May 31, 2016

Submitted by electronic mail
To: innovation@occ.treas.gov
By: The Shared Assessments Program

Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218
Mail Stop 9W-11
Washington, DC 20219

Re: Response to Request for Comments from the Office of Comptroller of the Currency (OCC) for the March 2016 "Supporting Responsible Innovation in the Federal Banking System" White Paper

Dear Ladies and Gentlemen:

The Shared Assessments Program appreciates the opportunity to comment on the proposed rulemaking by the OCC.

The program is led and supported by three tiers of industry collaboration and thought leadership who have contributed to the attached response.

Sincerely,

//S//

Catherine A Allen
President and CEO
The Santa Fe Group, Manager
Shared Assessments Program

About Shared Assessments

The Shared Assessments Program has been setting the standard in third party risk management since 2005.

STREAMLINING CONTROL ASSESSMENTS

The service provider control evaluation process has long been inefficient and costly for all parties. Each outsourcing organization produces and distributes its own proprietary questionnaire to each of its service providers. Service providers strain their resources to respond to diverse client information requests. Organizations struggle to manage oversight of third and fourth parties with the advancement of technology and heightened regulatory expectations. To ease the burden on both outsources and third parties and to create an industry standard, in 2005, six top tier financial services industry organizations, in conjunction with the Big 4 accounting firms and key industry service providers, formed the **Shared Assessments Program**.

Today 200+ corporate members, 14 software licensors and over 350 tool purchasers collaborate to use Shared Assessments Program content to manage third party risk and service provider oversight. Members represent a collaborative, global, peer community of information security, privacy and third party risk management leaders in industries that include financial services, insurance, brokerage, healthcare, retail and telecommunications. Shared Assessments offers education, best practices and methodologies for performing third party risk management. The Shared Assessments Program Tools follow a two-step approach to managing third party risks. Using industry-established best practices, the Shared Assessments Program follows a "trust, but verify" approach to conducting third party assessments, enabling organizations to fine-tune third party risk management program according to each company's strategy for managing risk.

Inputs from Members & Third Party Risk Thought Leaders

The program is led and supported by three tiers of industry collaboration and thought leadership, under coordination by the Santa Fe Group:

- **Advisory Board**: A cross-industry set of advisors, focused on key industry trends, governance, including tone at the top needs for Boards of Directors on cyber security, third party risk and corporate compliance.

- **Steering Committee:** An oversight committee of nominated and elected member companies that provides leadership, strategy and direction to program tool development, content and initiatives to improve third party risk management.

- **Technical Development Committees and Working Groups:** Professional working groups devoted to developing tools and content for third party risk in alignment with cross-industry regulatory and compliance obligations and best practices.

Key Shared Assessments Program Elements:

- Continuously monitors for new standards, regulations and risk areas.
- Accordingly updates the industry-leading third party risk management Program Tools, which include the:
    - Standardized Information Gathering (SIG) questionnaire, used to perform an initial assessment of your vendors.
    - Shared Assessments Agreed Upon Procedures (AUP), a tool for standardized onsite assessments.
    - Vendor Risk Management Maturity Model (VRMMM), a self-assessment tool used to determine the maturity of your own third party risk management program.

- Facilitates and shares the annual Vendor Risk Management Benchmark Study, in collaboration with global consulting firm Protiviti, to examine the maturity of organizations' current risk management programs across multiple verticals.
- Facilitates the Certified Third Party Risk Professional (CTPRP) program – the only certification program solely focused on third party risk management.
- Created and facilitates the game-changing Collaborative Onsite Assessments Program, which ensures a robust and consistent evaluation of a vendor's risk posture on common, shared services.
- Offers cutting-edge education and leadership opportunities through events, such as monthly Member Forum calls and the annual Shared Assessments Summit.

The 9th Annual Shared Assessments Summit was held in Baltimore the week of May 16th through the 20th, bringing together over 250 industry professionals and service provider organizations. At the Summit, the Shared Assessments Program initiated an outreach to its members to review and discuss the OCC White Paper, including discussions at the **2016 Advisory Board**, **Steering Committee** and a dedicated breakout session at the Summit. As part of its ongoing outreach and information sharing objectives, the **Regulatory Compliance Awareness Working Group** facilitated these activities to respond to the OCC's request for feedback.

1. WHAT CHALLENGES DO COMMUNITY BANKS FACE WITH REGARDS TO EMERGING TECHNOLOGY & FINANCIAL INNOVATION?

The top challenges community banks have shared within the Shared Assessments Community include:

- Managing the disproportionate **financial burden** of regulatory compliance for community banks in comparison to larger organizations, which minimizes the resources they have for spending on emerging technology and financial innovation.
- The capacity **to staff risk and compliance personnel** at the levels needed to address regulatory compliance and third party risk within their organizations, or be reliant on outside resources or vendors.

The *2015 Community Banking in the 21st Century Research & Policy Conference* published a study that estimated that compliance costs community banks $4.5 billion annually. From an objective perspective of profitability, it can be said that these costs represented 22% of community bank net income in 2014. Historically, community banks have relied on outside vendors or service providers in the technology space, being unable to staff those functions profitably in an 'in-house' model, given today's technology and risk landscape.

2. HOW CAN THE OCC FACILITATE RESPONSIBLE INNOVATION BY INSTITUTIONS OF ALL SIZES?

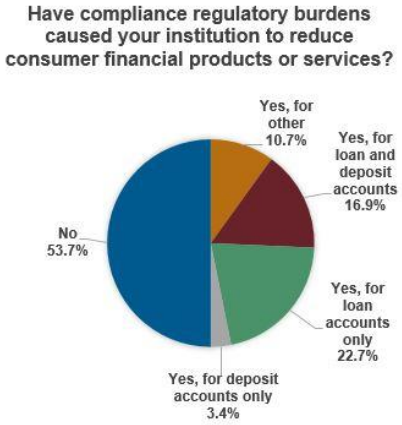
In a post Dodd-Frank world, the costs of compliance have increased across the board. Heightened expectations for larger financial organizations have required the expansion of staffing and implementation of enterprise risk management committees and structures.

A recent ABA Survey has shown that the regulatory burden has limited the expansion of bank products and services due to compliance. The survey found that the increased costs of compliance have led nearly 50% of banks to reduce their offerings, which creates opportunities for non-financial disrupters to emerge.

Considerations for Responsible Innovation:

- Ensure that innovative products anticipate and mitigate risks in the design phase wherever possible. Factor the inherent risk of the financial product based on the overall risk in the ecosystem.
- Consider the risk of consumer harm in the equation. Balance the benefits to the consumer when considering innovation from long term industry players versus new participants who may have little or no industry context.

2015 ABA Survey of Bank Compliance Officers



3. HOW CAN THE OCC ENHANCE ITS PROCESS FOR MONITORING AND ASSESSING INNOVATION WITHIN THE FEDERAL BANKING SYSTEM?

The pace of technology evolution will continue to grow faster than our regulatory frameworks or traditional statute driven compliance approaches. When Online Behavioral Advertising (OBA) first emerged, it created sparks for risk and privacy professionals, and the industry quickly created self-regulatory guidelines to foster innovation in digital marketing while meeting consumer needs for transparency and trust. While OBA was specific to targeted marketing, today's innovation with mobile, faster payments and alternative currencies creates different sectors or categories for compliance.

Considerations for Responsible Innovation:

- Consider the scale of the adoption of the technology as part of the risk assessment process, to prioritize which innovations require stronger consumer protection.
- Identify mechanisms to uncover customer dissatisfaction or harm from either complaints or the potential for unintended consequences of the new technology.
- When creating outreach to innovators – create key messages that translate compliance objectives and goals in business terms.
- Consider hosting innovation outreach for topic specific areas in third party risk like mobile, payments, cloud, to bring thought leaders of all sizes together to identify controls and best practices that foster innovation.

---

4. HOW WOULD ESTABLISHING A CENTRALIZED OFFICE OF INNOVATION WITHIN THE OCC FACILITATE MORE OPEN, TIMELY AND ONGOING DIALOG REGARDING OPPORTUNITIES FOR RESPONSIBLE INNOVATION?

Traditional "Technology Service Provider (TSP)" classifications by the FFIEC have been an important tool in third party service provider risk management and risk management in technology outsourcing. Business process outsourcing and usage of emerging technologies and innovative financial products requires a consultative approach vs. a prescription approach to oversight.

A centralized Office of Innovation could facilitate a discussion, but would likely be used primarily by the financial institutions directly under OCC governance. The OCC should expand its outreach to include Fintech firms with whom it has had little interaction previously. More aggressive outreach directly to Fintech firms could short circuit problems that arise when FIs (who often work with multiple regulators) find themselves checking with several regulators for appropriate guidance about new and innovative products.

Considerations for Responsible Innovation:

- Expand direct outreach to Fintech firms.
- Establish parameters for safe consultations – service providers and many banking organizations have trepidation for consulting or getting advice which turns into enforcement action.
- Identify if the mission of the center is a consultative one or permissions based culture to address the concern for reaching out.
- Consider the service level agreement to respond to an inquiry or question versus a full blown proposal; most innovation starts with a "proof of concept" or "market test."
- Consider how to create clear pathways for different categories of innovation (mobile, payments, lending, cloud) to ensure the balance of getting the right topic to the right area.
- Clarify roles between OCC & CFPB for innovation in financial products – when should an OCC centralized office be contacted versus the CFPB.

5. HOW COULD THE OCC PROVIDE GUIDANCE TO NONBANK INNOVATORS REGARDING ITS EXPECTATIONS FOR BANKS' INTERACTIONS AND PARTNERSHIPS WITH SUCH COMPANIES?

Most industry sectors don't have the prudential regulatory framework that exists in financial services. Understanding the difference between a compliance requirement that is a "law" vs. a "guideline" vs. and "expectation" can be difficult and nuanced without prior exposure to third party risk oversight.

The Direct Marketing Association is an example of a member driven self-regulatory trade association that established guidelines for effective marketing strategies to align on industry best practices. It provides working groups and committees to focus on channel marketing compliance. The Fintech sector has a broad reach and size/scale of types of offerings to the sector, including a trade association of established companies that focus on strategy in the Fintech space.

Similarly, Shared Assessments Program has partnered with the Cloud Security Alliance to leverage joint membership in their associations, to blend the strength of both organizations through industry collaboration.

Considerations for Responsible Innovation:

- Leverage and foster participation between industry trade associations or self-regulatory groups to address risk in innovation.
- Consider creating a set of guidelines or principles that represent the vision of responsible innovation to make expectations more clearly understood.
- Assess the ability to create a working group that includes trade associations from multiple disciplines to address risk in innovation.

6. WHAT ADDITIONAL TOOLS AND RESOURCES WOULD HELP COMMUNITY BANKERS INCORPORATE INNOVATION INTO THEIR STRATEGIC PLANNING PROCESSES?

All organizations invest in some level of strategic planning to address achieving their business goals and objectives. The ABA Survey of Bank Compliance Officers showed that 75% of respondents perform enterprise wide risk assessments. As the asset size grows, that percentage increases. A key strategic element from the white paper is that risk should not impede progress, so providing clear expectations will help focus community banks on the top risk/reward tradeoffs. Risk and Compliance Officers in community banks wear many hats, so prioritization is critical to performance management.

Considerations for Responsible Innovation:

- Provide key messages on OCC expectations for Boards of Directors.

- Provide tools that help educate non-bank participants understand financial services compliance ecosystem.
- Provide guidelines that establish rules of engagement that convey the objectives of responsible innovation.

7. WHAT ADDITIONAL GUIDANCE COULD SUPPORT RESPONSIBLE INNOVATION? HOW COULD THE OCC REVISE EXISTING GUIDANCE TO PROMOTE RESPONSIBLE INNOVATION?

The definition of responsible innovation can cross multiple product lines or areas of compliance within a banking organization. Establishing a core set of principles that can work across areas of compliance (retail payments, wholesale payments, technology outsourcing) will enable a broader understanding of goals and objectives.

Considerations for Responsible Innovation:

- Consider defining a self-assessment tool to evaluate a product for attributes that represent responsible innovation.
- Identify top priorities for compliance areas of focus (e.g. Retail Payments, Technology, etc.).
- Provide clarity on the examination expectations.

8. WHAT FORMS OF OUTREACH AND INFORMATION SHARING VENUES ARE MOST EFFECTIVE?

Proactive communication on the goals for responsible innovation is important to enable outreach to associations, working groups and partnerships. Getting service provider organizations and Fintech groups engaged early can bring their combined resources to the table to find solutions.

Topic specific roundtables and outreach to different categories of Fintech providers is important. Many traditional service providers are moving into the Fintech space, while others are new entrants without the collective knowledge of banking compliance requirements.

Considerations for Responsible Innovation:

- Consider topic specific roundtables.
- Establish a "Banking Privacy and Security Expectations 101" course to educate Fintech and nonbank organizations about financial services industry rules of the road.
- Factor the inherent risk of the financial product based on the overall risk in the ecosystem.

9. WHAT SHOULD THE OCC CONSIDER WITH RESPECT TO INNOVATION?

Technology is changing at a rapid pace – we are becoming the internet of everything. Compliance conveys the perception of "slowing down" innovation or stifling new ideas or new technologies. In reality building strong security early in the development process is more cost effective than fixing issues in production. Privacy by Design is a methodology used to build privacy controls up front and early. A similar methodology would be helpful to address the goals of Responsible Innovation for technology or service providers of all sizes.

Considerations for Responsible Innovation:

- Educate on the key threats and goals the oversight will address.
- Consider a tiered approach based on risk for categories of Fintech service providers.
- Provide expectations for functionality and scale to enable pilots, but create clear guidelines for long term examination obligations.

Thank you for the opportunity to comment on an extremely important topic and for your consideration of our feedback. You can learn more about the Shared Assessments Program at: http://www.sharedassessments.org.

Sincerely,

Catherine A Allen
President and CEO
The Santa Fe Group,
Manager Shared Assessments Program