Enhanced Authentication In Online Banking

Gregory D. Williamson
GE Money – America's

Abstract

The online banking environment has grown tremendously over the past several years and will continue to grow as financial institutions continue to strive to allow customers to complete money transfers, pay bills, and access critical information online. During this same time, online banking has been plagued by Internet criminals and fraudsters attempting to steal customer information. Phishing, pharming, and other types of attacks have become well known and are widely used as a means for fraudsters to obtain information from customers and access online banking accounts. As a result, authenticating customers logging onto their online banking service has become a crucial concern of financial institutions.

This research study portrays a clear picture of the need for enhanced authentication in online banking. It presents the main security concerns and criminal activities that are driving the need for stronger authentication, as well as showing the growth of the online channel that is being driven by consumers and financial institutions. This study simplifies and provides a resource for understanding the many options available when implementing enhanced authentication in the online banking environment. It provides detailed analysis of the many authentication solutions available, as well as a set of guidelines for selecting and implementing enhanced authentication, based on the learning and knowledge of industry experts and the consumer.

Introduction

Online banking is a highly profitable channel for financial institutions. It provides customers convenience and flexibility and can be provided at a lower cost than traditional branch banking. Online banking has grown and flourished over the years, but is now facing major challenges due to the risks of phishing, data compromises, and other attacks. The rise of these attacks has caused a decline in the use of online banking and has negatively affected consumer confidence in the ability of a financial institution to protect them. Consumers are questioning the safety of their money and information and are looking to banks to fix the problem. The problem has grown to the extent that consumers and the government are demanding a solution. Financial institutions must take the necessary steps to protect the online accounts of their customers; the need for enhanced authentication has become evident.

The need for stronger user authentication in an online banking environment has become necessary to ensure customer security, confidence, and acceptance of this

widely used channel for financial institutions. The standard means of user authentication, such as username and password, are no longer strong enough to ensure appropriate access control to customers' accounts and personal information. Financial institutions must be able to strengthen user authentication in the online environment to protect their customers and maintain confidence. They must also ensure that stronger authentication does not negatively impact users' online banking experience.

Financial institutions have spent a great deal of time and money developing online banking functionality to allow customers an easy and convenient way to manage their money. These changes have created the opportunity for customers to move away from using bank branches that are costly to operate. In fact, some banks are driving customers to the online channel by charging fees for tasks commonly available to a customer in a branch, such as charging for teller visits. Online customers have the ability to log into their accounts to pay bills, transfer money from one account to another, and perform account maintenance, such as address, phone, and e-mail changes. In many cases, accessing online accounts also gives the user the ability to see account numbers, routing numbers, balance, and transaction information. At one time, most of these services required customers to physically enter a brick and mortar building; these services can now be performed in an online environment. Financial institutions continue to add more services to the online channel, without increasing the amount of authentication needed to perform the services.

The minimal authentication required to access a financial institution's online site has proven to be a large problem. Fraudsters and hackers have utilized their expertise to con consumers into giving up critical information, allowing them to gain access to online banking accounts. To further complicate matters, the many data compromises that have occurred in the past few years are making consumers wary about how safe their information is. Customers expect to have the same amount of security in an online banking environment as they would in a regular banking environment. Financial institutions must take the next step to ensure the continued growth of the online banking channel and to reassure customers that their information and money is safe.

While the notion of enhanced authentication may seem simple, it is in fact a huge undertaking. Today, many financial institutions have a user login framework that is proven and well developed. Enhancing user authentication requires large projects that include resources from many functions of the institution. The need to enhance authentication protocols in financial institutions is further fueled by the FFIEC guidelines, which required financial institutions to implement stronger authentication by January 31, 2006.

The intent of this research project is to provide guidance for industry professionals to utilize when planning and implementing stronger authentication for financial institutions. Today, most information resources are published by vendors who provide solutions for enhanced authentication. While all of the available reports agree on the need for enhanced authentication, the reports are geared towards promoting a solution provided

by the vendor. The purpose of this research is to provide guidelines from the financial institutions' perspective.

This article presents the problems facing financial institutions and guidelines for implementing enhanced authentication for online banking. It presents a clear picture of the state of online banking security and the need for enhanced authentication for online banking. A combination of the researcher's own professional experience, in depth interviews with industry professionals who have implemented enhanced authentication, and surveys of consumers who use online banking were used to complete the research.

Growth of the Online Banking Channel

The beginning of the twenty first century has brought a dramatic increase in the use of the online channel for financial institutions. The number of users taking advantage of the services offered online by financial institutions continues to increase each year (Sullivan, 2005). The top three banking activities that customers engage in online are viewing their bank account information, utilizing bill payment services, and making payments on products that customers have with other financial institutions, such as a credit card or home equity loan (Ponemon, 2005).

comScore Networks Survey

In mid 2004, comScore Networks, an industry leader in the measurement and analysis of consumer behavior and attitudes, released a report on the state of online banking in the United States (comScore, 2005). The report found that over twenty-two million users logged into an account at the nation's top ten banks in the first quarter of 2000 alone (Strasburg, 2005). This number grew twenty-nine percent by the first quarter of 2003 (comScore, 2005). Of the twenty-two million users, twenty percent or 4.6 million people regularly used online bill payment services offered by the top ten financial institutions. This report also highlighted that the usage of online bill payment services increased by thirty-seven percent at the end of the first quarter 2004 (Strasburg, 2005). According to Jim Larrison, Vice President of comScore Financial Services Solutions, "Online banking and bill payment continues to be among the fastest growing applications on the Internet" (comScore, 2005).

Pew Internet & American Life Project Survey

According to a more recent survey published by Pew Internet and American Life Project, over fifty-three million people use Internet banking (Sullivan, 2005). This statistic represents forty-four percent of the Internet users and an astonishing one quarter of all U.S. based adults. Compared with a similar survey in late 2002, these new statistics represent a forty-seven percent increase in the number of Americans performing online banking. The growth of this channel is astonishing, in the year 2000, around fourteen million people used the Internet for banking; in 2002 the figure grew to thirty seven million (Fox, 2005). The survey also found on any given day, thirteen million Americans could be found performing banking tasks online, an increase of fifty-

eight percent from late 2002 (Fox, 2005). The report also illustrates the usage of online banking among male and females; men are more likely to perform online banking activities than women. In fact, forty-nine percent of men participate in online banking, while only thirty-nine percent of women have utilized the services (Fox, 2005). This is a noticeable difference from the 2002 findings, where men and women utilized online banking equally. Of those surveyed, the age group from twenty-eight to thirty-nine had the highest concentration attempting Internet banking. The Pew report also found that the rise in Internet banking is correlated with the market saturation of high speed Internet usage, such as cable and DSL (Fox, 2005). As demonstrated in Figure 1, all categories increased in the most recent survey, as compared to 2002. According to Betty Reiss, spokeswoman for Bank of America, at the end of 2004, 12.4 million users registered for Bank of America's online banking, representing about 50% of bank of America's checking account customers (Sullivan, 2005). The statement by Bank of America supports the finding of the Pew survey.

Figure 1: Growth in Online Banking (Fox, 2005)

Growth in online banking 2002-2004

The percentage of those in each group with internet connections who have tried online banking. In other words, 31% of online men had done online banking in October 2002 and 29% of online women had done it.

	October 2002 N=1027 internet users	*November 2004 N=537 internet users*
All internet users	30%	44%
Sex		
Men	31%	49%
Women	29%	39%
Age		
Generation Y (ages 18-27)	29%	38%
Generation X (ages 28-39)	34%	60%
Younger Baby Boomers (ages 40-49)	33%	42%
Older Baby Boomers (ages 50-58)	26%	49%
Household income		
Live in households earning less than $30,000	21%	32%
$30,000-$49,999	31%	44%
$50,000-$74,999	33%	51%
$75,000 or more	35%	55%
Educational attainment		
High school graduate	27%	42%
Some college	27%	41%
College and graduate school degree	37%	52%
Internet connection at home		
Dial-up	24%	35%
Broadband	35%	63%

Source: Pew Internet & American Life Project Surveys: Oct 7-27, 2002 (margin of error is±3%); Nov. 23-30, 2004 (margin of error is ±5%).

Convenience & Cost

Several factors can be attributed to a financial institution's push toward online banking, including the low cost of the channel, the competitive advantage, the convenience for the customer, and customer service (Ponemon, 2005). Financial institutions see the online channel as a low cost way to offer service and offer convenience to customers (Roche, 2005). One example of how online banking helps to reduce costs is allowing customers to view statements online, which results in a reduction of postal and paper costs. A typical online transaction costs financial institutions fractions less than a transaction that would occur with a human teller (Roche, 2005). The chart titled "Cost of Delivery" (Figure 2) is a good example of how online banking costs have reduced over the past few years. This chart focuses on smaller regional and community banks; it demonstrates that the cost per user has reduced by over 50% since 1999. This chart is a great example of the low costs of online banking for financial institutions.

Figure 2: Costs (Ponemon, 2005)

Cost of Delivery — Then and Now

	1999	2005
SERVICE BUREAU COSTS		
INTERNET COST PER USER	$1.50 – $3.00	$0.75 – $1.50
NEW CUSTOMER SETUP	$5.00	Never seen for Internet, up to $5.00 for bill pay
IN-BANK TRANSFERS	$0.25 – $0.75	$0.00
BILL PAY PER USER	$4.00 – $5.00	$1.50 – $4.50
PER BILL PAYMENT	$0.40 – $1.00	$0.33 – $0.55 (can be packaged w/per user)
IN-HOUSE EXPENSES		
SOFTWARE	$80,000 - $500,000+	$30,000 - $500,000+
MAINTENANCE	25% – 200%	15% – 25%

Costs During Course of 3-Year Contract

	1999	2005
IMPLEMENTATION	$ 60,000	$ 25,000
PER INTERNET USER FEES	$ 260,000	$ 775,000
PER BILL PAY USER FEES	$ 70,000	$ 550,000
PER BILL PAYMENT FEES	$ 25,000	$ 440,000
PER NEW BILL PAY USER FEES	$ 5,000	$ 0
TRAINING	$ 50,000	$ 5,000
CORE INTERFACE	$ 65,000	$ 40,000
COLA/TAX	$ 50,000	$ 185,000
TOTAL 3-YEAR COST	**$ 585,000**	**$ 2,020,000**
AVERAGE COST PER USER PER MONTH	**$ 4.40**	**$ 2.95**
BY COMPARISON: COST PER ACCOUNT FOR CORE PROCESSING	**$0.50 - $0.60**	**$0.40 - $0.55**

Source: Cornerstone Advisors Inc., Scottsdale, Ariz. Information gathered from about 200 banks ranging in asset size from $500 million to $5 billion

Decline in Consumer Trust

Online banking has seen dramatic growth in the past several years and will continue to grow in the years to come. This low cost channel for financial institutions offers unparalleled convenience for the consumer and excellent opportunities for all parties involved (Ponemon, 2005). While this channel continues to grow, it is essential that financial institutions understand the risks involved and build the necessary controls to combat those risks. Consumers have already begun to show distrust and concern about their security in online banking. While the growth is evident, it is crucial to note many recent reports discuss the growing trend of consumers losing trust in a financial institutions' ability to protect online banking accounts. A recent report by Informa Research indicated that from 2000-2003 consumer confidence in transacting online was

on the rise. However, in 2005 this confidence dropped from seventy percent to fifty-nine percent (RSA, 2005). Companies such as Gartner Research, RSA Security, Entrust Security, and the Ponemon Institute have recently published survey results demonstrating concern from consumers over their security when using online banking services.

Gartner

Gartner, the world's largest technology research and advisory firm, recently surveyed five thousand U.S. adults regarding consumer confidence in online banking. The report found that frequent media reports of consumer data compromises, disclosures of unauthorized access to sensitive personal data, and an increase of phishing attacks have had a negative impact on consumer confidence in online commerce (McCall, 2005). The survey found almost one third of those who bank online feel that online attacks have influenced their banking activities. Approximately three quarters of the same group login less frequently and nearly fourteen percent no longer use online banking to pay bills. The Gartner survey found that more than eighty percent of online consumers in the United States were concerned about online attacks and those attacks have affected their trust in email from unknown sources. According to Avivah Litan, Vice President and Research Director at Gartner, "This figure has serious implications for banks and other companies that want to use the email channel to communicate more cost effectively with their customer base, for example a bill sent electronically costs about half of what a bill costs when sent through regular mail" (McCall, 2005).

Entrust

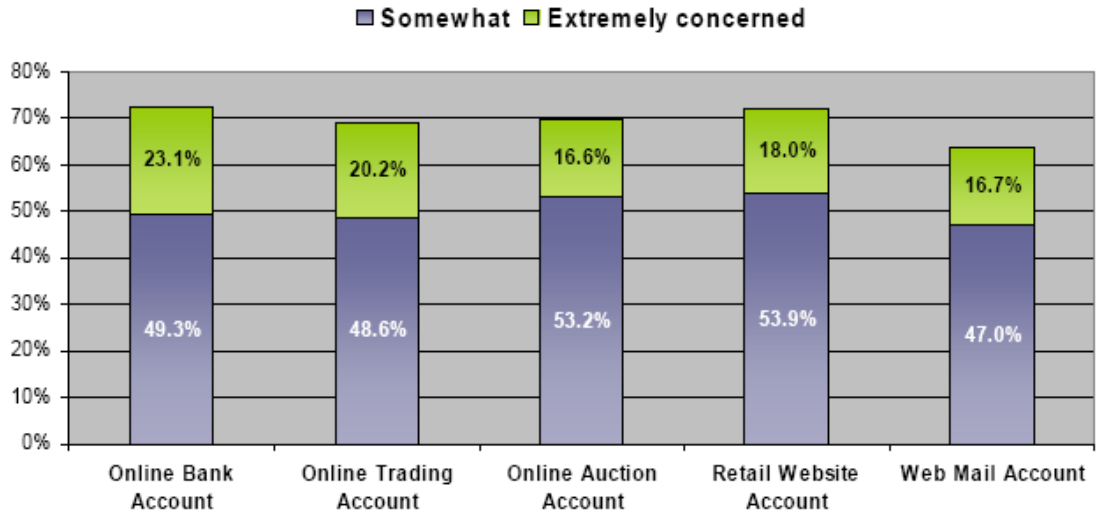
A survey conducted in October 2005, by Entrust, asked more than one thousand individuals in the United States about their online banking behavior (Entrust, 2005). Of those surveyed, sixty-seven percent indicated that they used online banking. These respondents were asked further questions about their concern of fraudulent websites, and how those websites affect their usage of online banking The survey found that eighteen percent of the respondents use online banking less or have stopped banking online altogether in the past year. Around one third of the respondents indicated a concern about not knowing if the banking website they were accessing was legitimate. The survey results also showed an overwhelming ninety-four percent of the respondents would use some sort of stronger authentication in addition to the standard username and password (Entrust, 2005).

RSA Security

RSA Security, a leader in protecting online identities and digital assets, has published the results of two separate surveys showing the concerns that consumers have over online security and identity protection. The first study, published in August 2005, set out to find how trends in Internet security and data security, such as phishing, pharming, and data breaches, have affected consumer's perceptions and behaviors with online banking (RSA, 2005). The survey was administered to more than eight thousand regular

users of online banking and was conducted by Light-Speed Research. It focused on four distinct groups: online traders, online auction participants, online bankers, and web portal mail users (RSA, 2005). The survey found that recent trends in online banking and data security have impacted consumers' perceptions of online safety. The study revealed that over one-fifth of all online consumers felt extremely threatened by online fraud. Two-thirds of the respondents stated they were nervous that someone would fraudulently access their online accounts, as shown in Figure 3 (RSA, 2005). The results of these questions prove to be very alarming for financial institutions spending a great deal of time and resources on pushing customers to online banking. Customers want to feel certain that their account information cannot be accessed illegitimately. The RSA survey also references a 2005 Forrester Research study that revealed concerns around online banking security have influenced thirty-five percent of potential users not to enroll in online banking or bill payment, forty-one percent to avoid applying online for financial products, and thirty-three percent to avoid shopping online with a credit card (RSA, 2005). These numbers all indicate that financial institutions must do more to help consumers feel safe when using online banking, paying bills, or simply viewing their account online.

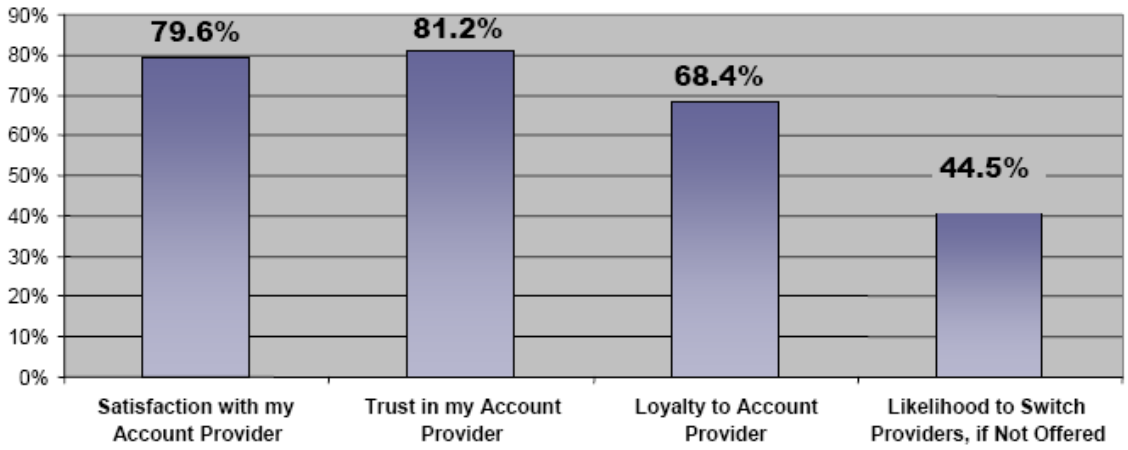
Figure 3: Concern for Fraudulent Access of an Account



Another survey conducted in February 2005, also sponsored by RSA Security, questioned over one thousand adults about their attitudes and perceptions related to online security. This study also found that nearly one-fifth of consumers surveyed refused to utilize their financial institution's Internet products (RSA Security, 2005). Even more interesting was that over fifty percent considered the standard user ID password login protocol not to be enough to protect their online information. Respondents indicated they do not feel financial institutions are doing enough to protect the personal information of the consumer. According to John Worrall, Vice President of Worldwide Marketing at RSA Security, "The message here is simple: if organizations want their customers to do business with them online, they need to implement stronger forms of information security" (RSA, 2005).

The August 2005 RSA study also asked consumers for their views regarding financial institutions implementing stronger authentication policies. The survey asked respondents what impact it would have if a financial institution were to offer stronger authentication services. The results showed an astonishing eighty percent of the respondents would experience increased satisfaction and have more trust in their financial institution (RSA, 2005). Just over two-thirds said they would increase their loyalty to the financial institution and around forty-five percent said they would be likely to switch to a financial institution that offered stronger authentication for its online banking, as shown in Figure 4 (RSA, 2005). These results suggest that consumers would adopt stronger authentication methods and that stronger authentication has an impact on consumers' attitudes and behaviors when conducting online banking. The report also implies that stronger authentication can have a positive impact on customer acquisition and retention.

Figure 4: Customer impact of offering stronger authentication solutions. (RSA Security 2, 2005)



Ponemon Institute

Another survey, conducted by Watchfire and the Ponemon Institute and released in April 2005, focused on understanding the relationship between trust in online banking and customer usage. The survey had a sampling of over twenty-three hundred adult Internet users from all geographic regions within the United States (Ponemon, 2005). The results of the study found that consumers who display a high level of trust in their financial institutions are more likely to utilize a variety of online banking services, such as bill payment (Sinrod, 2005). The study also revealed that customers with a high level of trust are more likely to remain with their bank (Ponemon, 2005). The results of the RSA security survey of August 2005 support the findings of this survey. According to the results, fifty-five percent of consumers with a great deal of trust in their financial institution do not visit other banks websites to learn about products and services; in other words these customers remain loyal to their banks (Ponemon, 2005). However, of that same population, fifty-seven percent of consumers with a high level of trust would take their business to another financial institution if their existing financial institution had only one privacy breach (Sinrod, 2005). The data indicates that any privacy or data security breach can have severe economic impacts on a financial institution. The

results show that no matter how high the level of trust a customer has in their financial institution, it will only take one mishandling of customer information to cause a customer to leave. This demonstrates the importance customers place on protecting their private information and bank accounts.

The surveys and reports referenced above show similar themes throughout. One of those themes is that customers are losing confidence in the ability of their financial institution to keep them safe online and to protect their account information. The second theme is that customers want to see stronger authentication implemented at their financial institutions. This research shows just how important it is that financial institutions understand the need for stronger authentication in their online banking environments.

Reasons for Customer Concern & Stronger Authentication

There are several main factors affecting why customers are concerned about their online banking security. The same factors are also driving the need for enhanced authentication for online banking solutions. These factors include the growing number of phishing attacks, the increased usage of pharming and malware, and widespread data security breaches.

Phishing

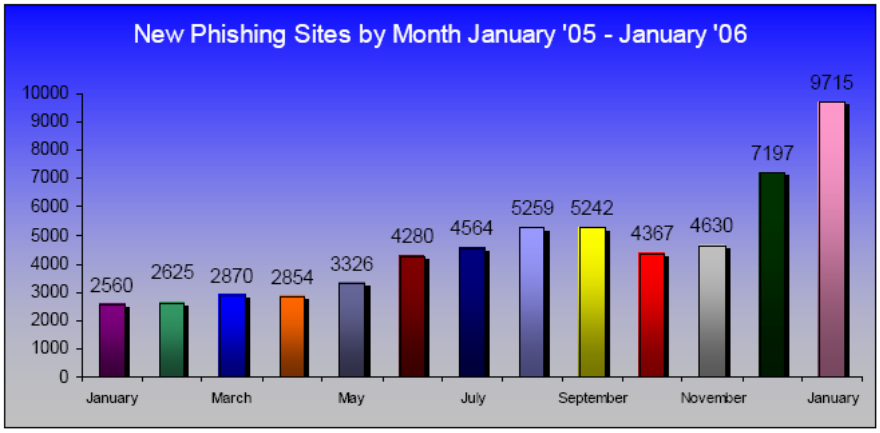
Phishing has become a large concern of those involved in Internet security, as it impacts almost all organizations that do business online. Phishing is largely responsible for the distrust many consumers have of Internet banking. Gartner estimates that in 2003, phishing related losses to credit card issuers in the U.S. was over $1.28 billion (Emigh, 2005).

The researcher defines phishing as: A technique used to deceptively obtain information, including personal data, banking and credit information, passwords and other account numbers from Internet users by using emails and websites designed to look like a legitimate business, financial institution, or government agency. The purpose of obtaining the information is usually to commit identity theft or identity fraud. Phishing is an evolving scam; with every attack comes a new method to help the phisher lure more victims. It is difficult to detect and prevent attacks because they seldom have the same characteristics. There are several different types of phishing attacks including misleading e-mails, man-in-the-middle, URL obfuscation, page content overriding, malware phishing, key loggers and screen grabbers, session hijackers, web Trojans, IP address manipulation, and system reconfiguration attacks.

Not only can several of these schemes be used in conjunction with each other, new permutations appear continually, as the Anti-Phishing Working Group monthly report show (Figure 5). In January 2006, 17,877 unique phishing reports were recorded. January also brought a large increase in the number of unique phishing sites launched

(APWG, 2006). The January number of 9,715, was an increase of 110% since November of 2005, and the growth of unique sites has continued for the past year, as shown by figure 2.7 (APWG, 2006). The January report also showed that ninety-two percent of all attacks were against financial institutions, further damaging trust in online banking (APWG, 2006). The APWG also tracks malware attacks with its reports. In January, the report indicated that phishing trojans reached an all time high; these attacks increased 130% from eight months earlier (APWG, 2006). The APWG reports show that phishing attacks continue to plague online banking and the Internet as a whole.

Figure 5: New Phishing Sites (APWG, 2006)



Phishing attacks are a major problem for consumers and financial institutions. These attacks are growing and evolving at rates that are very difficult for security professionals to keep up with. They also demonstrate the need for stronger authentication in online banking and for all financial institutions.

Data Breaches

Data security is on everyone's mind, from concerned consumers, to privacy groups. Over the past several years, hundreds of data breaches have led to millions of consumers' personal information being lost or stolen (ID Analytics, 2006). These attacks and breaches are occurring at alarming rates. Figure 6 shows a sample of large breaches over a three month time period in the beginning of 2005 (PrivacyRights.org, 2006), including financial institutions, large retailers, and information providers.

This small sample, which only represents a fraction of the total known breaches, shows over 2.2 million pieces of information being lost or stolen. According to ID Analytics, a leader in fraud prevention, fifty-seven percent of breached identities occurred in the financial services industry (ID Analytics, 2006). ID Analytics research also reported that sixty-eight percent of breaches are intentional breaches (ID Analytics, 2006).

Data breaches occurring in large organizations often are highly publicized. The publication of these breaches adds to the uncertainty of many consumers in using Internet banking. Breaches, such as the DSW incident, result in many consumers having account type information stolen, allowing fraudsters to gain the necessary

information they need to replicate a credit card account. Other breaches, such as the LexisNexis breach, permit attackers to obtain identity level information, such as Social Security number, date of birth, and other identifiable information (ID Analytics, 2006). This information also makes it simple for attackers to open accounts and take over accounts in an online environment. These breaches are occurring more often than ever, prompting legislators to begin thinking about stricter legislation.

Figure 6: Sample of Recent Breaches (Privacy Right's Clearing House, 2006)

DATE MADE PUBLIC	NAME (Location)	TYPE OF BREACH	NUMBER
Feb. 15, 2005	ChoicePoint (Alpharetta, GA)	Bogus accounts established by ID thieves	145,000
8-Mar-05	DSW/Retail Ventures (Columbus, OH)	Hacking	100,000
10-Mar-05	LexisNexis (Dayton, OH)	Passwords compromised	32,000
8-Mar-05	DSW/Retail Ventures (Columbus, OH)	Hacking	100,000
18-Apr-05	DSW/ Retail Ventures (Columbus, OH)	Hacking	Additional 1,300,000
28-Apr-05	Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000

Risks Driving the Need for Change

The different types of attacks described above have a huge impact on the consumer, as well as financial institutions. The increased reputation risks and cost pressures on financial institutions exploit the need for stronger methods of authenticating customers as a way to fight against the attacks described above. The main risks that financial institutions face are:

- Loss of Consumer Confidence: "E-Commerce sites represent a multi-million dollar investment as well as a key revenue generating infrastructure for many businesses, especially those in the financial, retail, online auction and Internet Service Provider (ISP) markets" (VeriSign, n.d.). Every time an institution becomes the victim of an attack, customers lose confidence in the institution's ability to protect them on the Internet. Consumers feel very vulnerable when they receive phishing emails or hear of new breaches. Any institution, whether it is a government agency, a retailer, or a financial institution suffers a loss of integrity when it becomes victim of an attack; consumers wonder if the institution can truly protect their identity, when the institution cannot protect itself.

- Reputation Impact: Once an institution becomes victim to an attack its image is damaged, it begins to lose face among competitors, and its integrity is questioned by both consumers and competitors. In a recent interview David Jevans, Chairman of the Anti-Phishing Working Group (APWG), stated "Brand is everything. There is a lot of brand risk. Fraud is easier to sweep under the rug.

It is very different when one million people are getting emails from you. Are they likely to do business with you? What's a bank's whole thing? Security. Safety. Trust. Anything that undermines those things can't be good" (Krebsbach, 2004).

- Financial Impact: APWG estimates a phishing attack can cost a financial institution between $100,000 and $150,000 per attack ("Anti-Phishing," 2004). Some of the costs that are absorbed by a financial institution during and after an attack include response, identification, and clean up. Responding to an attack consists of identifying the source of the email and website and immediately shutting it down. This takes manpower, often causing resources to be pulled away from their other duties. Communications need to be sent immediately to all customers to warn them of the threat and to give them instructions on what to do if they have already fallen victim. Press releases need to be made to the appropriate venues so that people who may do not receive the communications have another means of hearing about the attack (Rasmussen, 2004). Also, once the attack occurs, calls to customer service will start pouring in and the company will have to be ready to handle those calls. One large U.S. bank reported that after a phishing attack they fielded around 90,000 calls per hour (Krebsbach, 2004).

Stronger Authentication

Financial institutions must do more to protect themselves and their customers from ongoing phishing attacks and data breaches. They must ensure that consumers feel safe when using online banking features. While much is being done to control phishing attacks and data breaches, those controls will not suffice in protecting the consumer. Financial institutions cannot stop attackers from launching new attacks, but they can control the level of authentication it takes to enter their sites. They can limit and deter attackers by making it far too difficult to have success in obtaining fraudulent access to a customers account. Financial institutions must move away from today's standard user name and password protocol by implementing stronger methods of authentication. Single factor authentication in online banking is no longer sufficient to protect accounts.

The Federal Financial Institutions Examination Council (FFIEC) issued new guidance on October 11, 2005, requiring banks to reassess their login protocols.
"The FFIEC agencies consider single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."
The authentication guidance requires institutions to implement or have made significant progress in implementing enhanced authentication by the end of 2006. It calls for financial institutions to put into operation enhanced authentication based on the risk of what is offered on their site (FFIEC Guidance, 2005). Now financial institutions not only have the pressure of consumers, but they have a mandate by government regulatory agencies stating they must enhance authentication. Enhanced authentication of the customer at login or while the user is transacting in their online account can be

implemented in a variety of different ways, many of which are based on the factors of authentication.

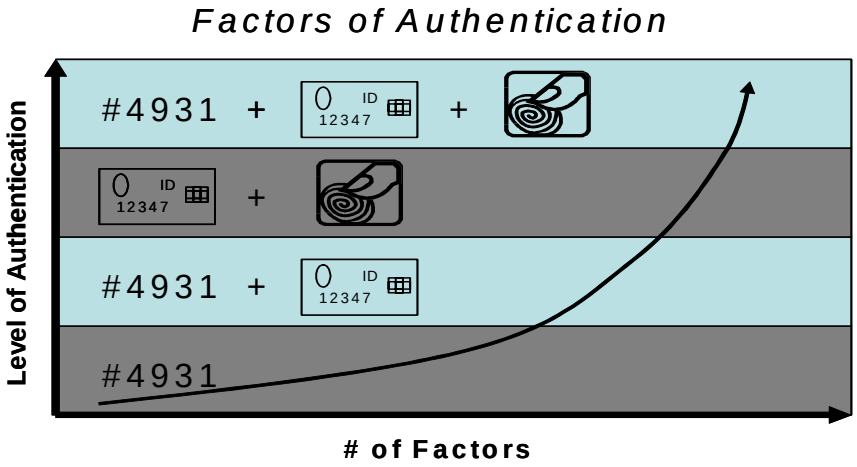
Multi-Factor Authentication

Authentication techniques can be split into three categories.

- Something a person knows: password, PIN, mother's maiden name.
- Something a person has: ID card, key fob, or credit card.
- Something a person is: biometric, voice recognition, fingerprint, facial recognition.

Multi-Factor authentication is using more than one of these factors to make authentication stronger. Figure 7 shows the relationship between the level of authentication and the number of factors. The more levels used in an authentication system the stronger the authentication. As more factors of authentication are added, the security becomes more reliable and the level of fraud deterrence increases.

Figure 7: Factors of Authentication



Most consumers are familiar with using something a person knows, as it is the most widely used. Almost all financial institutions today require at least user name and password to login to online banking. In order to help ensure that customers accounts are safe against attacks such as phishing, financial institutions must use more levels of authentication. By adding another, such as a one-time password token, the phisher may have trouble accessing the account.

Something a Person Knows

While something a person knows is the most widely used (including user name and password, or shared secrets), some would argue that it is the least secure form of authentication as it can be easily compromised. The most common example of a shared secret is a password or PIN (FFIEC, 2005). However, shared secrets also include questions that require specific knowledge of something about the customer. These are questions such as "Which address have you previously been associated with?" or "What is the name of the city you were born in?" Shared secrets are often selected during the initial enrollment process or can be added as an additional security

process after enrollment (Entrust 3, 2005). Often times the customers can select from a list of questions provided by the authenticator or create their own question; the customer then provides the answer to the question. The shared secret can then be used as an additional authenticator when a customer is attempting access. The important thing to remember about shared secrets is that they should be something that is not normally used for account purposes and that only the customer would know.

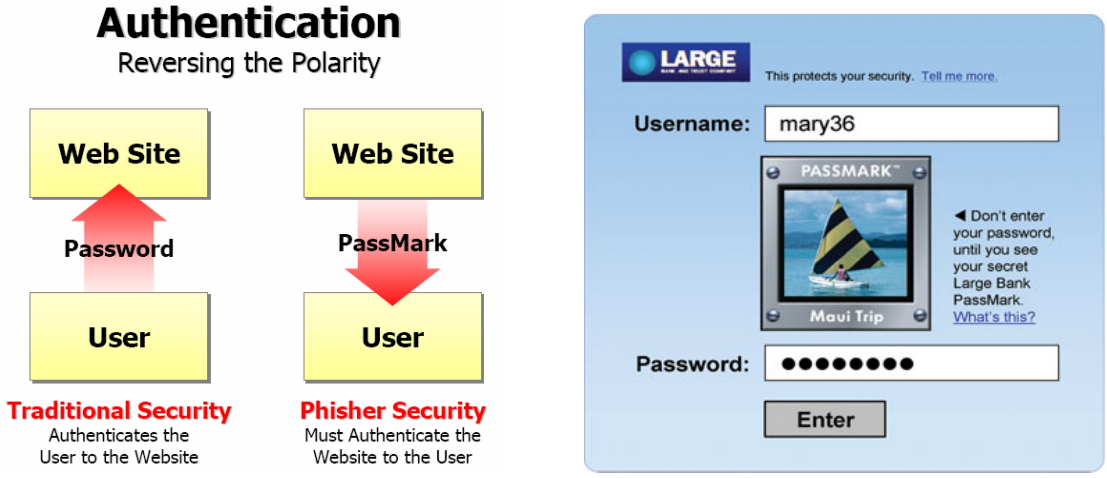
Shared secrets have a low cost to the financial institution, since they can be simply added to the login page and only require the capture of a small amount of additional information (FDIC, 2005). Shared secrets are also very easy to use from a customer stand point. They can be added to a standard login with minimal impact to the customer's login process (FFIEC, 2005). They also require no additional hardware for the customer to buy or install.

A disadvantage of using shared secrets is that since they are stored by the financial institution, they can be easily compromised. Another disadvantage is customers may use the same shared secrets for several different financial institutions, which will increase the probability of the shared secret being compromised.

Mutual Authentication

Mutual authentication is a form of authentication that helps the customer to know they are at the actual site or receiving a legitimate communication from the financial institution (Passmark Security, n.d.). This form of authentication is a reverse of the standard authentication protocol which authenticates the customer to the site. In mutual authentication the site authenticates to the customer (FDIC, 2005). Mutual authentication, such as a small image that the customer chooses, can be displayed to the customer when they load the website or open a communication. An example can be seen in Figure 8. This form of authentication is unique for each customer, giving the customer a tool to help identify that the site they are attempting to access is legitimate.

Figure 8: PassMark Security Mutual Authentication



Mutual authentication specifically addresses concerns raised from phishing and pharming, as the attacker's deceptive email or illegitimate site will not be able to show the customer's self selected mutual authentication (FDIC, 2005). This type of authentication can be very successful in combating the malware type attacks. While The example in Figure 8 is a very sophisticated way of mutual authentication,; financial institutions could also use something as simple as a pass phrase or numeric code that is displayed to the user when they attempt to access a site. This can be less expensive than using a visual such as a picture.

Mutual authentication is a customer friendly authentication tool. It is important that the proper education be conducted so that the customer knows they should not respond to or enter the financial institution's website, unless they see the mutual authentication (Passmark Security, n.d.). A strength of mutual authentication is that it allows the customer to have a higher level of trust in any communication they receive from the institution and it allows customers to feel safe when logging into their accounts. Mutual authentication is a great addition to any authentication protocol. However, it should not be used as an additional way to authenticate the customer, as mutual authentication only enhances the authentication of the site to the customer.

Something a Person Has

Something a person has is the second level of authentication; this level represents some sort of physical device that a person has that may be used in a multi factor authentication protocol. This level of authentication is usually considered stronger than something a person knows. This authentication level could include tokens such as a USB device, a grid card, a smart card, or a password generator. This level could also include out of band authentication, such as a one time password that is emailed or provided via text messaging, as well as PC fingerprinting.

Tokens are a device that the person has in their possession, such as a USB token. The

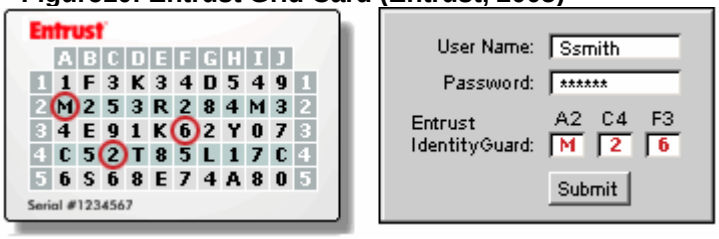
Figure 9: USB Token (Aladdin 2006)

USB token device is a small piece of hardware usually around the size of a key, as shown in Figure 9 (FFIEC, 2005). USB devices are more widely known for their use as memory sticks. Once the computer recognizes the device it can be used as an additional authenticator. Each device contains some sort of unique identifier. When a customer attempts to login to the secure area the system will first look for this device; if the system recognizes the device, the customer will be asked for their password (FDIC, 2005). The use of the USB and password together represent multi factor authentication. Since USB devices are so small they are convenient for a customer to carry and use, and they are not easily tampered with or duplicated.

Grid cards allow additional authentication to be deployed to customers via a printed card. The printed card contains a variety of numbers, letters, and characters arranged

in a grid (Entrust, 2005). The grid card can be distributed to customers and they can be prompted to use the card at login. As Figure 10 shows, the customer would enter their user name and password as well as characters from various random locations on the grid card. Grid cards provide strong security since they allow for different values to be entered during each login. This means that for an attacker to compromise the login credential he or she would have to obtain all of the information from the grid card

Figure10: Entrust Grid Card (Entrust, 2005)



(Entrust, 2005). Grid cards are very cost effective, requiring only a small piece of paper to be sent to the customer. Reissues can be done quickly and with little cost.

Smart cards are basically credit cards that contain a microprocessor chip allowing the card to store and process data (FFEIC, 2005). Smart cards have multiple uses, but most importantly they have the ability to enhance the authentication process. To be read, smart cards require readers to be attached to a computer (FDIC, 2005). The user would simply insert the card into the reader; the reader would validate the authenticity of the smart card, and if it validates, the user would be prompted to enter his or her password (FFIEC, 2005). Smart cards are a relatively simple and very secure form of authentication. They are extremely hard to duplicate and are tamper resistant (FDIC, 2005). Smart cards can be provided to customers as part of their credit or debit card. However, smart cards do have some drawbacks. Since the use of a reader is required, the customer will need to install additional hardware on their computer. This additional hardware can be intimidating and non user friendly, especially for those who are not technically savvy. Due to the need for additional software and the need to issue smart cards, this option can be difficult to justify as a form of additional authentication.

Password generating tokens provide a unique password to the customer at every login (FFIEC, 2005). These devices have a small screen that displays a password for around sixty seconds. The password changes at the end of the time frame, as shown in Figure 11. In a typical set up, the customer will be asked to enter their username and

Figure 11: RSA Password Token (RSA Security, 2005)

password, followed by the current code displayed on the token device (FFIEC, 2005). Password generating tokens provide excellent security due to the unpredictability and randomness they provide.

Password generating tokens can be costly for an institution to deploy, since they must be purchased and distributed to the end user. In some cases, this cost could be absorbed by the customer, however, customers may not want to pay for this additional security. Some financial institutions may benefit from using this solution in a targeted approach. For instance, tokens could be deployed for a high end, high risk account, such as a brokerage account. Another drawback of using a password generating token is whenever the customer wants to access their account they must have their token available to them. This can become burdensome to the customer.

Another form of the "something a person has" method of authentication is known as out of band authentication. This is usually in the form of a one time password. Out of band authentication uses other communication channels to authenticate the customer or a transaction (Entrust, 2005). This method usually consists of the financial institution providing a one time use password or code to the customer for certain login attempts or transactions. Out of band authentication provides a secure and convenient way of authenticating customers by using existing communication channels such as email, text messages to mobile phones, or voice call to telephones. This is illustrated in Figure 12 (Entrust, 2005). For instance, a financial institution may chose to send a one time password to a customer who is attempting to transfer funds to another bank. Before the transaction is completed the financial institution would send the password to the email address on file. In order to complete the transaction, the customer would need to retrieve the one time password and enter it. Out of band authentication provides a simple way to authenticate customers based on information and communication channels that already exist (FFIEC, 2005). No software, hardware, or any additional devices are required. The cost is very low for the financial institution as they can use existing infrastructure to accomplish this form of authentication.

Machine Authentication, or PC fingerprinting, is a developing and widely used form of authentication (FFIEC, 2005). This type of authentication uses the customer's computer as a second form of authentication (PassMark Security, n.d.). Machine authentication is the process of gathering information about the customer's computer, such as serial numbers, MAC addresses of parts in the computer, system configuration information, and other identifying information that is unique to each machine. A profile is then built for the user and the machine. The profile is captured and stored on the machine for future use by the authentication system (PassMark Security, n.d.). Once the PC fingerprint is gathered, the system knows what machine attributes should be present when the user attempts to access their online bank account (Entrust, 2005). This type of authentication usually requires the user to register the machine at first sign on. If a customer logs in from another computer the system will know to further scrutinize the login attempt. At this point the system can prompt for additional authentication, such as out of band authentication or shared secret questions. This method of authentication is widely popular due to the fact that in most cases there is no noticeable impact to the user (FFIEC, 2005). The user does not need to remember any special code or keep track of any extra piece of equipment.

Something a Person Is

The final level of authentication to be discussed is known as something a person is; most often this level will include biometrics. Biometrics is using some type of physical feature of the user as a way to authenticate that user (FFIEC, 2005). It identifies people on the basis of a physiological trait, such as a finger print, a facial structure, voice recognition, or iris configuration (FDIC, 2005). In an online banking environment the most practical form of biometrics is fingerprint recognition. To use biometrics as a form of authentication, the user's feature must be captured. During this process, known as enrollment, samples of the user's traits are gathered and a "template" is created. For instance, if a customer is being enrolled in a fingerprint authentication program, the financial institution would scan the customer's fingerprint and create a template or model to be matched for future authentication (FFIEC, 2005). The template is stored for future use. Once the enrollment is complete, the template can be matched against in future access or login attempts. Biometric identifiers are used in conjunction with a user name and password to create a multi-factor authentication system.

Biometric authentication provides a very strong level of authentication, as it is very difficult to replicate the physiological features of another person. However, this type of authentication does have more drawbacks than other forms of authentication. To use biometric authentication, hardware must be provided to each user, making the cost of deployment expensive. Another cost associated with this form of authentication is storing the template for each customer (FDIC, 2005). This includes the need for significant encryption during storage and transfer process. Biometric authentication is often not perceived as "customer friendly," and many customers may view the use of biometrics as a privacy concern. The average online banking customer may feel that this level of authentication is too strong and too obtrusive for online banking. Another drawback of this type of authentication is the need to have a reader present in order to access the account. In other words, if the user is at a location where a reader is not present, he or she will not be able to login to their account.

Modes of Authentication Implementation

The two most widely used modes of implementation are blanket authentication and risk based authentication. In blanket authentication, the chosen method of enhanced authentication, such as entering the information from a grid card or token, is used at every login attempt. This form of implementation is strong because the customer is always required to use the enhanced authentication. However, for the same reason blanket authentication can have more impact on the customer. This is why some financial institutions prefer to use a risk based authentication protocol.

Risk based implementation allows the financial institution to only trigger enhanced authentication when the risk level is appropriate (Entrust, 2005). Machine authentication is often used in a risk based authentication set up. The machine authentication will run in the background and only ask the customer for additional

authentication if the computer is not recognized. In a risk based authentication system, the institution decides if additional authentication is necessary. If the risk is deemed appropriate, enhanced authentication will be triggered, such as a one time password delivered via an out of band communication (PassMark Security, n.d.). Risk based authentication can also be used during the session to prompt for additional authentication when the customer performs a certain high risk transaction, such as a money transfer or an address change (Entrust, 2005). Risk based authentication is very beneficial to the customer because additional steps are only required if something is out of the ordinary, such as the login attempt is from a new machine.

These two types of implementation modes can be used in conjunction with any of the methods of enhanced authentication. Financial institutions must decide which one suits their needs the best and understand how much impact they want to have on the customer login experience.

Gathering Knowledge From Industry Experts And Consumers

In order to provide a clear, well rounded set of guidelines for implementing enhanced authentication, the researcher used a combination of his own professional experience, knowledge from industry subject matter experts, and data from a detailed survey.

In order to gather the appropriate insight and set forth the appropriate guidelines, the researcher conducted a series of six interviews with industry subject matter experts. The interviews were open discussion in format and aimed at gathering insights from the participants regarding their experience with this topic. The interview population consisted of three categories. The first was an interview of two professionals who have played an integral part in implementing enhanced authentication solutions for their institutions. In these interviews, the researcher discussed the participants' thoughts on enhanced authentication, roadblocks they faced, and any advice they would want to share. The second category focused on people who are in the process of implementing a solution for their institution. These interviews discussed some of the same topics as the first group. The third and final category focused on experts from vendors who provide solutions to financial institutions for enhanced authentication. With this final group the researcher discussed the interviewees' views on the best solution for authentication and what vendors can offer to make the process easier on an institution.

One of the major concerns of financial institutions is how implementing enhanced authentication will impact customers. In order to measure this, the researcher conducted a comprehensive survey, which was distributed to 324 people, to poll their feelings and attitudes towards stronger authentication in online banking. The survey was conducted using surveymonkey.com, a widely used online survey company. The survey was distributed to employees of a financial institution located in the Cincinnati area. It was sent via an email to each employee's work email address. The email contained a brief overview and description of the survey's purpose. A copy of the email can be found in Appendix 1. The sample produced a diverse range of experience and

knowledge in regard to authentication and online banking. It appears that there may be a small percent of respondents who have a strong understanding of enhanced authentication, but the majority of the respondents had little to no knowledge of online banking authentication. The participation in this survey was completely optional, so all participants chose to participate on their own accord.

The survey questions focused on what consumers feel is an acceptable level of authentication, how much change they will accept, and how much inconvenience they will tolerate. The questions were mostly closed-ended questions. The closed-ended questions allowed the researcher to gather the information needed, while making it simple for the user to complete the survey. The survey focused on five categories: demographical data, online banking usage, online banking security concerns, current login authentication, and additional login authentication. The survey can be found in Appendix 1.

Interview Results

The information gathered during the six interviews focused on the areas of implementation, customer impact, and business impact. The interviewees were very forthcoming with their experiences and feelings regarding the questions they were asked. While the researcher had hoped to interview between nine and twelve industry experts, it became very difficult to obtain the cooperation of industry experts who were directly involved in enhanced authentication for online banking. Some contacts were reluctant to participate because they did not want to give out too much information regarding their business. Another obstacle the researcher faced was the timing of the interviews. The interviews all took place during the summer months, when many industry professionals take vacations. This made scheduling difficult and also impacted the number of interviews that were conducted. Another obstacle was many of the interviewees have meetings, conferences, and other business that must be attended to first. Scheduling around the needs of the interviewees proved difficult. However, even with the obstacles it was possible to set up time with the six interviewees and engage in meaningful discussions.

The first part of the interview focused on what the interviewee saw as the main advantages of enhanced authentication. The three main responses that were discussed by the interviewees were to strengthen security of the online banking site, to increase customer confidence in online banking, and to comply with federal regulations. When discussing the drawbacks of enhanced authentication, one theme that emerged was the possibility of creating a false sense of security for the customer. Interviewees felt that it was possible the customer could feel too secure, even though there is no silver bullet for security. The customer would still need to be educated on the fact that additional authentication enhances the customers security greatly, but there is always a risk of compromise.

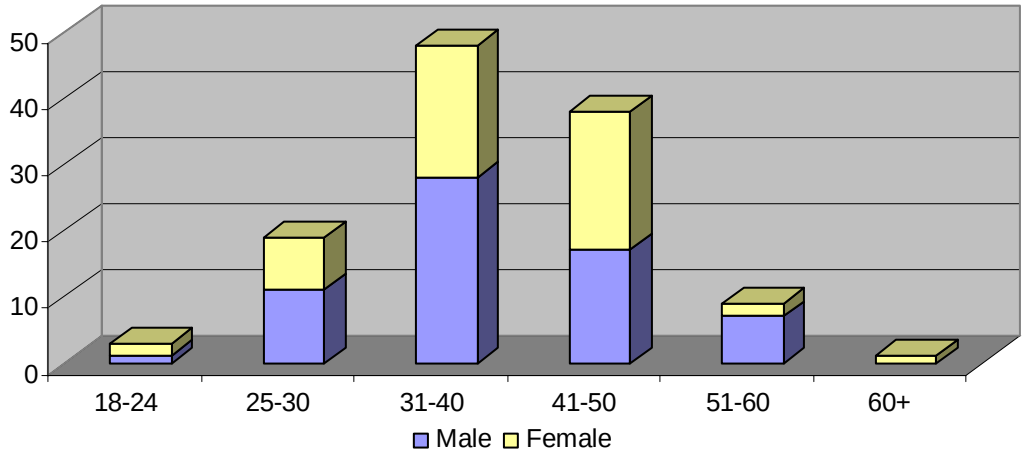
Customer acceptance and impact was another main discussion point during the interviews. Interviewees agreed on the fact that regardless of how much impact the

changes will have on the customer, it is important that communication to the customer be clear and concise. Education should take place early and be ongoing to ensure that the customer fully understands the goals of the enhancement, as well as the limitations. Another theme that came out of the discussions was that the interviewees felt there was a split in customer opinion about whether the authentication should be something that is visible or physical or something that is done behind the scenes. The view was that some of the population likes to have something there to make them feel safer, while some prefer no change to the existing process.

Results of the Online Survey

The survey produced one hundred nineteen responses during the three weeks it was open. This represented a thirty five percent response rate in the survey. The first two questions in the survey focused on demographics of the respondents. The survey was

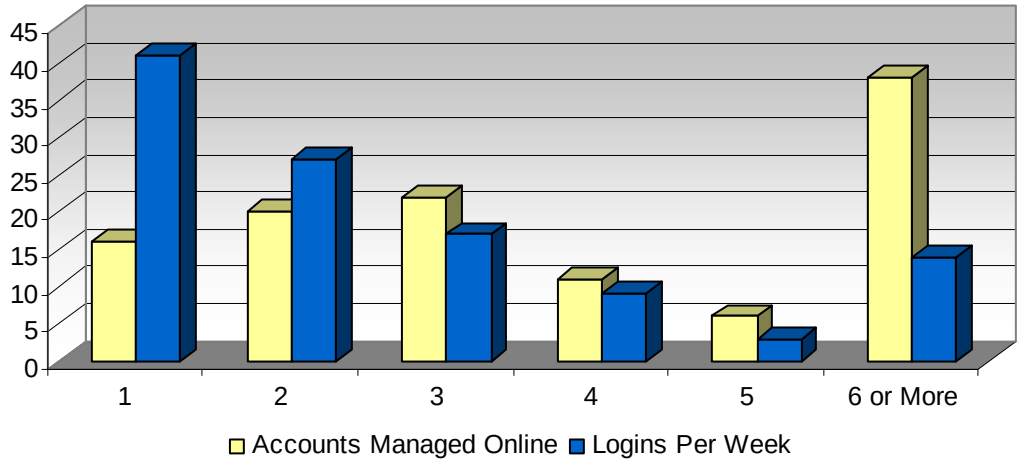
Figure 12: Age Range by Male vs. Female



relatively even in terms a male to female ratio, with sixty-five respondents being male and fifty-four respondents being female. The majority of the sample was between the ages of thirty-one to forty, which represented thirty-nine percent or forty-eight respondents, as shown in Figure 12.

The next four questions focused on the respondent's typical usage of online banking.

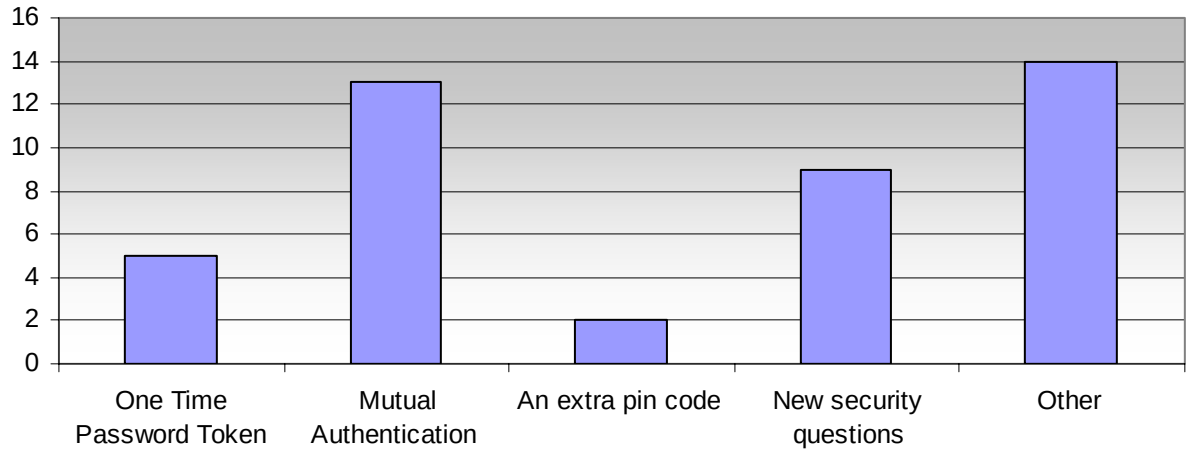
Figure 13: Logins Per Week & Accounts Managed Online



An overwhelming ninety-five percent of the respondents stated that they use online banking, and about forty-eight percent of those who do bank online manage four or more accounts. Fifty-two percent of the respondents stated that they manage three or fewer accounts online. Of those respondents who indicated they bank online, thirty-five percent stated they login to their account once a week, twenty-three percent said they login twice a week, while the remaining forty-five percent login three or more times per/ week, as shown in Figure 13. When asked about specific functions being performed online, seventy-nine percent of respondents said they use the online bill pay option and eighty-six percent of respondents prefer to update information, such as address and phone number, online.

The third section of the survey asked respondents about the current login procedures they experience during their banking online. The first question in the section asked respondents if the only login credentials required were user name and password. Eighty-seven percent stated that only these two were required, while thirteen percent indicated that some sort of additional piece was required. When asked if any noticeable changes had been made to their bank's login process in the last six months, one third of the respondents said that they did notice changes. The most prevalent change noticed by the respondents was the addition of mutual authentication, such as a unique picture displayed at every login. Thirty-percent of those who had noticed some change in their login process stated mutual authentication has been added. The second most prevalent addition to authentication was the introduction of new challenge questions, such as "What is the city you were born in?" Twelve percent indicated the addition of a one time password token and five percent stated an extra PIN was added to the login process, as shown in Figure 14. Other changes noticed by respondents include the use

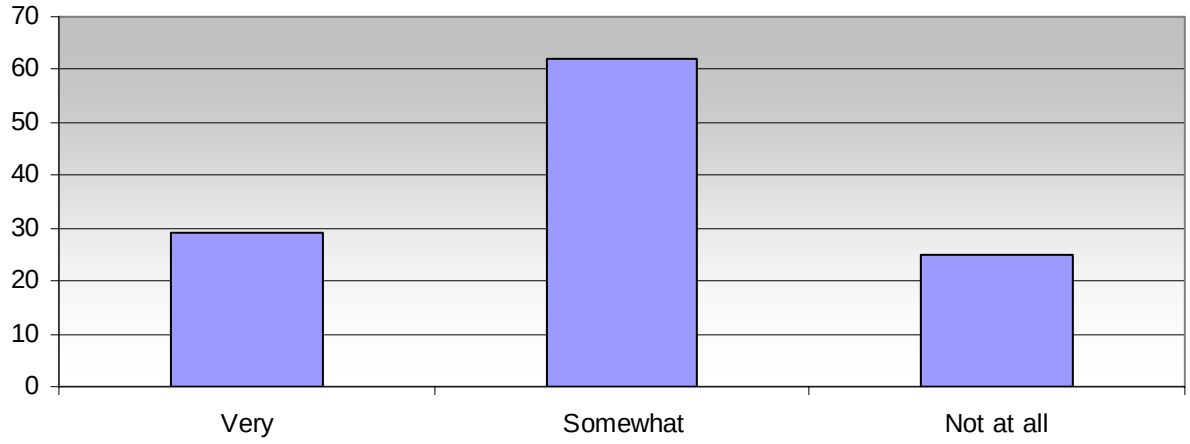
Figure 14: Authentication Noticed by Respondents



of a dynamic key board for pin entry, where the customer enters his pin through a keyboard that is displayed on the screen rather that using the standard keyboard, the elimination of Social Security number as a user name, and a self selected PIN that is displayed to the customer prior to login.

The next section of questions focused on consumer perceptions with online banking. The first question in this section asked respondents how concerned they are about their online accounts being compromised. Fifty-three percent stated they were somewhat

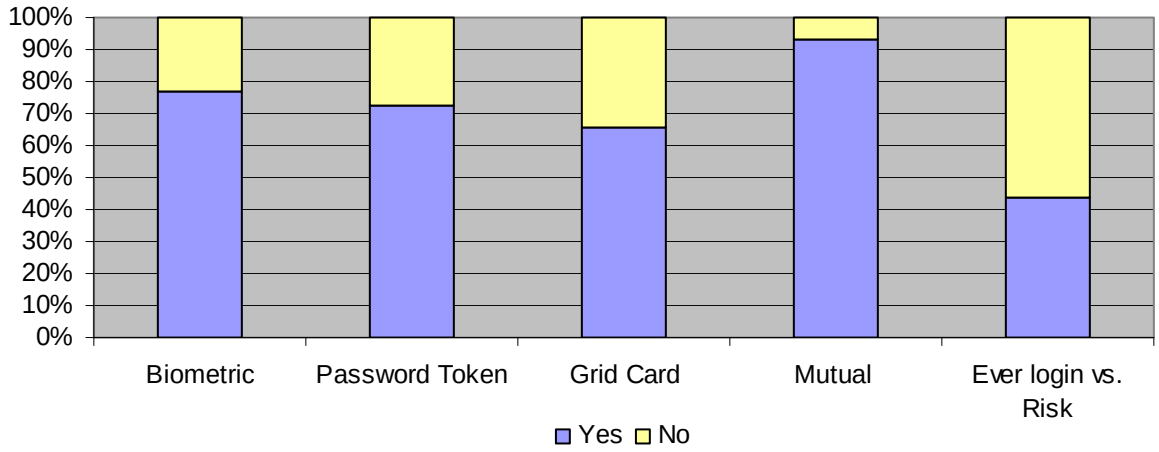
Figure 15: Concern Level



concerned, twenty-five percent said they were very concerned, and twenty-two percent said they were not concerned at all, as shown in Figure 15. When asked if they the felt their bank was doing enough to protect their online accounts, seventy-seven percent of respondents stated they felt their bank was doing enough to protect them. When asked if the respondent had ever received a phishing email, sixty-three percent said they had and only one percent had responded to the email.

The final section of the survey asked respondents about their comfort level with enhanced authentication. The first question asked the respondent if they would be willing to use additional authentication besides username and password. Ninety-five percent of the survey respondents indicated they would use additional authentication. In order to understand what types of authentication the customer felt was acceptable, the survey asked about specific forms of authentication. When asked about using a biometric based authentication tool such as a fingerprint, seventy five percent stated they would use a biometric based authentication tool. The next form of authentication presented was a password generating token. Seventy-three percent of the respondents indicated they would be willing to use this type of device. When asked about using a grid card type authentication tool, forty-five percent indicated they would not use this

Figure 16: Respondents Acceptance of Authentication Methods



type of authentication tool, as shown in Figure16. When asked about using mutual authentication, such as a picture, for online banking, ninety-three percent of the respondents indicated they would use this type of authentication. Respondents were then asked if they preferred additional authentication that may take longer at every login or only when the bank identified there was great enough risk to prompt for additional authentication. Over half of the respondents stated they prefer only when the bank deems the risk great enough, with fifty eight percent preferring the risk based approach. The final question asked the respondent if they would be willing to pay for any type of additional authentication. Ninety five percent indicated they would not pay for any type of additional authentication.

Discussion Of Research

The survey that was conducted by the researcher helped to provide an understanding of the feelings of consumers who use and do not use online banking. The survey demonstrated the respondents were in large part online banking users and that the majority of the users would be open to enhanced authentication. However, it is important to note that the fact that the survey was distributed to employees of a financial institution, may have influenced that. The survey was sent to three hundred and twenty four employees of a large global employer. The researcher was hoping to distribute the survey to approximately six hundred people, however, due to a site consolidation at the

location, several employees had already moved to a new site. When contacting other sites of the employer, the researcher found that their policies prevented them from sending this type of survey to employees. This decreased the sample size. The survey was taken by one hundred nineteen respondents, representing a thirty seven percent response rate. The response rate was very strong and exceeded the researcher's expectations.

The survey found that over forty-five percent of respondents manage four or more accounts online and of that two thirds manage six or more accounts online. This demonstrates that many users are turning to the online channel to manage their accounts. The survey also showed that of the sample population, seventy-one percent of the respondents log into their accounts between one and three time per week. This indicates that the average user logs into their account at least once every three to four days.

An interesting result of the survey was that eighty-eight percent of respondents indicated that their bank only requires username and password when logging in. Many financial institutions are moving to implement stronger authentication to protect themselves and the customer and to meet FFIEC guidelines. This shows that many banks either have not implemented new authentication or have chosen to implement some form of backend control. To further drive this point, thirty-seven percent of respondents indicated that while they had been notified by their bank in the last six months that changes would be made to their login process, they had not yet seen any noticeable changes. The researcher believes that many of these banks are notifying their customers well in advance to ensure that there are no surprises when changes actually do occur. When conducting interviews with the subject matter experts, the researcher found that all of those interviewed agreed that financial institutions should make clear communication to the customer very early in the process. The interviewees felt that this will help to eliminate any surprises and allow time for the customer to learn about the changes.

Of those respondents who indicated they have seen additional authentication, thirty-percent indicated they saw mutual authentication, such as a picture. This is not surprising, as one of the nation's largest financial institutions has recently implemented a solution that includes mutual authentication. The researcher was surprised by the fact that a small number of respondents indicated their bank is using a token as the additional form of authentication. It would have been beneficial to understand the type of online account, i.e. brokerage or high yield savings.

The survey showed that a large segment, ninety-five percent, of respondents bank online and many manage multiple accounts online. However, in the same population twenty-five percent of respondents indicated they were very concerned about their online bank account being compromised and another fifty-three percent stated they were somewhat concerned. This may show that while the concern is present for many customers it is not strong enough to stop them from using online banking. One of the subject matter experts mentioned in the interview that the customer is not liable for the

losses if his or her account is compromised or taken over. He pointed out that when this occurs the financial institution is liable for the losses.

The final section of the survey was aimed at determining customers' views of enhanced authentication. This section asked specific questions about types of authentication and how comfortable the user would be with using them. The researcher was somewhat surprised that ninety-five percent of the respondents were receptive to the idea of enhanced authentication. The researcher believed this number would be high, but the response was overwhelmingly in favor of enhanced authentication. The results of the question asking if respondents would be open to using biometric based authentication were unexpected as well. Seventy-six percent of the respondents indicated they would use this type of authentication. The researcher expected this result to be more around twenty to twenty-five percent. It would have been beneficial to ask participants more probing question regarding what types of biometrics they would be open to using and also to understand what concerns those who were not open to using biometrics had. These findings may indicate that some consumers are beginning to warm up to the use of biometrics. Many computer makers are now including fingerprint recognition technology on laptops as an authentication method for logging into the computer. The fingerprint is probably the most widely used form of biometric authentication today. However, if an institution chooses to implement a biometric form of authentication, the researcher firmly believes they would have to have an alternate form for those customers who have strong privacy beliefs.

Customers supported using a biometric slightly more than they supported using a token. Seventy-three percent of respondents indicated they would be willing to use some sort of token as a means of authentication. This was also slightly higher than expected by the researcher. Since this type of authentication requires the customer to have the token with them to log into the account, the researcher thought that the respondents might prefer not to use this type of authentication method. The same can be said for the grid card, which was slightly lower than the token; forty-five percent indicated they would not use the grid card. The token may have been slightly higher because people view this as a safe and sound form of authentication; respondents may have seen this as a more secure way of protecting them. The respondents may not have placed much emphasis on convenience for this question. Another reason respondents may be more receptive to biometrics is that it is easy to use, in the sense that it is always with you. Fingerprints, voice prints, and other forms of biometrics are literally a part of the customer, where a token or grid card may not be something a person carries on them and it could easily be lost. In hindsight, the researcher sees that it may have been beneficial to ask the respondents which one of these solutions they prefer. The questions in the survey simply presented each solution and asked if the respondents would be open to using it. This additional questions would have allowed the researcher to analyze what respondents felt were their top choices for implementation.

Mutual authentication is becoming a widely used form of authentication to help protect customers from phishing attacks. This form of authentication is very customer focused, and provides the customer with a way to have more confidence that they are actually at

the legitimate site. The survey results indicated that ninety-three percent of the sample would prefer to use some sort of mutual authentication. This form of authentication was overwhelmingly accepted by the respondents and may indicate the consumers' preference to see some sort authentication. The researcher believes that mutual authentication boosts the customers' confidence in the security of the web site. On the other hand, the subject matter expert interviews revealed that the interviewees believed consumers actually are split fifty/fifty. Many consumers prefer to feel safe and like the added security and visual effects that indicate they are secure, while others do not want the hassle of having to look for a picture or any additional steps when logging into their account. The results of a question asking whether customers would rather have multi-factor authentication at every login or only when the bank deems the risk is high enough (as described in the risk based authentication section) indicated that forty-four percent of respondents preferred every login. The remaining fifty-six percent of the respondents preferred only when the bank deems the risk great enough. The findings of this question support the beliefs of the interviewees.

A major takeaway for financial institutions from this survey is that ninety three percent of respondents stated they would not pay for enhanced authentication. This indicates that customers expect stronger authentication in their online banking experience, but they expect the bank to provide it as a standard feature and not as a cost to the customer.

Guidelines for Implementing Enhanced Authentication Solutions

In order to provide a resource to help drive successful implementation of enhanced authentication in online banking, the following guidelines are presented. These guidelines were developed based on the consumer survey, interviews with industry experts, extensive research, and professional experience. These guidelines are intended to provide a roadmap for implementing stronger authentication with both the business and customer needs in mind.

1) Clearly define what you are solving when implementing enhanced authentication.

Enhanced authentication can solve several different problems, but in order to implement the correct solution one must understand what is being solved. There are several different reasons for enhancing authentication of a financial institution website: strengthening a weak security protocol, helping to control fraud loss dollars, increasing customer confidence and usage, and/or complying with federal requirements. Whether implementing for one or more of these reasons, it is important to clearly understand what is being solved as this will aid choosing the right solution.

2) Complete a risk assessment to evaluate the risk associated with the specific services and features offered on the financial institution's online servicing site.

In order to ensure the appropriate authentication levels are being deployed, a thorough risk assessment of the entire online banking system should be conducted. According to the FFIEC risk assessment guidance, "A risk assessment is a necessary prerequisite to the formation of strategies that guide the institution as it develops, implements, tests,

and maintains its information systems security posture" (FFIEC Information Security Guidance, n.d.). A successful risk assessment for implementing enhanced authentication for online banking should evaluate the current login process, the transactional capabilities, the customer information that can be viewed, the volume of transactions and logins, and the type of accounts being accessed, for instance, credit cards, consumer vs. business accounts, and/or checking. It is important to remember to not only evaluate the risk to the institution when completing a risk assessment, but the risk to the customer. Often institutions look at the risk assessment as a way to measure the risks to the institution; however, they must remember they have an obligation to protect the customer. As required by section 501(b) of the GLBA, financial institutions must "protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer." Risk assessments should be used to evaluate the risk present on the online servicing site as a way to help guide the institution in selecting the appropriate enhanced authentication solution. A risk assessment template is provided in Appendix 2.

The risk assessment will help to evaluate the need and level of authentication that is necessary. The risk assessment should assess the functionality that is available on the website, such as money transfer, bill pay, account maintenance and any other features. It should also review the current security features and the user information, such as the number of users and their average balance.

3) Understand the various types of solutions available for multi-factor authentication.

When implementing a multi-factor authentication solution, it is important to first understand all of the forms of authentication available. It is important to understand the main characteristics of each form of authentication, including the cost range, the level of authentication provided, the longevity of the solution, the customer impact, and the ease of use. By gaining an understanding of the types of authentication available and clearly understanding what the solution is solving for, it will become simpler to select an enhanced authentication solution.

4) Evaluate the impacts, both positive and negative, to the customer experience.

Perhaps one of the most important pieces of implementing multi-factor authentication is evaluating the impact to the customer's experience. Depending on the type of authentication chosen the customer's impact can vary greatly. Some solutions can be implemented without the customer knowing any change has occurred. Other solutions may require the customer to go through an enrollment process, and additional solutions may require the customer to have physical instruments in hand to access their account. Financial institutions should determine how much impact they are comfortable with imposing on the customer.

Whenever possible, financial institutions should survey existing users to understand what level of impact they will be comfortable with. Financial institutions could also conduct focus groups to solicit customer feedback. In the survey conducted for this paper, the researcher found that ninety-five percent of consumers who were surveyed

would be receptive to additional authentication and seventy-two percent of those surveyed would even utilize a token form of authentication. It is ultimately the financial institution's responsibility to determine the impact to the customer. However, it is important to remember that a bad customer experience could cause customers to move away from the less expensive online channel or to choose a new financial institution.

5) Evaluate the cost of implementing each solution as well as the benefit the solution will provide.

Carefully weigh the cost of the solution with the benefit it will provide. It may be beneficial to quantify the loss amount currently occurring as a result of attacks, such as phishing. There may be numbers used in the cost benefit calculation that are difficult to measure, but will have a huge impact on the organization. Examples of this include, but are not limited to, customers who may begin using the online channel because they feel safer, thus saving the institution money by having less branch transactions. Another example is the cost of losing customers because they do not feel safe. In most instances, the cost benefit for enhancing authentication can be easily justified simply because of the marketing benefit strong authentication can provide.

6) Evaluate developing an internal solution or a vendor solution.

There are many solutions that can be implemented for enhanced authentication, and some can be implemented internally without the use of a vendor. For instance, some financial institutions use a form of mutual authentication where the customer chooses a four digit code, and every time they login, the code is displayed on the login page. This is a relatively easy way to show the customer that the site they are at is legitimate. Internal solutions can be a quick and easy way to implement enhanced authentication. On the other hand, many vendors specialize in specific forms of authentication. For instance, RSA Consumer Solutions has as suite of products for all levels of enhanced authentication for online banking. These vendors have expertise and can implement solutions quickly and often for a low cost.

7) Select a solution that meets the specific needs of the organization.

One of the most difficult steps of implementing multi-factor authentication is choosing the correct solution that meets all objectives of project. First evaluating all of the subjects described in the previous guidelines, may make the choice simpler. Ensure that the solution that is chosen corresponds with the level of risk identified in the risk assessment and meets the customer impact findings that were concluded from surveys or focus groups.

It is important to remember there is no perfect solution; in fact, there is no such thing as perfect security. A solution must be chosen to meet the needs of the specific financial institution. The following are additional guidelines derived from interviews with industry experts who have been actively involved with implementing enhanced authentication.

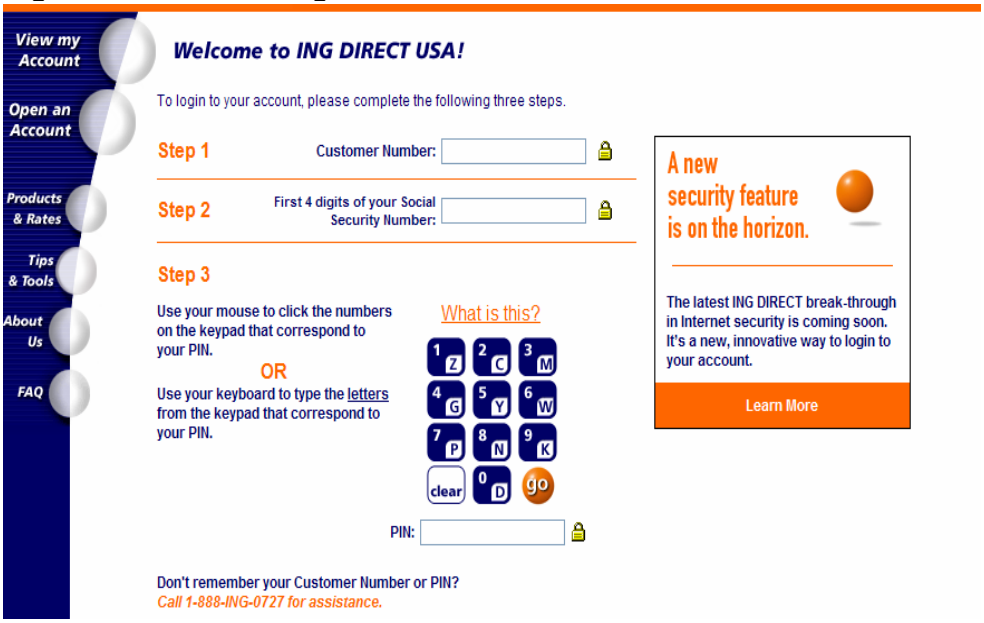
a. Choose a solution that can be used enterprise wide, allowing for management of one system and providing a consistent solution for the customer.

b. Select a solution that can be easily integrated into the existing architecture of the website. This will limit the amount of confusion to the customer.
c. Ensure the solution is "user friendly." Limit the amount of impact on the customer as much as possible.
d. Include authentication that the customer can visibly see or recognize. This will help to reemphasize that the institution is working to protect the customer.
e. When possible, choose a solution that requires no hardware or software for the customer to install. This will prevent customers who are not "technically savvy" from having a bad user experience.
f. Many solutions on the market today offer fraud databases and modeling that can predict if the login attempt is from a fraudulent customer or if the IP address that the login attempt is coming from has been used by a fraudster in the past. Choosing a solution with this functionality will help to protect the bank and the customer.
g. Ensure the solution is going to last for several years and can be easily updated. This will help to prevent frequent changes to the customer's login experience.
h. Protect against man-in-the-middle attacks. As financial institutions tighten their authentication protocols, attackers will use more man-in-the-middle attacks. Many risk based authentication systems protect against these attacks by identifying the machine attempting login.

8) Communicate to the customer

Once a solution is chosen, if any noticeable change to the customer experience is occurring, begin notifying the customer. It is important to make the change for the customer easy and unsurprising. An immediate change may make the customer wary and increase calls to the bank. Whenever possible begin communication several weeks ahead of time. Let the customer know that changes are being made to protect their

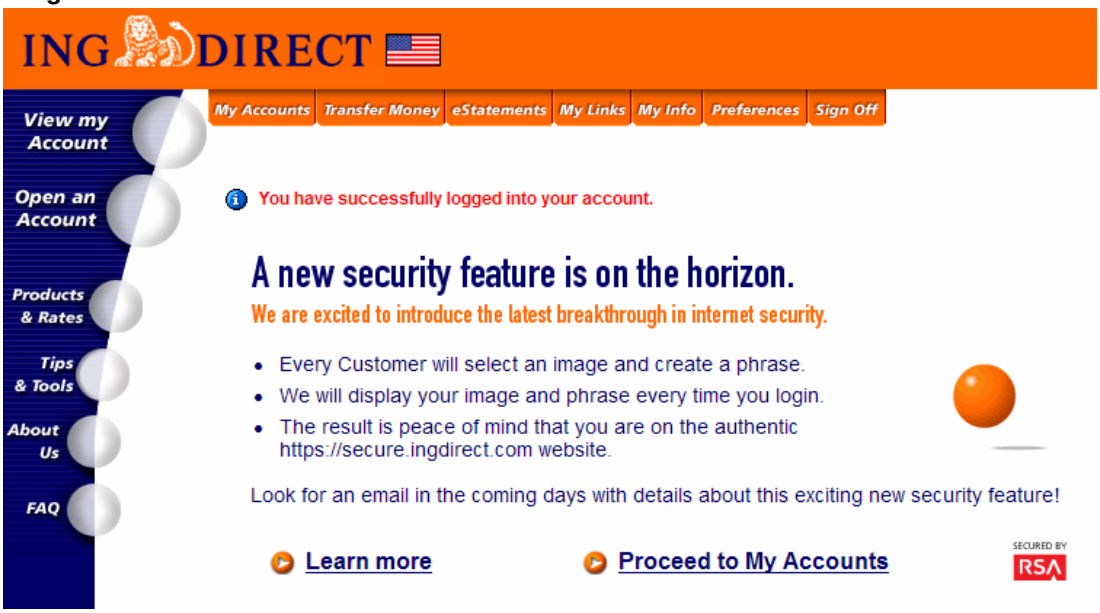
Figure 17: ING Direct Login



accounts. For instance, on this login page for ING Direct (Figure 17), a message is displayed noting that changes are coming to the login process.

Once the customer logs into their account successfully, they see a full page message explaining that new security features are coming and information about the features, as shown in Figure 18.

Figure 18: ING Direct Communication



This example paints a clear picture to the customer that changes will be made to the login process shortly and that the customer will be required to enroll in the new process.

Implementing new authentication, even the smallest change, can have a significant impact on the customer experience, making it important that the customer is aware of any change that will affect what they are used to. The communication part of implementation can also be used as a marketing tool. Customers are very wary of their security as it relates to online banking. In fact, the researcher's survey showed that seventy-eight percent of respondents indicated they were somewhat or very concerned about their account being compromised. By using authentication enhancements as a way to market to customers that the institution is making changes to protect the customer, the institution can reassure current customers and possibly win new ones. According to a subject matter expert, interviewed by the researcher, "Customers like to know something is being done." Several of the interviewees also discussed the importance of providing a page that discuses, in detail, the changes being made, providing training to the customer when necessary, and providing a FAQ section for the customer to review. Financial institutions should also explain to the customer that by making changes and enhancing authentication, the institution will be able to provide more services to the customer in the online channel. This will help to make the user experience more enjoyable.

9) **Implement tracking to evaluate the effectiveness of the solution.**
In order to measure the effectiveness and performance of a solution it is recommended that tracking be put in place. Tracking may look at the number of times good customers are unable to login, the number of times frauds are able to login, the number of times fraudsters are stopped, and many other measures. It is also recommended that surveys and focus groups be conducted with customers post implementation. Tracking measures will help to fine tune the solution.

10) **Continue to evaluate the effectiveness of the solution and the customer experience.**
Because fraud and Internet security are always evolving areas, fraudsters will continue to break any controls implemented. It is important to continue to measure the effectiveness of the authentication controls and how customers perceive them. As fraudsters develop new ways to circumvent the controls, the financial institution must evaluate existing controls. It is important to implement a solution with a long shelf life and one that can be easily updated.

Conclusion

It is evident that online crime and fraud against online banking is not going away and will only continue to grow and adapt. Over the past several years, the industry has already seen an enormous amount of adaptation from online criminals attempting to steal the information of unsuspecting consumers. Financial institutions see the Internet as the banking channel of the future and will continue to move more products to it to help reduce their costs and increase convenience for the customer. Fraudsters know this and see the opportunity to steal information and money without ever leaving their computer desk. Financial institutions have long relied on user names and passwords as a means of protection and authentication for the customer. However, as riskier products are moving to the online channel, such as bill pays and money transfers, this once standard form of authentication is no longer strong enough to protect the bank or the customer. Fraudsters have mastered the art of phishing and continue to transform their attacks to steal information from consumers. This has prompted the need for stronger authentication to help control who is accessing online banking sites and performing risky transactions. Enhanced authentication is one way of helping to secure customers and protect the banks reputation.

There is no “silver bullet” when implementing enhanced authentication. It is important that each individual financial institution decide the right form of authentication for itself and its customers. Every financial institution will face obstacles specific to its institution while implementing enhanced authentication. The important thing is that each institution evaluates its needs and selects the appropriate form of authentication. By using the guidelines that were developed as a result of consumer research and industry expert knowledge, the researcher believes that a financial institution will be able successfully choose and implement the appropriate solution with fewer obstacles.

Over the past several months, the researcher has been involved in the planning and researching of solutions for enhanced authentication in online banking, as well as conducting in depth research on this topic. The results of this research study demonstrate the need for enhanced authentication in online banking. The federal government has issued regulations to ensure that financial institutions are performing the right authentication to protect their customers. Additionally, media outlets around the world continuously highlight data breaches and scams that target the safety of online banking. Several initiatives have begun to help prevent these scams and deter criminals from launching these attacks. We will never be able to stop the attacks, but financial institutions can do more to control who accesses their sites by enhancing the authentication techniques and controls they use. The information presented here is to be used as a roadmap for implementing enhanced authentication and selecting the appropriate tools to do so.

During the research process several ideas for continued research became evident. Some areas may provide the industry with important knowledge, including using authentication tools such as PC fingerprinting for opening new accounts in an online environment. In other words, how can these tools be used to authenticate new customers for financial institutions? Another research topic suggestion would be to evaluate the success of some of the enhanced authentication programs that different financial institutions have implemented. Hopefully, many other research projects will come out of this one to advance the industry and to ensure that all financial institutions have the right tools and information to provide protection for customers and their personal information.

About the Author

Greg Williamson is currently a Manager of Fraud Strategy at GE Money – America's in Cincinnati, OH. He has a Bachelor of Science Degree in Economic Crime Investigation and Masters Degree in Economic Crime Management from Utica College. He can be reached at gregorydwilliamson@gmail.com.

Appendix 1
Survey Email

This survey is being conducted to help obtain an understanding of consumer's attitudes towards online banking. The results of this survey will be used in a professional thesis regarding Enhanced Authentication in Online Banking. The thesis is being completed as part of the requirements for completion of a Masters Degree in Economic Crime Management at Utica College.

This survey is completely voluntary and the results are anonymous. The survey should not take more than 5 minutes to complete.

Your participation is greatly appreciated.

Thanks,
Greg Williamson
Fraud Strategy Analyst

Survey

Survey Overview
The online banking environment has grown tremendously over the past several years and will continue to grow as financial institutions continue to strive to allow customers to complete money transfers, pay bills, and access critical information online. During this same time, online banking has been plagued by Internet criminals and fraudsters attempting to steal customer information. Phishing, pharming and other types of attacks have become well known and are widely used as a means for fraudsters to obtain information from customers and access online banking accounts. As a result, authenticating customers logging onto their online banking service has become a crucial concern of financial institutions.

This survey is being conducted to help obtain an understanding of consumer's attitudes towards online banking. This study is being conducted by Greg Williamson, a graduate student at Utica College, 1600 Burrstone Road, Utica, NY 13502. The results of this survey will be used in a professional thesis regarding Enhanced Authentication in Online Banking. The thesis is being completed as part of the requirements for completion of a Masters Degree in Economic Crime Management at Utica College.

This paragraph outlines your rights as a participant in this survey of Enhanced Authentication for Online Banking. The survey will explore the participants thoughts and feelings relating to enhanced authentication for online banking. This survey is intended to help gather insight into implementing stronger authentication for customers of online banking. It will provide detailed analysis of the many authentication solutions available and it will provide a set of guidelines for selecting and implementing enhanced authentication, based on the learning and knowledge of industry experts as well as the consumer.

Questions related to this project may be directed to Greg Williamson at (513) 826-1975.

It will take about 5 minutes of each respondent's time.

I understand that
1. Taking part in this study is entirely voluntary.
2. It is my right to decline to answer any question that I am asked.
3. I am free to end the survey at any time.
4. My name and identity will remain anonymous in any publications or discussions.
5. The company name will remain anonymous in any publications or discussions.

Please click on "Next" to begin the survey and thank you for your participation.

Demographics

1. Please indicate you sex:
   ☐ Male
   ☐ Female

2. Age Range:
   ☐ 18-24
   ☐ 25-30
   ☐ 31-40
   ☐ 41-50
   ☐ 51-60
   ☐ 60+

Online Banking Usage:

3. Do you currently use any type of online Banking or Online Account Management (i.e. Checking account, Savings, Accounts, or Credit Accounts)?
   ☐ Yes
   ☐ No

4. If yes, to question 3, how many accounts do you currently manage online?
   ☐ 1
   ☐ 2
   ☐ 3
   ☐ 4
   ☐ 5
   ☐ 6 or more

5. How many times a week o you log in to your accounts?
   ☐ 1
   ☐ 2
   ☐ 3
   ☐ 4

☐ 5
☐ 6 or more

6. Do you use online bill payments options?
   ☐ Yes
   ☐ No

7. Do you prefer to update your account (i.e. email changes, phone changes, address changes) online?
   ☐ Yes
   ☐ No

Login Authentication

8. When logging into you account, does you bank require only user name and password?
   ☐ Yes
   ☐ No

9. In the last six months, has your bank made any changes to your login process?
   ☐ Yes
   ☐ No

10. If yes, were any of the following added?
(Choose all that apply)
☐ One Time Password Token
☐ Mutual Authentication such as a Picture
☐ An extra pin code you must enter
☐ New security questions, such as city you were born, favorite pet, etc.
☐ Other

Please explain any of the options selected above?

11. In the last six months, has your bank or financial institution informed you that changes had been made to their web site to protect you account, but you have not seen or noticed any difference?
   ☐ Yes
   ☐ No

Online Security Concerns

12. How concerned about your online banking account becoming compromised?
   ☐ Not at all
   ☐ Somewhat
   ☐ Very

13. Do you feel your bank is doing enough to protect you and your information online?
   ☐ Yes

☐ No

14. Have ever received a phishing email?
☐ Yes
☐ No

15. Have you ever become victim to a phishing email?
☐ Yes
☐ No

Comfort with Enhanced Authentication

16. In order to protect you online bank account, would you be willing to use additional authentication besides username and password.
☐ Yes
☐ No

17. If your bank **required** you to enroll in a biometric based authentication login, where you had to provide your finger print at log in would you (Bank would provide tools to do this)?
☐ Yes
☐ No

18. If your bank **asked** you to enroll in a biometric based authentication login, where you had to provide your finger print at log in would you (Bank would provide tools to do this)?
☐ Yes
☐ No

19. Would you be willing to use one of the following one time password generating tokens to login to your account?

    a. A one time password token is something you would possess and contains a random number generator that changes every 1 minute or so.
    ☐ Yes
    ☐ No

    b. A grid card where every time you logged in, you were required fill in a value from the card. For example:

Grid Card

	A	**B**	**C**
1	X	Z	@
2	9	*	m
3	L	5	I

Login One: Enter A3
Login Two: Enter C5

☐ Yes
☐ No

20. Would you prefer additional authentication that may take longer and require additional pieces of hardware at every login or only when your bank identified there was great enough risk to prompt you for additional authentication?
    ☐ Every Log in
    ☐ Only when bank deems risk great enough

21. If your bank required you to pay for the addition authentication, would you?
    ☐ Yes
    ☐ No

Appendix 2
Risk Assessment Template

(Click to access.)

Risk Assement Template.xls

References

Aladdin. (2006). eToken PRO USB - Security and Two Factor Authentication. Retrieved March 27, 2006, from http://www.aladdin.com/etoken/pro/usb.asp

APWG. (2006, March 24). January Phishing Trends Report. Retrieved March 27, 2006, from http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf

Anti-Phishing Working Group. (2003, December). Proposed Solutions to Address the Threat of Email Spoofing Scams. Retrieved October 1, 2004, from http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf

Anti-Phishing.org. (2004, September 13). Phishing Archive – Paypal Attack September 13. Retrieved October 8, 2004, from http://www.antiphishing.org/phishing_archive.html

comScore Networks. (2004, June 17). Press Release: comScore Analysis Reveals Usage of Online Banking and Bill Payment Have Grown Dramatically in the Past Year. Retrieved February 7. 2006, from http://www.comscore.com/press/release.asp?press=467

Emigh, A. (2005, October 3). Online Identity Theft: Phishing Technology, chokepoints and Countermeasures, Retrieved February, 4, 2006, from http://www.antiphishing.org/Phishing-dhs-report.pdf

Entrust 1. (2005, October). Consumer Perspectives on Online Banking Security. Retrieved February 4, 2006, from www.entrust.com/resources/download.cfm/22314

Entrust 2. (2004, October 19). Survey Finds Identity Theft Negatively Impacting Consumer Use of the Internet. Retrieved February 4, 2006, from http://www.entrust.com/news/2004/archive2004_6026.htm

Entrust 3. (2005). Customer Perspectives on Identity Theft and Phishing: Entrust Internet Security Survey. Retrieved February, 4, 2006, from http://www.entrust.com/resources/download.cfm/21961

FDIC. (2005, June 17). Putting an End to Account Hijacking. Division of Superviosn and Comsumer Protection. Retrieved February 11, 2006, from http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf

FDIC Financial Institution Letter. (2005, July 22). Spyware: Guidance on Mitigating Risks From Spyware. Retrieved February 11, 2006, from http://www.fdic.gov/news/news/financial/2005/fil6605a.html

FFIEC. (2005, October 12). FFIEC Guidance: Authentication in an Internet Banking Environment. Retrieved February 4, 2006, from http://www.ffiec.gov/pdf/authentication_guidance.pdf

Fox, S. (2005, February). The State of Online Banking. PEW Internet & American Life Project. Retrieved February 11, 2006, from http://www.pewInternet.org/pdfs/PIP_Online_Banking_2005.pdf#search='The%20State%20of%20Online%20Banking%20Pew

ID Analytics (2006, January). National Data Breach Analysis. ID Analytics.

Informa Research Services. (2005, August 4). Internet Banks Lose Consumer Confidence According to Study. Retrieved February, 11 2006, from http://www.informars.com/news/08_04_05.html

Krebsbach, K. (2004, June). Goin' Phishing: These Growing Emails have defrauded clients and banks of 1.2 billion. But what's the reputational cost?, *US Banker*, Vol. 114, No. 6. Retrieved October 3, 2004, from Lexis-Nexis Academic Database.

McCall, T. (2005, June 23). Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce. Roberthttp://www.gartner.com/press_releases/asset_129754_11.html

PassMark Security, LLC. (n.d.). Protecting Your Customers from Phishing Attacks. Retrieved October 4, 2004, from www.passmarksecurity.com

Ponemon Institute. (2005, April 5). Privacy Trust Survey for Online Banking. Retrieved February 11, 2006, from http://www.watchfire.com/news/whitepapers.aspx#finserv

Privacy Rights Clearing House (2006, April 1). A Chronology of Data Breaches Reported Since Choicepoint. Retrieved April 1, 2006, from www.privacyrights.org/ar/chrondatabreaches.thn

Rasmussen, R. (2004, April 5). Phishing Prevention: Making Yourself a Hard Target. Anti-Phishing Working Group. Retrieved September 12, 2004, from the Anti-Phishing Working Group Members Area.

Roche, T. Online Cost and Service Issues Intersect With DDA Growth Plans. Retrieved February 4, 2006, from http://www.bai.org/bankingstrategies/2005-jul-aug/online/index.asp

RSA. (2005, August 18). The True Cost of Protecting Customers Online Accounts. Retrieved February 11, 2006, from https://rsasecurity1.rsc03.net/servlet/campaignrespondent

RSA Security. (2005). RSA Security Consumer Study Reveals Major Concerns Over Online Security and Identity Protection. Retrieved February 11. 2006, from http://www.rsasecurity.com/press_release.asp?doc_id=5522&id=1034

Sinrod, E. (2005, April 13). Trust and Online Banking. USA Today. Retrieved February 11, 2005, from http://www.usatoday.com/tech/columnist/ericjsinrod/2005-04-13-online-banking_x.htm

Strasburg, J. (2005, May 28). Online banking grows; More customers logging on, but security is issue to some. Retrieved February 11, 2005, from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/05/28/BUGV4CVUVL1.DTL&feed=rss.business

Sullivan, B. (2005, May 25). Click! Online banking usage soars. Retrieved February 7, 2006, from http://www.msnbc.msn.com/id/6936297

Watchfire and IBM. (2003). The State of online financial services. Retrieved February 11, 2006, from http://www.watchfire.com/news/whitepapers.aspx#finserv