Lithium

FSI Social Media Compliance Guide

contents

You know your firm has to get serious about social. But how do you navigate the labyrinth of regulations? What do you need to know in order to create a sound social media strategy for your financial institution?

Here are some key insights drawn on the final guidance issued in December 2013 by the Federal Financial Institutions Examination Council (FFIEC) to help you create a framework around your go-forward social strategy. This information provides context, but is not all-inclusive to the applicable laws, regulations, guidance, or industry rules.

So what exactly is social media? Basic question, right? Banking and financial institutions have varying definitions. The FFIEC has defined it as:

"Social media is considered to be a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video....For purposes of this Guidance, messages sent via traditional email or text message, standing alone, do not constitute social media....Messages sent though social media channels are social media." [1]

Examples given of social media given include micro-blogging sites (Facebook, Google, MySpace, Twitter); forums, blogs, customer review websites and bulletin boards (Yelp); photo and video sites (Flickr and YouTube), professional networking sites (LinkedIn); virtual worlds (Second Life) and social games (Farmville, Cityville). FFIEC says that "social media can be distinguished from other online media in that its communication tends to be more interactive."

intention matters —define It

Why use social media? "Because everyone else is" won't fly. Neither will: "our customers expect us to." The FFIEC Guidance explicitly details that FSIs must have documented strategic goals for using social media that are measurable and reported periodically to the Board of Directors and Senior Management. The business purposes may vary—you may want to increase brand exposure, attract new customers, improve brand loyalty, provide incentives, market products and services—no matter what you want to achieve.

Social Media Intensions

social media risk management

The loudest message to come out of the FFIEC Guidance is the emphasis repeatedly placed on risk management--specifically as it relates to social media and the corresponding risk of harm to customers, compliance and legal risk, operational risk and reputation risk:

"Each institution is responsible for carrying out an appropriate risk assessment and maintaining a risk management program that is appropriate and tailored to the particular institution's size, activities, and risk profile."[2]

You must assess and determine your level of risk based on the extent you use social media. The scope of social media usage varies by institution, of course; and with it, the proportional level of risk. Rather than issue specific guidelines on how social may or may not be used (assuming FINRA, SEC, NAIC, and other regulations are incorporated usage), the FFIEC charges institutions with effectively monitoring and mitigating risk. This gives institutions realtively broad freedom to use social media (within regulations) as they wish, as long as there are internal controls and risk programs in place to address the level of risk their social media usage creates. (It's important to note that risk management is applicable to all means of communicating information with, to and about customers—not just social media.)

Components of a Social Media Risk Management Program from FFIEC Social Media Guidance Dec 2013:

- Governance structure with clear roles and responsibilities in which the Board of Directors or Senior Management direct how using social media contributes to the strategic goals of the institution and establish controls and ongoing assessment of risk in social media activities.
- 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. You need to include methodologies to address risks from online posting, edits, replies and retention.
- Risk management process for selecting and managing third-party relationships in connection with social media (see Third-party Sites/Posts below).
- 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. Be sure to define impermissible activities.
- Oversight process for monitoring information posted to proprietary social media sites administered by the FSI or a contracted third party.
- Audit and compliance functions to ensure ongoing compliance with internal policies and all laws, regulations, and guidance.
- Parameters for providing appropriate reporting to the FSI's Board/Senior Management that enable periodic evaluation of the effectiveness of the social media program and whether the program is achieving its stated objectives. This implies that benchmarks and metrics must be in place to gauge effectiveness.

Your social media risk management program will interrelate with marketing, IT, and compliance. As such, it needs to be informed by these functions as well.

disclosure regulations

There are numerous regulations applicable to how FSIs use social media. Outlined below are some of the major regulations that affect social media and are referenced by the FFIEC. The Final Guidance points out that it is the FSI's responsibility to be mindful and aware of all existing laws, regulations, guidance and industry rules that apply to how you do business and evaluate how these laws apply to social media. This includes being aware of emerging social trends and social media sites that could impact your risk.

Deposit and Lending Products

Truth in Savings Act/Regulation DD and Part 707 – requires disclosures about fees, annual percentage yields, interest rates and may not be misleading in any way. You may link directly to this information.

Fair Lending Laws: Equal Credit Opportunity Act/ Regulation B and Fair Housing Act – ensures nondiscrimination toward applicants; timeframes for notifying applicants of results; preserving prescreened solicitations/criteria; adverse action reports; and prohibits requesting, collecting, or using information on race, color, religion, national origin, familial status, handicap or sex in applications. If using a third-party site for collecting this info, FSIs need to be sure that they are not gathering or exposing this data in the application process.

Truth in Lending Act/Regulation Z – governs advertising policies for credit products, requires timely disclosures about loan terms and costs, and clear and conspicuous display of disclosures. Can use a table/schedule that is located on a different webpage, if the table/schedule is clear and easy to find.

Real Estate Settlement Procedures Act – prohibits certain activities in connection with federally-related mortgage loans. RESPA has specific timing issues for disclosures.

Fair Debt Collection Practices Act – restricts how debt collectors may collect debts and prohibits them from disclosing publicly that a consumer owes a debt. If social media is used to contact consumers, their families or friends, it may violate the FDCPA. Disclosing the existence of the debt on social media or harassing/embarrassing consumers about their debts may violate this.

Unfair, Deceptive, or Abusive Acts or Practices – prohibits 'unfair or deceptive acts or practices in or affecting commerce.' An act or practice can be unfair, deceptive, or abusive despite technical compliance with laws. Social media information should be accurate, consistent with other info delivered through other channels, and not misleading.

Deposit Insurance or Share Insurance – FDIC or NCUA membership and deposit insurance or share insurance logo display rules apply equally to all advertising. FDIC must be included if the name of the insured institution is named; but is not permitted if the ad relates solely to nondeposit product or hybrid products. Must display NCUA anywhere it accepts deposits or opens accounts—including online. On Nondeposit Investment Products the FSI must fully inform customers that these products are not covered by FDIC/NCUA.

Payment Systems

According to the FFIEC, under existing law, no additional disclosure requirements apply simply because social media is involved (for example, providing a portal through which consumers access their accounts). There are existing regulations that apply:

Electronic Fund Transfer Act/Regulation E – requires disclosures and error resolution procedures to consumers who engage in EFT and remittance transfers.

Rules Applicable to Check Transactions – covers payments by check and not EFT, governed by applicable industry rules and/or Article 4 of the Uniform Commercial Code of the relevant state, as well as the Expedited Fund Availability Act, implemented by Regulation CC.

secrecy, community, privacy regulations

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

The BSA/AML indicates that FSIs must have a compliance program that includes training for all employees—from operational staff to the board of directors. It must include appropriate internal controls to ensure effective risk management and compliance with recordkeeping and reporting. Internal controls must apply to e-banking through the use of social media and e-banking products and services offered in the context of social media. In relation to this, the FFIEC warns FSIs to be aware of emerging risks, including virtual worlds/virtual economies that facilitate money laundering and terrorist financing.

Community Reinvestment Act

This law requires FSIs to maintain a public file that includes all written comments received from the public (and any responses made by the institution) for the current year and each of the prior two calendar years that specifically relate to the FSI's performance in helping to meet community credit needs. FSIs need to include social media comments only received on sites run by or on behalf of the institution, not those found elsewhere on the Internet.

Privacy

Gramm-Leach-Bliley Act Privacy Rules and Data Security Guidelines – whenever an FSI collects or has access to consumer data it must evaluate if these rules apply. Clearly disclose privacy policies on social media under GLBA. Be very careful how consumer information is used.

CAN-SPAM Act and Telephone Consumer Protection Act – establish requirements for sending unsolicited commercial messages (spam) or phone calls/SMS. Evaluate social media use in regards to these laws.

Children's Online Privacy Protection Act – requires users to attest that they are at least 13 years of age; should monitor if collecting info/posts from anyone under 13. If an institution is using its own social media site, you should be especially careful to establish, post and follow policies restricting access to the site to users 13 or older. This becomes even more important when you use gamification or virtual worlds that would naturally attract children under the age of 13.

Fair Credit Reporting Act – contains restrictions and requirements when making solicitations using eligibility information, responding to direct disputes, and collecting medical information in connection with loan eligibility—including when social media is used to do so.

content regulations

Supervision and Approval of Content

While the FFIEC Final Guidance does not directly comment on this, FINRA and the NAIC specify that rules regarding supervision and approval of communication content differ depending on whether they are "static" or "real-time" communications. Static content is loosely defined as content that remains on your page (such as your Facebook profile information) and must be pre-approved by a FSI principal before it is posted. Real-time (responses on Facebook or Twitter) are not required to be pre-approved. The line between what is static vs real-time is still being drawn. It's important to note that all communication needs to be supervised and monitored even if it does not require pre-approval.[3]

Third Party Sites/Posts

Who's in control of your Facebook page? The challenge with using third-party sites is that you are not able to control how those sites operate, what policies they adopt/change, or how they use consumer information. Additionally, many third-party sites, such as Facebook, do not have archiving capabilities, which is a key requirement for FSIs in using social media. The FFIEC strongly encourages FSIs to carefully weigh the risk of using third-party sites and to conduct due diligence before engaging a third-party provider. It holds FSIs responsible to regularly monitor all info placed on third-party sites. One way FSIs can avoid having to worry about this issue is to develop their own social media site—a customer community, for instance—that they fully own, control and customize. Doing so also helps drive people to your own social property and allows you to have a stronger relationship with customers, too.

Third party posts on social media pages are not considered communications by the FSI, unless the institution has "adopted" or "entangled" itself in the content. Both FINRA and the NAIC agree that an institution "adopts" content by involving itself in the preparation of the content and becomes "entangled" when it endorses or approves the content.[4] This is tricky territory only as long as the content violates a rule or regulation. FSIs may adopt and entangle themselves in content that is lawful. FSIs are encouraged to have policies and procedures to deal with third-party posts, including how they will address removing explicit or illegal third-party posts from their social media sites.

Recordkeeping and Archiving

The spine of all FSI social media usage is the requirement to archive and record communications. FSIs must determine what are required records, then purchase or build software to appropriately record, back-up and store social media communications/interactions for required periods of time. These records must be easily accessible for eDiscovery. Archiving also applies to social media used for business purposes on personal devices. If recordkeeping is not automated, you need to train and spot-check employees on when and how to archive their data.

additional references

The FFIEC final guidance provides a framework for you to develop a customized social media strategy that enhances your customer experience, drives loyalty, and increases revenue. Its heavy focus on risk management and monitoring/supervision allows you plenty of room to innovate the way you use social. Rather than follow the path others are meandering, why not cut a new trail? Design your social strategy with customer experience best practices as its foundation, shore it up with the appropriate regulatory boundaries, recordkeeping, and supervision; and be bold in embracing social as the transformative way you engage with your customers.

For additional reference:

FINRA Regulatory Notices:

Social Media Websites, January 2010:
http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf

Social Media Website and Use of Personal Devices for Business Communications, August 2011:
http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p124186.pdf

NAIC:

The Use of Social Media in Insurance:
http://www.naic.org/store/free/USM-OP.pdf

resources

1. Federal Financial Institutions Examination Council, Social Media: Consumer Compliance Risk Management Guidance
2. ibid
3. Bloomberg BNA, Social Media Law & Policy Report, Financial Services
4. ibid
5.

Lithium

About Lithium Technologies: Lithium social software helps companies unlock the passion of their customers. Lithium powers amazing social customer experiences for more than 300 iconic brands including AT&T, BT, BestBuy, Indosat, Sephora, Skype and Telstra. The 100% SaaS-based Lithium Social Customer Experience™ platform enables brands to build and engage vibrant customer communities to drive sales, reduce service costs, accelerate innovation and grow brand advocacy. For more information, visit lithium.com,or connect with us on Twitter, Facebook and our own community–the Lithosphere. Lithium is privately held with corporate headquarters in San Francisco and offices across Europe, Asia and Australia.