions and not for the actions of third parties.

Gramm-Leach-Bliley Act (GLBA) Privacy Requirements

The Guidance specifically refers to the GLBA privacy requirements. It says these requirements relating to the privacy and security of consumer information are relevant to social media when, for example, the institution integrates social media into customers' online account experience or takes applications though social media portals. In these situations, the Guidance expects financial institutions using social media to disclose

their privacy policies and not give the appearance they are treating consumer information carelessly.

To the extent the final version of the Guidance includes these provisions, we request the FFIEC provide clarifications in two areas. First, for certain forms of social media, such as Facebook, we request clarification that financial institutions may post general information on privacy policies. The FFIEC should not expect that the financial institution's privacy notice would need to be provided to visitors of the institution's Facebook page. It would be impractical for financial institutions to comply with the mail or electronic delivery requirements for these notices in these situations.

Second, to the extent privacy information would be expected to be posted on Twitter, this would not be practical due to the 140 character limitation. Although a link can be provided on a tweet, this would limit the other information that could be provided. For this reason, the Guidance should indicate that posting privacy information should not be expected if it would be impractical.

Even if the expectation is to post a policy, as opposed to a notice, such a requirement to post a privacy policy would be confusing for consumers since Facebook, as well as other social media sites, have their own privacy policies, and consumers may have difficulty distinguishing among these policies. At a minimum, this would require a careful, and perhaps lengthy, explanation as to the distinction between these policies, which may only serve to further confuse consumers. In addition, this would be impossible on sites, such as Twitter, that impose space limitations. This confusion could be further compounded on certain social media sites, such as Facebook, which also include apps that may have their own policies as well.

In these situations, the Guidance could suggest financial institutions include a simple message on social media sites that consumers should be cautious when providing information in these situations, due to the mostly public nature of social media and because institutions have no effective control over information posted on publicly available sections of social media sites. To the extent any privacy policy applies to social media postings, it is the policy of the social media sites themselves that would be most applicable in such situations.

Children's Online Privacy Protection Act (COPPA)

Under the Guidance, a financial institution should evaluate the extent it is covered under COPPA through its social media activities. Specifically, the Guidance addresses the following issues with regard to COPPA:

- Certain social media platforms require users to attest they are at least 13 years

old. A financial institution using those sites may rely on that policy. However, the institution must still monitor whether it is actually collecting personal information from someone who is under the age of 13.

- A financial institution maintaining its own social media site should establish, post, and follow policies for restricting access to the site to only users 13 and older, especially if these sites could attract children under 13, such as features resembling video games.

As for the first bullet above, we are concerned with the requirement that the financial institution must monitor whether it is actually collecting personal information from someone who is under the age of 13. We agree institutions should take the actions required to comply with the COPPA requirements if information comes to them to indicate the individual is under the age of 13. However, we would be concerned if this were interpreted to mean financial institutions would have to undergo any specific investigation to determine the age of a user, as this would impose significant, additional burdens. For this reason, we request this provision be clarified to indicate no such affirmative investigation would be required.

As for the second bullet above, we believe it conflicts with the COPPA requirements, specifically the "frequently asked questions (FAQs)" the FTC has issued (available at http://www.ftc.gov/privacy/coppafaqs.shtm). Specifically, we are concerned with the reference to "post" the policies for restricting access to the site to those 13 and older. The reason for our concern is that the FTC's FAQs 38 and 39, when read together, indicate it would not be appropriate to "post" a policy on the site stating those under the age of 13 are not allowed to participate without parental consent.

Specifically, FAQ 38 references a "teen-directed" site by stating such a site may attract minors and the site operator can "age screen," as long as it does not encourage minors to falsify their age, and then references FAQ 39 that clarifies age information should be asked in a neutral manner, such as drop down menu in which the consumer selects his or her month and year of birth. FAQ 39 also specifically indicates such a neutral manner includes "not encouraging children to falsify their age information, for example, by stating that visitors under 13 cannot participate on your website or should ask their parents before participating."

In our view, FAQs 38 and 39 suggest that posting a policy restricting access to those 13 and older, as advocated by the Guidance, is not consistent with asking for the age of the consumer in a neutral manner that does not encourage minors to falsify their age. For this reason, we request the Guidance be changed so it is consistent with these FTC FAQs.

Advertisements of Deposit Insurance

The Guidance indicates that the requirements regarding Federal Deposit Insurance Corporation (FDIC) membership and deposit insurance apply equally to advertising and other activities conducted via social media. With regard to displaying the FDIC official advertising statement, 12 CFR Part 328 includes a number of exceptions to the general rule that advertisements for deposits or non-specific banking products require the membership statement. For example, 12 CFR Section 328.3(d)(9) provides an exception in which advertisements are not required if they "are of the type or character that make impractical to include the official advertising statement, including, but not limited to, promotional items such as calendars, matchbooks, pens, pencils, and key chains." The Guidance should specifically clarify that certain social media activities and communications, such as those with character or type limitations, would qualify for such an exception.

Equal Housing Opportunity Logo

We have a similar concern with the requirement to post the Equal Housing Opportunity logo. The issue is whether a post or a tweet is considered an advertisement that would require such a logo, as required under the FHA. We note the Guidance indicates such logos should be posted on Facebook pages. However, we request the Guidance clarify that other posts and tweets are not advertisements that would require the logo as it is not possible or practical to include the logo in these contexts.

CAN-SPAM Act and Telephone Consumer Protection Act

The Guidance indicates both the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) and the Telephone Consumer Protection Act may be relevant if an institution sends unsolicited communications to consumers via social media. This provision goes on to state these restrictions could apply to communications via a social media platform's messaging feature. We believe this reference to such a "messaging feature" should be deleted as this is a complex issue that should be specifically analyzed and addressed by the Federal Communications Commission and the FTC.

Technological Impediments

In the Guidance the FFIEC requests information as to whether there are any technological or other impediments to financial institutions' compliance with applicable laws, regulations, and policies when using social media. As outlined in other sections of this letter, our significant concern here is financial institutions are not able to control,

through technology or otherwise, third-party use of social media that implicates the institutions. It is also difficult to isolate social media to a particular region, so any requirement addressing territorial restrictions would pose technology challenges for financial institutions.

* * * * * * * * * * * * *

Thank you for the opportunity to comment on the proposed Guidance. If you have any questions or wish to discuss these issues further, please feel free to contact me at (202) 255-6366 or at jbloch@cbanet.org.

Sincerely,

Jeffrey P. Bloch
Associate General Counsel