OBER | KALER
Attorneys at Law

Social Media Compliance Issues for Community Banks

March 20, 2014

www.ober.com

Community Bank Advantages

- Standing in the Community
- Customer Care
- Superior Customer Service

Social media offers an opportunity to establish an additional community presence and tap into existing community goodwill

Regulatory Guidance

- FFIEC issues "Social Media: Consumer Compliance Risk Management Guidance," FIL-56-2013 (December 11, 2013)

http://www.fdic.gov/news/news/financial/2013/fil13056.html

- Concern: this form of customer interaction tends to be both informal and dynamic and may occur in a less secure environment

- "Reminds institutions that they must properly address risks, including compliance, operational, third-party, and reputation risks, that arise in connection with social media activities"

Types of Social Media

Interactive online communication in which users can generate and share content through text, images, audio, and/or video

- Micro-blogging sites (e.g., Facebook, Twitter, Google Plus, and MySpace)
- Professional networking (e.g., LinkedIn)
- Forums, blogs, customer review web sites and bulletin boards (e.g., Yelp)
- Photo and video sites (e.g., Flickr and YouTube)
- Virtual worlds (e.g., Second Life)
- Social games (e.g., FarmVille and CityVille)

Bank Uses of Social Media

- Advertising and marketing
- Providing incentives
- Facilitating applications for new accounts
- Inviting feedback from the public
- Engaging with existing and potential customers
  - Customer Service
  - Complaints
- Monitoring the Bank's online profile and reputation
- Monitoring competitors

Social Media Risk Management Program

- Should identify, measure, monitor, and control the risks related to social media
- Program size/complexity commensurate with involvement
- Even if the institution does not use the medium, it should
  - Consider the potential for negative comments or complaints that may arise within the many social media platforms
  - When appropriate monitor for such comments and/or respond to them
- Should involve participation of specialists in compliance, technology, IT, legal, human resources, and marketing

Program Elements: Governance Structure

- Governance structure – Board of Directors and/or senior management
  - Establish strategic goals to be accomplished by use of social media, e.g.
    - Increased brand awareness
    - Product advertising
    - Researching new customer bases
  - Establish controls and ongoing assessment of risk in social media activities
  - Establish clear roles and responsibilities

Program Elements: Policies and Procedures

- Either stand-alone or incorporated into other policies and procedures
- Cover the use and monitoring of social media
- Compliance with consumer protection laws and regulations
- Should incorporate methods for addressing risks from online postings, edits, replies and retention
  - Not expected to monitor all Internet communications for complaints and inquiries about the institution (though not a bad idea to some extent)
  - Institution may establish specified channels on its proprietary social media sites that customers must use for submitting complaints

Program Elements: Third Parties

- Software companies, consultants, hosting sites, etc. – possible exposure to reputation risk
- Institution should evaluate and perform appropriate due diligence on third party service providers, including
  - The third party's reputation in the marketplace
  - The third party's policies, including policies on collection and handling of consumer and bank customer information
  - The process and frequency of changes to the third party's policies
  - The control that the institution has over the third party's actions
- Institution is responsible for its social media sites, even if sites are owned/maintained by third parties

Program Elements: Employee Training

- Should focus on official, work-related use of social media
- To the extent permissible, may address personal use of social media, including defining impermissible activities
- Should address risks associated with employee use
  - 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
  - Potential compliance risk, operational risk, and reputation risk
- Requires tight control over the message and the messenger on proprietary social media sites

Program Elements: Audit and Reporting

- An internal oversight process for monitoring information posted to the institution's proprietary social media sites
- Include in the audit and compliance function
- Require periodic reporting and evaluation to the board/senior management

Risk Areas

- Compliance and Legal Risk
- Reputation Risk
- Operational Risk

Compliance Risk – Advertising

- Informal posts may be advertising
- Advertising loan products – TILA, Reg Z
- Advertising deposit products – Truth in Savings, Reg DD
- Fair lending – ECOA and Fair Housing Act
- False and deceptive advertising – UDAAP
- Endorsements
- Official advertising statements – FDIC and “Equal Housing Lender” advertising statements; nondeposit investment products

Compliance Risk – Customer Interactions

- Taking loan applications –
  - TILA/Reg Z
  - RESPA
  - Fair Lending/Fair Housing
- Customer service –
  - Fair lending
  - FCRA
  - RESPA
  - FDCPA
- Payment Systems – Reg E; check transactions; Reg CC

Compliance Risk – BSA/AML

- Incorporate social media into Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program
  - Policies
  - Compliance officer
  - Independent testing
  - Employee training
- Customer identification and due diligence
- Monitoring for suspicious activities/suspicious activity report (SAR) filings
- Maintaining records of electronic funds transfers

Compliance Risk – Privacy

- Gramm-Leach-Bliley and Data Security Guidelines
  - Privacy policy disclosure
  - Secure treatment of customer information delivered through social media channels
- CAN-SPAM Act and Telephone Consumer Protection Act
- Children's Online Privacy Protection Act
- Fair Credit Reporting Act (FCRA)

Compliance Risk – CRA

- Under Community Reinvestment Act (CRA), institutions must maintain a public file that includes
  - 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 community credit needs
  - responses to those comments, if comments and responses do not reflect adversely on the good name/reputation of any persons other than the institution, or publication would violate the law
- Requirements apply to comments received through social media channels
- CRA does not necessarily apply to comments made on Internet sites not run by or on behalf of the Institution

Reputation Risk

- Fraud and Brand Identity
  - Monitor and address fraudulent use of the institution's brand
  - Appropriately address harmful or inaccurate statements
- Third Party Concerns
- Privacy – develop special sensitivity to any use of customer information over social media channels
- Consumer Complaints and Inquiries – establish specific channel to receive complaints and inquiries and respond in a timely manner to all complaints and inquiries on other social media sites
- Employee Use of Social Media

Operational Risk

- Operational Risk = IT Risk
- Can be external (hacking, malware) or internal events
- References:

http://ithandbook.ffiec.gov/it-booklets.aspx

http://ithandbook.ffiec.gov/

http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf

http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf

Conclusion and Questions