
FFIEC Issues Draft Guidance on Financial Institutions' Use of Social Media

2013-01-24

The Federal Financial Institutions Examination Council ("FFIEC"), the council of federal agencies with responsibility for supervising financial institutions, issued draft guidance yesterday on financial institutions' use of social media platforms to interact with their customers and clients.¹ The draft guidance identifies broad categories of legal, reputational, and operational risk that reliance on social media may raise for financial institutions, and in each of those categories identifies examples of particular laws, regulations, and practices that deserve attention. Its most basic message is that "financial institution[s] should have a risk management program that allows [them] to identify, measure, monitor and control the risks related to social media."² Like the FFIEC's July 2012 statement on cloud computing, the draft guidance reflects the FFIEC's heightened attention to financial institutions' use of new technologies.³ It invites comments—including in response to the question whether there are "technological or other impediments to financial institutions' compliance with otherwise applicable laws, regulations, and policies when using social media"—that are due March 25.⁴

Legal, Reputational and Operational Risks

The draft guidance groups its recommendations in three categories: legal, reputational, and operational risks. In the first, the draft guidance identifies a number of laws and their implementing regulations as potentially relevant to financial institutions' collection, distribution, and maintenance of information through social media platforms and thus as worthy of careful review. Those include the Truth in Savings Act/Regulation DD and Part 707, the Equal Credit Opportunity Act, the Fair Housing Act, the Truth in Lending Act/Regulation Z, the Fair Debt Collection Practices Act, the "unfair or deceptive acts or practices" ("UDAP") prohibition in Section 5 of the Federal Trade Commission Act and the "unfair, deceptive, or abusive acts or practices" ("UDAAP") prohibition in the CFPB Act, the Electronic Fund Transfer Act, the Bank Secrecy Act, the Community Reinvestment Act, and several laws governing privacy and data security, including the Gramm-Leach-Bliley Act, the CAN-SPAM Act, the Telephone Consumer Protection Act, and the Children's Online Privacy Protection Act. With respect to the UDAP prohibition in Section 5 of the FTC Act and the UDAAP prohibition in the CFPB Act, the draft guidance asserts that "[a]n act can be unfair, deceptive, or abusive despite

technical compliance with other laws.”⁵

With respect to reputational risks, the draft guidance highlights several areas of potential concern: on-line fraud and its possible effect on brand identity; reliance on third-party service providers and the need for adequate monitoring; transparency and privacy obligations in dealing with customers and clients; and employee use of social media.⁶

Regarding operational risk, the draft guidance reminds regulated institutions and their third-party IT service providers to consult the FFIEC’s IT Examination Handbook, and particularly its booklets on Outsourcing Technology Services and Information Security.⁷ Companies should also be aware of the booklet on Supervision of Technology Service Providers, which was just revised in October 2012.⁸

Risk Management

In stressing that financial institutions should have an appropriate risk management program in place to cope with potential risks from social media use, the draft guidance notes that such a program should include: clear internal assignments of roles and responsibilities, policies and procedures, due diligence processes, employee training programs, oversight processes, audit and compliance functions, and channels for reporting up the chain of command.⁹

Call for Comments

The draft guidance invites comments on all aspects of its proposed recommendations and poses three particular 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 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 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?” Comments are due by March 25.

¹ The FFIEC’s member agencies are the Office of the Comptroller of the Currency (“OCC”), Board of Governors of the Federal Reserve System (“Federal Reserve”), Federal Deposit Insurance Corporation (“FDIC”), National Credit Union Administration (“NCUA”), Consumer Financial Protection Bureau (“CFPB”), and the State Liaison Committee. The draft guidance is [available here](#) and at 78 Federal Register 4848 (Jan. 23, 2013).

² 78 Fed. Reg. at 4850.

³ See FFIEC, Statement on Outsourced Cloud Computing (July 10, 2012), [available here](#).

⁴ 78 Fed. Reg. at 4849.

⁵*Id.* at 4851.

⁶*Id.* at 4853-54.

⁷*Id.* at 4854.

⁸ The chapter is available at [http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers-\(tsp\).aspx](http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers-(tsp).aspx).

⁹ 78 Fed. Reg. at 4850.