

FFIEC Releases Final Guidance for Financial Institutions Using Social Media

December 23, 2013

The Federal Financial Institutions Examination Council (the “FFIEC”) has released final guidance addressing the applicability of federal consumer protection and compliance laws, regulations, and policies to activities conducted via social media by financial institutions. The final guidance does not impose any new requirements on financial institutions; rather, it is intended to clarify existing laws and help financial institutions understand potential risks associated with the use of social media and how to address and manage those risks.

The final guidance defines social media as a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. Some examples of social media are Facebook, Twitter, Yelp and LinkedIn. The FFIEC advises financial institutions to have a risk management program designed to identify, measure, monitor and control the risks related to social media use. Each financial institution should develop a risk management program based on the size, complexity, and mix of social media activities engaged in by the institution.

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 directs 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 establishes 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 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.

The final guidance identifies the major risk areas related to social media as compliance and legal risks, operational risks, and reputation risks.

Compliance and Legal Risk

Compliance risk is the potential for violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. The final guidance clarifies that existing laws and regulations do not contain exceptions regarding the use of social media; therefore, a financial institution should comply with applicable laws and regulations as it does when it engages in these activities through other media.

A list of existing laws and regulations that may be relevant to a financial institution's social media activities is included in the guidance. Some laws and regulations identified in the final guidance are: (i) the Truth in Savings Act/Regulation DD, (ii) the Equal Credit Opportunity Act/Regulation B, (iii) the Fair Housing Act, (iv) the Truth in Lending Act/Regulation Z, (v) the Real Estate Settlement Procedures Act, (vi) the Fair Debt Collection Practices Act, (vii) Section 5 of the Federal Trade Commission Act (unfair, deceptive, or abusive acts and practices), (viii) deposit insurance rules, (ix) the Electronic Fund Transfer Act/Regulation E, (x) the Bank Secrecy Act and anti-money laundering laws and regulations, (xi) the Community Reinvestment Act, and (xii) privacy laws.

Reputation Risk

Reputation Risk is the risk arising from negative public opinion. The final guidance provides that a financial institution engaged in social media activities must be sensitive to, and properly manage, the reputation risks that arise from those activities. Reputation risk can arise in the following areas: (i) fraud and brand identity, (ii) concerns with using third parties in connection with social media activities, (iii) privacy concerns, (iv) consumer complaints and inquiries, and (v) employee use of social media sites.

Operational Risk

Operational Risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The FFIEC advises financial institutions to 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.

The final guidance can be found at <http://www.fdic.gov/news/news/financial/2013/fil13056.pdf>.

If you have any questions regarding the final guidance, please feel free to contact Joseph D. Simon at 516-357-3710 or via email at jsimon@cullenanddykman.com, or Elizabeth A. Murphy at 516-296-9154 or via email at emurphy@cullenanddykman.com.

Practices

- Banking and Financial Services
- Regulatory and Compliance

Industries

- Financial Institutions

Attorneys

- Joseph D. Simon