Banking Regulatory Response – the Case of Strong Authentication

Paul D. Witman
California Lutheran University
witman@ieee.org

ABSTRACT
The United States banking industry was directed by its regulatory agencies to provide authentication stronger than single factor for “high risk” transactions, as a defense against phishing, by year-end 2006. Financial institutions had a wide array of options available to them to meet this requirement, and there was considerable latitude in how to interpret the regulatory guidance. This paper presents the results of a multiple case study, reviewing regulation, regulatory intent, and financial institution response, particularly under time pressure. Theories from institutional theory provide a framework for reviewing the response.

Keywords
Phishing, strong authentication, financial institution, regulation, regulatory impact

INTRODUCTION
In October 2005, in response to a growing volume of phishing attacks, the Federal Financial Institutions Examination Council (FFIEC)1 issued guidance directing US financial institutions (FIs) to examine the risk profile of the functionality that they offered on the Internet and ensure that appropriate measures were taken to protect customer privacy and data integrity, and to protect against online fraud (FFIEC, 2005). This Guidance requires compliance by year-end 2006.

This Guidance was not ultimately a surprise to the industry. At least one observer of banking regulatory trends note that regulation of consumer safety issues in the electronic area have been in existence for some time, and were anticipated to be the subject of additional regulation in the future (Spong, 2000, pp. 215, 254). The October 2005 Guidance was an update and replacement of Guidance issued in 2001 (FFIEC, 2001a).

Phishing is defined as online attacks that attempt to extract confidential information from individuals. Numerous attack approaches are used to obtain this information. These include deceptive messages that convince a user to give out confidential information (delivered via e-mail most often, but also via voice or fax, in some cases), malware attacks that capture keystrokes or specific online banking credentials, DNS-based attacks that corrupt the mapping of domain names to IP addresses, and “man-in-the-middle” attacks that insert an attack server between the user and a legitimate web server (Emigh, 2005).

The FFIEC’s Guidance emphasizes strengthening the authentication process for high-risk transactions. However, there is considerable latitude in the types of mechanisms that may be judged compliant with the Guidance (FFIEC, 2005). Based on this Guidance, it seems that most institutions are likely to choose solutions that result in stronger authentication of the end user.

RESEARCH QUESTIONS AND METHODOLOGY
Key research questions included:

- How did the Guidance impact decision-making at the financial institution?
- How did informal industry networks affect FI understanding of the Guidance?

---

1 The FFIEC is an interagency body that prescribes principles and standards for regulatory agencies responsible for the regulation of the US banking industry. These include the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Deposit Insurance Corporation (FFIEC, 2006).
What were the results as of the year-end 2006 deadline?

Key research questions for this study are of the “how” form, along with “what” questions related to the organizations’ overall results. No control of individual subjects’ behavior was required to conduct the study as the objective is to study what has happened relatively recently and what is happening, leading to a focus on contemporary events.

Given those conditions, Yin recommends a case study model, with elements of archival analysis to answer the more empirical questions of what, how many, and how much. Again, given the nature of the primary research questions focusing on “how”, an explanatory case study is indicated (Yin, 2003, p. 6).

Study participants were recruited from three medium-sized financial institutions, ranging from approximately US$800 million to US$2 billion in assets. In addition, one individual from a financial institution technology service provider was interviewed, as were two individuals from the banking regulatory agencies. The regulatory representatives were chosen based on recommendations from industry interviewees. The sample size for the financial institutions and regulators was based on the notion of “saturation” – where further data collection appears to add little new knowledge (Robson, 2002, p. 199). We also reviewed the production web sites of twelve of the largest banks operating in the United States to observe their visible rate of compliance with the Guidance as of February 2007.

Table 1 provides a list of interviewees and their institutions and roles. All have between 10 and 30 years of experience in the banking industry.

<table>
<thead>
<tr>
<th>Identification</th>
<th>Institution</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry 1</td>
<td>Medium-size eastern US bank</td>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>Industry 3</td>
<td>Large southwestern US credit union</td>
<td>Head, Electronic Services</td>
</tr>
<tr>
<td>Industry 5</td>
<td>Technology service provider</td>
<td>Chief Risk Officer</td>
</tr>
<tr>
<td>Industry 4</td>
<td>Technology service provider</td>
<td>Product Manager with responsibility for Security</td>
</tr>
<tr>
<td>Industry 6</td>
<td>Large eastern US credit union</td>
<td>Head, Electronic Services</td>
</tr>
<tr>
<td>Regulator 1</td>
<td>An FFIEC-member agency (Agency A)</td>
<td>Technology Specialist</td>
</tr>
<tr>
<td>Regulator 2</td>
<td>An FFIEC-member agency (Agency B)</td>
<td>Technology Specialist</td>
</tr>
</tbody>
</table>

The research results were reviewed and comments provided by some of the interviewees, strengthening the validity of the research. No substantive changes were requested by the reviewers (Industry 1, 2007a; Industry 6, 2007a).

LITERATURE REVIEW

As might be expected, the imposition of a regulatory requirement has resulted in the offering of a wide array of alternative technologies to address the requirement. As with most security problems, a defense-in-depth solution is appropriate (Whitman & Mattord, 2003, p. 225). The Guidance calls out this option as well with its reference to “layered security and other controls” (FFIEC, 2005). Such depth might include phishing detection tools (e.g., EarthLink, 2006), tools to assist the user to recognize a valid web site or valid e-mails (e.g., PassMark Security, 2005), and tools to strongly authenticate the user. Financial institutions could also deploy tools to track the creation of spoof web sites (Emigh, 2005, pp. 14-15), to take down such sites before they cause significant damage, and to monitor the launch of e-mail-based phishing attacks (Cyota, 2005).

Several categories of strong authentication solutions have appeared in the market, including:

1. Hardware and software one-time password tokens,
2. SmartCards,
3. Non-electronic challenge-response tokens,
4. Risk-based challenge models,
5. “PC as second factor” server-side software models, and...
6. Client-server software models (Witman, 2006).

Each of these solutions provides different levels of ease of use and usefulness to the user and varying levels of administrative costs to the institution. However, as of this writing only two of these approaches (“PC as second factor” software models and risk-based challenge models) have achieved significant market presence for consumers (Regulator 1, 2007; Regulator 2, 2007).

Schneier (2005) notes the limitations of two-factor authentication to defend against certain types of attacks. These include man-in-the-middle attacks where the attacker passes the user’s credentials through to the real bank system, and Trojan or malware attacks that compromise the end user’s PC. Without additional defenses against these and future attacks, strong authentication is only a partial solution. Some of the additional controls called out by the 2005 Guidance and otherwise available to FIs will contribute to protecting the consumer. These controls include user education and active monitoring of online activities, both called out in the 2005 Guidance. Other facilities available to FIs include anti-phishing tools in web browsers, phishing site shutdown facilities, and tracking creation of phishing sites before deployment.

As financial institutions add stronger authentication to their online banking experience, they will need to ensure both usability and a sense of security for the end user. Tubin (2005) noted the need to strengthen authentication while maintaining customer convenience or usability. Tan and Teo (2000) also found that security and perceived risk was a statistically significant, though weak predictor of adoption among consumers in Singapore. Finally, Kolodinsky et al (2004) found a significant and positive relationship between the perceived safety and simplicity of PC banking with the adoption of this technology. This will affect both the choice of technology and how that technology is ultimately marketed to the end users.

The Guidance required compliance within a relatively short timeframe – fifteen months from issuance. Knowing that many financial institutions impose a year-end moratorium on system changes (Industry 3 & Industry 5, 2007), the actual time available was closer to twelve or thirteen months. Most FIs are dependent on a technology service provider (TSP) for Internet services and so the FI’s compliance timeline was driven in large part by the timeline of their providers. This led to a comparison of this Guidance with the challenges (on a smaller scale) with the Year 2000 challenges faced by the financial services industry.

Cannon and Woszczyński (2002) discuss institutional theory and organizational ecology theories as they contributed to explaining the behavior of technology managers on Year 2000 projects. Institutional theory (Van de Ven & Poole, 1995), as interpreted and applied by Cannon and Woszczyński, identifies three key pressures that may affect manager decision making. These include sensitivity to the efforts of other similar organizations (mimetic isomorphism), sensitivity to perceptions of the IT profession’s responsibility (normative isomorphism), and sensitivity to the stated and unstated demands of stakeholders within the organization (coercive isomorphism) (Cannon & Woszczyński, 2002). Given the relatively lower visibility of the FFIEC Guidance relative to the Year 2000 issues for industry the notions of normative isomorphism seem less likely to play a major role in influencing decision making at FIs. These various types of isomorphism may contribute to the decision-making process for IT managers involved in making decisions related to strong authentication. As such, it is useful to understand which types were reported to have contributed to the decisions made by the case study participants.

Cannon and Woszczyński (2002) also examine organizational ecology (Hannan & Freeman, 1977), which looks at the fit of an organization’s resource needs into the resource capabilities of its environment. However, their assessment focused on the revolutionary nature of the impact of the Year 2000 changes being implemented in many companies. The FFIEC Guidance does not mandate sweeping changes to applications and impacts a fairly small portion of the technology required for bank operations. As such, organizational ecology does not appear to be a fit with the decision-making models employed for FFIEC compliance but will be considered as a potential rival theory (Yin, 2003, pp. 77-80).

INDUSTRY PERSPECTIVE

Financial institutions took a variety of marketing approaches to expose these new security features to their customers. Some took the approach of describing the changes as something mandated by regulation while others took a more proactive “we’re doing this to help protect you” stance. This latter model may lead to an advantage for the institution, standing out as being more protective than its competitors. Still others described the changes with some degree of technical detail but did not clearly identify the cause, leaving consumers to wonder what the motivation was. The impact of these differences seemed to support the notion that security was important to users. Those FIs which promoted the change from a proactive protection viewpoint seemed to get fewer questions and have fewer issues than those which used a more technical or regulatory-based presentation (Industry 4, 2007). This also bore out the positions of Tubin (2005) as well as Tan and Teo (2000), regarding the importance of maintaining usability and marketing security.
There was a considerable range of interpretation latitude in the October 2005 Guidance. At some levels the Guidance seemed quite clear – e.g., “the agencies no longer view single factor authentication … as acceptable for high risk transactions” (FFIEC, 2005). However, other areas left considerably more room for interpretation, including the use of the word “should” as opposed to “must”, and the title of the document itself as “Guidance”. In addition, the Guidance directed institutions to “make available” the appropriate changes to their processes and systems by year-end 2006 but did not explicitly prohibit allowing users to opt into the service. Allowing users to opt in would considerably reduce the cutover burden on the financial institution, as only a limited subset of users would then utilize the feature (Industry 6, 2007b).

It was clear from the interviews that some institutions’ interpretation of the Guidance was driven at least in part by their standard approach to regulatory guidance. Some institutions tended to take a “letter of the law” approach while others generally aimed to satisfy the spirit of the law and to work with the regulators to determine how much of the stated requirements will actually be required and enforced (Industry 6, 2007b). At least one of the respondents held that view briefly, until the FFIEC issued its Frequently Asked Questions in August (FFIEC, 2006).

At least one respondent in an FI’s technology organization briefly held the common misconception that only a risk assessment and plan were required by year-end 2006. The risk officer in this same institution initially took the more conservative view that full compliance would be required (Industry 3 & Industry 5, 2007). Other institutions started with a variety of perspectives on the initial Guidance. One reported believing that “substantial compliance” would be sufficient – nearly complete, solid plans in place, and perhaps in beta test (Industry 1, 2007b). Others took the more conservative view that full letter of the law compliance would be required in time for the year end deadline (Industry 6, 2007b).

While the regulatory agencies report that they worked primarily through technology service providers (TSP’s) to ensure availability of solutions for FIs, one respondent found itself in the position of managing its TSP for one of its Internet offerings. This was operated by the FI as at in-house data center and the vendor had the understanding from its regulatory contacts that only “substantial compliance” was necessary, resulting in a slowdown in its activities. Subsequent discussions with the vendor led to an acceleration of development and delivery. This ultimately provided the FI with a December 2006, deployment of the product (Industry 1, 2007b).

Technology and operations executives had to deal not only with regulators and vendors but also with their own internal stakeholders (coercive isomorphism). In one case, these stakeholders acquired varied perceptions of the Guidance from industry discussions (mimetic isomorphism). These discussions led to the understanding that hardware tokens or some other physical multi-factor authentication would be required. This resulted in questioning of the technology and operations staff and eventually the validation of their positions. The stakeholders were ultimately convinced that discussion with the examiners responsible for the institution had provided more specific guidance that could be trusted for planning purposes. This same respondent also reported some flexibility from the regulators as discussed among industry executives in September 2006 – some requiring substantial compliance, others requiring full compliance. Some of this may have been due to different regional perspectives or different perceptions from individual examiners (Industry 1, 2007b).

Respondent results varied based on their technology vendors and their rollout plans to their customers. Two of the respondents made strengthened authentication live to consumers before year-end 2006. The third had planned for a late-2006 launch but determined after discussion with its technology provider and its regulator that a phased rollout finishing in late first quarter 2007 would be acceptable.

This institution had a high awareness of the Guidance in early 2006, having had discussions with its examiners and with its key technology providers. The FI went through its initial risk assessment early in 2006 and made the decision to roll out strong authentication using a PC-as-a-second-factor model by late 2006 pending development by its technology service provider. Organizationally, the FI took a “letter of the law” approach, believing that full compliance with mandatory enrollment would be absolutely required. At least one individual in the FI’s technology group felt that there could be room for discussion with the regulators but the organizational “letter of the law” approach won out initially (Industry 6, 2007b).

As the FI neared the target date for initial voluntary enrollment in October 2006, the FI became increasingly uncomfortable with the risk of impact on its consumers. The final mandatory phase of the rollout would come late in the year when there was a natural spike in Internet activity for consumers to retrieve end of year tax information, plan for holiday spending, etc. Even if all of the technology worked well, the institution was concerned about the potential for issues in user understanding, which would trigger a spike in calls to its call center (Industry 6, 2007b).

Subsequent discussion with the FI’s internal compliance staff led to a push (coercive isomorphism) for full mandatory compliance by year-end 2006, though discussion with the FI’s examiners confirmed that there was some flexibility available. The FI ultimately made plans to deploy the stronger authentication in an “opt-in” form in the fourth quarter of 2006, and has
firm plans to make the feature progressively more visible and more mandatory over time until it becomes mandatory for all users by early in the second quarter of 2007 (Industry 6, 2007b).

It was interesting to note, for industry readers of the Guidance, that the 2005 Guidance referred to Internet banking in its title, while the 2001 Guidance referred to electronic banking. This led to some confusion in the industry about whether voice response (telephone banking) systems were addressed by the Guidance. While the 2005 Guidance is clear about this, it is not obvious from the title, and the reference to telephone banking is somewhat obscure. That issue was clarified in the FAQ’s that came out ten months later, in August 2006. This led to some rather late attention on the issues around phone banking systems but still in time for the year-end 2006 deadline (Industry 3 & Industry 5, 2007).

Figure 1 provides an overview of the timeline of events described in these cases. Key financial institution events are on the upper side of the timeline; key regulatory events are on the lower side.

![Figure 1. Guidance events timeline](image)

As a point of comparison to the results of small and mid-sized financial institutions, we reviewed the web sites and Internet banking sites of twelve of the largest FIs operating in the US. No contact was established with the FIs; rather, the intent of the review was to evaluate the public view of the authentication process given that part of the Guidance calls for educating consumers, which should include identifying potential changes to the login process.

All twelve institutions offered bill pay services, a form of transfer of funds to other parties, and thus likely subject to the definition of “high risk”. Seven of these twelve showed no evidence of stronger authentication in place. Four of the twelve were clearly in production with stronger authentication – three with a model that identified the user’s PC as the second factor and one that clearly used risk elements on which to base challenge questions for potentially risky login attempts. The twelfth provided documentation in its login help files that indicated it was doing some form of risk analysis. However, it wasn’t clear that this risk analysis was being done in real time in order to interdict login attempts or whether it was conducted after the fact to detect potential fraud.

It is worth noting the observations of one of the industry respondents regarding the differential impact on small and large institutions. While larger institutions may have more resources available to create and market the requisite technology changes they often have a larger number of users, and perturbations to that user experience can result in very large impacts to customer service operations. Accordingly, larger institutions often have to spend significantly more calendar time after technology readiness in a gradual deployment of technology to minimize impact to customer and customer service alike (Industry 6, 2007b).

**REGULATOR PERSPECTIVE**

The regulators intended, as of the initial release of the Guidance in October 2005, that stronger authentication and full compliance with the Guidance would be viewed as mandatory for all users by year-end 2006 for all high-risk transactions. Due to the nature of the interaction between the five regulatory agencies that make up the FFIEC, the specific language is sometimes the subject of negotiation among the various agencies (Regulator 2, 2007). The regulators understand that the Guidance offered the potential for misinterpretation, and undertook a substantial information campaign within the industry to clarify and communicate the expectations (Regulator 1, 2007). These included discussions between examiners and individual institutions, cover letters to FIs from their regulatory agencies (e.g., NCUA, 2005), along with a multi-page “Frequently Asked Questions” list (FFIEC, 2006).
The goal of the updated Guidance was to keep FIs aware of the heightened risk in the electronic banking environment since the 2001 Guidance was issued. As one regulator put it, “Times have changed” (Regulator 1, 2007). The 2005 Guidance followed essentially the same themes as the 2001 Guidance, with four key differences:

1) It noted that the agencies viewed single-factor authentication, without other compensating controls, as inadequate;
2) It provided a range of suggestions about potential technology and process solutions that would strengthen the authentication process;
3) It mandated customer education to help customers to help themselves stay safe; and
4) It provided a deadline for compliance of year-end 2006.

The Guidance was very clear in that the foundation for the process was the risk assessment, to be conducted as part of an ongoing program of risk assessment for the FI. From that risk assessment and from the Guidance definition of “high risk”, the FI could then determine what additional steps if any were required. Those additional steps for authentication might call for multi-factor authentication, layered security, and other controls (Regulator 1, 2007).

The most common misconception among FIs was the understanding that they only had to complete their risk assessment by year-end 2006 (Regulator 1, 2007). Anecdotal evidence suggests this misconception held for some time, as there were advertisements from risk assessment providers running as late as November 2006, reminding potential buyers of the need to complete their risk assessment in time for the year-end deadline (Bankers Online, 2006).

The regulators describe the general reaction from industry as one of relief. The industry had been expecting the issuance of the Guidance for some months before and had anticipated the possibility that the Guidance might be very prescriptive and constraining. As such, the nature of the Guidance as being more flexible and remaining risk-driven, was perceived to be viewed positively by the industry. In addition, larger FIs were believed to already be using stronger authentication models, at least for commercial customers. Both larger FIs and many technology service providers had been working for some time on the problems before the Guidance was issued (Regulator 2, 2007).

As the year-end target date has passed, the regulatory agencies have continued their semi-formal process of working with the institutions for which they are responsible. Final confirmation of an FI’s level of compliance cannot be determined by an examiner without a formal examination. This process would require review of the FI’s risk assessment, the steps they have taken to mitigate those risks, and the resulting level of compliance with the Guidance (Regulator 2, 2007).

The technology market for financial institutions in the United States is fairly concentrated, in that about 90% of one agency’s group of FIs are serviced by approximately fifteen technology providers for Internet banking services. Some of these operate with an outsourcing model while others operate the technology in-house, with software licensed from a technology provider. Thus, the agencies are able to get a good insight into the level of industry compliance by working with these technology providers and understanding the state of compliance and deployment of their software solutions. Based on these conversations the interviewees both believed that between 60 and 80% of the FIs in their area of responsibility either were already or were capable of becoming in compliance with the Guidance by the end of 2006, with many scheduled to become compliant in the first quarter of 2007, and a few more in the second quarter of 2007 (Regulator 1, 2007; Regulator 2, 2007).

Most of those FIs seem to be using what one of the regulators described as a layered solution. One solution used a cookie or similar client-side storage to identify the PC and tie it to the user. Another model was risk-based, using either IP geolocation or other PC-specific factors to assess risk and further challenge the user at login for risky logins. Most FIs are deploying the product as mandatory for all users, though some are doing so on a phased-in basis (Regulator 1, 2007).

There were a small number of key definitional issues in the Guidance, as indicated by confusion and questions in the industry. The first of these, as noted previously, was with the flexibility in some of the wording allowing for interpretation as to exactly what was required by year-end 2006. Also, the term “high risk” was clearly defined as “access to customer information or movement of funds to other parties” (FFIEC, 2005). However, the term “customer data” was not clearly defined in the original Guidance but rather referred to another document for a complete definition (FFIEC, 2001b).

This second document defined customer information as “non-public personal information”, leading to a perception among many in the industry that such data would include account balances. However, in discussion with the regulators about whether there were examples of electronic banking systems that had only “low risk” transactions, one of the examples given was of a system that provided only access to balances and funds transfers among the user’s owned accounts but no visibility to, for example, full account numbers (Regulator 2, 2007). Such systems might include many phone banking systems and some very limited Internet banking systems that masked full account numbers.
In comparing the 2001 and 2005 Guidance documents, it is reasonable to concur with the regulators that FIs which had consistently followed the 2001 Guidance would not have been surprised or unduly pressured by the 2005 Guidance. Larger and more forward-thinking institutions and technology service providers had been making plans to offer stronger authentication capabilities ahead of the issuance of the 2005 Guidance (Regulator 2, 2007). The 2001 Guidance clearly calls for the industry to use appropriate risk analyses to evaluate the effectiveness of its controls, and as such prudent institutions might well have been making plans for deployment of such solutions.

However, it is also clear that the industry tends to operate on the basis of a somewhat level playing field. Few institutions have both the institutional leadership and the technology capability to make major changes ahead of the bulk of their competitors, nor can they afford to risk alienating their users with a user experience that has not been well-planned and tested (Tubin, 2005).

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This study has documented initial results of the US banking industry’s response to October 2005 Guidance requiring the industry to provide stronger authentication for consumers. The research has shown that regulators believe the industry is largely in compliance with the Guidance, and has either enabled the requisite technology and process changes or has plans in place to do so in the near future.

The interviews and documents have demonstrated the effects of mimetic and coercive isomorphism on industry participants. There was significant impact of mimetic isomorphism among industry participants as they worked with their technology vendors and collaborated in informal meetings with other industry members. In addition, there was evidence of coercive isomorphism within individual institutions, both from organizational superiors, as well as from internal audit, risk, and compliance organizations. As anticipated, there was relatively little evidence of normative isomorphism, or of any view of the IT professionals as implementing revolutionary changes at the level of the Year 2000 events.

Financial institutions have had to adopt strong authentication solutions that allow them to meet the regulatory requirements in a timely fashion. Those solutions had to provide effective security to protect the institution’s customers and reputation along with ease of use, to protect the end user experience and customer loyalty. Future research should be undertaken to more quantitatively assess the rate of institutional deployment of strong authentication solutions along with measurements to assess the individual user adoption of, and satisfaction with, the technologies.

Online banking log records may provide insight into the impact of the stronger authentication on the online banking experience, on online banking adoption, and on continuance. Quantitative analysis of changes in adoption and continuance patterns from before and after deployment of stronger authentication may provide insight into the impact of the technology and process changes on consumers. In addition, a survey of FI technical and customer service staff could be undertaken to evaluate the impact of the rollout of strong authentication on customer service and customer satisfaction. Finally, quantitative analysis of deployment approaches across a broad range of FIs may be possible, working with various technology service providers.

Future research should also monitor the evolution of the threats against the industry, which are reported to be evolving already in the face of stronger authentication on the online channel. The response to those threats will certainly result in new commercial technology offerings (e.g., Evers, 2006), and may result in added regulation as well. The next steps “depend on the bad guys” (Regulator 2, 2007).
REFERENCES

16. Industry 6. (2007a). E-mail comments on review of research draft. To P. Witman (E-mail comments on review of research draft). Simi Valley, CA.