Banking on Social Media
Understanding and Implementing the FFIEC Social Media Guidelines
Contents

I. Executive Summary ................................................3
II. Social Media and the Banking Industry ....................4
III. Adding Regulation to the Equation ..........................5
    FFIEC Social Media Guidelines Dissected ..................5
    Compliance and legal ..........................................6
    Reputational ....................................................6
    Operational .....................................................6
IV. Key Takeaways from the FFIEC Guidance ...............8
    Supervision .....................................................8
    Safeguarding customer information .......................8
    Content Standards .............................................9
    Recordkeeping ................................................9
V. Appendix ..........................................................11
Executive Summary

Guidelines released by the Federal Financial Institutions Examination Council (FFIEC) in 2013 served to clarify for banking institutions, credit unions and other financial institutions how they could use social media within the framework of compliance.

With the increasing importance of social media as a communications channel for the banking and finance industry, it is important that organizations decode the guidelines and understand how they might be implemented in the business on a practical level.
Social Media and the Banking Industry

When even the Office of the Comptroller of the Currency\(^1\) stops distributing paper copies of its news and issuances in favor of email, Facebook and Twitter, it is clear that a step change is underway. Like the securities industry before it, banks are interested in using social media to connect with their customers. However, operating in one of the most regulated industries in the world means that banks, unlike others, have to take a more studied approach to the risks posed by social media.

For the industry as a whole, consumers are driving this change. They are turning away from using their bank branches, with 45% of consumers visiting their local branch fewer than five times a year\(^2\). More and more, they are turning to online channels, in particular, social media to research and connect. Amongst Millennials, 56% are more likely to go to social networks to look for brand content than on search engines or other online news feeds\(^3\). For online banks in particular, 40% of customers under 30 based their bank selection in part on a recommendation from someone they know\(^4\). The increasing use of social networks is also reflected in the habits of Boomers. This generation controls more than three-quarters of America’s wealth, and they are also the fastest growing group of social media users\(^5\).

Banks all over the world are starting to respond to this change. Out of the 50 largest banks in the world, over 90% are now on Facebook and 88% are on Twitter\(^6\).

---

Adding Regulation to the Equation

In response to requests from the retail banking industry for clarification around the use of social media, the FFIEC coordinated the activities of multiple federal banking regulators to craft usage guidelines. The draft guidelines were open to consultation and the FFIEC deliberated on the comments received from member organizations. The final guidance, titled **Social Media: Consumer Compliance Risk Management Guidance** was issued in December 2013, and is currently enforced.

About the Federal Financial Institutions Examinations Council (FFIEC)

The FFIEC was established in 1979 to promote uniformity in the supervision of financial institutions. The Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System (Board); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); and the Consumer Financial Protection Bureau (CFPB) (collectively, the Agencies) will use it as supervisory guidance for the institutions that they supervise, and the State Liaison Committee (SLC) of the FFIEC encourages state regulators to adopt the Guidance.

FFIEC Social Media Guidelines Dissected

The FFIEC acknowledges that banks face unique challenges when allowing their employees to use social media to communicate with prospective and existing customers due to its interactive and more informal nature. The guidance urges banks to develop a risk management program to control the risks related to social media. The guidance also recommends that those financial institutions that elect not to use social media still need to put processes in place to proactively monitor and respond to negative comments.

Like the guidelines released by other industry regulators such as the Financial Industry Regulatory Authority (FINRA), the SEC and the Investment Industry Regulatory Organization of Canada (IIROC), this guidance from the FFIEC does not create any new rules and regulations. Instead, it seeks to help banks interpret how existing advertising, supervisory and other requirements might impact social media communications.

Unlike the other regulators however, this guidance highlights the need for risk management. Financial institutions are encouraged to identify and put processes in place to mitigate three areas of risk:

---

1. Compliance and legal
An extensive number of existing regulations and their impact on social media communications is discussed in the FFIEC guidelines (see complete list in Appendix 1). Here are some of them:

- Existing advertising rules detailed in The Fair Lending and Truth in Lending Acts apply to social media. After all, social media is just another form of communications and should be treated as such.
- According to the principles laid out in the Fair Debt Collection Practices Act, debt collectors may not use social media to inappropriately to contact consumers, their families and friends, or to disclose the existence of a debt, or harass or embarrass consumers about their debts.
- A financial institution may not engage in any advertising or other practice via social media that could be deemed “unfair,” “deceptive,” or “abusive.” Information on social media sites must be accurate, consistent and not misleading.
- Recordkeeping requirements from the Bank Secrecy Act, Anti-Money Laundering Programs, and the Community Reinvestment Act also apply to social media communications.

2. Reputational
The FFIEC also cautions that social media could lend itself to situations that could present a risk to the reputation of an organization, even though the firm may have not actually violated any laws. Firms are advised that risk could arise from:

- Fraud and Brand Identity. Some of the risks of using social media include negative comments, spoofs and fraudsters masquerading as the institution. The guidance suggests the firms use social media monitoring tools and to create and follow communications plans should negative events occur.
- Third Parties. Even though a firm may outsource social media management to a third party, ultimately, negative events will reflect poorly on the institution itself and create reputational damage. Therefore, the guidance suggests careful due diligence and ongoing monitoring when working with third parties.
- Privacy. The guidance recommends creating processes to safeguard consumers should they post personal information (such as account and social security numbers) on the financial institution’s social media site to avoid reputational damage to the institution.
- Consumer Complaints and Inquiries. Consumers may post critical or inaccurate statements, or make specific complaints about errors or fees on social media. Financial institutions are advised create and execute processes to monitor and respond to these complaints in a timely manner. One suggestion is to set up channels expressly for this purpose. However firms are advised to evaluate their own risk tolerance and be prepared to monitor and respond to complaints on a broader basis.

3. Operational
The FFIEC suggests that firms evaluate how their processes, people or systems might stand up to the risks posed by the firm’s use of information technology (IT), including social media. Social media accounts could be vulnerable to being hacked. Once hacked, an organization’s social media accounts could be used to distribute malicious software. This means that a firm should have systems in place to prevent this and safeguard customer information.
Practical Ways to Move Forward

The FFIEC advises financial institutions to develop the risk management program with input from across the organization. This means eliciting and including feedback from compliance, technology, information security, legal, human resources, marketing and the lines of business.

Specific components of the program should include:

- Governance structure with clear roles and responsibilities
- Policies that address consumer protection laws and regulations; processes for managing third parties
- Training on employee usage polices
- Audit processes to ensure ongoing compliance with rules and regulations
- Reporting to senior management on how using social media contributes to the strategic goals of the institution

Power 100 Banks on Social Media

In January 2013, The Financial Brand launched a study to monitor the social media activity of roughly 2,000 banks and credit unions on Facebook, and another 2,500 banks and credit unions on Twitter. The study now also monitors YouTube activity. The results are published quarterly and provide a way for banks and credit unions in English-speaking countries around the world to benchmark their social media activity against their contemporaries.

Power 100 List:
www.thefinancialbrand.com/power-100

Wells Fargo – Using Social Media to Connect with Customers and Potential Customers

Wells Fargo uses several social media channels to accomplish different objectives. The company primarily uses Twitter to offer an additional customer service channel to its customers on @AskWellsFargo. The company uses YouTube to reach out to its small business banking clients, and have a blog specifically targeting women investors interested in saving for retirement.

The Importance of Listening

Susan Gardella, VP & Social Media Program Manager was keen to demonstrate how Wells Fargo’s social media team actively listens for comments made on social media, which enable the company to take a proactive approach to dealing with customer comments before they have a chance to spiral into crises that are damaging to the company’s brand reputation.

A few years ago, the company had set up a donation service to enable members of the public to give towards the Haitian emergency fund. However, a member of public noted that the company was taking a percentage of the donation as an administrative fee. Enraged, this person set up a Facebook group which soon garnered a lot of ‘Likes’ and negative publicity for the bank.

More recently, the company enabled customers to donate towards the Japanese tsunami relief effort via its ATMs. Very quickly, the social media team picked up some negative chatter about whether the company was benefiting from the donations, and they were able to reply to set the record straight before it became an issue.

Key Takeaways from the FFIEC Guidance

There are several takeaways that we glean by looking through that extensive list of existing rules and how they impact on social media. There are four areas of consideration:

1. Supervision

One of the common themes that run through not just the guidance released by the FFIEC, but other regulatory bodies as well, is the need for institutions to supervise communications. From a practical point of view, this could mean ensuring that employees do not collect personal information from anyone under the age of 13. It might be to supervise employees to ensure that they do not improperly collect or use personal information such as religion or ethnicity to make decisions on lending products. Or it might also be to ensure that private customer information is not inadvertently or purposely disclosed by employees in the course of using social media tools.

Best Practice Recommendation

Other regulated firms that are further along in their adoption of social media have found it helpful to adapt written supervisory procedures already in place. Moreover, rather than block the use of social media, firms are increasingly taking the approach of enabling its compliant use. This could take the form of adapting existing workflow approvals to pre-approve static content that can be published on social media.

Principle-based employee social media polices that are enforceable, demonstrate a thoughtful approach to the regulators. It is also recommended that firms limit registered persons’ access to social media unless they are trained in advance and their social media communications are actively monitored and supervised.

2. Safeguarding customer information

Institutions need to demonstrate that any information retained on customers from bank account details, to data that personally identifies customers and messages sent and received from customers is being kept securely and remain private. In practice, this could, for instance, mean that frontline staff managing an institution’s Twitter feed should be made aware that they should not ask customers for personal details over the social network. Instead they should try to contact that customer to resolve any issues via a secure, one-to-one communication.
**Best Practice Recommendation**

Aside from having employee use policies in place for the appropriate use of social media, and providing practical training to staff to deal with situations that arise, institutions can also deploy technology to automatically detect and put on ‘hold’ any messages from being sent until a supervisor is able to review.

3. **Content Standards**

There are well established content standards for print material that now apply to social media. Communications with the public must be accurate, fair, balanced and not misleading. Factors that would impact investment decisions must be disclosed. In the case of some social media outlets, such as Twitter, which limit the number of characters for each message, this could be in the form of a hyperlink to a webpage that contains the full disclosure of risk and terms and conditions.

**Best Practice Recommendation**

Institutions need to consider whether the medium used is appropriate to the message that it is trying to deliver. For instance, social media might be the appropriate medium to share saving tips but not necessarily appropriate to advertise a new mortgage product. Institutions need to ensure that relevant hyperlinks to risk and other additional information are provided if this cannot be covered in the original message, for instance, when using Twitter with its character limitations.

4. **Recordkeeping**

Social media communications need to be retained as part of an institution’s obligations to prevent money laundering, and also to fulfill existing obligations for retaining comments made by the public. Before launching any social media initiative, institutions need to consider how they will capture and preserve social media communications.

**Best Practice Recommendation**

Institutions should evaluate and adopt technology solutions that provide the ability to capture, archive and enable social media communications to be retrieved.
mBank – Reinventing Online Banking

Its parent company may be a bricks and mortar bank, but mBank\(^9\) was started as an internet-only bank in 2000, which rapidly grew to become Poland's largest online bank and its third largest retail bank.

In 2012, the company realized that they needed a complete redesign of the bank in response to changes in the marketplace. The redesign was based on four key tenets - real-time marketing; Personal Financial Management; mobile banking; and social media.

The re-launched mBank now allowed its customers to transfer money using SMS and Facebook conveniently. Its customers need not remember, or ask for account numbers and can use phone numbers or social network connections instead. Recipients of the money transfer are automatically notified on their Facebook landing page:

This innovative service on Facebook won mBank FinovateEurope 2013’s Best of Show award and a lot of press coverage.

\(^9\) mBank: the world's first mobile social bank within a bank, Chris Skinner, Jun 19, 2013
### Appendix 1:

**Compliance & Legal Risk**

#### Deposit & Lending Products

<table>
<thead>
<tr>
<th>Rule</th>
<th>Purpose</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truth in Savings Act/ Regulation DD and Part 707</td>
<td>Imposes disclosure requirements designed to enable consumers to make informed decisions about deposit accounts. May not be misleading or incomplete.</td>
<td>Customers must receive all required disclosures. Consider a link to additional information for posts that contain trigger words such as “bonus” or “APY”).</td>
</tr>
<tr>
<td>Fair Lending Laws: Equal Credit Opportunity Act/Regulation B and Fair Housing Act</td>
<td>Prohibits discrimination in any aspect of a credit transaction or in the sale and rental of housing, in mortgage lending, and in appraisals of residential real property.</td>
<td>Banks have same requirements when using social media as other forms of advertising. Although social media sites may request certain information, banks must not improperly request, collect, or use such information such as color, religion, national origin, or sex, in violation of applicable fair lending laws. Supervision is required.</td>
</tr>
<tr>
<td>Truth in Lending Act / Regulation Z</td>
<td>Designed to promote informed use of consumer credit by requiring thorough disclosures about terms and costs.</td>
<td>Same advertising rules apply when using social media. Customers must receive all of the required disclosures. Clarifying information may be located on a different page (or link) from the main advertisement. As above, consider including a link within post to additional information.</td>
</tr>
<tr>
<td>Rule</td>
<td>Purpose</td>
<td>Recommendation</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Real Estate Settlement Procedures Act (RESPA)</td>
<td>Prohibits certain activities in connection with federally related mortgage loans. Includes specific timing for disclosures.</td>
<td>Same disclosures requirements apply to applications taken electronically, including via social media. Customers must receive all required disclosures.</td>
</tr>
<tr>
<td>Fair Debt Collection Practices Act (FDCPA)</td>
<td>Restricts how debt collectors collect debts.</td>
<td>Debt collectors may not use social media to inappropriately contact consumers, their families and friends, or to disclose the existence of a debt, or harass or embarrass consumers about their debts. Supervision required.</td>
</tr>
<tr>
<td>Unfair, Deceptive, or Abusive Acts or Practices (FTC, Dodd Frank)</td>
<td>Prohibits unfair, deceptive, or abusive acts or practices.</td>
<td>A financial institution may not engage in any advertising or other practice via social media that could be deemed “unfair,” “deceptive,” or “abusive.” Information on social media sites must be accurate, consistent and not misleading. Supervision required.</td>
</tr>
<tr>
<td>Deposit Insurance or Share Insurance</td>
<td>Advertising requirements regarding FDIC or NCUA membership and deposit insurance or share insurance.</td>
<td>Same advertising rules for notice of membership apply when using social media. Must include “Member FDIC”, “Federally insured by NCUA”; font must be clearly legible.</td>
</tr>
</tbody>
</table>
### Payment Systems

<table>
<thead>
<tr>
<th>Rule</th>
<th>Purpose</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Fund Transfer Act / Regulation E Rules Applicable to Check Transactions</td>
<td>Specific protections, including disclosures to consumers.</td>
<td>Same disclosures requirements apply to social media. Customers must receive all required disclosures. Disclosures must be “clear and conspicuous” and “readily understandable”. As above, consider including a link within post to additional information.</td>
</tr>
<tr>
<td>Bank Secrecy Act / Anti-Money Laundering Programs (BSA / AML)</td>
<td>Financial institutions must have compliance program, training, and internal controls to ensure effective risk management and adherence to recordkeeping and reporting requirements.</td>
<td>Same recordkeeping and reporting requirements apply to social media. Applies to all customers, products and services, including customers engaging in electronic banking (e-banking) through the use of social media, and e-banking products and services offered in the context of social media. Additionally, virtual internet games and digital currencies present a higher risk for money laundering and terrorist financing and should be monitored accordingly.</td>
</tr>
<tr>
<td>Community Reinvestment Act (CRA)</td>
<td>Recordkeeping requirements for comments made by the public.</td>
<td>Retain records of written communications made on sites run by or on behalf of the institution that specifically relate to the institution’s performance in helping to meet community credit needs.</td>
</tr>
<tr>
<td>Rule</td>
<td>Purpose</td>
<td>Recommendation</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act Privacy Rules and Data Security Guidelines</td>
<td>Requirements relating to privacy and security of consumer information.</td>
<td>Clearly disclose privacy policies and safeguard customer information. Particularly relevant when a financial institution integrates social media components into customers’ online account experience or takes applications via social media networks.</td>
</tr>
<tr>
<td>CAN-SPAM Act and Telephone Consumer Protection Act.</td>
<td>Requirements for sending unsolicited commercial messages.</td>
<td>May be relevant if a financial institution sends unsolicited communications to consumers via social media. Consider caution when using one-to-one private communications on social media.</td>
</tr>
<tr>
<td>Children’s Online Privacy Protection Act</td>
<td>Obligations pertaining to commercial websites and online services that collect, use, or disclose personal information from children under 13.</td>
<td>Carefully monitor collection personal information of children under 13. Establish, post, and follow policies restricting access to the sites maintained by the institution to users 13 or older, especially when those sites could attract children (such as virtual worlds and features that resemble video games.)</td>
</tr>
<tr>
<td>Fair Credit Reporting Act</td>
<td>Requirements for making solicitations using eligibility information, responding to direct disputes, and collecting medical information in connection with loan eligibility.</td>
<td>Applies when social media is used for these activities.</td>
</tr>
</tbody>
</table>