
# SOCIAL MEDIA AND NETWORKING COMPLIANCE

**JONATHAN FOXX**
President and Managing Director
Lenders Compliance Group, Inc.

When you think of advertising, do you include social media? These days, most of you do!

However, social media compliance - which I shall call "SMC" - is a considerable undertaking, far more involved than just issuing a policy and procedure. Often, implementing SMC includes working with internet technology and information security professionals, collaborating with sales, compliance, legal, marketing, and human resources personnel, and ensuring that virtually all employees understand their own obligations with respect to using internet communications.

We have drafted SMC policy statements that call for constant vigilance by management and appointed staff to monitor for and find the appropriate remedies to transgressions relating to use of a company's name, logo, products, and services, in casual and even formal social media interactions.

Recently, Federal Financial Institutions Examination Council (FFIEC) issued a request for comments, entitled Social Media: Consumer Compliance Risk Management Guidance ("Notice").[1] FFIEC issued this notice on behalf of its six members, Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System (FRB); the Federal Deposit Insurance Corporation (FDIC); the National Credit Union Administration (NCUA); and the Consumer Financial Protection Bureau (CFPB) (collectively, the "Agencies"); and the State Liaison Committee (SLC). Succinctly put, whatever the federal agencies eventually adopt, the states will issue the final guidance as a supervisory guidance not only to the institutions that are, by extension, under its supervision but also through the State Liaison Committee, thereby encouraging state regulators to adopt the guidance.

This means that institutions will be expected to use the forthcoming guidance in their efforts to ensure that their policies and procedures provide oversight and controls commensurate with the risks posed by their social media activities. State agencies that adopt the guidance will expect the entities that they regulate to use the guidance in their efforts to ensure that their risk management and consumer protection practices adequately address the compliance and reputation risks raised by activities conducted via social media.

In this article, I will consider certain features of FFIEC's social media Notice as well as some important subjects to be addressed in constructing an SMC policy and procedure.

**DEFINING SOCIAL MEDIA**

Social media has been defined in a number of ways. For purposes of the proposed guidance, the Agencies consider social media to be a form of interactive online communication in which users can generate and share content through text, images, audio and/or video.

Social media can take many forms, including, but not limited to, micro-blogging sites (i.e., Facebook, Google Plus, MySpace, and Twitter); forums, blogs, customer review Websites and bulletin boards (i.e., Yelp); photo and video sites (i.e., Flickr and YouTube); sites that enable professional networking (i.e., LinkedIn); virtual worlds (i.e., Second Life); and social games (i.e., FarmVille and CityVille).

A simple test to distinguish social media from other online media is that the social media communication tends to be more interactive.

**USE OF SOCIAL MEDIA**

Financial institutions use social media in a variety of ways, including marketing, providing incentives, facilitating applications for new accounts, inviting feedback from the public, and engaging with existing and potential customers.

For instance, social media has been used to receive and respond to complaints. They have been used to provide loan pricing. Since this form of customer interaction tends to be informal and occurs in a less secure environment, it presents some unique challenges to financial institutions.

To manage potential risks to financial institutions and consumers, however, financial institutions should ensure their risk management programs provide oversight and controls commensurate with the risks presented by the types of social media in which the financial institution is engaged.

**RISKS OF SOCIAL MEDIA**

The use of social media by a financial institution to attract and interact with customers can impact a financial institution's risk profile.

The increased risks can include the risk of harm to consumers, compliance and legal risk, operational risk, and reputation risk.

Increased risk can arise from a variety of directions, including poor due diligence, oversight, or control on the part of the financial institution. Obviously, procedures must be implemented that help financial institutions to identify potential risk areas and appropriately address as well as ensure that they are aware of their responsibilities to oversee and control these risks within their overall risk management program.

Therefore, financial institutions should address the applicability of existing federal consumer protection and compliance laws, regulations, and policies to activities conducted via social media by banks, savings associations, and credit unions, as well as by nonbank entities supervised by the CFPB.

**RISK MANAGEMENT**

A financial institution should have a risk management program that allows it to identify, measure, monitor, and control the risks related to social media. The size and complexity of the risk management program should be commensurate with the breadth of the financial institution's involvement in this medium.

FFIEC gives this rule of thumb: a financial institution that relies heavily on social media to attract and acquire new customers should have a more detailed program than one using social media only to a very limited extent.

The risk management program should be designed with participation from specialists in compliance, technology, information security, legal, human resources, and marketing. FFIEC makes it clear that a financial institution that has chosen not to use social media should still be prepared to address the potential for negative comments or complaints that may arise within the many social media platforms and provide guidance for employee use of social media.

In FFIEC's view, there are seven components of a risk management program:

1) A **governance structure** with clear roles and responsibilities whereby the board of directors or senior management direct 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;

2) **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, regulations, and guidance. Policies and procedures should incorporate methodologies to address risks from online postings, edits, replies, and retention;

3) A **due diligence process** for selecting and managing third-party service provider relationships in connection with social media;

4) 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;

5) An **oversight process for monitoring information** posted to proprietary social media sites administered by the financial institution or a contracted third party;

6) **Audit and compliance functions** to ensure ongoing compliance with internal policies and all applicable laws, regulations, and guidance; and,

7) 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.

**RISK AREAS**

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

Compliance and legal risk arise from the potential for violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. These risks also arise in situations in which the financial institution's policies and procedures governing certain products or activities may not have kept pace with changes in the marketplace.

Furthermore, the potential for defamation or libel risk exists where there is broad distribution of information exchanges. Failure to adequately address these risks can expose an institution to enforcement actions and/or civil lawsuits.

To the extent that a bank or nonbank uses social media to engage in lending, it must comply with applicable laws and regulations as when it engages in these activities through other media.

## LAWS AND REGULATIONS

The following laws and regulations may be relevant to a financial institution's social media activities. This list is not all-inclusive. Each financial institution should ensure that it periodically evaluates and controls its use of social media to ensure compliance with all applicable federal, state, and local laws, regulations, and guidance.

Social media may be used to market products and originate new accounts. When used to do either, a financial institution must take steps to ensure that advertising, account origination, and document retention are performed in compliance with applicable consumer protection and compliance laws and regulations. These include, but are not limited to:

### FAIR LENDING LAWS, EQUAL CREDIT OPPORTUNITY ACT (REGULATION B), FAIR HOUSING ACT

A financial institution should ensure that its use of social media does not violate fair lending laws.

Equal Credit Opportunity Act,[2] as implemented by Regulation B, prohibits creditors from making any oral or written statement, in advertising or other marketing techniques, to applicants or prospective applicants that would discourage on a prohibited basis a reasonable person from making or pursuing an application. However, a creditor may affirmatively solicit or encourage members of traditionally disadvantaged groups to apply for credit, especially groups that might not normally seek credit from that creditor.[3]

- Creditors must also observe the time frames outlined under Regulation B for notifying applicants of the outcome of their applications or requesting additional information for incomplete applications, whether those applications are received via social media or through other channels.

- As with all prescreened solicitations, a creditor must preserve prescreened solicitations disseminated through social media, as well as the prescreening criteria, in accordance with Regulation B.[4]

- When denying credit, a creditor must provide an adverse action notice detailing the specific reasons for the decision or notifying the applicant of his or her right to request the specific reasons for the decision.[5] This requirement applies whether the information used to deny credit comes from social media or other sources.

- It is also important to note that creditors may not, with limited exceptions, request certain information, such as information about an applicant's race, color, religion, national origin, or sex. Since social media platforms may collect such information about participants in various ways, a creditor should ensure that it is not requesting, collecting, or otherwise using such information in violation of applicable fair lending laws.

- Particularly if the social media platform is maintained by a third party that may request or require users to provide personal information such as age and/or sex or use data mining technology to obtain such information from social media sites, the creditor should ensure that it does not itself improperly request, collect, or use such information or give the appearance of doing so.

The Fair Housing Act (FHA)[6] prohibits discrimination based on race, color, national origin, religion, sex, familial status, or handicap in the sale and rental of housing, in mortgage lending, and in appraisals of residential real property. In addition, the FHA makes it unlawful to advertise or make any statement that indicates a limitation or preference based on race, color, national origin, religion, sex, familial status, or handicap. This prohibition applies to all advertising media, including social media sites. For example, if a financial institution engages in residential mortgage lending and maintains a presence on Facebook, the Equal Housing Opportunity logo must be displayed on its Facebook page, as applicable.[7]

**TRUTH IN LENDING ACT (REGULATION Z)**

Any social media communication in which a creditor advertises credit products must comply with Regulation Z's advertising provisions.

Regulation Z,[8] the implementing regulation of the Truth in Lending Act (TILA), broadly defines advertisements as any commercial messages that promote consumer credit, and the official commentary to Regulation Z states that the regulation's advertising rules apply to advertisements delivered electronically. In addition, Regulation Z is designed to promote the informed use of consumer credit by requiring disclosures about loan terms and costs. The disclosure requirements vary based on whether the credit is open-end or closed-end. Further, within those two broad categories, additional specific requirements apply to certain types of loans such as private education loans, home secured loans, and credit card accounts.

- Regulation Z requires that advertisements relating to credit present certain information in a clear and conspicuous manner. It includes requirements regarding the proper disclosure of the annual percentage rate and other loan features. If an advertisement for credit states specific credit terms, it must state only those terms that actually are or will be arranged or offered by the creditor.

- For electronic advertisements, such as those delivered via social media, Regulation Z permits providing the required information on a table or schedule that is located on a different page from the main advertisement if that table or schedule is clear and conspicuous and the advertisement clearly refers to the page or location.

- Regulation Z requires that, for consumer loan applications taken electronically, including via social media, the financial institution must provide the consumer with all Regulation Z disclosures within the required time frames.

**REAL ESTATE SETTLEMENT PROCEDURES ACT (RESPA)**

RESPA[9], through its implementing Regulation X, prohibits certain activities in connection with federally related mortgage loans. These prohibitions include fee splitting, as well as giving or accepting a fee, kickback, or thing of value in exchange for referrals of settlement service business. RESPA also has specific timing requirements for certain disclosures. These requirements apply to applications taken electronically, including via social media.

**FAIR DEBT COLLECTION PRACTICES ACT**

The Fair Debt Collection Practices Act (FDCPA)[10] restricts how debt collectors (generally defined as third parties collecting others' debts and entities collecting debts on their own behalf if they use a different name) may collect debts.

The FDCPA generally prohibits debt collectors from publicly disclosing that a consumer owes a debt. Using social media to inappropriately contact consumers, or their families and friends, may violate the restrictions on contacting consumers imposed by the FDCPA.

Communicating via social media in a manner that discloses the existence of a debt or to harass or embarrass consumers about their debts (i.e., a debt collector writing about a debt on a Facebook wall) or making false or misleading representations may violate the FDCPA.

**UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAP)**

Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[11]

Sections 1031 and 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act[12] prohibit unfair, deceptive, or abusive acts or practices. An act or practice can be unfair, deceptive, or abusive despite technical compliance with other laws. A financial institution should not engage in any advertising or other practice via social media that could be deemed "unfair," "deceptive," or "abusive." As with other forms of communication, a financial institution should ensure that information it communicates on social media sites is accurate, consistent with other information delivered through electronic media, and not misleading.[13]

**PAYMENT SYSTEMS**

If social media is used to facilitate a consumer's use of payment systems, a financial institution should keep in mind the laws, regulations, and industry rules regarding payments that may apply, including those providing disclosure and other rights to consumers.

Under existing law, no additional disclosure requirements apply simply because social media is involved (for instance, providing a portal through which consumers access their accounts at a financial institution). Rather, the financial institution should continue to be aware of the existing laws, regulations, guidance, and industry rules that apply to payment systems and evaluate which will apply.

These may include the Electronic Fund Transfer Act (Regulation E).

The Electronic Fund Transfer Act (EFTA)[14] and its implementing Regulation E provide consumers with, among other things, protections regarding "electronic fund transfers" (EFT), defined broadly to include any transfer of funds initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of debiting or crediting a consumer's account at a financial institution. These protections include required disclosures and error resolution procedures. (Note: when a payment occurs via a check-based transaction rather than an EFT, the transaction will be governed by applicable industry rules[15] and/or Article 4[16] of the Uniform Commercial Code of the relevant state, as well as the Expedited Funds Availability Act, as implemented by Regulation CC.[17])

### BANK SECRECY ACT & ANTI-MONEY LAUNDERING PROGRAMS (BSA & AML)

As required by the Bank Secrecy Act (BSA)[18] and applicable regulations,[19] financial institutions and certain other entities must have a compliance program that incorporates training from operational staff to the board of directors. Among other elements, the compliance program must include appropriate internal controls to ensure effective risk management and compliance with recordkeeping and reporting requirements under the BSA. Internal controls are the financial institution's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the financial institution.

At a minimum, internal controls include, but are not limited to: Implementing an effective customer identification program; implementing risk-based customer due diligence policies, procedures, and processes; understanding expected customer activity; monitoring for unusual or suspicious transactions; and maintaining records of electronic funds transfers.

An institution's BSA/AML program must provide for the following minimum components: a system of internal controls to ensure ongoing compliance; independent testing of BSA/AML compliance, a designated BSA compliance officer responsible for managing compliance, and training for appropriate personnel. These controls should apply to all customers, products and services, including customers engaging in electronic banking (so-called "e-banking") through the use of social media, and e-banking products and services offered in the context of social media.

Financial institutions should also be aware of emerging areas of BSA/AML risk in the virtual world. For example, illicit actors are increasingly using Internet games involving virtual economies, allowing gamers to cash out, as a way to launder money. Virtual world Internet games and digital currencies present a higher risk for money laundering and terrorist financing and should be monitored accordingly.

## MAJOR RISKS

### PRIVACY, GLBA, AND DATA SECURITY

Privacy rules have particular relevance to social media when, for instance, a bank or nonbank collects, or otherwise has access to, information from or about consumers.

### GRAMM-LEACH-BLILEY ACT PRIVACY RULES AND DATA SECURITY GUIDELINES[20]

Title V of the Gramm-Leach-Bliley Act (GLBA) establishes requirements relating to the privacy and security of consumer information.

Whenever a financial institution collects, or otherwise has access to, information from or about consumers, it should evaluate whether these rules will apply. The rules have particular relevance to social media when, for instance, a financial institution integrates social media components into customers' online account experience or takes applications via social media portals.

A financial institution using social media should clearly disclose its privacy policies as required under GLBA.

Even when there is no "consumer" or "customer" relationship triggering GLBA requirements, a financial institution will likely face reputation risk if it appears to be treating any consumer information carelessly or if it appears to be less than transparent regarding the privacy policies that apply on one or more social media sites that the financial institution uses.

### CAN-SPAM Act and Telephone Consumer Protection

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[21] and Telephone Consumer Protection Act (TCPA)[22] may be relevant if a financial institution sends unsolicited communications to consumers via social media. The CAN-SPAM Act and TCPA, and their implementing rules,[23] establish requirements for sending unsolicited commercial messages ("spam") and unsolicited communications by telephone or short message service (SMS) text message, respectively. These restrictions could apply to communications via a social media platform's messaging feature.

### Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA)[24] contains restrictions and requirements concerning making solicitations using eligibility information, responding to direct disputes, and collecting medical information in connection with loan eligibility. The FCRA applies when social media is used for these activities.

### Reputation Risk

Reputation risk is the risk arising from negative public opinion. Activities that result in dissatisfied consumers and/or negative publicity could harm the reputation and standing of the financial institution, even if the financial institution has not violated any law. Privacy and transparency issues, as well as other consumer protection concerns, arise in social media environments. Therefore, a financial institution engaged in social media activities must be sensitive to, and properly manage, the reputation risks that arise from those activities.

**FRAUD AND BRAND IDENTITY**

Financial institutions should be aware that protecting their brand identity in a social media context can be challenging. Risk may arise in many ways, such as through comments made by social media users, spoofs of institution communications, and activities in which fraudsters masquerade as the institution. Financial institutions should consider the use of social media monitoring tools and techniques to identify heightened risk, and respond appropriately.

Financial institutions should have appropriate policies in place to monitor and address in a timely manner the fraudulent use of the financial institution's brand, such as through phishing or spoofing attacks.

**THIRD PARTY CONCERNS[25]**

Working with third parties to provide social media services can expose financial institutions to substantial reputation risk. A bank or nonbank should regularly monitor the information it places on social media sites. This monitoring is the direct responsibility of the financial institution, even when such functions may be delegated to third parties. Even if a social media site is owned and maintained by a third party, consumers using the financial institution's part of that site may blame the financial institution for problems that occur on that site, such as uses of their personal information they did not expect or changes to policies that are unclear.

The financial institution's ability to control content on a site owned or administered by a third party and to change policies regarding information provided through the site may vary depending on the particular site and the contractual arrangement with the third party. A financial institution should thus weigh these issues against the benefits of using a third party to conduct social media activities.

**PRIVACY CONCERNS**

Even when a financial institution complies with applicable privacy laws in its social media activities, it should consider the potential reaction by the public to any use of consumer information via social media. The financial institution should have procedures to address risks from occurrences such as members of the public posting confidential or sensitive information-for example, account numbers-on the financial institution's social media page or site.

**CONSUMER COMPLAINTS AND INQUIRIES**

Although a financial institution can take advantage of the public nature of social media to address customer complaints and questions, reputation risks exist when the financial institution does not address consumer questions or complaints in a timely or appropriate manner.

Further, the participatory nature of social media can expose a financial institution to reputation risks that may occur when users post critical or inaccurate statements. Compliance risk can also arise when a customer uses social media in an effort to initiate a dispute, such as an error dispute under Regulation E, a billing and reporting error under either Regulation X or Regulation Z, or a direct dispute about information furnished to a consumer; therefore, a financial institution should have monitoring procedures in place to address the potential for these statements or complaints to require further investigation. Some institutions have employed monitoring software to identify any active discussion of the institution on the Internet.

The bank or nonbank should also consider whether, and how, to respond to communications disparaging the financial institution on other parties' social media sites. To properly control these risks, financial institutions should consider the feasibility of monitoring 'question and answer', 'complaint', and 'community' forums on social media sites to ensure that such inquiries, complaints, or comments are addressed in a timely and appropriate manner.

**EMPLOYEE USE OF SOCIAL MEDIA SITES**

Financial institutions should be aware that employees' communications via social media - even through employees' own personal social media accounts - may be viewed by the public as reflecting the financial institution's official policies or may otherwise reflect poorly on the financial institution, depending on the form and content of the communications.

Employee communications can also subject the financial institution to compliance risk as well as reputation risk.

Therefore, financial institutions should establish appropriate policies to address employee participation in social media that implicates the financial institution. The Agencies do not intend to specifically address any employment law principles that may be relevant to employee use of social media. Each financial institution should evaluate the risks for itself and determine appropriate policies to adopt in light of those risks.

**OPERATIONAL RISK**

Operational risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events.[26] Operational risk includes the risks posed by a financial institution's use of information technology (IT), which encompasses social media.

In order to identify, monitor, and manage IT-related risks, I would recommend FFIEC's Information Technology Examination Handbook,[27] and also its booklets *Outsourcing Technology Services*[28] and *Information Security*[29] when using social media, and include social media in existing risk assessment and management programs.

Social media is one of several platforms vulnerable to account takeover and the distribution of malware. A financial institution should 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.

**POLICY AND PROCEDURES**

The guidance offered by FFIEC is intended to help financial institutions understand potential consumer compliance and legal risks, as well as related risks, such as reputation and operational risks associated with the use of social media, along with expectations for managing those risks. Although this guidance does not impose additional obligations on banks and nonbanks, as with any new process or product channel, financial institutions must manage potential risks associated with social media usage and access.

With this in mind, we recommend the following outline as the *de minimis* sections for an Social Media and Social Networking Policy and Procedures, conceived as a Employee Manual to be provided to and receipt thereof attested to by all affected employees:

**Overview**: Preamble and Purpose
**Your Identity Online**: Inside and Outside Workplace
**Creating Social Media Content**: Directives
**Managing Social Media Content**: Permissions and Prohibitions
**Fact Checking Your Posts**: Accuracy
**Correcting Errors Promptly**: Timing and Responses
**Leaving Comments**: Permissions, Proprietary Information
**Confidential and Privacy**: Disclosure Limitations
**Potential Conflicts and Red Flags**: Responsibilities

**Responding to a Negative Post**: Prior Approvals
**Posting Recommendations for Colleagues**: Prior Approvals
**Responding Directly to a Journalist**: Prior Approvals
**Building Your Virtual Footprint and Network**: Restrictions

Each section of this employee manual, where appropriate, must provide clear and unambiguous statements relating to directives, company procedures, permissions, prohibitions, employee responsibilities, prior approval processes, restrictions, and informative examples.

As noted previously, banks and nonbanks are using social media as a tool to generate new business and provide a dynamic environment to interact with consumers. Financial institutions must manage potential risks to themselves and consumers by ensuring that their risk management programs provide appropriate oversight and control to address the risks associated with social media.



[1] Federal Financial Institutions Examination Council (FFIEC). *Social Media: Consumer Compliance Risk Management Guidance*, Notice - Request for Comment, FR 78/15 (1/23/13)
[2] 15 U.S.C. 1601 et seq., 12 CFR pts. 202 and 1002
[3] 12 CFR pt. 1002, Comment 4(b)-2
[4] 12 CFR 1002.12(b)(7)
[5] 12 CFR 1002.9(a)(2)
[6] 42 U.S.C. 3601 et seq., 24 CFR pt. 100 (HUD)
[7] 12 CFR 128.4, 338.3, 390.145
[8] 15 U.S.C. 1601 et seq.; 12 CFR pts. 226 and 1026
[9] 12 U.S.C. 2607. See Interagency Guidance, *Weblinking: Identifying Risks and Risk Management Techniques*, (2003) http://www.occ.treas.gov/newsissuances/bulletins/2003/bulletin-2003–15a.pdf.
[10] 15 U.S.C. 1692-1692

[11] 15 U.S.C. 45
[12] 12 U.S.C. 5531, 5536
[13] See FTC Guidance, including *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, at http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf.
[14] 15 U.S.C. 1693 et seq., 12 CFR pts 205 and 1005
[15] See *Operating Rules of the National Automated Clearing House Association* (NACHA), available at http://www.achrulesonline.org/; Rules of the Electronic Check Clearinghouse Organization (ECCHO), available at https://www.eccho.org/cc/rules/Rules%20Summary-Mar%202012.pdf
[16] UCC Art. 4
[17] 12 CFR pt. 229
[18] ''Bank Secrecy Act'' is the name that has come to be applied to the Currency and Foreign Transactions Reporting Act (Titles I and II of Public Law 91–508), its amendments, and the other statutes referring to the subject matter of that Act. These statutes are codified at 12 U.S.C. 1829b, 1951–1959; 31 U.S.C. 5311–5314, 5316–5332; and notes thereto.
[19] Bank Secrecy Act regulations are found throughout 31 CFR Chapter X. Also, the federal banking agencies require institutions under their supervision to establish and maintain a BSA compliance program. See 12 CFR 21.21, 163.177 (OCC); 12 CFR 208.63, 211.5(m), 211.24(j) (FRB); 12 CFR 326.8, 390.354 (FDIC); 12 CFR 748.2 (NCUA). See also Treas. Dep't Order 180–01 (Sept. 26, 2002)
[20] 15 U.S.C. 6801 et seq., 12 CFR pt. 1016 (CFPB) and 16 CFR pt. 313 (FTC); Interagency Guidelines Establishing Information Security Standards, 12 CFR pt. 30, app B (OCC); 12 CFR pt. 208, app. D-2 and pt. 225, app. F (FRB); 12 CFR pt. 364, app. B (FDIC); Safeguards Rule, 16 CFR pt. 314 (FTC)
[21] 15 U.S.C. 7701 et seq.
[22] 47 U.S.C. 227
[23] 16 CFR pt. 316 (FTC); 47 CFR pts. 64 and 68 (FCC)
[24] 15 U.S.C. 1681–1681u
[25] 12 U.S.C. 1813(u). Guidance from the Agencies addressing third-party relationships is generally available on their respective Web sites. See, e.g., CFPB Bulletin 2012–03, *Service Providers* (Apr. 13, 2012), available at http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf; FDIC FIL 44–2208, *Managing Third-Party Risk* (June 6, 2008), available at http://www.fdic.gov/news/news/financial/2008/fil08044a.html; NCUA Letter 07-CU-13, *Evaluating Third Party Relationships* (Dec. 2007), available at http://www.ncua.gov/Resources/Documents/LCU2007-13.pdf; OCC Bulletin OCC 2001-47, *Third-Party Relationships* (Nov. 1, 2001), available at http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-47.html.
[26] *FFIEC IT Examination Handbook: Management booklet*, 2–3 (June 2004), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Management.pdf.
[27] Available at http://ithandbook.ffiec.gov/itbooklets.aspx
[28] Available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.
[29] Available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf