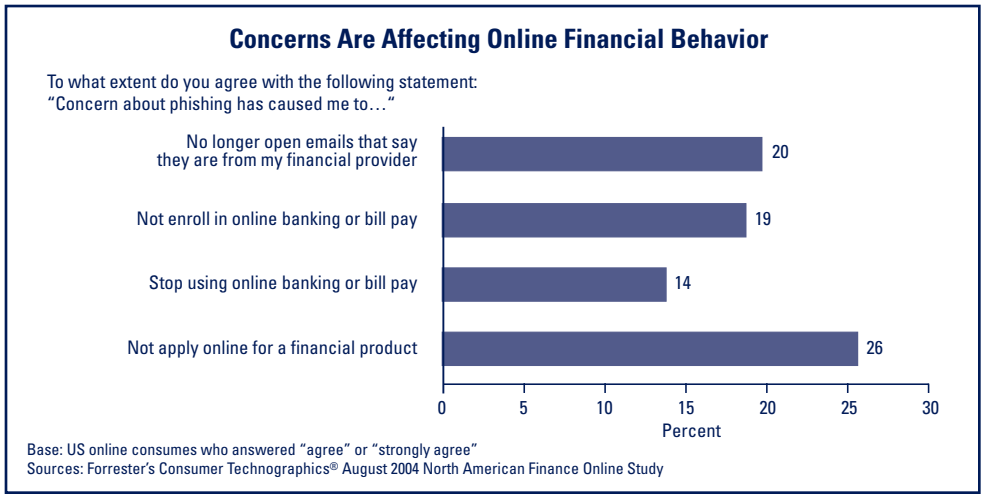
Online Delivery of Banking Services: Making Consumers Feel Secure

Much media attention recently has been focused on identity theft. Some of this publicity may suggest the Internet has evolved from a trusted tool for conducting research and legitimate business transactions to a medium whereby consumers' sensitive personal information can be stolen and used for criminal purposes. Social Security and credit card numbers, as well as bank account access data (such as passwords), are examples of some of the most sought-after information, providing perpetrators of identify theft access to bank balances and credit lines.

Many insured financial institutions rely heavily on the Internet to reach their customers, offering a wide variety of online banking services. In some cases, this practice has allowed banks and thrifts to consider scaling back brick-and-mortar facilities and staff required to conduct face-to-face banking transactions. However, security and privacy issues loom large in the minds of Internet users (see Chart 1). If financial institutions are to retain existing customers and attract new ones, they must create an online banking experience in which customers feel secure and have confidence their assets and personal information will not be compromised.

Highlighting another area of concern to customers of financial institutions, the results of a survey conducted by the ***Gartner Group*** in June 2005[1] show "the number of phishing attack e-mail recipients grew 28 percent this year....These and other breaches are exacting a steep toll on consumer confidence and will inhibit three-year e-commerce growth rates by 1 percent to 3 percent."[2] Issues concerning online users are highlighted in Chart 2, which emphasizes the level of concern about fraud and identity theft.

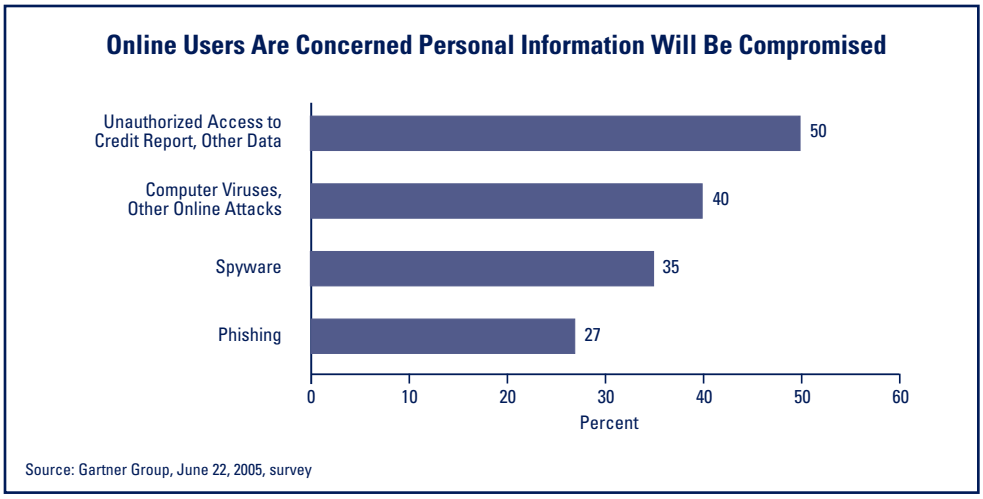
Chart 1



[1] Avivah Litan, "Increased Phishing and On-Line Attacks Cause Dip in Consumer Confidence," *Gartner* (June 22, 2005).

[2] The common phishing scenario is sending a fake e-mail (e-mail spoofing) purporting to come from a legitimate source and requesting information (such as a bank account number and password) or directing the victim to a fake Internet site where this information can be captured.

Chart 2



Concerns such as those identified in the Gartner Group survey and the high level of interest in preventing identity theft and safeguarding consumers' personal financial information prompted the FDIC to conduct its own study. The results of the study were released in mid-December 2004 in a publication entitled ***Putting an End to Account-Hijacking Identity Theft.***[3] The study has fostered debate among bankers, consumers, and regulators about how the risks posed by Internet-based financial services can be minimized. Following the publication of the study, the FDIC conducted several identity theft symposia featuring representatives from the banking industry, regulatory agencies, and consumer groups.[4] Participants considered the implications of conducting business on the Internet and initiatives for enhancing Internet security. Discussion focused on the areas of consumer privacy and protections, maintaining trust in the financial services industry, and the potential burden on smaller insured institutions that rely on external Internet service providers.

The overarching sentiment expressed during the symposia is that the problem of identity theft is not going away anytime soon. Although consumer protections are becoming more effective, hackers are becoming more sophisticated as well. In addition, while consumers want tightened security, they often are not willing to pay for it either through increased fees or any loss of convenience.

Many symposia participants recognized the banking industry must do a better job of self-regulating, for example, strengthening standards requiring companies to notify consumers whose data may have been lost or stolen. Participants acknowledged banks must do everything possible to prevent high-profile security breaches, such as those at ChoicePoint, LexisNexis, and Bank of America. Should more of these

[3] Federal Deposit Insurance Corporation, *Putting an End to Account-Hijacking Identity Theft* (December 14, 2004) available at https://www.fdic.gov/news/inactive-financial-institution-letters/2004/fil13204.html. A supplement to the study was released in June 2005 and is available at www.fdic.gov/news/news/financial/2005/fil5905.html. For purposes of this article, the results of the study and the supplement will be discussed as the results of the "study."

[4] The symposia were conducted in 2005 in Washington, D.C., (February 11), Atlanta (May 13), Los Angeles (June 17), and Chicago (September 22).

continued from pg. 13

incidents occur in the near term, the public may call for greater Federal government intervention, such as regulating where and how Social Security numbers are available on the Internet. Consumers also could be given the right to have their confidential information removed from computer systems of companies that have processed transactions for them or from systems maintained by data-brokering firms.

Another area of significant interest that emerged during the symposia relates to mitigating the level of risk inherent in conducting online transactions. Key questions posed during the symposia fall into four categories:

- **Risk reduction and risk mitigation** — What tools, policies, and procedures have proven most effective and can be considered best practices?
- **Risk transference** — Can insurance policies be designed to help protect consumers engaging in online financial transactions?
- **Risk acceptance** — Even though the goal of bankers and regulators is to minimize the level of risk inherent in online financial transactions, some level of risk always exists. How much risk are consumers willing to accept?
- **Risk avoidance** — How can the banking industry and regulators ensure consumers' confidential information is shared only with those who need it?

The following sections summarize the results of the FDIC study and key components of recently issued interagency guidance focusing on authentication[5] in an Internet environment.

What Level of Authentication Is Appropriate?

The FDIC study finds that traditional passwords consumers use to access their bank accounts via the Internet are too easily compromised and no longer represent an effective means to authenticate users. Once an Internet thief steals a password through phishing e-mails or other techniques, the consumer's accounts and personal information are at risk.

The study suggests a risk-based approach to identifying specific weaknesses in an insured institution's Internet banking system. For example, if online customers can view only non-sensitive information and are unable to transfer funds, the risk of harm to the customer is lower and, consequently, a less robust authentication method would be appropriate. On the other hand, if customers can transfer funds to other parties, this higher-risk transaction requires strong authentication procedures.

Authentication is based on the use of one or more of the following:

- Something you know, such as a password
- Something you have, such as an ATM card (a token)
- Something you are, such as a fingerprint (biometrics)

The vast majority of Internet-based financial services rely on single-factor authentication, usually a password, for customers to access their accounts. If an institution relies only on single-factor authentication, transactions are relatively easily compromised and lack adequate protection for sensitive consumer

[5] The process of identifying an individual traditionally based on a username and password. In security systems, authentication is distinct from authorization, the process of giving individuals access to system objects based on their identity. Authentication merely ensures the individual is who he or she claims to be, but says nothing about the individual's access rights.

information and funds. When a customer is tricked into disclosing a password, the thief could use the information to access the customer's accounts and potentially transfer funds.

A password combined with another form of authentication (i.e., two-factor authentication), such as an ATM card, provides much more reliable authentication. Multifactor authentication requires the user to supply at least one additional identification factor, such as a token-generated one-time password, USB token, smart card, or fingerprint.[6] Without the additional factor(s), a thief would not possess all credentials required to gain access to a customer's account. Therefore, multifactor authentication provides a more secure defense against identity theft.

The study describes one-time-password tokens, USB tokens, device authentication, geo-location, biometrics, and several other authentication technologies. The study also sheds light on how institutions may decide what technologies are right for them. Certain technologies present unique challenges. For example, the use of biometrics may not be appropriate for large, geographically dispersed customer bases. Biometrics (e.g., finger prints, iris structure, and facial features) are better suited to a captive audience, such as employees of a business housed in a single building. Insured financial institutions considering an authentication strategy should assess portability, ease of customer use, cost, effectiveness, ease of implementation, and the maturity of the technology.

In addition to discussing the shortcomings of traditional password authentication, the study concludes that financial institutions should

- Consider scanning software to identify and defend against phishing attacks;
- Strengthen education programs that advise customers about creating safe Internet experiences and recognizing attacks; and
- Continue to emphasize information sharing among the financial services industry, government, and technology service providers.

Regulators Work Together to Issue Guidance

Building on the results of the study and issues highlighted during the identity theft symposia, the Federal Financial Institutions Examination Council[7] (FFIEC) agencies issued guidance on October 12, 2005, entitled ***Authentication in an Internet Banking Environment.***[8] This guidance adopts the findings of the FDIC study relating to what constitutes effective customer authentication and recommends banks and thrifts offering Internet-based products and services use reliable and

[6] Tokens are small portable devices attached to a key ring carried by bank customers. One-time-password (OTP) tokens contain a small screen displaying several numbers. The token generates a random number every minute or so, which the customer enters into the online banking application. The financial institution receives the entered number and compares it with its records. A correctly entered number authenticates the customer and allows access. USB (universal serial bus) tokens, which can be plugged into the USB port of a bank customer's computer, contain unique identifying information that authenticates the customer.

[7] The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the FDIC, the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

[8] See FIL-103-2005: Financial Institution Letter "Authentication in an Internet Banking Environment" (October 12, 2005) available at https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html.

continued from pg. 15

effective methods to authenticate customers' identities. The authentication techniques explored should be appropriate to the risks associated with the products and services. As discussed previously, single-factor password based authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. In these instances, insured institutions should use multifactor authentication, layered security,[9] or other appropriate controls.[10] Examiners may criticize institutions that have not properly mitigated risks identified in the assessment.

As insured financial institutions begin to assess their risks as outlined in the interagency authentication guidance, they should consider each type of transaction consumers can initiate online. The types of transactions may include the following:

- Access to the bank's website for new product offerings or CD rates
- Access to an individual deposit account
- Access to a deposit account and an automatic bill-paying option
- Ability to transfer money from one account to a related account
- Ability to transfer money to a third party

The above transactions are ranked by level of risk (beginning with the lowest level) they represent to the institution and the customer. The first transaction allows access only to general bank information; customer information or bank accounts cannot be accessed. This transaction is considered relatively low risk and would not require strong access controls.

However, the last transaction, which allows an online customer to wire or transfer money to another party, should require more than a password to initiate. In this case the bank should require the customer to supply authentication credentials such as a one-time password token. This layered approach to authentication matches low-risk transactions with less robust solutions and higher-risk transactions with stronger solutions. Risks falling in the middle would be addressed according to the potential for compromise of sensitive data or assets.

Insured financial institutions must comply with the interagency authentication guidance by December 31, 2006. To do so, they should begin performing risk assessments as soon as possible and, based on the results of these assessments, implement stronger authentication strategies by year-end 2006.

The FDIC and the other bank regulatory agencies are aware of the time and effort required to comply with the new authentication guidance. However, compliance with this guidance will help ensure that customers continue using an Internet delivery channel in which many banks and thrifts have invested a significant amount of capital.

Robert D. Lee
Senior Technology Specialist

[9] Layered security refers to the layers of risk, from low to high, as well as the layers of authentication implemented, from weak to strong. Layers of authentication processes are matched with corresponding layers of risk.

[10] See "Industry Initiatives" box at the end of this article for examples of industry initiatives targeted at deterring Internet theft and fraud, including the implementation of multifactor authentication procedures.

Industry Initiatives

During the past couple of years, a number of banks and technology service providers have implemented multifactor authentication products for Internet-based financial services. For example, E-bank, a large thrift, piloted a one-time password token program for its commercial customers during 2004 and has now made the tokens available to all its Internet banking customers. Bank of America recently implemented new software-based authentication technologies that provide its 13 million Internet banking customers with another authentication factor.[11] Multifactor authentication represents an effective strategy for protecting customers' funds and sensitive information, in addition to promoting confidence in Internet-based financial services.

Consumer education also is an effective deterrent to Internet theft and fraud. Many financial institutions disseminate brochures offering tips about avoiding scams and suggesting steps customers should take if they believe they have become victims. Consumers also are urged to use regularly updated antivirus software, firewalls, anti-spyware, and other tools to avoid having their personal information compromised.

[11] Daniel Wolfe, "Online Banks Are Taking to Authentication Tokens," *American Banker* (June 6, 2005).