Authentication in Internet Banking: A Lesson in Risk Management

The business model that banks use to offer products and services to their customers has evolved significantly. Most banks have supplemented tellers, drive-ups, and other facilities with electronic capabilities, many of which are facilitated by the Internet. This shift to Internet-based banking and e-commerce in general is accompanied by new risks as well as an increase in existing risks. Security weaknesses in Internet-based processes create opportunities for savvy hackers to compromise systems and steal data. The Internet provides an effective and anonymous medium for thieves to advertise and sell the stolen data. In response, the bank regulatory agencies and the banking industry have sought ways to mitigate these vulnerabilities.

Authentication—the validation of a customer's identity—is a critical element of an effective information security program. This article defines authentication and describes instances when stronger authentication is needed, the authentication strategies some banks are using, and the roles and responsibilities of both bankers and regulators.

What Has Changed, and Why did the Old Processes Fail?

For years, financial institutions relied on user identification (IDs) and secret passwords to authenticate electronic banking customers. Because customers transacting business over telephone lines or through their computers could not show an ID card in person, user IDs and passwords served the same purpose—authenticating the customer to the financial institution. Using passwords as access credentials proved to be effective as long as the risks of compromise remained low.

When online banking (PC banking) emerged some years ago, passwords continued to provide reliable and secure access through dial-up connections and software provided by the financial institution. The online connection was made only to the bank, and opportunities to compromise the connection or steal access credentials were very limited. Although PC banking proved to be a viable product, problems such as slow dial-up connections and the expense of distributing and updating customer software prompted financial institutions to search for alternatives.

The Internet seemed to be the perfect answer. Rather than relying on banks to support and distribute online banking software, customers can simply access their financial information using their bank's Web site. Faster telecommunications offerings, such as digital subscriber line (DSL) and cable modems, provide the speed that dial-up connections lacked. But while the Internet offers a cheaper and faster product, it also contains serious new security vulnerabilities. Internet connections establish a pathway for hackers and thieves to access and steal sensitive personal information, including the banking records that many customers store on their home computers. Phishing, pharming, spyware, malware, worms, nimdas, viruses, buffer overflows, and spam—all relatively recent entries to our vocabulary—have raised electronic/Internet banking risk levels to new highs, and financial institutions have had to increase security measures to address those risks.

Financial institutions offering Internet banking products have generally done a good job of providing security-related information on their Web sites to both educate customers about the threats and instruct them on how to report suspected fraud. Providing educational materials to customers that explain how to recognize phishing e-mails and describe how to secure personal computers against viruses and Internet schemes

Authentication

continued from pg. 39

continues to be an important bank activity. Customer education adds value to banks' information security efforts, but banks still must address the risks of compromised access credentials.

The Regulatory Response

While numbers published in various periodicals and by consulting organizations place Internet fraud losses in the billions of dollars, it is very difficult to know just how large bank-specific losses are. One reason for this lack of information is that financial institutions are generally reluctant to discuss these issues publicly. Most financial institutions have borne these losses and not passed them on to the customers whose accounts were compromised. Financial institutions may simply cover these losses to avoid both the negative publicity and the legal requirements related to Internet fraud losses.

These losses often result from fraud committed using compromised access credentials. In response, in 2001 the Federal Financial Institution Examination Council (FFIEC) issued guidance titled *Authentication in an Electronic Banking Environment*.[1] This guidance explained the nature of a variety of threats and how banking customer access credentials could be compromised (stolen) and fraud perpetrated. However, the guidance lacked formal mandates and did not require action, so it did not prompt most financial institutions to act.

To draw attention to the issues associated with Internet banking fraud, in December 2004 the FDIC published a study focused on Internet ID theft—*Putting an End to Account-Hijacking Identity Theft*.[2] The study concluded that passwords alone were no longer an adequate authentication strategy when assets and personal information were at risk.

On October 12, 2005, the FFIEC issued further guidance titled *Authentication in an Internet Banking Environment*.[3] The new guidance, which replaced the 2001 guidance, required financial institutions to perform risk assessments of their electronic banking products and services. Institutions were expected to implement stronger authentication procedures for high-risk transactions, but they had considerable leeway regarding the authentication methods they chose to implement. They were expected to comply with the guidance by year-end 2006.

A common misinterpretation of the guidance made by both bankers and industry affiliates is that the banking agencies require multifactor authentication for high-risk transactions. In fact, what the guidance requires is *stronger* authentication to mitigate high risk. Traditional single-factor authentication should be augmented to create a level of security capable of coping with the risks of the transactions.

> Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer

[1] FIL-69-2001, *Authentication in an Electronic Banking Environment*, August 24, 2001, www.fdic.gov/news/news/financial/2001/fil0169.html.

[2] FIL-132-2004, *Identity Theft: Study on 'Account Hijacking' Identity Theft and Suggestions for Reducing Online Fraud*, December 14, 2004, www.fdic.gov/news/news/financial/2004/fil13204.html.

[3] FIL-103-2005, *Authentication in an Internet Banking Environment*, October 12, 2005, www.fdic.gov/news/news/financial/2005/fil10305.html.

information or the movement of funds to other parties.[4]

After careful study, the FFIEC agencies concluded that stronger authentication, including multifactor authentication, should be considered an industry best practice. They also concluded that multifactor authentication, layered security, and compensating controls could all mitigate different levels of risk. The authentication guidance provides a framework for improving online banking security by using stronger authentication.

What Is Authentication?

Successful authentication occurs when an individual presents evidence or proof that confirms a previously established identity. For example, if you moved to a new country, to establish residency you might have to present a number of documents that identify you. Once these documents have been scrutinized and found to be in order—part of a process called *enrollment*—you might then be issued an official government ID card for future use. This process of producing documents to prove an identity is commonly referred to as *identification*. *Authentication* occurs when you are later asked to produce the official ID card, such as when cashing a check—the ID card authenticates you as having been previously identified.

Bankers can accomplish and manage authentication easily with face-to-face customer interaction; however, authenticating a disparate customer base remotely connecting to Internet banking platforms using traditional physical security tools presents certain challenges:

- The distribution of software, hardware, cards, and other authentication-enabling technologies to a large Internet banking customer base is generally expensive to implement and administer.
- Banking customers are generally not receptive to paying security-related fees or enrolling in and installing security software and hardware on their home computers.

The difficulty and expense of implementing authentication standards typically increase proportionately with the strength and reliability of the solution. For instance, passwords present fewer challenges than fingerprint scanning. Authentication methodologies generally rely on one or more of the following three factors:

- Something you *know* (e.g., password)
- Something you *have* (e.g., ATM card)
- Something you *are* (e.g., fingerprint)

Requiring *one* of these factors to authenticate an individual is an example of single-factor authentication. Passwords are perhaps the most commonly used single-factor authentication methodology. Multifactor authentication consists of using two or more factors together. Using an ATM card is a common example of multifactor authentication—the card is something you have, and the personal identification number (PIN) is something you know. Both are required to complete a transaction. The use of two authentication factors in ATM transactions is considered strong authentication.

When Are Stronger Controls Necessary?

Banks traditionally have acknowledged the risks inherent in large dollar transactions, such as those initiated in commercial accounts and by customers who have high balances and corresponding activity. Stronger authentication, including multifactor authentication, has been an integral part of many financial institutions' risk management strategies for these higher-risk customers. But before the guidance was issued, most banks

[4] FIL-103-2005.

Authentication

continued from pg. 41

had not implemented stronger authentication for all customers. The guidance, while addressing both commercial and consumer accounts, is clearly directed at protecting the more vulnerable consumer account access credentials used in Internet banking. The mandated stronger authentication provides improved protection for all Internet banking customers.

The 2005 guidance instructed financial institutions to conduct and document the results of an Internet banking risk assessment. In the assessments, banks were required to identify high-risk transactions and, if they existed, strengthen Internet authentication standards if only passwords were used. The guidance defines high-risk transactions as those that allow the transfer of funds to third parties or provide access to nonpublic personal information. For example, bill pay, a common Internet banking product, allows funds to be transferred to third party payees. This is considered a high-risk transaction.

Today, the vast majority of banks that offer Internet banking are subject to the provisions of the guidance.[5] Telephone banking operations are also subject to the guidance when high-risk transactions can be conducted over the phone. It is important that financial institutions identify the banking systems and products that require stronger authentication and the degree of risk inherent in each. Internet banking transactions range from paying a small water bill to authorizing a large wire transfer. Obviously these two transactions are very different, and creating the wire transfer would carry much more risk than paying a water bill. The level of risk depends on the potential harm if the risk is left unmitigated.

Responding to the Challenges of Authentication

There are a variety of authentication products and services on the market, each with varying degrees of strength and reliability. Most FDIC-supervised institutions are customers of technology service providers (TSPs). Major TSPs have implemented authentication products from known vendors who use methodologies that the banking industry generally considers to be effective. Regulators, including the FDIC, have closely scrutinized and vetted TSP authentication product offerings. While many are not examples of true multifactor authentication, they can offer strong protection (especially when combined) and meet the provisions of the guidance. These products represent affordable and effective solutions for community banks.

FDIC-supervised banks should be in a good position to select an authentication product that mitigates the risks inherent in their Internet banking environments. While all the large TSPs have created and offer authentication products, it is up to the banks to install and properly implement them. As with any automation and security product, improper installation can render a solution ineffective.

Some TSPs offer tiers of authentication, with each tier relying on others to provide an effective overall solution. Since each tier must often be purchased separately, an institution may pick and choose pieces of a TSP's authentication product offering. Such a strategy can help minimize cost, but institutions may sometimes select pieces that do not work together effectively. Another common problem is weak authentication enrollment processes. For example, relying only on a weak password (such as a mother's maiden name) during the initial identification phase is a weak

[5] FIL-77-2006, *Frequently Asked Questions on Authentication in an Internet Banking Environment*, August 21, 2006, www.fdic.gov/news/news/financial/2006/fil06077.html.

enrollment procedure. A better enrollment process might involve mailing a unique password to the customer. The customer uses the unique password for the initial sign-on but then must change the password for future use.

Some banks have implemented controls that involve identifying the device used to establish the Internet banking connection. For example, the device (such as a computer, personal digital assistant, or cell phone) the customer uses to connect to the bank can be uniquely identified by the bank as belonging to the customer. This method of authenticating the customer—referred to as *device authentication*—is considered a compensating control that strengthens authentication.

Financial institutions often select two or three authentication solutions that can be implemented together to achieve acceptable levels of risk mitigation:

- Shared information—Secret information or images that are shared between the customer and the bank
- Device identification—A profile of the connecting device that can be used to authenticate the user in future transactions
- Geo-location—Establishing the geographic location from which the customer is connecting
- Internet Protocol (IP) intelligence—Using the customer's unique IP address
- Encrypted cookies—Special bits of data that the bank places on the customer's computer to assist in authenticating the customer
- Out-of-band communication—Cell phone call or e-mail message providing verification

Each of these processes alone adds strength to the authentication process. Combining several processes greatly increases the strength of the security and is an effective risk management strategy.

For consumer accounts, most banks are using combinations of geo-location, device identification, shared information, and IP intelligence, with challenge questions as the primary fallback. Challenge questions, generally set up at enrollment, involve the customer answering several questions. If a customer cannot be authenticated using normal routines, a challenge question is posed. A customer who answers correctly is authenticated and provided with access. The most effective challenge questions rotate from session to session; otherwise, they are little more than another password.

The agencies expect financial institutions to implement strategies that address the risks in their particular environment when considering how to authenticate Internet banking customers. Moreover, authentication processes should be implemented using logical and prudent risk management principles such as those described in the FFIEC *Information Technology Examination Handbook*, including:

- Classifying and ranking sensitive data, systems, and applications
- Assessing threats and vulnerabilities
- Evaluating control effectiveness[6]

Risk Management Procedures and Examiner Review

One of the primary factors that the agencies consider in reviewing banks' efforts to comply with the guidance is the risks and how the bank's authentication strategy mitigates those risks. When selecting authentication products and services, vetting the products offered by the TSP and performing vendor due diligence are critical for both financial institutions and service providers.

[6] FFIEC, *Information Technology Examination Handbook*, Information Security Booklet, Information Security, July, 2006, at www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm.

Authentication

continued from pg. 43

Due diligence should include acquiring a sound working knowledge of the technology and being able to both explain and defend the solution during regulatory scrutiny. Using a one-time password-generating token along with a user password is generally accepted as strong authentication, as is the two-factor authentication for ATM use discussed previously. Thus, examiner review and assessment of these technologies is fairly straightforward. On the other hand, evaluating technologies purchased from less well-known sources can be more difficult. If the bank has purchased a solution from a vendor whose claims are not easily understood or are filled with technical jargon, examiners may need to review the solution more closely. In some cases, information technology examination specialists may need to evaluate the solution.

Feedback from bankers indicates that the level of online banking fraud is down and that the guidance may have had a positive effect. During on-site examinations and telephone contacts earlier in the year, examiners began noting the progress banks have made in implementing authentication solutions. Although the effort is not yet complete, of more than 500 institutions assessed, 92 percent have complied with the guidance and implemented stronger authentication for their high-risk transactions. While a few institutions may have procrastinated thinking there would be relief through extended compliance dates, or otherwise may not have acted, most banks that have not yet complied with the guidance have plans in place and are making progress. Many of these banks are serviced by small, regional-based TSPs and may either be waiting for their turn to have a product installed or waiting for one to be tested and available for installation. The FDIC continues to monitor banks' compliance efforts and risk assessment efforts, and, if necessary, will consider enhancing examination procedures to include a formal review of banks' authentication strategies.

Authentication—One Part of Enterprise Risk Assessment

A common criticism of security processes in general is that they do not provide guarantees. In the real world, there are no guaranteed solutions to protect systems and data. Implementing strong authentication is only part of an effective enterprise-wide risk management program. Managing information technology risks is a dynamic proposition that should be proactive rather than reactive. Effectively managing authentication risks today may limit vulnerabilities in the future. Managing access credentials, whether for remote banking customers or bank employees accessing confidential systems, is an important element in a bank's information security plan and risk assessment. The authentication guidance provides the impetus for performing and managing periodic evaluations of the threats and vulnerabilities of Internet banking products and services as part of the bank's comprehensive risk management program.

Strong authentication practices coupled with other security policies such as back-end fraud detection are elements of an effective information security plan. And like any good plan that assesses risk, the plan must be revisited and revised regularly as the threat and vulnerability landscape changes. Technology changes daily, and the best way to maintain a proper defense is to keep a constant vigil. Internet banking risk assessments and evaluations should have a permanent place in every bank's enterprise risk assessment strategy.

Robert D. Lee
Senior Technology Specialist
Washington, DC