

# **Putting an End to Account-Hijacking Identity Theft**

Federal Deposit Insurance Corporation  
Division of Supervision and Consumer Protection  
Technology Supervision Branch  
December 14, 2004

This study presents the FDIC's findings on unauthorized access to financial institution accounts and how the financial industry and its regulators can mitigate these risks.

# **EXECUTIVE SUMMARY AND FINDINGS**

## **Background and Focus of Study**

Identity theft is one of the fastest growing types of consumer fraud. The Federal Trade Commission (FTC) has estimated that, during 2003, almost ten million Americans discovered they were the victims of identity theft, with a total cost to businesses and consumers approaching \$50 billion. This study focuses on a subset of identity theft that is of particular concern to financial institutions insured by the FDIC and to the institutions' customers: unauthorized access to and misuse of existing asset accounts primarily through phishing and hacking, hereinafter referred to as "account hijacking."

## **Prevalence and Impact of Account Hijacking**

While precise statistics on the prevalence of account hijacking are difficult to obtain, recent studies indicate that unauthorized access to checking accounts is the fastest growing form of identity theft. The FTC has estimated that almost 2 million U.S. adult Internet users experienced this fraud during the 12 months ending April 2004. Of those, 70 percent do their banking or pay their bills online and over half believed they received a phishing e-mail. Consumers are attributing risk to their use of the Internet to conduct financial transactions, and many experts believe that electronic fraud, especially account hijacking, will have the effect of slowing the growth of online banking and commerce.

## **Findings**

Fraudsters are taking advantage of the reliance on single-factor authentication for remote access to online banking, and the lack of e-mail and Web site authentication, to perpetrate account hijacking. Financial institutions and government should consider a number of steps to reduce online fraud, including:

1. Upgrading existing password-based single-factor customer authentication systems to two-factor authentication.
2. Using scanning software to proactively identify and defend against phishing attacks. The further development and use of fraud detection software to identify account hijacking, similar to existing software that detects credit card fraud, could also help to reduce account hijacking.
3. Strengthening educational programs to help consumers avoid online scams, such as phishing, that can lead to account hijacking and other forms of identity theft and take appropriate action to limit their liability.
4. Placing a continuing emphasis on information sharing among the financial services industry, government, and technology providers.

# TABLE OF CONTENTS

<b>BACKGROUND .....</b>	<b>4</b>
Definition of Identity Theft.....	4
Survey of the Problem of Account Hijacking.....	6
Summary .....	14
<b>LEGISLATIVE AND REGULATORY RESPONSES TO IDENTITY THEFT .....</b>	<b>15</b>
Standards for Protecting Information .....	15
Information to Consumers .....	16
Increased Penalties and Tools for Law Enforcement .....	16
Summary .....	17
<b>INDUSTRY RESPONSES TO IDENTITY THEFT .....</b>	<b>18</b>
Financial Services Information Sharing and Analysis Center .....	18
Anti-Phishing Working Group.....	19
Identity Theft Assistance Corporation.....	19
Infragard.....	20
Financial Institution Web Site Alerts.....	20
Summary .....	21
<b>THE USE OF TECHNOLOGY TO MITIGATE .....</b>	<b>22</b>
Scanning Tools .....	22
<i>Scanning Software</i> .....	22
<i>Server Log Analysis Software</i> .....	23
E-Mail Authentication (Sender ID) .....	24
User Authentication .....	25
<i>Shared Secrets</i> .....	26
<i>Tokens</i> .....	27
<i>Biometrics</i> .....	30
Summary .....	36
<b>FINDINGS.....</b>	<b>38</b>
<b>REFERENCES.....</b>	<b>39</b>

## BACKGROUND

Identity theft is one of the fastest growing types of consumer fraud.<sup>1</sup> With just a few key pieces of personal information (e.g., an individual’s name, address, social security number, financial institution account number, computer log on ID, or password), a criminal can access a consumer’s existing asset and credit accounts, create fraudulent new accounts in a consumer’s name, or create synthetic identities<sup>2</sup> that can be used to obtain services and credit fraudulently. During 2003, almost ten million Americans discovered they were the victims of identity theft, with a total cost to businesses and consumers approaching \$50 billion.<sup>3</sup>

The term “identity theft” is generally defined as the use of personal identifying information to commit some form of fraud. Although the range of consumer frauds and criminal acts coming under that definition is quite broad, this study focuses on the subset of identity theft that is of particular concern to financial institutions insured by the FDIC and to the institutions’ customers: unauthorized access to and misuse of existing financial institution asset accounts primarily through phishing and hacking.<sup>4</sup> This form of identity theft is referred to here as “account hijacking.” The present study examines how technology is used to commit account hijacking and the methods available to help prevent it.

The rest of this section surveys the various legal (and other) definitions of identity theft and defines the problem of account hijacking: how is it perpetrated, how prevalent is it, what is its financial effect, and how the industry and the public perceive it. The subsequent sections review the legislative and regulatory responses to identity theft, the financial industry’s responses to it, and the use of technology to mitigate account-hijacking identity theft. The final section presents the FDIC staff’s conclusions and recommendations.

### Definition of Identity Theft

The definition of identity theft was first codified in 1998 as part of the Identity Theft and Assumption Deterrence Act of 1998 (ID Theft Act).<sup>5</sup> The ID Theft Act made identity theft a stand-alone crime. More specifically, it amended the federal criminal code to make it a crime for anyone to

knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity

---

<sup>1</sup> FTC (2004a).

<sup>2</sup> Unlike typical identity theft fraud where a fraudster steals the identity of a real person and uses it to commit fraud, a synthetic identity is a completely fabricated identity that does not correspond to any actual person.

<sup>3</sup> FTC (2003).

<sup>4</sup> Phishing attacks use fraudulent or “spoofed” e-mails and Web sites to fool recipients into divulging confidential information, such as account user names and passwords, to criminals. Hacking is the unauthorized intrusion, perpetrated remotely, into a computer or network.

<sup>5</sup> Pub. L. 105-318.

that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.<sup>6</sup>

In 2003, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) amended the Fair Credit Reporting Act (FCRA) to include a civil definition of identity theft:

The term “identity theft” means a fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade Commission] may prescribe, by regulation.<sup>7</sup>

Pursuant to FACTA, the Federal Trade Commission (FTC) has recently proposed a more specific definition of identity theft which describes what is meant by the term “identifying information”:

- (a) The term “identity theft” means a fraud committed or attempted using the identifying information of another person without lawful authority.
- (b) The term “identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any-
  - (1) Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
  - (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
  - (3) Unique electronic identification number, address, or routing code; or
  - (4) Telecommunication identifying information or access device. . . .<sup>8</sup>

Although the FTC’s proposed definition refines the statute, both of them cover existing as well as newly created accounts, asset as well as credit accounts, and masquerading as someone else as well as creating a synthetic identity in an effort to obtain services or other benefits fraudulently. As noted above, the scope of this study is more narrowly defined, being limited to existing (but not newly created) accounts, asset (but not credit) accounts, and masquerading as someone else (but not creating a synthetic identity).

In its Identity Theft Survey Report, the FTC included a category of identity theft described as the “misuse of existing non-credit card account or account number.”<sup>9</sup> At least one organization within the financial services industry has created its own definition of identity theft specific to that industry and similar to the FTC’s category: the Identity Theft Assistance Center defines identity theft as either “account takeover” or the creation of a “fraudulent account.”<sup>10</sup> Account takeover—what the present study calls “account hijacking”—is further defined as the “assumption of a customer’s identity on a valid

---

<sup>6</sup> 18 U.S.C. §1028.

<sup>7</sup> 15 U.S.C. §1681a(q)(3).

<sup>8</sup> FTC (2004b).

<sup>9</sup> FTC (2003).

<sup>10</sup>ITAC (2004). See Article I, 19.

existing account.”<sup>11</sup> Once again, this study focuses on the unauthorized access to and misuse of existing asset accounts through phishing and hacking.

### **Survey of the Problem of Account Hijacking**

The expansion of electronic payment systems plays a part in account hijacking, since greater numbers of financial institution customers have access to electronic banking and bill-pay services, and formerly-wholesale automated clearing house (ACH) payments have become a vehicle for retail payments.<sup>12</sup> New forms of ACH transactions include Internet-authorized payments, debits authorized over the telephone, and check-to-ACH conversions at the point of purchase. With Internet banking almost universally available, ACH transactions have increased 15 percent from 1991 to 2001,<sup>13</sup> and in the second quarter of 2004 more than 2.2 billion ACH transactions were processed, compared to 1.85 billion in the second quarter of 2003.<sup>14</sup> However, financial institutions’ wider adoption of different forms of electronic payment systems, as well as the increasing number of customers using these services, have produced greater opportunities for electronic fraud.

Thus, although the problem of account hijacking is as yet relatively small, it is nonetheless serious for customers (both retail and commercial) and for financial institutions. The increasing access to alternative electronic payment systems means an increasing number of access points to financial institution systems, with each access point representing a pathway for a potential security breach. The increasing number of access points, coupled with the potential for anonymity afforded by electronic payment systems, facilitates electronic banking fraud.<sup>15</sup> Yet customers expect financial institutions to ensure the safety and security of their financial transactions however those transactions are effectuated. Public confidence in the financial system is predicated on this type of trust. The FDIC anticipates that as customers become more aware of actual instances of, or the potential for, account hijacking, they will expect financial institutions to implement solutions that protect their funds and their identities, while maintaining or increasing the level of convenience for them in accessing financial services.

The following sections of this study explain the ways of perpetrating account hijacking, its prevalence, its financial impact, and the industry’s and the public’s perceptions of it.

---

<sup>11</sup>Ibid. See Article I, 1.

<sup>12</sup>An ACH transaction is an electronic fund transfer between accounts. ACH transactions are governed by NACHA, the National Automated Clearing House Association. Typically, an ACH debit transaction is initiated when a payor gives permission to a third party (the payee) to debit its (the payor’s) checking or savings account using only a payor routing number and payor bank account number. The payee enters the ACH transaction at his or her own bank and instructs the Federal Reserve to clear the payment through the payor’s bank against the payor’s account. See also Sauerman and Corkill (2003).

<sup>13</sup>NACHA (2002).

<sup>14</sup>NACHA (2004).

<sup>15</sup>Tuthill (2002) estimates that 8 percent of e-commerce transactions coming from anonymous e-mail addresses are fraudulent.

### *Ways of Perpetrating Account Hijacking*

There are a limited number of ways to hijack deposit accounts. Each of them—and they may be used in concert with one another—relies on the misuse of information. The ways are phishing, hacking, retrieving hard-copy documents or looking over someone’s shoulder, using insiders, and loading malicious software onto a computer used by consumers.

Phishing is easy to implement, and financial service companies are the most frequent targets of phishing attacks.<sup>16</sup> In phishing, consumers are deceived—normally via deceptive e-mails, fake (spoofed) Web sites, or both—into providing fraudsters with their user names, passwords, and perhaps account numbers.<sup>17</sup> (Telephone-based phishing is used much less often because it is a more expensive and less efficient information-gathering technique.) The classic phishing attack involves a deceptive e-mail that purports to be from a legitimate financial institution. The e-mail typically tells the customer that there is some sort of problem with the customer’s account. The e-mail usually includes a hyperlink to a spoofed Web site that looks exactly like the site of a legitimate financial institution with which the consumer does business. The e-mail typically instructs the recipient to click on the included hyperlink, go to the financial institution Web site, and log in using the customer’s user name and password in order to “fix” the problem. In reality, the spoofed Web site is simply collecting customer user names and passwords in order to hijack accounts. The following is an example of an actual phishing e-mail:

---

<sup>16</sup> Ibid.

<sup>17</sup> Early spoofing was partly facilitated by a flaw in Microsoft’s Internet Explorer program. That flaw allowed fraudsters to hide the actual Internet address of a spoofed page and thereby fool users. The flaw has since been patched. See Chipman (2004) for more information.

-----Original Message-----

**From:** Citibank [mailto:Walliw\_Melba@1-base.com]  
**Sent:** Saturday, August 16, 2003 12:46 AM  
**To:**  
**Subject:** Your Checking Account at Citibank.



Dear Citibank customer,

We are letting you know, that you, as a Citibank checking account holder, must become acquainted with our new Terms & Conditions and agree to it.

Please, carefully read all the parts of our new Terms & Conditions and post your consent. Otherwise, we will have to suspend your Citibank checking account.

This measure is to prevent misunderstanding between us and our valued customers.

We are sorry for any inconvenience it may cause.

[Click here to access our Terms & Conditions page and not allow your Citibank checking account suspension.](#)

© 2003 Citibank. Citibank (West), FSB. Member FDIC. Citibank with Arc Design is a registered service mark of Citicorp.



A member of  Citigroup  
[Citigroup Privacy Promise](#)  
[Terms & Conditions](#)  
Copyright © 2003 Citicorp

Phishing relies on some customers' being vulnerable to each step in the ploy: the content of the deceptive e-mail, the directions in that e-mail to go to a spoofed Web site, the content of the spoofed site, and the instructions to provide user names and passwords. Phishing has become the most common technique for stealing the information necessary to hijack an account.<sup>18</sup>

Phishing e-mails can be sent either to a large number of people in the hope that a certain percentage of recipients will be actual customers of the spoofed financial institution (usually a large financial institution with a significant online customer base) or to actual known customers of a particular financial institution. This second method is generally

---

<sup>18</sup> O'Sullivan (2003).

more effective, but it is also harder to perpetrate because the fraudster needs to acquire some sort of customer list in order to target the deceptive e-mail. The FDIC has been the subject of six separate phishing attacks within the past year. The most recent attack occurred in September 2004, while this study was being written. From a fraudster's point of view, such an attack has the potential to be effective since it can reasonably be assumed that the majority of recipients maintain at least one FDIC insured account. A phishing e-mail targeting the FDIC is illustrated below:

Dear [REDACTED],  
Federal Deposit Insurance Corporation

As use of the Internet continues to expand, more banks and thrifts are using the Web to offer products and services or otherwise enhance communications with consumers.

The Internet offers the potential for safe, convenient new ways to shop for financial services and conduct banking business, any day, any time. However, safe banking online involves making good choices - decisions that will help you avoid costly surprises or even scams.

Due to concerns, for the safety and integrity of the **FDIC** community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive accounts, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in Bank account deletion. This notification expires on September 15th 2004.

Once you have updated your account records your Bank Account will not be interrupted and will continue as normal.

Please follow the link below  
and renew your account information.  
[http://www.fdic.gov/register/cgi-bin/fdic\\_intsafe/register.jsp](http://www.fdic.gov/register/cgi-bin/fdic_intsafe/register.jsp)

Fraudsters either use the user names, passwords, and account numbers themselves or, more commonly, sell the information to other fraudsters who will perpetrate the actual account hijacking. Up to 5 percent of the recipients of spoofed e-mails respond to them.<sup>19</sup> An estimated 19 percent of "those attacked" have clicked on the link in a phishing e-mail.<sup>20</sup> Most, if not all, large financial institutions and electronic bill-paying services (such as PayPal) have been hit with phishing attacks.<sup>21</sup> Because many phishing

---

<sup>19</sup> Anti-Phishing Working Group (2004); Loftesness (2004). Litan (2004a) cites 3 percent.

<sup>20</sup> Litan (2004a).

<sup>21</sup> Loftesness (2004).

attacks originate overseas and because the average life span of a phishing Web site is 2.25 days,<sup>22</sup> the sites are hard to shut down.

The second method of account hijacking mentioned above is to hack into financial institution or service provider computer systems and databases and steal confidential customer information. One industry source mentioned that financial institution sites are frequently targeted by hackers because financial institutions maintain so much valuable confidential information about their customers.

The third method of obtaining account information is far more labor-intensive: retrieving hard-copy documents that include customer names, account numbers, user names and/or passwords, or surreptitiously observing a customer accessing his or her account. Retrieving confidential documents from trash receptacles is called “dumpster diving.” Watching someone fill out personal information or input his or her password at an automated teller machine (ATM) is called “shoulder surfing.” It is hard to get large quantities of confidential information this way.

The fourth method of acquiring the confidential information necessary to hijack accounts is to use insiders. Some industry analysts and security professionals estimate that 65 to 70 percent of identity theft is committed with confidential information stolen by employees or participants in transactions or services.<sup>23</sup> In a survey conducted in 2003, an estimated half of all workers and managers who had access to customer information said that it would be either “easy” or “extremely easy” for workers to remove sensitive data from corporate databases. Two-thirds of the respondents believed that their coworkers, not hackers, posed the greatest risk to consumer privacy.<sup>24</sup> Insiders can sell the information or use it directly to commit identity theft. Because of the increased networking of internal operations and pervasiveness of huge customer databases, financial institution employees have access to more customer information than ever before. The exact size of the problem is unknown, but fraud is sometimes perpetrated by financial institution insiders, often in ways that require little technical sophistication.<sup>25</sup>

The fifth method of acquiring the information necessary to hijack accounts is by inserting malicious software (such as a keystroke logger<sup>26</sup>), often referred to as “spyware,” on a consumer’s personal computer at home or on a computer used by many consumers in a public facility like an Internet café.<sup>27</sup> Spyware can be surreptitiously loaded when a user opens a seemingly innocuous e-mail attachment or clicks on a pop-up advertisement. The spyware collects selected information (e.g., user names, passwords, and account numbers) from customers of certain financial institutions and forwards that information to the fraudster. Although one source asserts that keystroke loggers are not used much to

---

<sup>22</sup> Anti-Phishing Working Group (2004).

<sup>23</sup> For example, Chamberlain (2004), Ferchau (2004), Krebsbach (2004), and Sullivan (2004).

<sup>24</sup> Harris Interactive Market Research (2003).

<sup>25</sup> Randazzo et al. (2004).

<sup>26</sup> A keystroke logger is a program that records what the user types on the computer keyboard and sends that information to the person who installed the program.

<sup>27</sup> Litan et al. (2004).

commit traditional forms of identity theft,<sup>28</sup> the FTC held a forum in Washington, DC on April 19, 2004 devoted to the increasing popularity and effectiveness of monitoring software and the difficulty in defending against it.<sup>29</sup>

Regardless of the method used to steal confidential information, once the necessary information is in hand, the fraudster's goal is to gain access to a consumer or business account from which fund transfers can be executed. In the case of Internet banking, the fraudster, armed with both a valid user name and a valid password, can access the system by posing as a legitimate customer and can initiate one or more fund transfers to a fraudulent payee controlled by the fraudster that the fraudster has added to the customer's approved payee list. In the case of ACH debit fraud, a fraudster would initiate an unauthorized payment, using the fraudulently obtained account number to authorize the debit.

### *The Prevalence of Account Hijacking*

There is a large body of literature on credit and credit card fraud, but researchers have devoted little attention to account hijacking. Some information can be gleaned from recent work on the broader aspects of identity theft. The largest identity theft study to date, conducted by the FTC in March and April 2003, was based on information collected from over 4,000 adults in the United States.<sup>30</sup> It attempted to quantify the incidence of identity theft in the United States, focusing on credit theft. It reported that 19 percent of the estimated 9.91 million identity theft victims—that is, 1.8 million adults—said their existing checking or savings accounts had been misused alone or in combination with other forms of identity theft. As the “most serious problem the victim reported,” 2 percent of U.S. adults had experienced a “misuse of existing non-credit card accounts or account numbers,” including utility and cell phone accounts, within the previous five years, and 0.7 percent of adults experienced that form of identity theft within the preceding year. However, these numbers are of limited value for estimating the incidence of account hijacking because the methodology does not report response rate or weighting of results.

A recent study of unauthorized transfers from checking accounts indicates that an estimated 1.98 million U.S. adult Internet users had experienced this crime during the 12 months ending April 2004, and another 2.48 million had experienced it during the 12 months before that. Of five types of consumer fraud in that study,<sup>31</sup> unauthorized access to checking accounts was the fastest growing and the second most prevalent. Only 13 percent of consumers had discovered this fraud as the result of a notification by their financial institution. Of those who experienced this type of identity theft, 70 percent do their banking or pay their bills online. Over half of the victims believed they received a phishing e-mail, and 5 percent recalled providing sensitive information in response to such e-mails. The author of the study concludes that most of these thefts, if not

---

<sup>28</sup> Chipman (2004).

<sup>29</sup> FTC (2004c).

<sup>30</sup> FTC (2003).

<sup>31</sup> Litan (2004b). Unauthorized access to checking accounts, new-account fraud, check forgery, illegal credit card purchases, and fraudulent cash advances on credit cards.

perpetrated by an insider, were the result of a fraudster's obtaining account numbers or passwords or both and then accessing checking accounts through online payments, online banking transactions, or telephone banking services.<sup>32</sup> Since the study does not specify its methodology, it is of limited value for estimating the incidence of unauthorized checking-account access.

Another study estimates that illegal checking-account transfers will increase. Today they affect 1.4 percent of U.S. adult Internet users, but they are expected to rise to 2 percent by the end of 2006.<sup>33</sup>

In 2002, the FTC began a voluntary data collection effort to gather information on the number and types of identity theft being perpetrated against consumers. Table 1 shows the number and percentage of identity theft complaints associated with bank fraud. In 2003, the most recent year reported, over 17,000 complaints were received about the misuse of existing bank accounts; the majority of such misuse was probably check fraud. More than 10,000 complaints were also received about unauthorized electronic fund transfers from existing bank accounts—more than twice the number of complaints received the previous year.<sup>34</sup> These numbers, too, are of limited value for estimating the incidence of account hijacking because the system relies on the voluntary reporting of complaints by consumers who are aware of the service. Thus, these numbers must be seen as underestimating the magnitude of deposit account hijacking.

Table 1  
How Victims' Information Is Misused

	2001		2002		2003	
	Percentage of Complaints	Number of Complaints	Percentage of Complaints	Number of Complaints	Percentage of Complaints	Number of Complaints
Bank Fraud						
Existing Accounts	6.2	5,345	8.1	13,109	8.2	17,622
Electronic Fund Transfers	1.9	1,638	3.1	5,017	4.8	10,315
New Accounts	2.7	2,328	3.7	5,988	3.8	8,166
Unspecified	2.3	1,983	2	3,237	0.5	1,075
Total Bank Fraud	13	11,208	17	27,512	17	36,534
Total Identity-Theft Complaints		86,212		161,836		214,905

Source: FTC, Identity Theft Data Clearinghouse.

Other, less formal studies have indicated that identity theft, measured in ways that would include account hijacking, exists in small but persistent numbers. In a telephone survey of 2,000 U.S. adults conducted in 2000, approximately 1 percent of the respondents reported that they had been the victim of identity theft and that the person who had

<sup>32</sup> Ibid.

<sup>33</sup> Litan (forthcoming).

<sup>34</sup> It is unclear how much of this surge in complaints is due to increased awareness of the data collection effort and how much is a true increase in the number of such occurrences.

assumed their identity “took over [their] currently existing bank account.”<sup>35</sup> In an online survey of over 3,000 U.S. adults, 7 percent of the respondents said that “someone opened a bank account in their name or forged checks and obtained money from their account.”<sup>36</sup>

### *The Financial Impact of Identity Theft*

The FTC has estimated the cost of all forms of identity theft in 2002 at \$47.6 billion to businesses and financial institutions, and \$5.0 billion to consumer victims.<sup>37</sup> By way of comparison, identity theft-related losses due to credit card account takeovers at the two largest credit card-issuing organizations totaled \$46.1 million in 2000<sup>38</sup>, and total check fraud-related losses against commercial banks totaled \$698 million in 2001.<sup>39</sup> Direct fraud losses associated with new-account fraud, check forgery, unauthorized access to checking accounts, illegal credit card purchases, and fraudulent cash advances on credit cards, collectively, were estimated to total \$2.4 billion over the 12 months ending April 2004, or \$1,200 per victim.<sup>40</sup> Direct fraud losses associated only with account hijacking are believed to be a very small portion of those totals, but no known estimates exist.

According to the American Bankers Association, “the vast majority of banks have instituted a policy of making the customer whole in phishing attacks associated with credit cards.”<sup>41</sup> Litan finds that banks usually refund to customers the amounts lost because of fraud, especially if the customers report the fraud within 60 days.<sup>42</sup>

### *Industry and Public Perceptions*

The paucity of publicly available information on the financial impact of account hijacking does not mean that the industry is not concerned about this form of identity theft. Identity-theft fraud is the top concern among financial institutions of all sizes (see table 2). Among online consumers who were victims of new-account fraud, check forgery, unauthorized access to checking accounts, illegal credit card purchases, or fraudulent cash advances on credit cards, 17 percent believed their personal information had been stolen off the Internet, whereas 10 percent thought the crime happened because their wallets had been stolen.<sup>43</sup> Consumers are thus attributing risk to their use of the Internet to conduct financial transactions, and many experts believe that electronic fraud, specifically account hijacking, will slow the growth of online banking and commerce.<sup>44</sup>

---

<sup>35</sup> Star Systems (2002); no response rate was reported for this survey.

<sup>36</sup> Privacy and American Business (2003).

<sup>37</sup> FTC (2003).

<sup>38</sup> U.S. GAO (2002).

<sup>39</sup> ABA (2002).

<sup>40</sup> Litan (2004b).

<sup>41</sup> O’Sullivan (2003).

<sup>42</sup> Litan (2004b).

<sup>43</sup> Litan (2004b).

<sup>44</sup> See Litan (2004b), for example.

Table 2  
 Leading Threats against Deposit  
 Accounts, by Bank Size Group

Bank Asset Size	Identity Fraud	Debit Card	Internet	Organized Rings	Check Electronification	Other ACH
	Percentage of Banks					
Community Banks (<\$500 million)	38	17	18	11	8	5
Midsize (\$500 million to \$4.9 billion)	40	17	11	19	8	2
Regional (\$5 to \$49.9 billion)	40	0	6	37	3	3
Super Regional, Money-Center Banks (\$50 billion plus)	60	7	7	13	7	0

Source: American Bankers Association, Deposit Account Fraud Survey 2002.

Financial institutions are concerned about adverse consumer reactions to real or perceived security problems at their institutions. Financial institutions do not typically release information on computer security breaches, largely because they believe that negative publicity would hurt their image;<sup>45</sup> industry representatives and security experts assert that the indirect financial losses and public relations problems associated with a publicized security breach would be worse than the direct financial loss.<sup>46</sup> Some analysts, however, have suggested that the rapid rise in phishing attacks is threatening consumer confidence and that diminished consumer trust in online transactions will hurt all participants in Internet commerce.<sup>47</sup>

### Summary

Account hijacking commences with the theft of information by phishing, hacking, dumpster-diving, insider abuse, or monitoring software. While identity theft, in a broad sense, affects millions of Americans, less is known about the account hijacking subset of identity theft. Studies suggest that account hijacking is now a small but growing problem for financial institutions and consumers, and that conducting financial transactions online may place consumers at more risk.

<sup>45</sup> Gordon et al. (2004); Randazzo et al. (2004).

<sup>46</sup> Tuthill (2002); O'Sullivan (2003); Randazzo et al. (2004).

<sup>47</sup> Litan (2004a).

# LEGISLATIVE AND REGULATORY RESPONSES TO IDENTITY THEFT

Since 1998, when identity theft first became a federal crime, a number of statutes and regulations have clarified impermissible use of personal information and offered greater tools to law enforcement. However, no law or regulation is focused solely on account hijacking. These changes in federal law have either established standards for protecting information, provided consumers with more information about their credit history so they can be more vigilant in protecting their own identity, or increased criminal penalties for identity theft and enforcement tools in an effort to deter it. Each of these approaches is discussed below.

## **Standards for Protecting Information**

In 2001, the federal banking agencies (FBAs)<sup>48</sup> implemented section 501(b) of Gramm-Leach-Bliley Act (GLBA) by promulgating “Guidelines Establishing Standards for Safeguarding Customer Information.”<sup>49</sup> The objectives of the guidelines and of the written information-security program they require are to:

- Ensure the security and confidentiality of customer information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

In addition, the guidelines require financial institutions to require service providers with whom they contract to implement a security program designed to meet the Guidelines’ objectives.

The Fair and Accurate Credit Transactions Act of 2003 (FACTA), in Section 113, requires that account numbers on credit card receipts be shortened or “truncated” so that merchants, employees, or others who may have access to the receipts do not have access to consumers’ names and full credit card numbers. This provision does not require an implementing regulation. Section 216 of FACTA requires the FTC and the FBAs to promulgate regulations defining appropriate standards for the disposal of sensitive credit report information. Section 114 of FACTA, commonly referred to as the “red-flag” provision, requires the FTC and the FBAs to promulgate guidelines identifying patterns, practices and specific forms of identity theft, and regulations to implement the guidelines as part of an identity theft prevention program.

---

<sup>48</sup> Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

<sup>49</sup>FDIC (2001) and 12 CFR 364, Appendix B.

Although the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) focuses primarily on money laundering and terrorism, it does ensure strong customer identification programs which serve as a first-line deterrent against identity theft. Section 326, Verification of Identification, requires financial institutions to (1) implement a customer identification program for verifying the identity of any person seeking to open an account, and (2) maintain records of the information used to verify that person's identity.

### **Information to Consumers**

FACTA contains several provisions specifically intended to reduce identity theft. Section 211 requires the three major credit-reporting agencies to provide consumers, at their request, with a free copy of their own credit report at least once every 12 months. Credit reports allow consumers to discover and correct errors in their credit records and to ensure that accounts have not been fraudulently opened in their names. The FTC has published an implementing regulation.

Section 112 of FACTA permits consumers who have, or may have, been victimized by identity theft to place an alert on their credit files in order to warn potential new creditors that the consumer may be an identity-theft victim and that some of the information contained in the credit report may be a result of the fraud. The FTC is currently drafting an implementing regulation.

### **Increased Penalties and Tools for Law Enforcement**

The ID Theft Act makes identity theft a federal crime with penalties of up to 15 years' imprisonment and a maximum fine of \$250,000. It establishes that the person whose identity was stolen is a victim (previously, only the credit grantors who suffered monetary losses were considered victims). This legislation enables the Secret Service, the Federal Bureau of Investigation (FBI), and other law enforcement agencies to combat the crime of identity theft; it allows for the identity-theft victim to seek restitution if there is a conviction; and it establishes the FTC as the central agency to act as a clearinghouse for complaints (against credit-reporting agencies and credit grantors), referrals, and resources for assistance to victims of identity theft.<sup>50</sup>

The Identity Theft Penalty Enhancement Act (Penalty Enhancement Act) was signed into law on July 15, 2004. It expands the existing prohibition against identity theft to (1) cover possession of a means of identification of another with intent to commit specified unlawful activity, (2) increase penalties for violations, and (3) include acts of domestic terrorism within the scope of a prohibition against facilitating an act of international terrorism. To achieve these objectives, the Penalty Enhancement Act amends the federal criminal code to establish penalties for aggravated identity theft, which the act defines as knowingly transferring, possessing, or using, without lawful authority, a means of identifying another person during and in relation to specified felony violations. The

---

<sup>50</sup>Frank (1998).

Penalty Enhancement Act prescribes a two-year prison sentence for aggravated identity theft and an additional five-year prison sentence for felony violations pertaining to terrorist acts.

The Internet False Identification Prevention Act of 2000, closing a loophole left by the ID Theft Act, enables law enforcement agencies to pursue those who formerly could sell counterfeit social security cards legally by maintaining the fiction that such cards were “novelties” rather than counterfeit documents.<sup>51</sup>

## **Summary**

Each of these strategies (protecting information, customer disclosures, and increased penalties and tools for law enforcement) offers one or more mitigation techniques to deter identity theft, including account hijacking.

---

<sup>51</sup>Social Security Administration (2004).

## INDUSTRY RESPONSES TO IDENTITY THEFT

Successful frauds tend to be replicated until they no longer work. Financial institutions can help reduce identity theft, including account hijacking, by encouraging information sharing so that identity theft frauds are thwarted sooner. A number of such information-sharing efforts are noteworthy including those sponsored by the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Anti-Phishing Working Group (APWG), the Identity Theft Assistance Corporation (ITAC), and Infragard, in addition to individual financial institution Web sites.

### **Financial Services Information Sharing and Analysis Center**

The FS-ISAC, under the auspices of the President's Commission on Critical Infrastructure Protection, is a private partnership of major banks, brokerages, insurance companies, and utilities and is managed by a board of managers elected by the FS-ISAC membership.<sup>52</sup> The FS-ISAC has access to a secure database, analytic tools, and information-gathering and distribution facilities designed to allow authorized people to submit either anonymous or attributed reports about cyber and physical security threats, vulnerabilities, incidents, and recommended solutions. Members have access to information and analysis relating to information provided by other members and obtained from other sources, such as federal law enforcement agencies, technology providers, and security associations. Through FS-ISAC, some of the nation's leading experts in the financial services sector share and assess threat intelligence provided by its membership and by the National Infrastructure Protection Center (NIPC), an arm of the Department of Homeland Security, and other public and commercial sources. They help the NIPC prepare warnings of threats against the financial services infrastructure. Through the FS-ISAC, the financial service companies pass and receive incident information to and from the federal agencies that are responsible for seeking patterns that may indicate pending threats. The secure FS-ISAC Web site offers security information on the latest physical and cyber vulnerabilities, threats, and incidents related to the banking and finance industries. Physical-security, such as regional intelligence, travel advisories, benchmarking, and best practices, are also addressed. In December 2003, the FS-ISAC began devoting a \$2 million award from the U.S. Department of the Treasury to programs designed to enhance security awareness for all financial institutions, including providing members with secure collaboration, additional feeds for threats and vulnerabilities, confirmation of alerts, and new analytical capabilities.

---

<sup>52</sup> The President's Commission on Critical Infrastructure Protection was created on July 15, 1996, by Executive Order 13010 to bring the public and private sectors together to assess and develop strategies to address infrastructure vulnerabilities. The banking and finance sector was identified as one of eight critical infrastructures requiring review and assurance strategies, and in 1999, the banking and finance sector established FS-ISAC.

## **Anti-Phishing Working Group**

The APWG is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The APWG is composed of financial institutions, e-commerce providers, Internet service providers (ISPs), and vendors of e-mail services and software. The group's goal is to provide resources, technology, vision, and expertise to facilitate the rapid deployment of a solution to e-mail phishing scams. The APWG has over 630 members, including eight of the top ten U.S. banks and four of the top five ISPs.

A December 12, 2003, APWG white paper titled "Proposed Solutions to Address the Threat of E-mail Spoofing Scams" provides a brief overview of e-mail spoofing scams and offers four solutions:

- Strong Web site authentication
- Mail server authentication
- Digitally signed e-mail with desktop verification
- Digitally signed e-mail with gateway verification.

The APWG and the Financial Services Technology Consortium (FSTC)—a consortium of leading North American-based banks and other financial institutions that sponsors collaborative technology development—have agreed to work together to identify and evaluate solutions to phishing.

## **Identity Theft Assistance Corporation**

On October 28, 2003, the Financial Services Roundtable (Roundtable) and the Banking Information Technology Secretariat (BITS)<sup>53</sup> announced formation of the ITAC. ITAC is a resource to help victims of identity theft recover their financial identities and restore their credit ratings. ITAC's mission involves streamlining the recovery process and providing a simplified, consumer-friendly means to address the consequences of identity theft (including account hijacking). Equally important, ITAC will work with the FTC and law enforcement agencies, and the information it collects will be used to help prevent such crimes in the future.

ITAC builds on the "Fraud Reduction Guidelines: Strategies for Identity Theft Prevention and Victim Assistance," announced by the Roundtable and BITS in July 2003. The guidelines provide for (1) a single point of contact at financial service companies to whom victims can report cases of identity theft, and (2) the use of a uniform affidavit to record information about the fraud. Thus, victims report the particulars of their cases only once, to their primary financial institution, and then the information is sent on to

---

<sup>53</sup> The Financial Services Roundtable represents 100 of the largest integrated financial service companies providing banking, insurance, and investment products and services to the U.S. consumer. Member companies participate through their chief executive officers and other senior executives nominated by the Chief Executive Officers. BITS is a nonprofit industry consortium that shares membership with the Financial Services Roundtable. BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy, and integrity of financial transactions. The BITS board of directors is made up of the CEOs of 20 of the largest U.S. financial service companies, as well as representatives of the American Bankers Association and the Independent Community Bankers of America.

ITAC, if the customer consents. From this point forward, ITAC contacts all other companies where the victim has an account and where additional fraud may have occurred. Such a process will benefit consumers by relieving them of the stress and wasted hours of reporting their fraud cases to multiple institutions where they maintain accounts.

ITAC is currently conducting a pilot program to test its procedures and processes. Until the conclusion of the pilot, only members of the Roundtable and BITS are eligible to become members of ITAC. If the pilot is successful, ITAC plans to make its services available to other institutions.<sup>54</sup> ITAC, BITS, FTC, and law enforcement agencies are developing procedures for uploading data into the FTC's Identity Theft Data Clearinghouse so that law enforcement agencies will have direct access to the information collected by ITAC.

### **Infragard**

Infragard, an FBI program with private sector partners that began in 1996, is another effort to share information about cyber crime. It is an information-sharing and analysis resource serving the interests and combining the knowledge base of a wide range of members. Members include businesses, academic institutions, state and local law enforcement agencies, and others dedicated to sharing information and intelligence to prevent hostile acts against the United States. Each Infragard Chapter has an FBI special agent coordinator assigned to it, coordinating with the Cyber Division at FBI headquarters. Government organizations and their representatives are eligible for Infragard membership, and several FDIC regional offices participate. Infragard chapters are located across the United States and are linked with FBI field office territories.

### **Financial Institution Web Site Alerts**

Financial institutions are communicating directly with consumers to make them more aware of identity theft and phishing attacks and offering customers the means to report attacks quickly. Educating customers to be aware of the scams to which they may be exposed is one of the most effective ways to deter identity theft. Financial institutions that have been the target of spoofing seem to be more proactive in making information available to their customers than financial institutions that have not been targeted. FDIC staff reviewed the Web sites of several of the nation's largest banks and found that banks are displaying the following:

- Specific graphical examples of spoofed e-mails
- Examples of spoofed e-mail subject lines to watch for
- Toll-free numbers for reporting details about identity theft
- E-mail address for communicating information about identity theft
- Links to the FTC and other agencies for additional help
- Consumer alerts related to new developments
- Advice for preventing and reacting to identity theft.

---

<sup>54</sup> Engen (2004).

## **Summary**

The financial services industry has taken a number of recent steps to help prevent identity theft and mitigate the inconvenience experienced by consumers when it does occur. Consumer education and information sharing appear to be the cornerstones of these efforts.

## THE USE OF TECHNOLOGY TO MITIGATE ACCOUNT-HIJACKING IDENTITY THEFT

As discussed previously, account hijacking can be perpetrated in a number of ways. It can also be mitigated in a number of ways—that is, through the use of several different technologies.<sup>55</sup> Computer security experts recommend a layered approach to computer security because no single security technique is foolproof or sufficient to prevent identity theft. This section examines three types of technologies that, implemented at various levels, could be used to mitigate the risk of identity theft generally and account hijacking specifically:

- Scanning tools
- E-mail authentication
- User authentication.

Each technology is evaluated based upon ease of implementation, portability, effectiveness, and ease of customer use. A chart at the end of each section contains the ratings. All ratings are relative, comparing each technology only to others included in the study. The study does not attempt a cost comparison due to the fact that hardware and software costs vary greatly depending on the quantity purchased and other business relationships that may exist between the buyer and seller.

### Scanning Tools

The scanning tools discussed here are scanning software and server-log analysis.<sup>56</sup> These techniques are referred to as “presumptive forensics”—using investigative techniques to find potential problems.<sup>57</sup>

#### *Scanning Software*

Scanning software continuously scans millions of Internet Web sites looking for indications that the financial institution may be the target of a phishing attack.

#### What is it and how does it work?

Scanning software continuously scans the Internet for occurrences of the institution’s name, brands, trademarks, and slogans. The software also surveys, on a daily basis, Internet domain name servers (DNS) for like names that match specific alert patterns. The scanning software then examines the home page of any identified Web site for text matching the specified alert patterns. It also searches the Internet for secure sockets layer

---

<sup>55</sup> Consumer education continues to be an important strategy in preventing account hijacking (and identity theft in general), but it is not the focus of this section of the study.

<sup>56</sup> In the course of preparing this study, FDIC staff researched the existence of fraud detection software specifically designed to detect account hijacking, similar to existing software used to detect credit card fraud. Staff found no such product in widespread use and concluded that development is in the early stages.

<sup>57</sup> Swofford (2004).

(SSL) certificate common names. The scanning software reports back the names of the servers and the domain names that contain content similar to the financial institution's legitimate Web site.

#### Effectiveness/Protection

Scanning software helps financial institutions identify Web sites that may be pretending to be the financial institution or may be implying that the site has a legitimate relationship with the financial institution when in fact it does not.<sup>58</sup> Although scanning software is not foolproof, it can alert users to potentially fraudulent Web sites that have been set up to perpetrate account-hijacking fraud.

#### Ease of use and requirements

A financial institution can purchase and run scanning software itself, or can outsource this service to an independent service provider. In many cases, smaller financial institutions may choose to outsource this service.

#### Ratings for Scanning Software

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Easy	N/A	Moderate	N/A

#### *Server Log Analysis Software*

Server log analysis software is similar to the scanning software discussed above, except that it scans and analyzes the financial institution's own servers.

#### What is it and how does it work?

Server logs provide substantial information about the day-by-day activities of a computer network, and timely analysis of the logs can help an institution detect suspicious activity that may indicate that the institution is the victim of a phishing attack. However, server logs are voluminous, and reviewing them is time-consuming. Software can analyze web server logs in a matter of minutes and organize the information so a network administrator could detect a phishing scam before it went into effect.

#### Effectiveness/Protection

Server log analysis software may allow institutions not only to detect fraudsters as they plan their phishing attacks but also to alert the institutions' customers and even prevent an attack before it starts. The software can allow administrators to observe the development of the suspected phishing site, test hijacked accounts, and identify suspected phishers.

---

<sup>58</sup> Netcraft, Ltd. (2004).

### Ease of use and requirements

Those who review the reports produced by the log analysis software must be trained. Alternatively, the review may be outsourced. The software does not require complex implementation and can be installed as a stand-alone application. The software can easily be adjusted for any new pattern of attacks and for any type of server.

### Ratings for Log Analysis

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Easy	N/A	High	N/A

### **E-Mail Authentication (Sender ID)**

As discussed above, deceptive e-mails that appear to be from the consumer's financial institution are often the first step in a phishing attack that can ultimately lead to account hijacking. These e-mails can be made to look as if they are from the customer's financial institution, or the institution's address can actually be forged by a technique called "domain spoofing." In either case, consumers are tricked into divulging confidential information to a fraudster, and the information is used to hijack the consumers' accounts. This deception is made possible by the fact that Internet e-mail was not originally designed to authenticate the identity of the sender. E-mail can be authenticated, but implementing this solution is beyond the capability of any one party. Rather, e-mail authentication (Sender ID) requires the cooperation of software vendors, ISPs, and the Internet Engineering Task Force (IETF).

Sender ID is a combination of Microsoft's proposal for caller ID for e-mail, the sender policy framework (SPF), and a third specification called the submitter optimization.<sup>59</sup> The Sender ID technical specifications were recently submitted for review and approval, but the IETF rejected them on September 15, 2004. While it is unclear what effect this action will have, at least one large ISP has indicated that it is going to implement SPF and some software vendors have indicated they support Sender ID despite the IETF's decision.

### What is it and how does it work?

Sender ID verifies that each e-mail message originates from the Internet domain from which it claims to come by comparing the claimed address to the sender's actual server Internet Protocol (IP) address. Sender ID has the potential to change the entire Internet e-mail distribution system. All e-mail distributors would have to adjust the way they process their e-mail. The following is a brief step-by-step description of how Sender ID works:

- The sender sends an e-mail message to the recipient.
- The recipient's inbound mail server receives the e-mail.

---

<sup>59</sup> Microsoft Corporation (2004).

- The recipient's server checks in the DNS record for the published SPF record of the sending domain.
- The inbound e-mail server determines if the sending e-mail server's IP address matches the IP address that is published in the DNS record.
- If the addresses match, the e-mail is forwarded to the recipient. If not, the e-mail is rejected and the intended recipient never receives it.

This proposed standard would also be able to detect an attempt by a fraudster to register a domain name that closely resembled the name of a financial institution or other transactional Web site.

### Effectiveness/Protection

Eliminating domain spoofing will help legitimate senders protect their domain names and reputations and will help recipients more effectively identify and filter out phishing e-mails (as well as other types of spam). In addition, once phishers and spammers are forced to buy their own domain names, it will be easier to track them down.

### Ease of use and requirements

Sender ID will not require a change in the way users use e-mail. The filtering will be done by the ISP.

### Ratings for Sender ID

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Easy	Yes	High	Easy

### **User Authentication**

Authentication is the means of verifying the identity of a person or entity. It can also be used to verify that information received has not been altered. Closely associated and often confused with authentication is authorization, which determines the level of rights and privileges available to the authenticated user. Tying authentication and authorization together is referred to as identity management.

Generally the way to authenticate the user is to have the user present some sort of credential to prove his or her identity. A credential is generally one or more of the following:

- Something a person knows—most commonly a password. If the user types in the correct password, access is granted.
- Something a person has—most commonly a physical device referred to as a token. The user must physically connect the token to the computer in order to be granted access. Thus, tokens often require the user's computer to be outfitted with specific hardware to accept the token.
- Something a person is—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye.

This type of authentication is referred to as biometrics and often requires the installation of specific hardware on the system to be accessed.

Single-factor authentication involves the use of one of the three authentication credentials listed above, most commonly a password. Single-factor authentication is very common and is the method used by the vast majority of financial institutions for granting customers access to Internet-banking applications and by the vast majority of businesses for granting employees access to computer networks. The main problem with single-factor authentication is that passwords, the most commonly used factor, are often easy to guess, steal, or crack, and once a password is compromised the thief has the same access rights as the legitimate user. In addition, the legitimate user may not even know that his or her password has been compromised, since usually no physical evidence of the compromise exists.

The initial section of this study has documented the monetary damage that can be inflicted when passwords are compromised. The rise in account hijacking suggests that traditional single-factor authentication may not be adequate in today's online world.

Two-factor authentication has the potential to eliminate, or significantly reduce, account hijacking. Two-factor authentication uses two of the three types of credentials mentioned above (something a person knows or has or is) for establishing the user's identity. Two-factor authentication is most widely used today in connection with ATMs. To withdraw money from an ATM, the user must present both an ATM card (something the person has) and a password or PIN (something the person knows). A fraudster who succeeds in stealing just one or the other will not be able to pose as the legitimate account owner and access the ATM. Two-factor authentication can also involve the combination of a password (something a person knows) and a biometric (something a person is). Biometric authenticators (as well as tokens, which are something you have) are unique and not easily duplicated and can be disabled, so their ability to serve as an authentication device can be quickly revoked.<sup>60</sup> Two-factor authentication is significantly more secure than single-factor authentication because the compromise of one factor would not be enough to permit a fraudster to access the system and the additional factor (usually a token or biometric identifier) is extremely difficult to compromise. Almost all the phishing scams in use today could be thwarted by the use of two-factor authentication.

Most two-factor authentication systems use shared secrets, tokens (USB token devices, smart cards, or password-generating tokens), or biometrics.

### *Shared Secrets*

Shared secrets are questions that are asked during the authentication process, the answers to which a fraudster would be unlikely to know (e.g., the exact amount of the user's monthly mortgage payment).<sup>61</sup> The questions may also be obscure, such as "which of these addresses is familiar to you?" However, as more and more information is collected

---

<sup>60</sup> Rainbow Technologies (2002).

<sup>61</sup> ING DIRECT uses this technique. See [http://home.ingdirect.com/faqs/faqs\\_content.html](http://home.ingdirect.com/faqs/faqs_content.html).

in diffuse databases, the reliability of this technique comes into question. One person's obscure knowledge may be another person's public information, in which case more or different questions are needed. Or the information may be so obscure that the legitimate user would not be able to enter the correct answer in the requisite amount of time.

A newer shared-secret technique that may alleviate the problems of obscurity is being introduced into the market: a secret that is shared only between the institution and the user. This method would authenticate the site to the user by displaying the shared secret so that the user would know it was safe to enter his or her password.

#### What is it and how does it work?

A shared secret is a type of authentication that validates the Web site to the user by means of a shared secret that is unique to the user. At enrollment, the user selects an image from an image pool provided by the institution's Web site. Users can then change their shared secrets, just as they can change their passwords, by selecting a different one from the image pool or by uploading their own image. The image is displayed at the site before the user logs in. A fraudulent Web site would not display the pre-selected image, which is different for each user.

#### Effectiveness/Protection

Shared secrets can be an effective way to authenticate Web sites to users and can also be used to authenticate e-mails by embedding the shared-secret graphics in the e-mails themselves. The disadvantage of this method is that it is susceptible to man-in-the-middle attacks<sup>62</sup>, where the fraudster successfully impersonates the user and gains access to the shared secret.

#### Ease of use and requirements

Graphic shared secrets are simple to use, yet effective. Users need to be educated to understand that if their selected image does not appear, the Web site is a fake. This solution to the problem of user authentication requires no additional user hardware.

#### Ratings for Shared Secrets

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Easy	Yes	Moderate	Easy

#### *Tokens*

Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

---

<sup>62</sup> In a man-in-the-middle attack, a fraudster intercepts messages between the institution and the customer, learns the shared secret, and then impersonates the institution going forward. The customer is unaware of the fact that he or she is now communicating with the fraudster instead of the institution.

### USB Token Device: What is it and how does it work?

The USB token device is the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. A USB token usually contains a microprocessor and uses strong encryption to communicate with the various security applications on the user's computer. Once the USB token is recognized, the user is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

#### Effectiveness/Protection

USB tokens are one-piece, injection molded devices. If a token is forced open in an attempt to compromise it, the microprocessor becomes useless. The device has the ability to store digital certificates in the secure flash memory area that can be used in a public key infrastructure (PKI) environment.

#### Ease of Use and Requirements

The USB token is extremely user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

#### Ratings for USB Token Devices

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Easy	Yes	High	Easy

### Smart Card: What is it and how does it work?

A smart card is the size of a credit card, easy to carry, and hard to duplicate. Like a USB token, a smart card contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the user's computer. If the smart card is recognized as valid (first factor), the user is prompted to enter his or her password (second factor) to complete the authentication process.<sup>63</sup>

#### Effectiveness/Protection

Smart cards are hard to duplicate and tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials.

---

<sup>63</sup> Many federal agencies use smart cards for access to certain sensitive applications residing on their internal computer networks. The cards also functions as identification badges for entry into agency buildings.

### Ease of use and requirements

Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer.

### Ratings for Smart Cards

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Moderate	No	High	Easy

### Password-Generating Token: What is it and how does it work?

A password-generating token produces a unique pass-code (also known as a one-time password [OTP]) each time it is used. The token eliminates the need to memorize passwords and ensures that the same password is never used twice, so stealing a password is useless. The OTP is displayed on a small screen on the token. The user first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The user is authenticated if (1) the regular passwords match and (2) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password.<sup>64</sup> OTP tokens generally last 4 to 5 years before they need to be replaced.<sup>65</sup>

### Effectiveness/Protection

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs prevent cyber thieves from using information gained from keyboard logging.

### Ease of use and requirements

OTPs are user-friendly for the end user, but administering them may be cumbersome for the financial institution.

### Ratings for Password Generating Tokens

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Difficult	Yes	High	Easy

---

<sup>64</sup> FDIC staff are aware of at least one large U.S. bank that is in the process of beginning a pilot program to test the use of password-generating tokens by retail customers for remote access to the bank's Internet-banking system. At least one federal government agency uses this system for remote employee access to the agency's internal computer network.

<sup>65</sup> A "low tech" version of the password-generating token, commonly referred to as a scratch card, has been used in Europe for some time. The card contains a series of passwords that customers use in sequence, scratching off each one as it is used. The scratch card is given or mailed to customers when they sign up for online banking.

## *Biometrics*

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic. Physiological characteristics are things like fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called “enrollment.” In enrollment, samples of data are taken from one (or more) of our physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis.

Once enrolled, users interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the user. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the user is authenticated and granted access.

The National Institute of Standards and Technology (NIST) has developed standards to support biometric technologies. NIST has created a Common Biometric Exchange File Format (CBEFF) standard used to describe a set of data elements necessary to support biometric technologies. The CBEFF provides industry standards to:

- Facilitate the interchange of biometric data between different system components or between systems
- Promote the interoperability of biometric-based application programs and systems
- Provide forward compatibility for technology improvements
- Simplify the process of integrating software and hardware.

The comparison of the authentication sample to the stored template does not yield results that are 100 percent accurate. Most biometric applications can be adjusted to achieve different levels of accuracy and error rates. There are two classes of errors that must be considered:

- False Acceptance Rate (FAR): the probability that the system will accept a false biometric credential as legitimate.
- False Reject Rate (FRR): the probability that the system will reject a valid biometric credential.

The sensitivity of the data and the security environment in which biometric technologies will be implemented will dictate appropriate deviation standards, FRRs, and FARs. For instance, admittance to a Department of Defense classified database would require different security and authentication standards as compared to accessing a retail Web site. Biometric identifiers are generally not used as a single factor to authenticate individuals due to the difficulty of accurately tuning the system to avoid unreasonably high FARs or FRRs. They are more commonly used as part of a two-factor authentication system, being combined with a password (something a person knows) or a token (something a person has).

Some of the most common biometric technologies include:

- Fingerprint recognition
- Face recognition
- Voice recognition
- Keystroke recognition.
- Handwriting recognition
- Finger and hand geometry
- Retinal scan
- Iris scan

Biometric technologies should be considered and evaluated giving full consideration to the following characteristics:

- **Universality:** Every person should have the characteristic. People who are mute or without a fingerprint will need to be accommodated in some way.
- **Uniqueness:** Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.
- **Permanence:** The characteristics should not vary with time. A person's face, for example, may change with age.
- **Collectibility:** The characteristics must be easily collectible and measurable.
- **Performance:** The method must deliver accurate results under varied environmental circumstances.
- **Acceptability:** The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.
- **Circumvention:** The technology should be difficult to deceive.

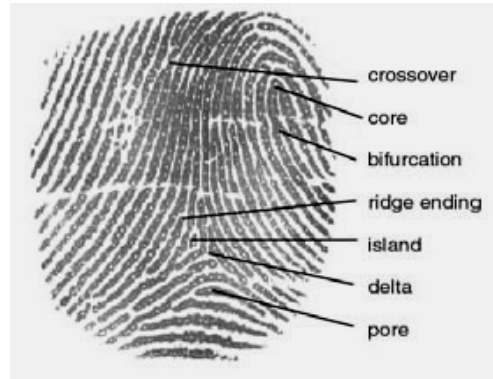
Each of the biometric technologies has inherent strengths and weaknesses. This study does not discuss finger and hand geometry, retinal scan, iris scan, or handwriting recognition because, in their current state of development, they are not practical for use by financial institution customers seeking to remotely log in to their institution's Internet-banking system. The four biometrics chosen for discussion are:

- Fingerprint recognition
- Face recognition
- Voice recognition
- Keystroke recognition.

### Fingerprint Recognition: What is it and how does it work?

Fingerprint technologies analyze global pattern schemas on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data that are extracted from fingerprints are extremely dense; the density explains why fingerprints are a very reliable means of identification. Fingerprint recognition systems store only data describing the exact fingerprint minutiae; images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone

scanning devices attached to a computer. Below is an image of a fingerprint with characteristic labels.



Effectiveness/Protection

Fingerprints are unique, and they are complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are considered to be among the most mature and accurate of the various biometric methods of identification.

Ease of use and requirements

Although end users should have little trouble using a fingerprint scanning device, this special piece of hardware—in addition to certain application software—must be installed on the user’s computer. Financial institution fingerprint implementation will vary according to vendor and degree of sophistication required. This technology is not portable since a scanning device needs to be installed on each participating user’s computer. However, fingerprint biometrics is generally considered easier to install and use than other, more complex technologies, such as iris scanning.<sup>66</sup> Enrollment can be performed either at the financial institution’s customer service center or by the customer remotely after he or she has received setup instructions and passwords. According to fingerprint technology vendors, there are several scenarios for remote enrollment that provide adequate security, but for large-dollar transaction accounts, the institution may request that customers appear in person.

Ratings for Fingerprint Recognition

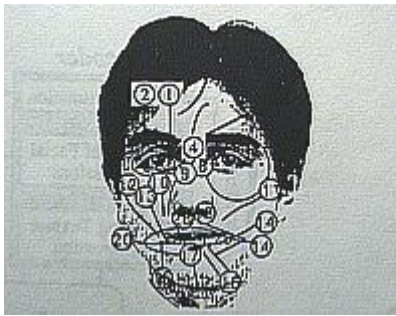
<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Moderate	No	High	Easy

---

<sup>66</sup> The FDIC staff are aware of financial institutions, domestic and foreign, that use fingerprint recognition and other biometric technologies to authenticate ATM users, eliminating the need for an ATM card and the expense of replacing lost or stolen cards.

## Face Recognition: What is it and how does it work?

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.



One face recognition technology, referred to as local feature analysis, looks at specific parts of the face that do not change significantly over time, such as:

- Upper sections of eye sockets
- Area surrounding cheek bones
- Sides of mouth
- Distance between eyes.

Data such as the distance between the eyes, the length of the nose, or the angle of the chin contribute collectively to the template.

A second method of face recognition is called the eigenface method. It looks at the face as a whole. A collection of face images is used to generate a two-dimensional gray-scale image to produce the biometric template.

### Effectiveness/Protection

Facial scans are only as good as the environment in which they are collected. The so-called mug-shot environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan sample. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Facial recognition, like all biometrics, produces results based on probabilities. Once the live scan is performed and compared with the template database, positive identifications are produced according to the level of accuracy set in the system. If the system is set to accept only a match that is determined to be 100 percent accurate, with no margin of error, the rejection rate increases dramatically. As accuracy variables decrease below 100

percent, rejection rates decrease likewise. Facial recognition is generally subject to larger margins of error than more established biometrics, such as fingerprint recognition. Financial institutions considering the use of face recognition for customer authentication should carefully evaluate the adverse consequences of an unacceptably high FAR or FRR.

Ease of use and requirements

Facial scanning is considered one of the easiest biometrics to use. A portable web cam sitting on a desktop computer will suffice. The connecting system must be able to support the web cam and must be loaded with software to create the template and communicate with the authenticating system. The technique is nonintrusive, and user acceptance is typically high.

Ratings for Face Recognition

<b>Implementation</b>	<b>Portability</b>	<b>Effectiveness</b>	<b>Ease of Use- Customer</b>
Moderate	No	Moderate	Easy

Voice Recognition: What is it and how does it work?

Voice biometrics works by digitizing a profile of a person’s speech to produce a stored model voice print, or template. Biometric technology reduces each spoken word to segments composed of several dominant frequencies called formants. Each segment has several tones that can be captured in a digital format. The tones collectively identify the speaker’s unique voice print. Voice prints are stored in databases in a manner similar to the storing of fingerprints or other biometric data.

To ensure a good-quality voice sample, a person usually recites some sort of text or pass phrase, which can be either a verbal phrase or a series of numbers. The phrase may be repeated several times before the sample is analyzed and accepted as a template in the database. When a person speaks the assigned pass phrase, certain words are extracted and compared with the stored template for that individual. When a user attempts to gain access to the system, his or her pass phrase is compared with the previously stored voice model.

Some voice recognition systems do not rely on a fixed set of enrolled pass phrases to verify a person’s identity. Instead, these systems are trained to recognize similarities between the voice patterns of individuals when the persons speak unfamiliar phrases and the stored templates.

Effectiveness/Protection

A person’s speech is subject to change depending on health and emotional state. Matching a voice print requires that the person speak in the normal voice that was used when the template was created at enrollment. If the person suffers from a physical ailment, such as a cold, or is unusually excited or depressed, the voice sample submitted













