FEBRUARY 2014

SOCIAL MEDIA:

CONSUMER COMPLIANCE RISK MANAGEMENT GUIDANCE

BAI LEARNING & DEVELOPMENT

BAI Learning & Development Whitepaper
Social Media: Consumer Compliance Risk Management Guidance

On December 11, 2013, the Federal Financial Institutions Examination Council (FFIEC) issued "Social Media: Consumer Compliance Risk Management Guidance" (Guidance) for financial institutions on the consumer compliance risks associated with social media.

The Guidance offers insights on implementing a risk management program to aid in the understanding and management of risks associated with social media. The Guidance does not impose any new requirements or mandatory actions; however, it implies that a financial institution is expected to have addressed social media usage, access, management and oversight in their risk management program.

Who is affected by the Guidance?

The Guidance is intended for all banks, savings associations, credit unions and nonbank entities (hereafter known as financial institutions) supervised by the OCC, Federal Reserve, FDIC, NCUA, and the CFPB.

What is Social Media?

Since social media is constantly changing and evolving, the definition of what constitutes social media is evolving as well. The Guidance provides illustrative examples and defines social media as a form of interactive online communication where users can generate and share content through text, images, audio, and/or video. Social media includes websites such as Facebook, Google Plus, Twitter, Yelp, Flickr, You Tube, LinkedIn, Social Life, and even games such as Farmville. Traditional emails or text messages do not fall under the umbrella of social media for purpose of the Guidance.

How are Financial Institutions Using Social Media?

Just as social media is evolving, so are the ways financial institutions are using it. Financial institutions may use social media to advertise to customers and/or potential customers, invite feedback from customers, communicate to the public and facilitate applications for accounts.

The good, and the bad, of social media is that it can disseminate information to a large number of people quickly. The challenges and risks are heightened due to the informal nature and the fact that this interactive communication is occurring in a less secure environment.

What are the Risk Areas?

Compliance and Legal Risks

Social media creates a heightened compliance and/or legal risk due to the potential for violations of laws and regulations. A financial institution risks that its policies and procedures may not have kept pace with emerging technologies or that employees may not be aware of certain requirements when using social media. Noncompliance can lead to potential enforcement actions and/or civil lawsuits. Therefore, it is imperative for financial institutions to have an understanding of the regulations that may be affected by social media.

Advertising

There are no exemptions for social media as it relates to advertising. Financial institutions need to ensure advertisements are clear and conspicuous and comply with the advertising requirements found in the following regulations:

- Truth in Savings Act/Regulation DD and Part 707
- Fair Lending Laws: Equal Credit Opportunity Act/Regulation B and Fair Housing Act
- Truth in Lending/Regulation Z
- Unfair, Deceptive, or Abusive Acts or Practices
- Deposit Insurance or Share Insurance
- Telephone Consumer Protection Act/CAN-SPAM Act
- Fair Credit Reporting Act/Fair and Accurate Credit Transactions Act

The financial institution must include all necessary disclosures when using social media to advertise including additional disclosures when triggering terms are utilized, FDIC insurance or NCUA Share Insurance requirements, and all other required disclosures. In addition, the advertisement must not be considered discouraging or unfair, deceptive or abusive. The advertisement must only advertise products and services and the related terms and conditions that are actually offered.

Loan or Deposit Applications

If the financial institution utilizes social media to facilitate or accept applications, the timing requirements and specific disclosures of the following regulations must be adhered to:

- Truth in Savings Act/Regulation DD and Part 707
- Equal Credit Opportunity Act/Regulation B
- Truth in Lending/Regulation Z
- Real Estate Settlement Procedures Act
- BSA/AML

The financial institution must confirm it is providing the necessary application disclosures in a timely manner. It must refrain from requesting information that is prohibited under Regulation B. The financial institution's Customer Identification Program must be adhered to and customer due diligence and enhanced due diligence procedures followed.

Collection of Debts

The financial institution must also be aware of the risks and the rules under the Fair Debt Collection Practices Act if debts are collected using social media. Financial institutions should ensure they are not disclosing the existence of a debt on social media, not harassing or embarrassing consumers about their debts, or making false or misleading representations.

Payment Systems

Social media may also be used to facilitate a consumer's use of payment systems. A financial institution should keep in mind laws, regulations, and other rules regarding payments including the Electronic Funds Transfer Act/Regulation E or rules applicable to check transactions.

Disputes

Customers may use social media to communicate issues or concerns. The financial institution should ensure that the comment does not constitute an error dispute under Regulation E, a billing error dispute under Regulation Z, or a direct dispute under FCRA. If one of those events is triggered, the financial institution must follow appropriate procedures.

Electronic Banking Products and Virtual Economies

A financial institution must also be aware of how social media affects the Bank Secrecy Act/Anti-Money Laundering Requirements. The financial institution's BSA/AML program should address the risks involved with electronic banking products offered in the context of social media as well as the risks associated with customers utilizing those products and services.

There are also a number of emerging risks in the virtual world such as with Internet games that allow for digital currencies. These virtual economies present a higher risk for money laundering and terrorist financing. The financial institution should ensure they are addressing the risks as applicable to the institution.

Receiving and Responding to Comments

From a Community Reinvestment Act perspective, the Public File must include all written comments received from the public and any responses for the current year and prior two years that specifically relate to how the financial institution is meeting the needs of its community. Comments received through social media sites run by or on behalf of the financial institution should be included. The financial institution does not need to include comments on social media sites not run by the financial institution.

Collecting and/or Sharing Customer Information

Privacy is a significant issue in the context of social media. The Gramm-Leach-Bliley Act Privacy Rules and Data Security Guidelines must be considered. The financial institution should disclose its privacy policy when using social media and treat all information received with proper security measures even when there is no consumer/customer relationship.

The FTC's Children's Online Privacy Protection Act has a number of requirements for operators of websites and online services directed at children younger than 13. Many social media platforms require that their users be 13 to have an account. A financial institution can rely on that assertion; however it should still monitor the website to confirm it is not collecting data from anyone under the age of 13.

Fair Credit Reporting Act requirements are triggered when the financial institution collects any medical information in connection with a loan.

Reputation Risk

Reputation risk results from negative public opinion. Even if the financial institution has not violated a law, negative opinions and posts from dissatisfied customers could harm the institution's image and brand identity.

Third party concerns also increase reputation risk when a third party is used to provide social media services. Even if the social media site is owned and maintained by a third party, the financial institution is ultimately responsible for the content. Prior to engaging the service provider, the financial institution should conduct thorough due diligence on the third party's reputation, policies including how the third party collects and handles consumer information, the process and frequency of policy change, and what, if any, control the institution may have over the third party's policies or actions, as well as the content.

Whether the financial institution or a third party manages the site, the financial institution should consider the potential reaction by the public to any use of consumer information obtained via social media. The financial institution should ensure it has procedures to respond in the event confidential or sensitive information is posted on the institution's website by a customer.

Social media can be used to address customer complaints and questions, but if it is not done in a timely manner it can increase reputation risk. A negative comment or customer complaint posted on social media can be seen by many in a short amount of time. It is important the financial institution responds to the complaint appropriately. The financial institution should also consider how to handle complaints received indirectly and posted on websites not owned or operated by the financial institution such as Yelp.

Operational Risk

Operational risk is the risk of loss resulting from failed or inadequate processes, people or systems. Social media should be included when the financial institution is assessing the risks associated with the use of information technology covered by the *FFIEC Information Technology Examination Handbook.* Social media is vulnerable to the distribution of malware and account takeover. Controls need to be in place to protect its systems and ensure the proper response in the case of a security event.

What Should Financial Institutions Do to Manage Risks for Social Media?

Social media should be included in the financial institution's risk management program. The program should be robust in identifying, measuring, monitoring and controlling the risks related to social media. The financial institution should examine the various ways it uses social media and the depth of its involvement. The financial institution should also consider the potential comments or complaints that may occur on any social media platform and examine what, if any, would be considered an appropriate response.

Employees may also use social media for professional or personal use. Employees could unknowingly subject the financial institution to compliance, operational or reputational risk, with their actions reflecting negatively on the financial institution. The financial institution should analyze what training is required. Policies and procedures should outline what is and is not acceptable behavior.

When creating the risk management program, the financial institution should involve a cross-departmental representation from compliance, technology, information security, legal, human resources, and marketing to ensure all aspects of social media usage is addressed. The program should also include guidance and training for employee official use of different social media sites.

The Guidance details the following areas that a risk management program should include:

- **Governance structure** – The Board of Directors or senior management set clear goals to establish how the financial institution intends to use social media to meet those goals. The structure should also establish risk tolerances, assessments and controls.
- **Policies and procedures –** Policies and procedures should cover the use and monitoring of social media, incorporating methodologies to address risks from online postings, replies and retention.
- **Third Party Relationships –** The risk management program should address the process for selecting and managing third party relationships in connection with social media.
- **Employee training program –** Training should discuss the policies and procedures for employee use in connection with official business as well as other uses as applicable including impermissible activities.
- **Oversight** – The program should outline a process for monitoring information posted to proprietary social media sites.
- **Audit and compliance function –** The financial institution should have a way to ensure compliance with laws and regulations, policies and procedures, and risk management.
- **Reporting –** Reports should be made to the Board of Directors evaluating the effectiveness of social media in meeting its initial goals.

B**AI Learning & Development**
Compliance Training Simplified

BAI Learning & Development provides industry-leading regulatory compliance training solutions to more than 1,500 banks, credit unions and regulatory agencies.

In addition to the BAI Learning Manager's state-of-the-art technology and compliance training courseware, customers have complimentary access to a robust collection of resources to supplement their knowledge of the regulatory environment and enhance financial training initiatives. The BAI Learning & Development online community, L&D Connect, links compliance and training professionals to one another, industry experts and to a host of complimentary BAI resources, including webinars and whitepapers.

To join L&D Connect, please click the L&D Connect icon in the Learning Manager or contact Customer Support Services. All compliance and training personnel from customer organizations are welcome to join.