**Richard F. Chambers**
Certified Internal Auditor
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
***President and Chief Executive Officer***

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

March 25, 2013

Ms. Judith E. Dupre, Executive Secretary
Federal Financial Institutions Examination Council
L. William Seidman Center, Mailstop B-7081a
3501 Fairfax Drive
Arlington, Virginia 22226-3550

RE: Social Media: Consumer Compliance Risk Management Guidance - Docket Number FFIEC-2013-0001

Dear Ms. Dupre:

On behalf of the over 180,000 members of The Institute of Internal Auditors (IIA), we are pleased to provide the attached comments on the Federal Financial Institutions Examination Council (FFIEC) proposed guidance entitled "Social Media: Consumer Compliance Risk Management Guidance." We are very supportive of the FFIEC's proposed guidance, which is designed to ensure all financial institutions effectively evaluate and manage risks associated with social media activities.

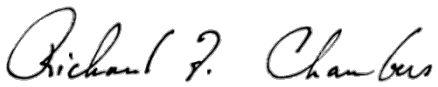
Regardless of size, industry, or geographic location, organizations are quickly elevating their social media presence which presents new risks and exposures that need to be effectively managed. Organizations should establish a clear social media strategy and develop policies that align with the enterprise's overall strategic goals. Guidance for financial institutions that helps balance risk and reward in this rapidly emerging space is certainly warranted in our view.

Attached are five comments regarding the exposure draft (Appendix A) as well as detailed responses to the three questions posed under Section III of the exposure draft (Appendix B). Our comments represent the culmination of observations gathered utilizing a core team of governance, compliance and audit experts who serve on The IIA's Professional Issues Committee (PIC). These individuals consist of Certified Internal Auditors, Certified Public Accountants, Chartered Accountants, Certified Risk Management Assurance professionals, audit executives and consultants who have worked in both public accounting and management positions in small, medium and large multinational organizations.

*Global Headquarters*
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org
www.globaliia.org

Thank you for the opportunity to provide comments. We value the opportunity to collaborate, share, contribute and learn and welcome further discussion on any of our observations.

Best Regards,



Richard F. Chambers, CIA, CGAP, CCSA, CRMA
President and Chief Executive Officer

**About The Institute of Internal Auditors**
The IIA is the global voice, acknowledged leader, principal educator, and recognized authority of the internal audit profession and maintains the International Standards for the Professional Practice of Internal Auditing (*Standards*). These principles-based standards are recognized globally and are available in 29 languages. The IIA represents more than 180,000 members across the globe and has 109 affiliates in 190 countries that serve members at the local level.

## APPENDIX A

1. Section III of the proposed guidance (Compliance Risk Management Expectations for Social Media), states "The risk management program should be designed with participation from specialists in compliance, technology, information security, legal, human resources, and marketing." We believe this should also include a role for internal audit, not specifically as part of the "design" of the program, but in an advisory role to provide assurance that all key risks and controls are appropriately considered. This should also include a role for external advisors or consultants, as needed, depending on the experience and expertise that exists within the company.

2. Also in Section III, seven components of a social media risk management program are specified. As applicable, below are comments on each of these components:

   - **A governance structure with clear roles and responsibilities.** No comments.
   - **Policies and procedures.** No comments.
   - **A due diligence process for selecting and managing third-party service provider relationships.** We recommend including monitoring risks associated with outsourcing social media to third party providers and that this component be rewritten as follows "a due diligence process for selecting, managing and risk monitoring of third party service providers with respect to their use of social media."
   - **An employee training program.** No comments.
   - **An oversight process for monitoring.** No comments.
   - **Audit and compliance functions to ensure ongoing compliance.** These functions (internal audit and compliance) are not usually an integral part of a risk management program; they provide assurance over the program. Therefore, we recommend that the following wording be considered, "Audit and compliance activities within the business to ensure ongoing compliance with internal policies and all applicable laws, regulations, and guidance, with separate, independent oversight from areas such as internal audit and compliance, as warranted."
   - **Parameters for providing appropriate reporting.** No comments.

3. Under "Employee Use of Social Media Sites", the exposure draft specifically excludes employment law principles. We believe employment law is an emerging area of risk exposure that can be partially addressed through clear policies, regular training, and awareness. Given the profile these types of incidents are receiving globally in the media, and in some cases resultant litigation, we believe the FFIEC guidance should include some direction on applicable employment law principles.

4. We believe incident response should have a higher profile and discussion within the body of the final guidance. The role of social media in crisis management, and how poor use or lack of control, of social media during a crisis can significantly exacerbate the severity and velocity of a crisis and possibly damage the reputation of financial institutions.

5. We believe there should be more discussion on the exposures to a financial institution of an employee purposefully, or more likely, inadvertently publishing information on social media that is material and should be disclosed through official channels. We believe the guidance should provide adequate direction on the risks, including potential violations of Regulation FD, associated with employee use of social media, especially with respect to the posting of any potentially relevant financial information.

## APPENDIX B

**Section III – Request for Comments**

**Q1. Are there other types of social media, or ways in which financial institutions are using social media, that are not included in the proposed guidance but that should be included?**

We believe the proposed guidance covers the mainstream types of social media. Any comments we have in this regard have been articulated in Appendix A.

**Q2. Are there other consumer protection laws, regulations, policies or concerns that may be implicated by financial institutions' use of social media that are not discussed in the proposed guidance but that should be discussed?**

While the guidance covers United States aspects well, we recommend some guidance around social media risks and cross-border issues. There should be some consideration of social media risks when operating in foreign locations, particularly where institutions operate outside the United States. For example, different jurisdictions have different privacy laws and the global nature of social media (which often impacts privacy issues) heightens cross-border risks of operation.

**Q3. Are there any technological or other impediments to financial institutions' compliance with otherwise applicable laws, regulations, and policies when using social media of which the Agencies should be aware?**

Given the nature of social media and its propensity to be transmitted via mobile devices, some discussion on the additional risks this brings to the organization would seem appropriate.