Financial Services Alert

# Social media risk management and FFIEC-proposed guidance

The Federal Financial Institutions Examination Council (FFIEC)[1] has issued proposed guidance on social media risk management titled Social Media: Consumer Compliance Proposed Guidance. This regulatory alert will provide background on the impact and increasing importance of social media to financial institutions' consumer compliance risk profile. The alert will then present an overview of the proposed guidance and a proposed framework for social media risk management that is broadly applicable.

Facebook has 800 million users worldwide. In the third quarter of 2011, US online users spent 16% of their time on Facebook.[2] This is a 2% increase from the previous year.[3] On average, 172 million people visit Facebook per day. According to an Ernst & Young survey, 67% of social media users say that social media influences their purchases.[4] Social media has become a powerful tool to increase market share. According to research that assessed the top 100 global brands that were the most active in social media, those brands saw an 18% increase in revenue from the previous year, while the least active brands saw a 6% decrease in revenue.[5] As a result of the seemingly exponential growth of social media and the increased direct and indirect participation by financial institutions, many governmental regulatory agencies are issuing compliance guidance on risks associated with social media usage.

The FFIEC issued proposed guidance to address the applicability of existing federal consumer protection and compliance laws, regulations and policies to activities conducted through social media by banks, savings associations, credit unions and non-bank entities, and new risks related to these requirements that are unique to these channels. This guidance is designed to provide financial institutions with an understanding of the potential compliance, legal, reputational and operational risks associated with the use of social media. This guidance provides regulatory expectations and suggestions for managing social media risks. This guidance broadly 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. Additionally, the definition of social media includes micro-blogging, forums, blogs,

Building a better working world

customer review websites and bulletin boards, photo and video sites, websites that enable professional networking, virtual worlds and social games. The FFIEC has distinguished social media from other forms of online media in that social media generally involves more interactive online communication. The guidance further notes that social media can and is being used by financial institutions for a variety of reasons, including advertising, marketing, providing incentives, facilitating applications for new accounts, inviting feedback from the public, and engaging with existing and potential customers. The guidance acknowledges that the informal and dynamic nature of some forms of social media interaction provides distinct and unique challenges to financial institutions.

**Risk management**

The FFIEC's proposed guidance discusses regulatory expectations for social media management by financial institutions. Financial institutions should have a risk management program that identifies, measures, monitors and controls social media risk. The guidance suggests a risk-based approach to social media compliance that looks to the breadth of the financial institution's involvement in social media in the compliance program. The guidance calls for cross-functional compliance teams, including Compliance, Technology, Information Security, Legal, Human Resources and Marketing. The guidance states that the components of a social media risk management program should include:

- A governance structure with clear roles and responsibilities dictated by the board of directors or senior management
- 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
- A due diligence process for selecting and managing third-party service provider 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
- 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, regulations and guidance
- Parameters for providing appropriate reporting to the financial institution's board of directors and senior management

**Types of social media risk**

The use of social media to attract and interact with customers can impact a financial institution's risk profile, including the potential for harm to consumers, as well as compliance, legal, operational and reputational risks.

The risk introduced by social media can impact a financial institution's overall risk rating. This guidance is intended to help financial institutions identify potential risks to ensure institutions are aware of their responsibilities to address these risks within their overall risk management program.

**Coverage**

The compliance and legal risks posed by social media derive from a wide array of existing consumer-based laws and agency regulations that have applicability to multiple business lines and channels, including this one. In most cases, the existing requirements that extend to traditional and electronic communications and services also apply to social media-based channels and services, even though they may be more informal by nature. The guidance provides potential legal and compliance risks related to deposit and lending products, payment systems offered via social media, including Bank Secrecy Act/Anti-Money Laundering (BSA/AML) programs, the Community Investment Act (CRA), and privacy obligations and impacts.

**Deposits**

Financial institutions use social media to market products and create new accounts. The FFIEC-proposed guidance states that, at a minimum, institutions should ensure that the advertising, origination and record retention policies comply with the Truth in Savings Act (TISA), as implemented by Regulation DD.

TISA requires disclosures about fees, annual percentage yield, interest rate and other terms. Disclosures must accurately represent the institution deposit account for consumers. TISA requires electronic advertisements (whose definition would include social media-based communications) containing certain triggering terms (e.g., APY) to provide clarifying information either on the page or through links.

Financial institutions must clearly state whether a deposit product is insured by the Federal Deposit Insurance Corporation (FDIC) or the National Credit Union Administration (NCUA) as applicable. Financial institutions must notify consumers that are marketed or sold non-deposit investment products that such products are not insured by the FDIC or the NCUA. The disclosures are required anywhere insured products are advertised, including social media sites.

**Lending**

The Real Estate Settlement Procedures Act (RESPA) and Regulation Z disclosure requirements apply to applications taken via social media. Unfair, deceptive and abusive practices (UDAAP) requirements

(Federal Trade Commission Act Section 5 and Sections 1031 and 1036 of the Dodd–Frank Wall Street Reform and Consumer Protection Act) related to false or misleading representations apply and the informal nature of some social media communications could result in heightened UDAAP risk. Financial institutions should ensure that communications through social media sites are accurate, not misleading, and consistent with information delivered through electronic media. Using social media to disclose a debt, harass, or embarrass a consumer would violate the Fair Debt Collection Practices Act (FDCPA).

**Advertisements**

Both Regulation B and the Federal Housing Administration (FHA) prohibit advertisements and marketing that use a prohibited basis to discourage an applicant. Regulation B provides time lines for requesting and notifying an applicant of the need for additional application information or notifying the applicant of credit decisions. These time lines also apply to applications solicited and submitted via social media. Pre-screened credit solicitations sent via social media are also subject to Regulation B.

The FHA prohibits any advertisement, including those on social media, that indicates a preference based on race, color, national origin, religion, sex, familial status or handicap. Use of social media sites which themselves are targeted to a specific audience could be challenged if they discourage access, and therefore applications, for a loan on a prohibited basis. Regulation Z requires all credit advertisements to be clear and conspicuous, including those done via electronic channels such as social media. Advertisements and applications taken via social media must provide consumers with disclosure in accordance with times allocated by Regulation Z.

**Payment systems**

Financial institutions should ensure that all applicable regulations and regulatory requirements, including disclosures, are adhered to when social media is utilized to initiate payment system transactions. For example, the Electronic Fund Transfer Act (EFTA), as implemented through Regulation E, requires certain consumer disclosures, rights and investigation timing requirements when an electronic funds transfer (including those initiated through social media) is initiated to debit or credit a consumer's account.

**Bank Secrecy Act/Anti-Money Laundering (BSA/AML)**

BSA compliance programs must include internal controls that ensure proper risk management and compliance with related recordkeeping and reporting requirements. Financial institutions should ensure BSA internal controls also address customers engaging in electronic banking through social media. The financial institutions' policies and procedures should include involvement with social media sites that involve virtual world gaming and internet-based payment systems, given their money laundering-related exposure.

**Community Reinvestment Act (CRA)**

The CRA requires covered financial institutions to maintain public files of written comments received from the public for the current and two prior years. This could potentially include comments posted on social media sites. Institutions should ensure that public comments' policies and procedures and archives include their social media site-sourced consumer comments.

**Privacy**

Social media poses privacy risks when a financial institution collects or has access to consumer information though them. FFIEC-proposed guidance states financial institutions should consider, at a minimum, the Gramm–Leach–Bliley Act (GLBA), the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN–SPAM), Telephone Consumer Protection Act (TCPA), Children's Online Privacy Protection Act (COPPA) and Fair Credit Reporting Act (FCRA) in assessing privacy and social media compliance.

The GLBA generally imposes regulatory requirements on privacy and security of consumer information when an institution collects or accesses information about consumers. Use of social media sites which capture this information routinely can heighten this risk. CAN-SPAM and the TCPA regulatory requirements apply to social media if the financial institution sends unsolicited communications or messages through social media.

COPPA imposes regulatory requirements on operators of commercial websites that direct communications to children under the age of 13 and collect, use or disclose personal information from children. Financial institutions should restrict and monitor the collection of personal information from children under 13. Lastly, the FCRA contains restrictions and requirements related to a financial institution's making solicitations to consumers using eligibility information, responding to direct credit reporting information disputes, and collecting medical information used to determine loan eligibility through any channel, including social media.

**Reputational risk**

The FFIEC defines reputational risk as the risk arising from negative public opinion, even in the absence of legal violation. The guidance states the financial institutions must be sensitive to and manage the risk associated with social media-related consumer privacy and transparency issues. Reputational risk can also arise out of fraud involving the brand identity (e.g., "spoofing" via social media), the improper activities of third parties used to host or manage social media sites, privacy issues when social media site personal data is used improperly or lost, and employee use of social media to communicate with customers of for their personal use where they reference or represent the institution.

To address these risks, financial institutions should be aware of any fraudulent or improper use of the institution's brand in social media. Financial institutions should use social media monitoring to be aware of and mitigate this risk. Policies should be implemented to identify and address fraudulent use of brand. Financial institutions are also responsible for monitoring the activities of third parties relied on for social media portal and content management. Financial institutions should carefully weigh the benefits of using a third party when their control over content and process is limited.

Financial institutions should be aware of consumer reactions when using consumer information on social media sites. Procedures should be implemented to address risks associated with public posting of confidential or sensitive consumer information.

Social media-posted customer complaints should be addressed with the same vigor as those received directly. Broader allegations against the institution should also be monitored and addressed. Responses should be handled and crafted with the same care as they would through written media channels.

Employees can subject the institution to reputational risk. Institutions should be aware that employee communications, even personal ones, on social media sites can be construed by consumers as official policies.

Financial institutions should develop a social media strategy that guides employee behavior. A social media policy should address how to respond to user-generated content and web comments. Common employee guidelines should include:

- Employees should always disclose that they are employees of the company when commenting on matters related to the company.
- Unless employees are company spokespeople, they should make it clear that their opinions do not represent the company.
- Employees should not comment on legal matters or the company's financial status.

**Operational risk**

The proposed guidance defines operational risk as the risk of an internal or external event causing a loss as a result of inadequate or failed processes, people or systems. The FFIEC specifically addresses information-technology-related social media risks. The FFIEC states that social media is vulnerable to account takeover and the distribution of malware.

**Social media regulatory governance**

The Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), Investment Industry Regulatory Organization of Canada (IIROC) and United Kingdom Financial Services Authority (UK FSA) have all issued guidance regarding social media risk and compliance.[6] The FFIEC-proposed guidance is a further extension of these existing governmental regulations. While the regulations and guidance issued by global regulators are generally similar, there are various differences that have meaningful impact. Financial institutions subject to oversight by multiple regulatory bodies must ensure that their social media governance and controls satisfy the requirements of each of their respective regulators.

**Governance of social media strategy**

Pursuant to the FFEIC guidance, firms are expected to expand their existing governance structures to ensure their policies and procedures provide oversight and controls commensurate with the risks posed by their social media activities. In particular, financial institutions' compliance programs must include appropriate oversight and monitoring and testing of these risks.

**Audit**

Social media audits are important in the monitoring of the overall social media governance. Social media audits offer insight into social media activities of employees and customers alike. Audits should assess compliance with social media policy, determine the effectiveness of the social media strategy and provide feedback for improvements.

**Conclusion**

Despite the uncertainty with new governmental regulations and potential standards for enforcement, the basic requirements related to social media compliance are consistent with those imposed on traditional and other electronic-based channels. Social media poses the same types of risk as other forms of electronic communication, including potential consumer harm, compliance, legal, operational and reputational risks. However, its unique characteristics, including high levels of interactivity, informality, the routine sharing and storage of personal information, the ability of users to reach large audiences instantaneously, and the proliferation of data channels and messages that need to be monitored, present some unique impacts and risks related to these requirements. The FFIEC's proposed guidance is intended to help financial institutions manage these potential risks through appropriate oversight and control of social media. Social media governance strategy, policy, monitoring and audits provide the guideposts for creating an effective social media risk management compliance program.

**Sources**

[1] The FFIEC is composed of the following regulatory agencies: Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), the Consumer Financial Protection Bureau (CFPB), and the State Liaison Committee (SLC).

[2] WSJ Blog/Digit: Live Blog: "Facebook Developer Conference, "Dow Jones News Service, 22 September 2011, via Factiva, Copyright 2011, Dow Jones & Company, Inc.

[3] WSJ Blog/MarketBeat: Live Blog: "Facebook Sucks Up a Ridiculously Huge and Growing Share of Our Time Wasted Online, "Dow Jones News Service, 26 September 2011, via Factiva, Copyright 2011, Dow Jones & Company, Inc.

[4] YouGov Social Media Survey, Ernst & Young, 2011.

[5] Quick Study: "Direct Correlation Established Between Social Media Engagement and Strong Financial Performance," PR News, 27 July 2009, via Factiva, Copyright 2011, Dow Jones & Company Inc.

[6] The SEC issued a National Examination Risk Alert for Investment Advisor Use of Social Media in January 2012. FINRA issued Regulatory Notice 11-39 in August 2011 and Regulatory Notice 10-06 in January 2010. IIROC issued IIROC Notice 11-0349 in December 2011. Lastly, the UK FSA issued the FSA Financial Promotions Industry Update in June 2012.

**Ernst & Young LLP contacts**

**Amy Brachio**
Partner
Advisory Financial Services
+1 202 327 7552
amy.brachio@ey.com

**Maureen Day**
Partner
Advisory Financial Services
+1 212 773 2783
maureen.day@ey.com

**Ryan Gorney**
Senior Manager, Advisory
Financial Services
+1 216 583 2688
ryan.gorney@ey.com

**Jason Lambertson**
Senior Manager, Advisory
Financial Services
704 350 9151
jason.lambertson@ey.com

**Ursula Nigrelli**
Senior Manager
Advisory Financial Services
+1 212 773 6306
ursula.nigrelli@ey.com

**Michael Patterson**
Principal, Advisory
Financial Services
+1 212 773 2824
michael.patterson1@ey.com

**Nancy Reich**
Executive Director, Advisory
Financial Services
+1 212 773 0300
nancy.reich@ey.com

EY | Assurance | Tax | Transactions | Advisory

**About EY**
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

**EY is a leader in serving the global financial services marketplace**
Nearly 35,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,500 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2013 Ernst & Young LLP.
All Rights Reserved.

SCORE No. CK0680
1307-1102810_NY

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

**www.ey.com**