



**Reducing the Delta Between  
New Regulations and Cost-Effective Practices  
Within the Financial Services Industry**

**A Study Sponsored By BITS/Financial Services Roundtable**

September 2009

# Table of Contents

Executive Summary .....	3
Objectives, Scope, and Approach .....	7
Objectives .....	7
Scope .....	7
Case Studies .....	7
Participants.....	8
Approach.....	8
Analysis and Observations .....	10
Summary Observations .....	10
Case Study Analysis .....	16
1. FFIEC Authentication in an Internet Banking Environment (2005) .....	16
2. FACTA Identity Theft Red Flags (2007).....	19
3. Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005) .....	21
Recommendations and Implementation Steps .....	23
Strategic Initiatives .....	23
Tactical Improvements .....	30
Appendix .....	31
1. Interview Detail on FFIEC Authentication in an Internet Banking Environment (2005).....	31
2. Interview Detail on FACTA Identity Theft Red Flags (2007).....	36
3. Interview Detail on Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005).....	39
Interview Detail on Additional Observations.....	40

# Executive Summary

## BACKGROUND

The purpose of this study is to identify opportunities for financial services industry participants—financial institutions, service providers, industry associations, and regulators—to work more efficiently to achieve timely, practical, and commercially reasonable practices for complying with new regulations and supervisory guidance for technology, security and privacy topics.

This paper was commissioned in December 2008 by BITS, the technology and operations division of the Financial Services Roundtable, and The Financial Services Roundtable’s Anthony T. Cluff Fund. It was conducted by Deloitte & Touche LLP.

To support our analysis, we selected three regulations or guidance to serve as representative examples of the process by which rules are disseminated and addressed by industry participants. These “case studies” include FFIEC Authentication Guidance (2005), FACTA’s Identify Theft Red Flag Regulation (2007), and Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005).

BITS and Deloitte<sup>1</sup> jointly identified three medium to large financial institutions and three “brand name” service providers that would be interviewed by Deloitte. One large insurance company was also identified to provide additional insights from a non-banking perspective. In total we met with approximately twenty-two individuals in fifteen meetings. The conversations were held “on background” and as such the identity of each participant is not being released. The financial services regulatory agencies declined to participate in the study in an official capacity, and as such we were unable to obtain their perspectives on the perceptions shared with us by the industry participants and on the feasibility of the recommendations.

Although we cannot publicly recognize the names of those who participated in this study, we extend our sincere thanks to them for their expertise and candor.

## KEY OBSERVATIONS

Through the course of the interviews with financial institutions and service providers, we heard literally hundreds of perspectives on the regulatory process. Different institutions have had different experiences, and different people within the same institution sometimes hold different perspectives. In analyzing the results of the interviews, six themes emerge on the regulatory and supervisory process:

### **1. Some aspects of the regulatory process appear to be working adequately:**

These include regulators selectively obtaining industry insight, and collaboration that resulted in guidance being risk-focused and not technology-specific or overly prescriptive.

---

<sup>1</sup> As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

- 2. The industry could benefit from changing how field examiners<sup>2</sup> support implementation:** Some respondents appear to have achieved effective and open working relationships with the local field examiners. However, the more common feedback was that field examiners do not adequately support the rollout of new regulation and guidance.
- 3. The process could benefit from crisp and clear communication of new regulation and guidance:** The participating financial institutions do not believe new regulations and guidance are communicated as effectively as they could be—both verbally and in writing.
- 4. Collaboration among participants to form regulation and guidance exists but can be improved:** Financial institutions and service providers interviewed believe that the process to form regulation and guidance could be much more collaborative among industry participants.
- 5. Service providers and regulators can benefit from symposiums that enable communication on regulatory matters:** Unlike financial institutions, service providers do not have an industry association to facilitate interactions with regulatory agencies or to support an understanding of how new regulations and guidance impact them.
- 6. Industry associations drive valuable communications among the participants, but there is an opportunity for them to further harness the perspectives of their members:** Financial institutions in the study believe that industry associations can provide additional services, enhance their capabilities, and structure the participation of their members to better harness the perspectives of the industry

#### RECOMMENDED STRATEGIC INITIATIVES

The results of the interviews with the financial institutions and service providers indicate that there are opportunities for all participants to take some action to improve the regulatory lifecycle. It is not simply a matter of the regulatory agencies changing their processes.

While some of the strategic initiatives are fundamental changes to the current process, the extent of this change should not necessarily deter industry participants from exploring them further. In many cases the proposed initiatives (or components of them) can be piloted so their impact is better understood. From there, where successful, they can be further implemented. And where not successful, they can be modified or discontinued.

The interviews with the financial institutions and service providers point to six strategic initiatives to help improve the regulatory process:

- 1. Use a centralized project management model to implement new regulation and guidance; better support the field examiner’s role in the process:** To achieve a more consistent dissemination of new regulation and guidance, regulators should consider adopting a centralized “project management” model, rather than relying predominantly on field examiners. This can be conducted in a manner that preserves

---

<sup>2</sup> Within this study we use the term “field examiner” to refer both to field examiners (who visit institutions on a set schedule) and on-site regulators (who are generally staffed full-time at financial institutions).

flexible, risk-based approaches. The recommendation also emphasizes training, communication, and information sharing.

**2. Improve collaboration on draft regulation and guidance:** Regulators should expand their efforts to gather industry feedback prior to the issuance of new regulations and guidance; the industry and regulators can function much more collaboratively.

**3. Industry associations should strengthen efforts to better harness the knowledge of their members:** Industry associations could undertake efforts to better structure their interactions with their memberships to better harness the knowledge and perspectives from across the industry.

**4. The industry should lead with a proactive agenda on operational regulation:** Financial institutions and industry associations should develop a proactive agenda that can be pursued by the industry and communicated to the regulatory agencies.

**5. Institutions should organize internally to better respond to regulations and guidance:** Institutions can pursue more effective operating models to more effectively navigate the regulatory environment—driving an agenda, responding to proposed requirements, and mobilizing to implement.

**6. Continue to engage service providers through regulatory agency-sponsored symposiums, but make sure service providers are aware of the opportunity:** There may be an opportunity for the regulators to improve communications with the service providers (and vice versa), so service providers are aware that this resource is available.

#### **OPPORTUNITIES BY PARTICIPANT**

In summary, these interviews indicate that there are a number of strategic and tactical initiatives that can be undertaken across the financial services industry participants to improve the regulatory lifecycle.

#### **Regulators can:**

- Better support the field examiner's role in the process, emphasizing training and communications; use a centralized project management model to implement new rules
- Expand efforts to gather industry feedback prior to the issuance of new regulations and guidance
- Communicate consistently; use standard terminology
- View technology from newer service providers with skepticism

#### **Financial Institutions can:**

- Lead with a proactive agenda; don't be on the defensive
- Organize internally to best respond to regulations and guidance
- Use the formal process such as comment letters
- Contact the regulatory agencies when it believes its field examiners are not appropriately interpreting regulation or guidance

**Service Providers can:**

- Engage with regulators through symposiums

**Industry Associations can:**

- Restructure efforts to engage participation from members
- Facilitate achieving many of the above recommendations

## Objectives, Scope, and Approach

### *Objectives*

The purpose of this study is to identify opportunities for financial services industry participants—financial institutions, service providers, industry associations, and regulators—to work more efficiently to achieve timely, practical, and commercially reasonable practices for complying with new regulations and supervisory guidance for technology, security and privacy topics.

The genesis of this study lies in a series of hypotheses developed by BITS:

- **Costly inefficiencies:** The current system by which new laws, with resulting new regulations and supervisory guidance, are developed and implemented is fraught with costly inefficiencies
- **Long duration and trial and error:** The period between the issuance of new regulations and supervisory guidance and industry agreement on leading practices tends to take a long period of time and involves costly trial and error among financial institutions, service providers, and regulatory agency examiners
- **Interagency complexity:** When multiple regulatory agencies are involved in the issuance of new regulations and supervisory guidance, they frequently seek different—and sometimes inconsistent or conflicting—levels of compliance in a series of “one-off” visits to financial institutions, particularly in the early stages of implementation. This process is inefficient and costly to the financial institutions as well as to the regulators
- **Opportunity to shorten duration:** Enhancements to the regulatory process can be developed that will result in achieving agreed-upon reasonable practices in a shorter period of time
- **Improvements to safety and soundness:** Enhancements to the regulatory process can be done in a manner that improves the safety, soundness, and cost effectiveness of the regulatory process

### *Scope*

This paper was commissioned in December 2008 by BITS, the technology and operations division of the Financial Services Roundtable, and The Financial Services Roundtable’s Anthony T. Cluff Fund. It was conducted by Deloitte & Touche LLP.

### **Case Studies**

To help manage the potentially large breadth of the study, BITS and Deloitte jointly defined the scope. They selected three regulations or guidance to serve as representative examples of the process by which regulations (or supervisory guidance) are disseminated and addressed by industry participants. These “case studies” consisted of:

- **2005 FFIEC Authentication Guidance:** The requirement for risk management controls to authenticate the identity of customers accessing Internet-based financial services

- **2007 FACTA’s Identify Theft Red Flag Regulation:** The requirement to develop and implement a preventative program to mitigate the risk of identity theft for both new and existing accounts
- **2005 Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act:** The requirement to notify customers when sensitive data is breached. This case study is focused on understanding the implications of regulation originating in both the Federal and state domains, sometimes with significant inconsistencies.

## **Participants**

BITS and Deloitte jointly identified three medium to large financial institutions and three “brand name” service providers that would be interviewed by Deloitte. One large insurance company was also identified to provide additional insights from a non-banking perspective. Deloitte made contact with each organization; all agreed to participate. In total we met with approximately 22 individuals in 15 meetings.

The conversations were held “on background” and as such the identity of each participant is not being released. Any identifying information has been removed to maintain their anonymity.

BITS shared a number of documents that outlined efforts of the industry to understand issues and educate industry participants on new regulation and guidance.

The financial services regulatory agencies declined to participate in the study in an official capacity. As such we were unable to obtain their perspectives on the perceptions shared with us by financial institutions and service providers. In addition, we were unable to include their insights into the feasibility of the recommendations, or to what extent some of them may be planned or in place.

Although we cannot publicly recognize the names of those who participated in this study, we extend our sincere thanks to them for their expertise and candor.

## ***Approach***

For financial institutions, the proposed approach was to interview five to seven representatives, generally from the following groups: Risk, Information Security, Privacy, Fraud, Compliance, and Legal.

For each service provider, the proposed approach was to interview one to three representatives, generally from the Government Relations or Regulatory Affairs areas, or who interact with legislators, regulators, or industry associations on regulatory and compliance matters.

While the focus of each individual discussion was slightly different, the objective was to gain a perspective on:

- **How the organization worked with industry participants** (e.g. regulators, financial institutions, industry associations, and other service providers) across the regulatory lifecycle—from the time where regulations or supervisory guidance were formed to the point where industry leading practices were developed

- **What approaches were successful or unsuccessful** in the process to educate regulators and the industry on the necessity of regulation or guidance, industry capabilities, potential solutions, and leading or commercially reasonable practices
- **Ideas for improving the process and interactions** so that a) the industry can achieve timely, practical and commercially reasonable practices for complying with new regulations and supervisory guidance prior to the compliance date and b) regulators have comfort that the industry is adequately addressing the risks or consumer protections that are the focus of the regulation or supervisory guidance

Representative questions included:

- Please walk us through how you participated in the lifecycle for each of the three case studies. How did you interact with industry participants throughout? What worked well in the process? What did not work well? What role did industry forums (e.g. conferences, conference calls) play?
- Are there points in the regulatory lifecycle where you would have liked to have had a greater voice, or you think the process or communication could have been improved and may have resulted in a better solution?
- Are there components of the regulatory process that are too long or too short?
- In the case studies, were there situations where the underlying issues to be addressed were within the purview of multiple regulatory agencies? Does there need to be better coordination among agencies in interacting with the industry on a particular topic, or is this coordination effective today?
- How aligned in the pursuit of a common objective are regulators, institutions, industry associations, and service providers? If they are not aligned, is there an opportunity to better align them?
- Is there an established, consistent method for participating in the regulatory lifecycle, or does it change from regulation to regulation? Is this good or bad?
- How effective have industry associations been at creating channels of communication among leading thinkers in the industry and with regulators? What could associations do differently to be more effective?
- Do you see opportunities to better educate regulators on industry capabilities, technological maturity? What would need to change?
- What improvements to the regulatory process would make it more efficient to achieve cost effective, commercially reasonable processes much earlier in the regulatory lifecycle?

# Analysis and Observations

## *Summary Observations*

### INTRODUCTION

The Analysis and Observations section is structured with a subsection devoted to each case study regulation or guidance. Key takeaways are summarized at the beginning of each case study; more detailed observations are included in the appendix and are organized by interviewee.

Before presenting the summary observations, we would like to share some perspectives on the data and its implications.

- **Facts and perceptions:** Interviews yield two types of information: facts and perceptions. Facts are those pieces of information that actually happened, e.g. a conversation that took place, or how an organization responded to the guidance. Perceptions are those opinions that are “true” in the mind of the interviewee. An example might be a belief that something didn’t happen, simply because that person did not participate in it. For the purposes of this study, both facts and perceptions are the “data set” from which we draw our conclusions. In the recommendations section, we will address not only a set of solutions to improve the regulatory process, but also ideas on what can be done to increase “transparency” and address perceptions
- **Operational versus business-impacting rules:** Institutions view regulation and guidance as falling into two categories: operational or business-impacting. We heard that the general response to operational regulation and guidance (e.g. IT security, consumer privacy, fraud) is to “get it done.” Institutions may respond to business-impacting regulation and guidance (e.g. credit card interest rates and terms and conditions) much differently and with much more vigor. As this study deals with operational aspects, the application of its findings may not be appropriate in business impacting situations
- **Number of regulators:** Reducing the number of regulatory agencies was a topic that we heard on several occasions. This is a topic that has been brought up with increasing frequency in the press and in debate in the US Congress. As an option for improving the regulatory process, it is out of scope for the purposes of this study

### KEY OBSERVATIONS

Through the course of the interviews with financial institutions and service providers, we heard literally hundreds of perspectives on the regulatory process. Different institutions have had different experiences, and different people within the same institution sometimes hold different perspectives. In analyzing the results of the interviews, six themes emerge on the regulatory and supervisory process:

1. Some aspects of the regulatory process appear to be working adequately
2. The industry could benefit from changing how field examiners support implementation

3. The process could benefit from crisp and clear communication of new regulation and guidance
4. Collaboration among participants to form regulation and guidance exists but can be improved
5. Service providers and regulators can benefit from symposiums that enable communication on regulatory matters
6. Industry associations drive valuable communications among the participants, but there is an opportunity for them to further harness the perspectives of their members

Further detail on these six conclusions is provided below:

### **1. Some aspects of the regulatory process appear to be working adequately**

While we gathered a diverse set of opinions, a number of interviewees provided positive views of the regulatory process. Examples include:

- **Regulators obtaining insights:** Regulatory agencies appear to be selectively obtaining insight from institutions and thought-leading vendors prior to releasing guidance (This process is not entirely “transparent” or visible to other participants)
- **Effective results:** The communication and interaction among financial institutions, service providers, industry associations and regulators is generally effective in recommending that guidance be risk-focused and not technology-specific or overly prescriptive, especially in the case of FFIEC Authentication guidance
- **Training of field examiners:** The regulators pursue efforts to train their field examiners on topics such as authentication, and have worked with major vendors to obtain education and awareness (through webinars) from vendors
- **Good relationships with field examiners:** Some institutions have a great deal of respect for their field examiners and have developed collaborative and effective approaches to implementing new regulation and guidance. (However, some other institutions have not met with the same success.)
- **Outreach efforts:** Regulators have conducted outreach efforts such as a webinar on Red Flags to help institutions understand the regulation

### **2. The industry could benefit from changing how field examiners support implementation**

**Some respondents appear to have achieved effective and open working relationships with the local field examiners. However, the more common feedback was that field examiners do not adequately support the rollout of new regulation and guidance.**

Local field examiners have primary oversight of financial institutions and are furthermore responsible for the oversight of each institution’s response to new regulation and guidance.

Some respondents appear to have achieved effective and open working relationships with the local field examiners. However, the more common feedback was that field examiners do not adequately support the rollout of new regulation and guidance. Perspectives include:

- **One way conversations:** Conversations with regulators are “one way”, meaning that financial institutions and service providers provide interpretations and plans, but field examiners do not provide any meaningful feedback. Comments provided include:
  - Insight is withheld because field examiners want financial institutions to solve their own problems
  - A perception that field examiners are reluctant to offer insights because they do not receive appropriate training and communication from Washington
  - Insight is not provided because field examiners do not want to be held accountable for setting the bar too low
  - While the regulators in Washington are comfortable with a risk based approach, field examiners are not
- **Sharing successes:** Insights into how other institutions are addressing requirements are generally not shared
- **Inconsistent interpretations:** A belief that examiners are not consistently interpreting guidance across financial institutions
  - Field examiners monitoring compliance at a service provider did not raise concerns with the service provider’s platform during its development/ enhancement (to comply with new regulation). After the platform was built and deployed to customers, a field examiner at one of the customer sites cited it for not being fully compliant
- **Need for new examiners:** The belief that the training of field examiners is not as much of an issue as the need for higher quality field examiners, which will only happen if Congress and the regulatory agencies increase their pay scales
- **Disconnect between authors and implementers:** A view that the regulators who write guidance are different from those who enforce it, which leads to different interpretations
- **Rewards system:** A perception that the reward system for field examiners measures who has the “best” financial institution (e.g. safest, most compliant) drives stronger interpretation of regulations by the field examiners
- **Recommendation to implement a specific technology:** A belief that field examiners wanted a financial institution to simply implement a specific technology that was being implemented at another large institution

In contrast to this, one service provider said that, in response to a request from the regulators, it provided training to examiners to help them become more knowledgeable on authentication topics and enforce compliance more consistently.

### 3. The process could benefit from crisp and clear communication of new regulation and guidance

**The participating financial institutions do not believe new regulations and guidance are communicated as effectively as they could be—both verbally and in writing**

A number of interviewees provided perspective on how regulation and guidance are communicated to the industry. These include how it is written, how it is disseminated, and at what point in the regulatory cycle it is produced. This is separate from the comments made previously that were related specifically to field examiners.

Related to written guidance:

- **Lack of consistent terminology:** A belief that there is a lack of clear and consistent terminology in written guidance, which causes confusion in interpretation
  - Terms such as security breach, identify theft, privacy, information security, and application have very specific meaning
  - One interviewee pointed out that the regulators did a good job in clearly defining “application” in the May 2008 Application Security bulletin<sup>3</sup>
- **Expansion of scope:** A perception that in cases where terminology has not been defined, the scope of regulation expanded based on questions asked by the financial institutions. One financial institution believes that if they had not asked if Interactive Voice Response (IVR)<sup>4</sup> was included in FFIEC Authentication in an Internet Banking Environment, it may not have been
- **Cognizance of downstream implications:** A desire among some financial institutions for regulation to be written with an understanding of the downstream implications. For example:
  - When the final identity theft red flags regulation was published with 26 “illustrative examples”, there was some confusion among participants over whether the red flags were requirements
  - Some institutions are still addressing the ramifications of this situation in the education of their internal auditors, who are questioning why each red flag was not implemented

Related to how it is disseminated:

- **Interagency challenges:** A belief that there are special challenges for institutions in trying to comply with interagency guidance. The view from some financial institutions is that when guidance is explained by regulators in

---

<sup>3</sup> *OCC Bulletin 2008-16*, May 8, 2008.

<sup>4</sup> Interactive Voice Response (IVR) is an interactive telephone technology that accepts voice and keypad inputs to interact with callers, gather information, provide information, and route calls. In the financial services industry it is traditionally used, for example, to provide balance and transaction information, and to help route calls to specific operators based on the purpose of the call.

Washington, each agency tends to emphasize its own particular perspective, rather than the agreed upon interagency guidance

Related to timing:

- **FAQ timing:** Some financial institutions commented that Frequently Asked Questions (FAQs) are issued too closely to or after compliance dates. In the situation of Red Flags, the compliance date was November 2008, and FAQs were not issued until June 2009. If FAQs cause meaningful changes to interpretation of regulation or guidance, then a late release date may not allow sufficient time to implement revised approaches for compliance

#### **4. Collaboration among participants to form regulation and guidance exists but can be improved**

**Financial institutions and service providers interviewed believe that the process to form regulation and guidance could be much more collaborative among industry participants**

Based on these particular case studies, the general perspective from both financial institutions and service providers is that the communication and interaction among participants was generally effective in making recommendations to improve regulations and guidance. However, a number of interviewees provided feedback on the process to form guidance.

- **Regulators seek perspectives:** Appreciation for those situations where the regulators sought perspectives from the industry prior to the issuance of guidance
- **More collaboration before draft issuance:** Belief that there is an opportunity for more collaboration between regulators and the industry before draft regulation or guidance is issued, as both groups have similar objectives such as protecting customers and combating fraud
- **Need to escalate internally:** A belief that the internal Government Affairs departments at financial institutions are not knowledgeable about security and privacy issues, and they could be made more so to help drive the agenda
- **Concern with traditional response mechanisms:** Some concern that the “traditional” industry response mechanisms such as comment letters and some industry mobilization efforts may result in adversarial relationships between financial institutions and regulators. A view that the process goes back 50 years, and is largely the same, while the world has changed over that time
- **“Black Box” view of the regulatory process:** A belief by some that the regulatory process is a “black box” and that financial institutions do not know if feedback on proposed guidance matters. Moreover, a belief that if financial institutions knew that feedback mattered, they would participate more actively
- **Small service providers have had too much influence:** A concern that service providers—especially smaller ones with untested solutions—have exerted excessive influence in shaping regulations and guidance, and that the regulators are overly receptive to their technology “solutions.” In addition, an acknowledgement that service providers are effectively using the comment letter

process to make their views known, and are responding in greater numbers than financial institutions

## **5. Service providers and regulators can benefit from symposiums that enable communication on regulatory matters**

Unlike financial institutions, service providers do not have an industry association to facilitate interactions with regulatory agencies or to support an understanding of how new regulations and guidance impact them.

Regulatory agencies have sponsored various symposiums for service providers, but one service provider pointed out that the last one was held in 1993. As the regulatory agencies have held several service provider symposiums since this date on topics such as pandemics and authentication, this statement indicates that there may not be adequate communication and awareness among service providers that this resource is available.

## **6. Industry associations drive valuable communications among the participants, but there is an opportunity for them to further harness the perspectives of their members**

**Financial institutions in the study believe that industry associations can provide additional services, enhance their capabilities, and structure the participation of their members to better harness the perspectives of the industry**

Industry participants generally believe that industry associations such as BITS add value by bringing industry participants (e.g. financial institutions and regulatory agencies) together to discuss issues and solutions, enabling a network of experts and peers across institutions, and voicing opinions that financial institutions do not want to individually or publicly voice.

Participants also provided feedback that industry associations such as BITS can enhance their capabilities to address risk topics, can provide additional services of value to the industry, and need to reorganize participation in forums and conference calls to better gain perspectives from its members.

Related to improving capabilities:

- **Great facilitators, but need risk managers:** Belief that while industry associations such as BITS have strong facilitators, they could be strengthened (and more responsive) if they had strong risk managers on their staff

Related to providing additional services:

- **Insights into metrics and response strategies:** Additional value could be added by disseminating hard-to-obtain metrics that would be valuable in responding to regulators (e.g. how many AML people are on staff), and real time insights into how other financial institutions are complying with regulation and guidelines
- **Reframing positions:** A belief that in an environment in which increased regulation is likely, BITS should take on a more aggressive advocacy role and reframe the way in which it frames its positions. For example, considering the large infusion of government funds into financial institutions, BITS could take the

position that taxpayer money would be better invested in an environment that is more efficient, and costs can be lowered by reducing overlapping regulation

Related to industry participation:

- **Need for increased participation:** A view that there is sometimes very little participation and input by institutions on calls, which reduces the value of the conversation. Participants on calls may range from senior executives to project managers, and not knowing who is on the line causes attendees to remain silent
- **Identifying participants:** Belief that BITS needs to take a more structured approach to identifying resources from each institution who should be participating in various initiatives and on calls. Belief that broad communications from BITS asking for participation can create confusion within a financial institution
- **Segment participation:** Belief that industry association forums need to be segmented by financial institution size, as different types of institutions face different issues including organizational complexity, legacy environment, and maturity

## *Case Study Analysis*

### **1. FFIEC Authentication in an Internet Banking Environment (2005)**

#### **BACKGROUND**

In October 2005 the Federal Financial Institutions Examination Council (made up of the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration) released updated guidance on the risks and risk management controls necessary to authenticate the identity of customers accessing Internet-based financial services. The guidance, *Authentication in an Internet Banking Environment* was issued—in the words of the FFIEC—“to reflect the many significant legal and technical challenges with respect to the protection of customer information, increasing incident of identity theft and fraud, and the introduction of improved authentication technologies and other risk management strategies.”<sup>5</sup> The guidance replaced the FFIEC’s *Authentication in an Electronic Banking Environment*, which had been issued in 2001 and had been nonbinding.

The interagency guidance was a significant change from the technology-specific direction guidance appeared to have been taking as reflected in the FDIC’s study *Putting an End to Account-Hijacking Identity Theft*, issued in December 2004.

On August 15, 2006, the FFIEC agencies released a FAQs document on the guidance. The compliance date was set for the end of December 2006.

Prior to the release of the guidance, BITS developed a policy statement that articulated the Financial Services Roundtable’s position on authentication mandates. Policy statements are reviewed and approved by member company CEOs of the Roundtable

---

<sup>5</sup> See *Authentication in an Electronic Banking Environment*, August 8, 2001 (<http://www.ffiec.gov/pdf/pr080801.pdf>).

and serve as the primary means of outlining the association's advocacy views. Once the guidelines were released, BITS convened and facilitated multiple information-sharing sessions between BITS members and representatives of the Federal regulatory agencies that comprise the FFIEC.

#### **SUMMARY PERSPECTIVE**

The three financial institutions and two service providers interviewed on authentication guidance identified a number of positive perspectives, challenges, and specific recommendations to improve the regulatory process.

##### *Positive Feedback*

- **Regulatory feedback cycle worked:** The general perspective from both financial institutions and service providers is that the communication and interaction among participants was effective in recommending that the guidance be risk-focused and not technology-specific or overly prescriptive. Participants also voiced their belief that authentication is something necessary to protect customers and institutions; the guidance as it stands is not something they are opposed to
- **Regulators sought feedback:** Regulators actively sought out institutions and service providers to get perspectives on authentication prior to the finalization of the guidance
- **Good working relationships:** One institution in particular cited good, open working relationships with its onsite regulators as important in developing a common sense solution

##### *Neutral Feedback*

- **Operational regulation:** Two financial institutions viewed regulation and guidance as falling into two categories: "operational" or "business impacting." Operational refers to topics such as IT security, consumer privacy, safety and soundness, and fraud prevention. The general philosophy for responding to operational regulation is to simply "get it done." Business impacting refers to regulation and guidance that would change the business model. An example is the regulation of credit card interest rates, late fees, and other terms and conditions. Institutions may respond to business impacting regulation and guidance much differently and with much more vigor

##### *Challenges*

- **Service provider influence:** All three financial institutions cited concerns with service providers exerting excessive influence in shaping the guidance. This comment was predominantly aimed at smaller untested firms but one interviewee called out a number of large firms. There was a general view that regulators were overly receptive to the smaller firms with "solutions" that were too technology-specific. (As a counterpoint, a large service provider noted that it advocated on behalf of its customers for the regulators to pursue a risk-based approach and that the regulators were receptive to the feedback.)
- **Service providers use comment letters:** Service providers are effectively using the comment letter process to make their views known, and are responding in greater numbers than financial institutions. According to one interviewee, in the case of

FFIEC Authentication, out of thousands of banks perhaps only seventeen wrote a comment letter, while more than twice as many service providers did so

- **Lack of clarity in the guidance:** There is a perception that interagency guidance is challenging because even though it is agreed upon among agencies, each agency tends to pursue (or explain) it based on its own perspective. A lack of clear and consistent terminology in the guidance was cited for causing confusion. Lastly, there is a perspective that the regulators did not know exactly what they wanted when the guidance was issued, and the scope expanded as institutions asked additional questions
- **Training/calibration of examiners:** The interviewees generally spoke with their peers at other institutions to share perspectives on the guidance and gain insight on complying with its requirements. There is a perception that local field examiners are not adequately trained on guidance, and therefore interpret it inconsistently. This means that what is acceptable to one regulator at one financial institution may not be allowed by another regulator at another. A service provider expressed frustration that it communicated with its regulators frequently as it developed a solution, but after the solution was built and deployed, a field examiner at one of the customer sites cited a module within it for not being compliant. In contrast to this, one service provider said it was asked for and provided training to regulatory examiners so they could become knowledgeable on authentication topics and enforce compliance more consistently. Finally, there were views that the regulators who write guidance are different from those who enforce it, which leads to different interpretations
- **Pressure to use solutions in place at other financial institutions:** Financial institutions cited pressure from field examiners to implement approaches that were implemented at other institutions. This seemed to contradict the individual risk based approach set forth in the guidance
- **Tight compliance deadlines:** One large financial institution stated that the compliance deadline was too short for an institution of its size, and that it created an unnecessary burden

#### *Recommendations*

- **Opportunity to be proactive.** There is an opportunity for financial institutions to escalate industry issues and emerging threats more formally to their executive management and regulatory affairs groups—and proactively address these issues with legislative bodies and regulators. A specific topic the industry could rally around is the currently unregulated financial aggregation websites which provide risk to authentication methods by having customers reveal their login credentials. Finally, there is a general belief that industry participants have the opportunity to work much more closely to achieve good outcomes for the industry

Additional recommendations to improve the process that were not raised by the interviewees themselves are detailed in the “Recommendations and Implementation Steps” section.

## 2. FACTA Identity Theft Red Flags (2007)

### BACKGROUND

The impetus for FACTA Identity Theft Red Flags was the belief that identity thieves were using people's personally identifying information to open new accounts and misuse existing accounts. The final rules<sup>6</sup> were issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The final rules became effective on January 1, 2008; the compliance deadline was November 1, 2008. (The FTC is delaying enforcement for entities under its jurisdiction until August 1, 2009. The financial regulators did not extend the deadline.)

A financial institution's program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The program must also help a financial institution to:

- Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the program
- Detect red flags that have been incorporated into the program
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft, and
- Update the program periodically to reflect changes in risks from identity theft

The agencies also issued guidelines to assist financial institutions and creditors in developing and implementing a program, including a supplement that provides examples of 26 "red flags" which give the requirements their common name. These red flags are not a checklist, but rather are examples that financial institutions and creditors may want to use as a starting point. The final rules also require credit and debit card issuers to develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. In addition, the final rules require users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency.

### SUMMARY PERSPECTIVE

The three financial institutions and two service providers interviewed on identify theft red flags note a number of positive perspectives, challenges, and specific recommendations to improve the regulatory process.

---

<sup>6</sup> See *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*, November 9, 2007

(<http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>)

### *Positive*

- **Effective operating and governance models may ease the response and implementation process:** Financial institutions that have effective models to address regulatory issues seem to have a more successful experience in achieving compliance than those that need to navigate a traditionally “decentralized” environment. Two of the financial institutions interviewed had relatively positive views of the regulatory process and achieving compliance. One in particular considers itself to have a very open and collaborative working relationship with the regulators, and a Compliance organization structure that can quickly assess the impact of regulation across the business and understand implications. The other has each of its attorneys dedicated to a particular regulatory topic (e.g. fraud); he or she works closely with the various lines of business and understands the implication of regulations on the business. A third financial institution, which had a generally less positive view of the regulatory process, also appeared to be more decentralized in its response

### *Challenges*

- **Prescriptive regulation:** Although the regulation was finalized with the 26 red flags termed as “illustrative examples”, there was some level of confusion among participants during the process over whether the red flags were requirements. One institution is still addressing the ramifications of this situation in the education of its internal auditors, who are questioning why each red flag was not implemented. This speaks to the need to issue proposed regulations with a view to the downstream implications. Some institutions on the other hand believed instantly that the 26 were only examples
- **Long time period from issuance to implementation:** Almost all interviewees commented on the long duration from issuance of the regulation to its implementation. One financial institution noted that they have had turnover in the people who were originally focused on this; long durations require additional investment in getting people up to speed on the situation
- **Concern over traditional industry response mechanisms:** One financial institution in particular voiced concerns over the “traditional” comment letter process, noting that they believe it tends to result in an adversarial relationship between financial institutions and regulators. One participant noted that the process goes back 50 years, and is largely the same, while the world has changed over that time. Another perspective was that the industry response was overblown. One financial institution relayed that on an industry association call another institution said that it had dozens of people on taskforces to address red flags. The view of the first institution was that the industry tends to stereotypically jump to worst case interpretations
- **Communication:** There was continued feedback that communication and insight from the field examiners is not where it needs to be. There is a view that communication with the regulators is “one way.” The regulators are not providing perspective, guidance, or insights into how others are addressing the regulation. There was also a perspective that the field examiners are not receiving appropriate training, guidance and communication from Washington, and that this adds to their reluctance to offer insights and opinions. One interviewee stated that the issue is not training so much as the need for Congress and the

regulatory agencies to increase their pay scale so they can recruit higher quality people

- **Some desire for industry standards:** There was some desire to see standard industry practices and consistency, especially in operational regulation that is based on a risk management framework. The view is that when an industry standard isn't set, there is a tendency to implement a solution much greater than necessary

#### *Recommendations*

- **Need for service provider forum:** One service provider stated that the last symposium for service providers was in 1993. It believes these forums should be resurrected to provide clear and consistent information to service providers. This is necessary because there is no organization for service providers; they need the regulatory agencies to provide the structure to bring them together. (The regulatory agencies have held several service provider symposiums since 1993 on topics such as pandemics and authentication, which indicates that there may not be enough communication and awareness in the industry that this resource is available.)
- **Early perspectives from industry participants:** One financial institution noted that there is an opportunity for more collaboration before draft regulations are issued; regulators should get the perspective of institutions earlier in the process. The view is that both entities have the desire to protect customers, and they can share perspectives on the topic earlier

### **3. Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005)**

#### **BACKGROUND**

The FFIEC agencies jointly issued *Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (FIL-27-2005) on April 1, 2005. The guidance is an interpretation of section 501(b) of the Gramm-Leach-Bliley Act and the Interagency Guidelines Establishing Information Security Standards (12 CFR 364, Appendix B). The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) was signed into law in 1999. The interpretive guidance states that financial institutions should develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider. The interpretive guidance describes the appropriate elements of a financial institution's response program, including customer notification procedures.<sup>7</sup>

At a minimum, an institution's response program must have procedures to address:

---

<sup>7</sup> *Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, April 1, 2005 (<http://www.fdic.gov/news/news/financial/2005/fil2705.pdf>)

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information
- Consistent with the agencies' Suspicious Activity Report (SAR) regulations, filing a timely SAR, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information
- Notifying customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it

Because the guidance was merely an interpretation of 501(b), it had no effective date.

Since the issuance of this guidance, most states have issued much more stringent and prescriptive regulation on data breach notification.

This case study is focused on understanding the implications of regulation originating in both the Federal and state domains, sometimes with significant inconsistencies.

#### **SUMMARY PERSPECTIVE**

The general view on the breach notifications section of the Gramm-Leach-Bliley Act and the implications on future regulation are mixed.

No interviewees identified breach notification requirements coming from the states as a significant burden. The majority of those we interviewed implemented solutions that "raise the bar" and address across all states the standards put forward by the toughest state.

One institution commented that meeting the individual state requirements is a normal cost of doing business in the United States.

Some institutions commented that addressing fewer sources of standards is certainly easier than addressing more. To this end, they suggested that the federal government should put forward regulation that is more comprehensive, and which preempts states governments from having to act on their own.

# Recommendations and Implementation Steps

## INTRODUCTION

The results of the interviews with the financial institutions and service providers indicate that there are opportunities for all participants to take some action to improve the regulatory lifecycle. It is not simply a matter of the regulatory agencies changing their processes.

The recommendations are divided into two types: “strategic initiatives” and “tactical improvements.” Strategic initiatives are undertakings that require detailed planning and structured execution. These should have a medium to large impact on the regulatory lifecycle. Tactical improvements are undertakings that are more basic in nature and should require less planning and effort to implement. Individually a tactical improvement may have a low impact, but a number of them taken in concert could have a more significant result.

For each strategic initiative we have outlined a number of activities. In some cases these are visions of the future process, and in others they are the major work steps to begin implementation.

While some of the strategic initiatives are fundamental changes to the current process, the extent of this change should not necessarily deter industry participants from exploring them further. In many cases the proposed initiatives (or components of them) can be piloted so their impact is better understood. From there, where successful, they can be further implemented. And where not successful, they can be modified or discontinued.

The interviews with the financial institutions and service providers point to six strategic initiatives to help improve the regulatory process:

1. Use a centralized project management model to implement new regulation and guidance; better support the field examiner’s role in the process.
2. Improve collaboration on draft regulation and guidance
3. Industry associations should strengthen efforts to better harness the knowledge of their members
4. The industry should lead with a proactive agenda on operational regulation
5. Institutions should organize internally to better respond to regulations and guidance
6. Continue to engage service providers through regulatory agency-sponsored symposiums, but make sure service providers are aware of the opportunity

### *Strategic Initiatives*

- 1. Use a centralized project management model to implement new regulation and guidance; better support the field examiner’s role in the process.**

**To achieve a more consistent dissemination of new regulation and guidance, regulators should consider adopting a centralized “project management” model, rather than relying**

**predominantly on field examiners. This can be conducted in a manner that preserves flexible, risk-based approaches.**

With few exceptions, one of the greatest challenges voiced in the interviews was that field examiners are not adequately supporting the roll-out of new regulation and guidance. Financial institutions and service providers alike expressed concern that field examiners are not forthcoming with information, might not be adequately trained, are providing inconsistent information from institution to institution, and are too far removed from understanding the original intent of regulation or guidance.

To achieve a greater level of consistency and better address the needs of the financial institutions, regulators could build on traditional program and project management principles, used frequently to effectively and consistently manage large implementation efforts. Some concepts include:

- **Steering committee:** Convene a steering committee that is responsible for overseeing the successful rollout of a particular regulation or guidance, and determining what changes may be required to draft rules. In the event of interagency guidance, the steering committee could be made up of representatives from each of the participating agencies
- **Program manager and core team:** Select a program manager who is responsible for the day-to-day management of the rollout. Build a “core team” of resources to support the program manager with communications, tracking questions, issues, etc. For continuity, include an expert who participated in forming the regulation or guidance. (This could be a part time or advisory role.)
- **Create implementation teams, if necessary:** Depending on scope or complexity of a particular regulation or guidance, create one or more “implementation teams” that report directly to the program manager. These teams could be structured by financial institution size, region, or other attribute (possibly building on an existing structure already in use by the regulatory agencies). They would manage the rollout to a smaller set of financial institutions
- **Define role of field examiner:** Define and manage the responsibilities of the field examiners with respect to the rollout of new guidance, especially in the early stages of rollout. Their responsibilities could range from actively overseeing the financial institution’s development of an approach (particularly at medium to larger institutions), to simply having knowledge of it based on participation in meetings with the financial institution and implementation teams. Field examiners can be an asset to the process, and there is an opportunity to better integrate them into it
- **Comprehensive training:** Develop training manuals and conduct training of regulators to promote consistent enforcement
- **Communications strategy:** Follow a communications strategy and protocol that drives consistent messages to financial institutions and appropriate service providers
- **Regular communications:** Hold regular conference calls and meetings designed to consistently and comprehensively answer questions from institutions. Invite both industry participants and field examiners so they hear the same messages

- **Share insights** into how different institutions have proposed implementing the guidance
- **Gather questions:** Oversee efforts to gather questions from across the industry, and provide consistent answers (e.g. questions are routed to the core program management team)
- **Manage issues and risks:** Actively manage issues and risks (e.g. such as the need to revise draft guidance) and escalate to the Steering Committee for decisions
- **Gather data to understand success:** Conduct some level of data gathering and reporting to understand the level of understanding or adoption across the financial system

While a centralized team approach may appear to be more resource intensive, it may actually enable financial institutions and regulators to remove inefficient iterations from the process, and do more with less.

Some institutions have very effective and collaborative working relationships with their field examiners. Others do not. The skill set, communication style, and personality traits of a particular field examiner or banking representative is likely a factor in the effectiveness of these relationships. This means that while the regulatory agencies could institute more rigorous training for field examiners on new regulations and guidance, it may not achieve the desired level of consistency. A program such as the one outlined above would better integrate field examiners into a larger process and help drive consistency across the banking system.

## **2. Improve collaboration on draft regulation and guidance.**

**Regulators should expand their efforts to gather industry feedback prior to the issuance of new regulations and guidance; the industry and regulators can function much more collaboratively.**

Regulators and financial institutions appear to agree on the need to address “operational” issues such as IT security, consumer privacy, and fraud. The difference often appears to be in perspectives on “how” to address them.

Many interviewees stated that they appreciated those situations where the regulators sought perspectives from the industry prior to the issuance of guidance, or where there were industry association symposiums held on a particular issue. There is an opportunity to expand this effort, not only in gaining industry perspectives, but also in providing some level of transparency into the efforts of the regulators so the industry knows it is happening.

This recommendation is made with the understanding that the regulatory proposal and rulemaking process is driven by the legal infrastructure in which the regulators operate. Thus, process change may need to be preceded by legal changes to that rulemaking process.

A framework for a collaborative initiative might function as follows:

- **Select an issue:** The regulators could select an issue that is under consideration for guidance and agree to pilot a more collaborative approach

- **Determine legal framework:** Develop a strategy to make activities comply with any “open hearings” type laws
- **Sample institutions:** Regulators could gauge true interest by speaking with a sample of financial institutions and thought-leading service providers
- **Shore up support:** Announce that some guidance will be issued and the objective is to gain early feedback into it. This will help shore up support from the institutions (i.e. this is not about creating new regulation, but about providing early feedback into regulation that will be issued)
- **Convene a working group:** Based on interest from financial institutions, regulators could convene a working group of engaged, constructive, thought-leading participants
- **Define the issue, explore options:** Work through defining the core issue to be resolved, then options on how to resolve it
- **Engage industry associations** for subject matter expertise and in communicating efforts of the pilot initiative
- **Merge into normal process:** Proceed with normal rule making process (e.g. comment letters, etc.)
- **Evaluate success:** Create metrics and evaluate the process against the more traditional process (e.g. is the process a black box, is it adversarial, is the comment period shorter, are significant revisions necessary, is implementation satisfactory)

This effort could be a first step in addressing the feedback from the industry that the regulatory process is a “black box” and that the traditional industry response mechanisms may result in more adversarial relationships between financial institutions and regulators. Moreover, it could also help to shorten the traditional comment period, define more effective solutions, and achieve faster implementation of new guidance.

### **3. Industry associations should strengthen efforts to better harness the knowledge of their members.**

**Industry associations could undertake additional efforts to strengthen their interactions with their memberships to better harness the knowledge and perspectives from across the industry.**

One of the success factors in working collaboratively across financial institutions and the regulators is making sure that the leading thinking from the industry is presented. The feedback from many financial institutions is that industry associations such as BITS can strengthen efforts to structure the participation of its members to better harness the perspective of the industry.

To this end, BITS could consider:

- **Strategy for obtaining participants:** Reevaluate how it secures participants from the institutions, working closely with its advisory council and board on strategy, and working exclusively through a key liaison at each back to identify participants

- **Define roles:** Clearly defining roles, responsibilities, and attributes of ideal participants—paying special attention to the level of person that should attend (e.g. executive or project manager)
- **Discontinuing broad communications** to each bank seeking participation
- **Consider segmentation:** Develop a strategy to determine if committees, phone calls, forums, and other venues for communication should be segmented (by an attribute such as financial institution size), so the conversation is more valuable to each group of participants
  - **Subcommittees:** BITS could consider the use of subcommittees to gather the perspectives from each group and an overarching committee to synthesize these perspectives
  - **Segregate beginners:** Consider holding a series of “beginners” calls throughout the response efforts, so those financial institutions who are late to the process do not hold back the other institutions
- **Define expectations:** Define the expectations for participants on calls (e.g. talk or listen) both to change behavior and to set expectations. For example, if the purpose of a call is for the audience to listen, people should not leave with the impression that participation was low
- **Use participation strategies:** Incorporate strategies to improve participation. For example, if institutions are not asking questions because they do not want to be identified, enable them to send real time questions via email

#### 4. The industry should lead with a proactive agenda on operational regulation

**Financial institutions and industry associations should develop a proactive agenda that can be pursued by the industry and communicated to the regulatory agencies.**

There is some belief among financial institutions and service providers that the industry is in a defensive or reactive mode when it comes to responding to and implementing new regulation and guidance. The industry can be much more proactive in identifying a platform of operational issues, which in turn can help collaboratively drive the regulators’ agendas. This aligns with what we heard about the shared objectives of the regulators and industry (e.g. prevention of fraud, protection of customers, etc.) and the belief that the industry is facing regulation and guidance because it did not effectively communicate that many of the components of new regulation or guidance were already in place.

There is also a view that much regulation in the security and privacy space is overlapping. The specifics of this were out of scope for this study, but a number of participants believe that mapping new regulation or guidance to a framework or standard (e.g. ISO) would be effective at communicating where new regulation already exists and where it may be needed.

Developing a proactive agenda could be led by an industry association such as BITS which could:

- **Convene a group** of thought-leading financial institutions who have the pulse on operational issues that need to be addressed

- **Develop guiding principles** for how financial institutions can more proactively drive an agenda of operational issues
- **Collect suggestions** for specific initiatives that the industry and/or regulators could pursue. Some suggestions provided included:
  - Oversight of personal finance management websites which provide aggregated views of a consumer's financial position, but also pose a risk to authentication methods by having customers reveal their login credentials
  - Federated ID
- **Select an industry framework** or standard (e.g. ISO) and map existing regulation or guidance it to identify where regulation already exists and where it does not
- **Service providers:** Invite thought-leading service providers to the discussion
- **Prioritize and develop positions:** Create an inventory of operational issues, prioritize the list through discussions with a broader group of financial institutions, and begin to develop positions on each
- **Initiate discussions with regulators** to share perspectives and collaborate on an agenda

## 5. Institutions should organize internally to better respond to regulations and guidance.

**Institutions can pursue more effective operating models to more effectively navigate the regulatory environment—driving an agenda, responding to proposed requirements, and mobilizing to implement.**

To more effectively navigate the regulatory lifecycle, financial institutions can consider changes to their operating models. These changes could help drive the regulatory agenda, support responding to proposed regulation or draft guidance, and successfully mobilize to implement new regulation and guidance.

Throughout this paper we have commented on effective practices in place at financial institutions, as well as opportunities to improve those practices. These include:

- **Escalate perspectives** to executives and Government Relations/Regulatory Affairs departments on operational issues that have the potential to become future regulatory initiatives
- **View the pipeline:** Have an effective mechanism in place to spot and understand regulations and guidance that is in the pipeline
- **Create specialists on regulatory topics:** Consider aligning individuals in Legal or Compliance with particular regulatory topics (e.g. authentication, privacy) so one person can quickly coordinate and understand implications, overlaps, and who from the organization needs to become involved
- **Effective internal communication channels:** Where a financial institution has a number of business lines, have a structure in place that can quickly assess implications across the business lines and business units—including Information

Technology. Make sure there is clear communication between the group making commitments to the field examiners, and those groups who will need to perform the work (e.g. IT)

- **Build risk management capabilities:** Put less focus on building “compliance oriented” structures, and more on building risk management perspectives and capabilities.
- **Build risk management capabilities, rather than Enable honest conversations:** Where there are already regular risk management and compliance meetings in place, consider adding, if communication needs to be more honest and direct, a less frequent risk and compliance meeting with a smaller audience
- **Meet regularly with regulators** to share progress and obtain feedback

#### **6. Continue to engage service providers through regulatory agency-sponsored symposiums, but make sure service providers are aware of the opportunity.**

**There may be an opportunity for the regulators to improve communications with the service providers (and vice versa), so service providers are aware that this resource is available.**

The regulatory agencies should continue to sponsor service provider symposiums that provide clear and consistent information on regulatory matters to service providers. These symposiums can be especially valuable because service providers do not have an industry association to facilitate interactions with regulatory agencies or to support an understanding of how new regulations and guidance impact them.

There may be an opportunity for the regulators to improve communications with the service providers (and vice versa), so service providers are aware that this resource is available.

- For service providers with regulated operations, each field examiner should confirm the point of contacts within the company that should be made aware of service provider symposiums
- For service providers without regulated operations, the regulatory agencies could expand their database of service provider contacts by
  - enabling enrollment or sign-up on regulatory agency websites
  - obtaining contact names from previously submitted comment letters
  - allowing service providers to sign-up at various industry events
  - working with financial industry associations who may be able to provide additional contacts
  - using its network of field examiners at financial institutions to submit the names of active service providers who should be made aware of service provider symposiums

On a regular basis, the regulatory agencies could ask each service provider to identify the individual(s) who should receive communications on upcoming events.

## ***Tactical Improvements***

Tactical improvements are undertakings that are more basic in nature and should require less planning and effort to implement. Individually a tactical improvement may have a low impact, but a number of them taken in concert could have a more significant result. As these recommendations are fairly straight-forward, they are not described in great detail. Based on the interviews, opportunities include:

1. Until other mechanisms are put in place, financial institutions should continue to take advantage of using comment letters to voice their perspectives and help educate the regulatory agencies
2. In situations where a financial institution believes that its field examiners are not appropriately interpreting regulation or guidance, the institution should confer with the regulatory agency contact listed on the regulation or guidance
3. When issuing rules, regulators should include a section on terminology and define terms
4. Regulators could make an effort to be cognizant that that technology “solutions” from smaller service providers may be untested
5. If there are delays in issuing documents (such as FAQs) related to a regulation or guidance, regulators should attempt to communicate some insight into when they might be issued

# Appendix

## 1. Interview Detail on FFIEC Authentication in an Internet Banking Environment (2005)

### DETAILED PERSPECTIVES BY INSTITUTION/SERVICE PROVIDER

#### *Financial Institution A*

Financial Institution A provided perspectives on the challenges of interagency guidance, a disconnect between those writing guidance and those implementing it, the “calibration” or training of examiners to drive consistent application of regulation across institutions, consistent terminology, and the role of service providers in influencing guidance.

At the time of this guidance, Financial Institution A stated that it did not have a mature operating model in place to monitor the regulatory landscape and coordinate its response across the organization. The predominant method of responding through this regulation was through BITS.

Financial Institution A believes that interagency guidance is “inherently bad” and that there are special challenges for institutions trying to comply with it. Their view is that there are conflicting interests among the regulatory agencies, and through a negotiation process the agencies present a mutually agreed upon written document.<sup>8</sup> However, when the guidance is explained verbally, the regulators appear to revert to the original opinions or perspectives of their own agencies. This causes confusion among the financial institutions.

The example cited for this is the three two-hour calls BITS hosted on FFIEC authentication guidance. Over the course of the three calls, the regulators explained the guidance first as “authentication”, then as “not authentication but layered security”, and finally as “layered security with good authentication.”

Financial Institution A believes that regulators do not conduct training necessary to “calibrate” their examiners so that rules are consistently applied across institutions. Financial Institution A cited that a regulatory agency admitted this on a BITS call. This is important because examiners provide input to institutions as they develop plans to comply with regulation. Institutions communicate with each other to determine appropriate practices to comply with regulation. It is frustrating to institutions when they see a competitor achieve compliance with an approach that their own examiner does not agree with, or when they are not able to pursue a solution that they have seen accepted among their peers.

Financial Institution A perceives that something is lost in the handoff between those crafting rules and those overseeing the implementation of them. In this case both the institution and the field examiners are interpreting guidance for the first time, which leads

---

<sup>8</sup> Financial Institution A cited an agency’s decision to issue guidance on application security in May 2008 (OCC Bulletin 2008-16) as another example of conflicting interests across regulatory agencies. The guidance was not interagency, but solely through one agency. According to the institution, at a BITS forum on the topic, the regulatory representatives announced that they “agree to disagree.”

to confusion. They believe that someone who crafted the rules should help lead the implementation of those rules, rather than moving on to craft the next set of guidance.

Financial Institution A commented that the guidance is mistitled and this caused confusion. While the official title is *Authentication in an Internet Banking Environment*, the guidance is also applicable to ATMs and call centers. Their view is that the regulators create confusion when they loosely use terms such as security breach, identify theft, privacy, information security. To them, each of these terms has a very specific meaning. (They also pointed out that the regulators did a good job in clearly defining “application” in the May 2008 Application Security guidance.)

A final comment from Financial Institution A is that service providers—regardless of size—hold too much sway over the regulatory process, and overly influence regulators by touting untested “solutions.” While there is no way to prevent service providers from talking to the regulators, Financial Institution A felt that industry associations should try to avoid creating environments where service providers can easily access regulators. They cited that when BITS held a forum on authentication guidance, the service provider session was scheduled just after the examiner roundtable, and that created an environment for both groups to interact.

#### ***Financial Institution B***

Financial Institution B generally found the regulatory process to address authentication a positive experience, though they did provide some perspectives on service provider influence and the consistency of implementation across financial institutions over time.

Financial Institution B holds a particular philosophy on regulation that helps shape its perspective. First, it differentiates between “operational regulation” (e.g. safety and soundness, IT security) and “business-impacting regulation” (e.g. credit card interest rates and terms and conditions). Business impacting regulation may be addressed very assertively. The general response to operational regulation is: “let’s just figure out a way to get it done.” The Financial Institution’s view is that much of the Federal regulation in security and privacy is not innovative, and should be in place anyway.

Second, Financial Institution B’s perspective from Compliance and Risk Management is that they have developed very strong working relationships with the regulators, and they have a good organizational structure to support responsiveness. This operating model has led, in their view, to common sense approaches for complying with regulation and guidance.

Financial Institution B views the regulatory process for authentication as a positive experience. The Information Technology group remarked that one regulatory agency called from Washington to gather perspectives on the issue before guidance was released. They commented that the efforts of BITS, especially in bringing the industry and regulators together on conference calls to share information, serve as a good model. The Financial Institution also views BITS as successful in structuring a dialog that showed the regulators that they need not dictate what technology financial services companies should use, and in showing the effectiveness of incorporating compensating controls.

Financial Institution B believes that service providers had a larger voice in driving the regulation than the industry. Financial Institution B believes that service providers are effectively using the comment letter process to make their views known, and are

responding in greater numbers than financial institutions. According to this institution, for FFIEC Authentication, out of thousands of banks only perhaps seventeen wrote a comment letter, while more than twice as many service providers did so. Financial Institution B also perceived that many of the service providers were smaller (“fly-by-night”) and did not have credible solutions, yet their perspective was taken seriously by the regulators.

Finally, Financial Institution B perceived that those institutions who implemented solutions later “did better” than those institutions that implemented solutions earlier. More specifically, the regulatory agencies embraced the risk management aspects more fully as time progressed.

### *Financial Institution C*

Financial Institution C provided perspectives on the overall objectives of the regulators and clarity of guidance, the influence of service providers, tight compliance dates, and being compared to other financial institutions by the regulators. The Financial Institution also shared perspectives on emerging issues in the authentication domain.

Financial Institution C believes the authentication guidance was not well defined (had “a lot of grey areas”) and that the regulators didn’t know exactly what they wanted. An example cited is that when the financial institution asked if Interactive Voice Response (IVR) was included, the regulators responded “um, ye...yes!” Two issues emerge. The first is that the regulation could have been clearer, and specific terms could have been defined. The second is that the financial institution now feels hesitant to ask questions, believing that if they had not asked about IVR, it may not have been in scope.

Financial Institution C believes that service providers had too much voice in influencing the regulators, and that the regulators were overly receptive to claims made by service providers. The Financial Institution viewed many of the service providers as “brand new” with untested solutions. They also commented that as regulators assessed the technology landscape, they should have also considered that there was not enough technology capacity or scale across the service providers to support specific technology solutions for the entire industry. According to this institution, this serves as further support for a risk based model.

While Financial Institution C believes the final guidance was correct, they feel strongly that the compressed timeline was not. Once guidance was issued, they had fourteen months to interpret and implement a solution across a large company with many electronic channels.

Of particular concern to Financial Institution C was the continued pressure from the examiners to implement a technology that was being implemented by another large financial institution. The Financial Institution had a number of contentious conversations with its examiners, because the institution did not want its response to be tied to one particular tool. One perspective outlined is that while regulators in Washington may be open to a risk based assessment, the local field examiners are held accountable, and lean toward tactical solutions. The Financial Institution also feels that the guidance provided by field examiners was not consistent.

The Financial Institution also shared perspectives on emerging issues in the authentication domain. The Financial Institution is concerned about the proliferation of financial account aggregation websites. Customers are giving away their login

credentials to have simplified access to many of their accounts. The Financial Institution expressed concern about security levels at these firms, and wondered what would happen to the data and servers should one of these firms go out of business. The Financial Institution believes that these companies/sites should be regulated—not only should the playing field be level, but also there is a need for customers to be protected. There is an opportunity for the financial services industry to champion this issue with the regulators.

#### *Service Provider A*

Service Provider A provided a positive perspective on the regulatory process—especially with respect to the regulators gathering information on authentication and pursuing training for its examiners. Service Provider A shared insights into service provider/regulator interactions, and the perception of industry participants on this interaction. Finally, Service Provider A shared opinions on how the financial industry can better educate legislators and regulators on industry issues and perspectives, and how the industry can work more collaboratively on industry issues.

Service Provider A stated that when the FDIC issued its 2004 study *Putting an End to Account- Hijacking Identity Theft*, it talked to different experts in the field. Because Service Provider A understood the landscape of authentication and had experts in this area, our interviewee put the FDIC in touch with technical experts in the company. These experts spoke to the FDIC not only about what existed in authentication, but also about what was coming. Service Provider A encouraged the FDIC to not be technology-specific, as a specific technology would only have supported a short-term solution until threats or technology evolved.

Service Provider A believes that its foresight into authentication technology helped to shape the broader risk-based and layered approach that was put forward in the authentication guidelines.

Service Provider A's view of the regulatory process is that the regulators came to "a pretty good place" with FFIEC authentication. Service Provider A would support more guidance being developed in this manner.

Service Provider A noted that some financial institutions were caught off guard when the study was circulated and their first reaction was to simply say "kill this" and push back. Service Provider A believes that now that the guidance has been largely implemented, people generally say that it works.

Service Provider A believes that the regulators did a good job in getting the examiners trained uniformly across the FFIEC as the regulation was implemented. In addition, the regulators asked Service Provider A to conduct a webinar for its examiners on emerging fraud trends, including cross-channel fraud, after the FFIEC guidance deadline had passed, in order to stay informed of evolving threats. Service Provider A believes that the regulators try to consistently understand the threats, the practices and technologies that can help mitigate those threats, and that they conduct ongoing training across the FFIEC institutions for the examiners.

Service Provider A shared its perspective on the perception some industry participants may have on its interaction with the regulators. Service Provider A stated that there was some mistrust by the financial industry associations on what companies such as his tell the regulators. Service Provider A stated that it advocated on behalf of its customers to

help them address their risks. Service Provider A stated that many customers knew it was having discussions with the regulators and were grateful. Service Provider A also said that the leading voices at the financial industry associations weren't focused on the authentication topic and the regulators knew that Service Provider A was. Finally, Service Provider A stated that the financial services industry is an important customer. It does not advise the regulators to be prescriptive or advocate for additional regulation on the financial industry.

Service Provider A also stated that the regulators came to them because they knew the content and because service providers are generally collaborative. An overly defensive stance by the financial industry prompts the regulators to go to the service providers for information.

Service Provider A commented that at the time, the lobbyists for financial institutions knew very little about issues such as authentication. While Chief Information Security Officers (CISOs) talked to other CISOs, they were not escalating issues to more senior executives, lobbyists, or industry associations. Service Provider A believes that the industry needs to escalate and get in front of issues earlier, rather than defensively react to proposed regulation.

With regard to industry associations, Service Provider A believes that BITS had some good representatives focused on this topic, but that they didn't have anyone who could talk technically about authentication at the time the FDIC report was issued.

Finally, Service Provider A stated that there is and will be some dynamic tension between the regulators and the industry. However, if regulators, institutions and service providers worked more closely, they could accomplish a lot. There is a great deal of expertise at the CISO level and with the financial services regulators who are eager to learn.

#### *Service Provider B*

Service Provider B stated that it has very good relationships with its examiners and has worked hard to achieve this state. However, Service Provider B shared its perspective on inconsistency across examiners.

Service Provider B worked closely with the regulators to develop solutions for multifactor authentication, sharing its interpretations of the guidance and plans for its work to achieve compliance. Service Provider B updated its products by the deadline of December 2006. However, in mid-2007 a field examiner at a client using Service Provider B's technology cited the client for not having multifactor authentication for administration in place. When Service Provider B was developing its solution, sharing plans and progress with the regulators, none of the regulators provided any feedback that authentication was needed for this component. Service Provider B does not think there is consistency among the agencies in what the field examiners are examining. Moreover, Service Provider B was told that guidance on authentication for administration was forthcoming; it has been over a year and has yet to be issued. Service Provider B stated that it wants to—and is in its best interest to—comply with regulation, but regulators need to communicate better so it can do so.

## 2. Interview Detail on FACTA Identity Theft Red Flags (2007)

### DETAILED PERSPECTIVES BY INSTITUTION/SERVICE PROVIDER

#### *Financial Institution A*

Financial Institution A's perspective on FACTA Red Flags called out the difference between "business" and "operational" regulation, some concern over the potentially prescriptive nature of the regulation, the length of time to implement, and the view that a good organizational structure can make compliance easier.

Financial Institution A prefaced its comments on FACTA Red Flags by noting that when regulatory issues may affect its core business—such as regulation on credit card late fees—it will vigorously and proactively communicate its position. But on "operational" regulation, while they submit comment letters and convey their opinions, their primary focus is on achieving compliance. They take the perspective that they can only be passionate about so many things, and because many of the operational regulations are "motherhood and apple pie", they cannot really be opposed anyway.

When the proposed rule came out in July 2006, Financial Institution A attended multiple forums and also submitted a comment letter. They stated that in situations where they feel strongly about an issue, they try to coordinate the content in their comment letters with those of other institutions. In this case they did not.

Financial Institution A had some concerns with the 26 red flags being interpreted as prescriptive rather than serving as examples. External counsel advised them to proceed as if they were examples.

The "jury is still out" on getting a view from the regulators on whether they interpreted and implemented their solution adequately, as Financial Institution A has not yet had the regulatory examination that covers Red Flags. Financial Institution A added, however, that its own internal audit group is having some difficulty in not considering the 26 flags as prescriptive requirements.

Financial Institution A commented that the implementation of FACTA has taken an extremely long time, as the legislation was originally passed in the early 1990's, though amended in 2003. Their perspective is that organizations (both financial institutions and regulators) lose focus over time, and this creates inefficiencies. Each time the regulation is resurrected, people have to invest time in getting up to speed again. Moreover, people who originally provided feedback have since left the organization, and this creates a disconnect.

Finally, Financial Institution A provided some perspective on their organizational structure which they believe makes compliance easier. They have aligned their attorneys in the Legal department with specific issues (e.g. authentication). The assigned attorney follows the end-to-end process from regulatory monitoring, to response, to implementation. The attorney understands how regulations on the topic overlap, how the business operates, and with whom to work in the various business units to determine implications and response. By having a point person on a topic who serves the enterprise, Financial Institution A is able to understand not only the regulation, but also the implications to the business. From a regulatory response perspective, this organizational structure enables the organization to quickly understand implications and how it should respond.

### ***Financial Institution B***

Financial Institution B's perspective is that FACTA Red Flags made sense. They believed that it was aligned with its anti-money laundering program and how the financial institution manages a central view of customers. Moreover, they came to the conclusion that they may be better situated to respond than some of their competitors. Hence, they did not participate in the process to provide a different perspective to the regulators. They took a passive role with the industry, and participated in various CIO groups and industry association discussions—mostly in a “listening” capacity.

Financial Institution B has a strong relationship with its regulators and believes that they can be very open and transparent with them on their perspectives and plans. They view their interactions as collaborative, not defensive. In this case the financial institution met with the regulators and came up with a common sense solution that met both of their objectives and was cost effective. Financial Institution B believes that involving regulators early and putting forward a proposed solution are keys to success.

Financial Institution B shared that they viewed the 26 red flags as examples, not mandates or prescriptive regulation.

Financial Institution B provided some perspective that they thought the industry response was “overblown.” Specifically they said that some of the financial institutions had dozens of people on taskforces. They believe the industry tends to jump to worst case interpretations.

Financial Institution B put forward the view that comment letters and traditional responses tend to result in an adversarial relationship between financial institutions and regulators. They believe that extreme positions get plugged into comment letters (because there are “too many cooks in the kitchen”). They also believe that comment letters seem to be formulaic, i.e. “we strongly disagree with the proposed regulations...we have this in place already...nobody cares about the consumers more than we do...this regulation will add an unacceptable burden and cost to the banking system.” The implication is that the response to proposed regulation has become routine.

While Financial Institution B made an early decision to move forward quickly because the regulation was aligned with its capabilities and competitive position, it simultaneously voiced an interest in seeing standard industry practices and consistency. Their view is that when an industry standard isn't set, there is a tendency to implement a solution much more stringent than necessary.

### ***Financial Institution C***

Financial Institution C views the regulatory comment period as a “black box.” After it received the draft regulation, it provided a comment letter. It believes that Regulators had already decided what they wanted the rules to be and were not going to make significant changes in response to input from Institutions or Service Providers. When the final regulation (and preamble) was issued, many of the comments it made were not included.

Financial Institution C believed that problems with definitions (e.g. what is a “covered account”) and lack of clarity around whether the Red Flags that appeared in the rule were mandatory or merely examples, complicated the process.

From a timing perspective, Financial Institution C believed the rules were long on development and short on implementation time. To meet deadlines, Financial Institution C started implementation of Red Flags several months before the final rules were issued. Moreover, the FAQ document (at the time of this interview) had not been issued by the Regulators. (It was issued in June 2009.) In general if FAQs cause meaningful changes to interpretation of regulation or guidance, then a late release date may not allow sufficient time to implement revised approaches for compliance.

Financial Institution C expressed frustration that its conversations with regulators were “one way.” It met with its field examiners on a quarterly basis to discuss interpretation and progress, but did not receive any meaningful feedback from them. On one occasion, the feedback from the field examiners was that “we haven’t gotten our heads around it.”

Financial Institution C also has the sense that poor communications from the regulators affects not only financial institutions but also the regulatory community. The institution said that after the regulators delivered a webinar on Red Flags to financial institutions, the local field examiners approached their institution, said they had heard a webinar had been conducted, and asked for copies of the materials. The Financial Institution believes that regulators in Washington did not take the time to raise awareness among its own field examiners before engaging in industry outreach.

Financial Institution C believes that industry associations were not out in front on interpretation of Red Flags. One interviewee voiced a perspective that some of the BITS conference calls focused on foundational elements and introductory material rather than more advanced or substantial insights.

In the end, Financial Institution C concluded it was already fulfilling the intent of the FACTA Identity Theft Red Flags and, for the most part, found the implementation to be a documentation exercise.

The exam to test the financial institution’s compliance with Red Flags has not yet been conducted. A concern is that the examiners conducting the review will rely on a different interpretation to judge compliance.

In discussing this regulation, the financial institution stressed that it would be a good idea for the regulators to get the perspective from institutions earlier, before it issues draft regulations. It said that they are in general agreement with the objectives of the regulators, and they both want to protect customers. There is an opportunity for more collaboration.

The Financial Institution also said that the agencies need to be put in a position to hire more of the “best and brightest.” It views training as a bandage. The top salary for regulators is too low and the agencies need more good people and sufficient staff to do the work.

#### *Service Provider A*

The interviewee at Service Provider A did not take an active role the regulatory life cycle for FACTA Identity Theft Red Flags. He stated that the time period of three to four years to achieve a final rule seemed excessive and that he was not sure how effective the rule would be given the delayed implementation by the FTC covered entities.

### *Service Provider B*

Service Provider B considers itself to have strong relationships with its regulators. However, it stated that Regulators were less forthcoming than usual with insight, encouraging Service Provider B to read the Examiner's handbook for additional perspective and insight.

The service provider believes that Regulators do not like to "consult" or otherwise provide advice about "how" to comply with requirements. The regulators would not provide any insight into how other firms were achieving compliance. The service provider stated that it wants to comply, and would like more cooperation and insight from the regulators. On the flip side, however, it understands that the regulators likely do not want to risk sacrificing market creativity and objectivity, an essential part of risk management. Nevertheless, more collaboration and insights from the regulators were desired.

The service provider suggested that the regulators hold a FFIEC Risk Assessment 101 class to better explain requirements and expectations. Their view is that "risk assessment" is esoteric and academic, and there are no specifics on how to conduct it.

Service Provider B relies on its own staff to identify and track legislation and regulation on the horizon. It participated in forums on the topic with industry associations such as BITS, but its status as a service provider precludes it from membership.

The service provider stated that the last symposium for service providers was in 1993. It believes these forums should be resurrected to provide clear and consistent information to service providers. This is necessary because there is no organization for service providers; they need the regulatory agencies to provide the structure to bring them together. (Note: The regulatory agencies have held several service provider symposiums since 1993 on topics such as pandemics and authentication. This indicates that there may not be enough communication and awareness in the industry that this resource is available.)

## **3. Interview Detail on Interpretive Guidance on Customer Breach Notification in the Gramm-Leach-Bliley Act (2005)**

### **DETAILED PERSPECTIVES BY INSTITUTION/SERVICE PROVIDER**

#### *Financial Institution A*

In regulation that is state-specific, Financial Institution A usually raises the bar to meet the requirements of the toughest state and applies it equally across all states. This reduces the complexity of having to customize a response state by state. However, Financial Institution A believes that regulations such as GLBA should more comprehensively address customer and other information it seeks to protect and remove the imperative for states to fill any perceived gaps with state-specific regulation.

#### *Financial Institution B*

Financial Institution B recognizes Federal breach notification requirements as a baseline. Financial Institution B acknowledged that state-specific notification requirements increase the complexity that financial institutions have to manage. However, Financial Institution B also said that it has to deal with different state laws for other business

processes as well, such as real estate secured lending. Financial Institution B believed it was just the nature of doing business in the United States.

#### *Financial Institution C*

Financial Institution C said it would be much easier to comply with breach notification requirements if there was a single national standard. Financial Institution C believes that customers should be notified in the event of a breach, but cautioned that the many breach notification laws in place results in too many notifications that unnecessarily scare customers (i.e. the real potential for identity theft or fraud is low) or overload them with confusing information.

#### *Service Provider A*

When it came to implementing requirements, Service Provider A believed the fewer the number of potentially conflicting standards the better.

Service Provider A believes that the key to a successful national standard is to draft requirements that adequately address the various industry concerns so that the states do not have a reason to take action on their own.

#### *Service Provider B*

Service Provider B did not have any comments on breach notification.

### **Interview Detail on Additional Observations**

Through the course of our interviews, the participants provided additional perspectives on the regulatory process that were outside of the case study framework. These observations are summarized in this section.

#### **PERSPECTIVES BY INSTITUTION/SERVICE PROVIDER**

##### *Financial Institution A*

**More communication between industry and regulators prior to issuance of draft guidance:** Financial Institution A stated that once a draft regulation is issued, it is too late to address the regulation itself. The focus becomes primarily on how to comply. Communication between the industry and regulators needs to take place before draft regulations are issued. Financial Institution A said that in some cases (e.g. such as the Risk-Based Pricing Rule) regulators are interested in talking to them, initiate a conversation, and share advance proposals—and this type of communication should happen more often.

**Being organized internally to respond to proposed rules is important:** One area for improvement Financial Institution A identified for itself is the process to identify stakeholders when trying to *comment* on proposed rules. Financial Institution A considers itself better at responding to regulation than monitoring and responding to proposed rules.

**Outside counsel is instrumental to understanding regulations:** Financial Institution A's Legal department speaks with outside counsel weekly to understand the regulatory pipeline and the implications of both proposed and issued guidelines. Financial

Institution A considers outside counsel the primary provider of updates on regulatory happenings.

**Mixed view of value of industry groups:** Financial Institution A stated that it perceives other participants in industry forums to not be as knowledgeable on the subject matter as it is, and this makes industry forums a less valuable source from which to get information. Financial Institution A considers industry forums a useful environment in which to push opinions. Moreover, through industry associations, they can make contact easily with the right people to address regulatory questions.

**Need to educate Congress on the amount of regulatory oversight:** Financial Institution A believes a key challenge is educating Congress and legislators on the amount of regulatory oversight that already exists within the financial services industry. Financial Institution A believes that legislative bodies tend to write legislation on an industry by industry basis, that it overlaps, and there is no real appreciation of the cost burden it drives.

**New approach for BITS:** Financial Institution A believes that in an environment in which increased regulation is likely and in which there may be some challenges in educating regulators on industry perspectives, BITS should consider changing the way in which it frames its arguments. BITS should take on a more aggressive advocacy role and reframe the way in which it frames its positions. For example, considering the large infusion of government funds into financial institutions, BITS could take the position that taxpayer money would be better invested in an environment that is more efficient, and costs can be lowered by reducing overlapping regulation. Also, TARP funds need to be addressed as there is an inherent conflict between the pressures to loan the money while keeping credit standards high.

#### *Financial Institution B*

**Perception that the reward system for field examiners drives increased requirements:** Financial Institution B voiced the view that each field examiner team is in competition with the field examiner teams at other financial institutions. They are measured on who has the “best” (e.g. safest, most compliant) financial institution. Therefore, each team pushes for the most stringent interpretation of regulations.

**No collaboration between financial institutions / Need for secure forums:** Although financial institutions are being attacked by the same groups of criminals, they are not collaborating on response strategies and solutions. The barrier to cooperation is anti-trust laws and concerns over revealing information to competitors. There is a lot of room in the industry to collaborate on this topic. Moreover, financial institutions need a secure environment to talk about security and privacy concerns in the industry. The IT department is invited to present at various industry events, but declines to do so to keep its strategy and tactics confidential (and more secure) and to avoid becoming more of a target for criminals.

**Need for industry association to segment membership:** Perception that industry association forums need to be stratified by financial institution size, as different groups of financial institutions are facing different issues based on size, legacy environment, and maturity.

**View of industry association value:** Industry groups add value by voicing opinions that the financial institutions do not want to voice, bringing industry players together (e.g.

financial institutions and regulatory agencies), and enabling a network of experts and peers across institutions.

**Belief the industry is on the defensive:** The industry is reactive to the regulatory environment. The industry should be on the offensive, not the defensive, but the timing may be bad now. It would be good to advance a security agenda through an industry association. The industry could also consider pushing for federated identity (Federal ID) to support consumer banking security.

**Need to involve government affairs:** The Government Affairs department is not knowledgeable about security and privacy, and they could be made more so to help drive the agenda.

**Regulator should focus on the big picture:** In general, the regulators tend to focus on the small “nits and gnats.” They should work with the financial institution more on the big picture view to make sure “we aren’t leaving the barn door open.”

**Need to control the messages:** The banking industry needs to take further measures to educate consumers and legislators on security and privacy and related topics. In actuality, the financial institution’s losses to electronic fraud are less than \$250,000 per year; the financial institution absorbs this cost, not the consumer. The risk message is being controlled and distorted by vocal and biased parties.

**Use an enterprise risk management framework:** There is an opportunity to drive the risk agenda by taking risk topics and breaking them down into an enterprise risk management framework. When regulations are proposed, they can be mapped to the framework to avoid duplication and promote the right solutions.

**Industry associations need risk managers:** While industry associations such as BITS have strong facilitators, they could be strengthened (and more responsive) if they had strong risk managers on their staff.

**Current Successes of Industry Associations:** Industry associations such as BITS are viewed as successful in bringing industry players together to discuss issues and solutions, and in voicing opinions when the company does not want to be the public voice.

**Needs from Industry Associations:** Industry associations such as BITS could add additional value by disseminating hard-to-obtain metrics that would be valuable in responding to regulators (e.g. how many AML people are on staff), and in providing real time insights in to how other financial institutions are responding to comply with regulation and guidelines.

### *Financial Institution C*

**Regulatory Process as a “Black Box”:** Financial Institution C commented that the regulatory process is a “black box” and they didn’t know if feedback on proposed guidance matters. Financial Institution C believes that institutions need to know that their input matters, and if they know that, they will participate more actively and do more.

**BITS Participants:** Financial Institution C believes that BITS needs to take a more structured approach to identifying resources from each institution who should be participating in various initiatives and calls. There is a belief that the broad communications from BITS asking for participation creates confusion within the financial institution, because the institution does not know who is participating from its

organization. One interviewee recommended that BITS address this by working more closely with its advisory council and board—and to use a key liaison at the financial institution, not broad communications, to get involvement.

**BITS Calls:** Financial Institution C commented that there is still very little participation and input by institutions on calls, which reduces the value of the conversation. One interviewee commented that the level of audience on calls may range from senior executives to project managers, and not knowing who is on the call causes attendees to remain silent.

*Service Provider A*

Service Provider A did not have any additional observations.

*Service Provider B*

Service Provider B did not have any additional observations.

## Authors

---

### Walter Hoogmoed

Principal  
Financial Services  
Deloitte & Touche LLP  
whoogmoed@deloitte.com  
+1 973 602 5840

### John Graetz

Principal  
Financial Services  
Deloitte & Touche LLP  
jgraetz@deloitte.com  
+1 415 783 4242

### Edward Appert

Senior Manager  
Financial Services  
Deloitte & Touche LLP  
eappert@deloitte.com  
+1 212 436 7511

## About Deloitte

---

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touch Tohmatsu