

BITS

FINANCIAL SERVICES
R O U N D T A B L E

FRAUD PREVENTION STRATEGIES FOR INTERNET BANKING

APRIL 2003

A PUBLICATION OF THE BITS FRAUD REDUCTION STEERING COMMITTEE

BITS
805 15TH STREET NW, SUITE 600
WASHINGTON DC 20005
(202) 289-4322

WWW.BITSINFO.ORG

FRAUD PREVENTION STRATEGIES FOR INTERNET BANKING

TABLE OF CONTENTS

THE BITS FRAUD REDUCTION STEERING COMMITTEE	3
ABOUT BITS	4
I. EXECUTIVE SUMMARY	5
II. OVERVIEW OF THE PROJECT	6
A. Background.....	6
B. Project Organization and White Paper Availability.....	6
C. Data Gathering.....	6
III. DEFINING THE PROBLEM	7
IV. RISK MITIGATION TOOLS	10
V. BASIC CONTROLS FOR NEW ACCOUNT OPENINGS ONLINE	11
A. Processes.....	11
B. Successful Strategies.....	12
VI. BASIC CONTROLS FOR ONLINE BANKING ENROLLMENT	16
A. Identification and Authentication.....	16
B. Post Authentication Setup.....	17
C. Operational Controls After Enrollment.....	17
D. Additional Fraud Prevention and Detection Tools.....	18
VII. MONITORING CONTROLS FOR BILL PAYMENT SERVICES	20
A. BP and EBPP Enrollment.....	20
B. High or Risky Transaction Review.....	20
VIII. INTERNAL ORGANIZATION FOR MITIGATING ONLINE BANKING RISKS	22
A. Address the Risks to be Managed.....	22
B. Maximize Existing Investments.....	22
C. Provide Vision and Visibility Across the Institution.....	23
D. Facilitate Hiring and Training.....	23
IX. TRACKING AND REPORTING LOSSES ASSOCIATED WITH ONLINE BANKING	25
X. CONSUMER EDUCATION	27
XI. CONCLUSION	29

THE BITS FRAUD REDUCTION STEERING COMMITTEE

CO-CHAIRS: Shirley Inscoe, Wachovia
Bob Jones, FleetBoston

STAFF: Robin M. Slade, BITS

The BITS Fraud Reduction Steering Committee was created to:

- Reduce payment-related fraud losses.
- Secure a critical mass of financial institutions to participate in a shared account database and standardized data collection process.
- Identify successful strategies for reducing check fraud and make those strategies available to the industry.
- Assess fraud risk exposure to electronification and develop strategies to minimize losses

Working Groups under the BITS Fraud Reduction Program include:

- Collections Working Group – Chair: Jim Regan, The Bank of New York
- Debit Card/ATM Fraud – Chair: Laura Sullivan, Citizens Bank
- Electronification – Chair: Dick Clausen, Bank of America
- Identity Theft – Chair: Joe Triano, Citigroup Inc.
- Internet Fraud – Chair: Gayle Helm, Wells Fargo & Co.
- Legal & Regulatory – Chair: Maureen Wharton, J.P. Morgan Chase & Co.
- Shared Databases – Chair: Jan Otwell, J.P. Morgan Chase & Co.
- Statistics – Chair: Rachel Floars, BB&T
- Successful Strategies – Chair: Peter Baldassaro, Hibernia Corp.

INSTITUTIONS THAT PARTICIPATED IN DRAFTING THIS WHITE PAPER

American Express Centurion Bank
Bank of America Corporation
BANK ONE CORPORATION
Capital One Financial Corporation
Citigroup Inc.
Compass Bancshares, Inc.
Credit Union National Association (CUNA)
First Tennessee Bank
Huntington Bancshares Incorporated
J.P. Morgan Chase & Co.
NetBank
The PNC Financial Services Group, Inc.
SunTrust Banks, Inc.
U.S. Bancorp
Wachovia Corporation
Washington Mutual, Inc.
Wells Fargo & Company

ABOUT BITS

BITS, the Technology Group for the Financial Services Roundtable, was created in 1996 to foster the growth of electronic commerce for the benefit of financial institutions and their customers. Members of this non-profit industry consortium include the 100 largest integrated financial institutions in the United States. Throughout its work, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. Major areas of emphasis are security, crisis management coordination, payments strategies, privacy, leveraging industry infrastructure, fraud reduction, and standards. BITS promotes the development of superior, market-driven technologies to strengthen the financial institution-customer relationship, to leverage resources and infrastructure across the industry, and to maintain the industry's position at the heart of the payments system. BITS' Board of Directors is composed of the Chairmen and CEOs of some of the largest U.S. financial services holding companies as well as representatives of the American Bankers Association and the Independent Community Bankers of America.

BITS

805 FIFTEENTH STREET NW, SUITE 600
WASHINGTON, DC 20005
WWW.BITSINFO.ORG
(202) 289-4322

I. EXECUTIVE SUMMARY

This white paper was created by specialists in Internet risk management under the direction of the BITS Internet Fraud Working Group. The Group's purpose is to address Internet fraud, a specific and costly subset of the overall fraud threats faced by financial institutions.

This paper focuses on the most frequent methods by which Internet banking fraud is perpetrated:

- **identity theft;**
- **“friendly fraud,”** or fraud committed by a trusted relative or friend; and
- **internal fraud,** that is, fraud perpetrated by a financial institution employee.

The proliferation of the use of the Internet for financial transactions warrants a baseline level of awareness and vigilance at all institutions. This paper was written to inform financial institutions—regardless of whether or not they offer Internet banking services—about Internet fraud. When a fraud is committed, it behooves every institution, whether or not it is ultimately responsible, to be aware of how Internet fraud occurs and the ways in which it can be prevented. Further, awareness of these issues, in an age in which most customers use the Internet in one way or another, simply makes good business sense. Taking steps to minimize Internet fraud risk and build consumer confidence in Internet banking benefits consumers and builds trust in the industry as a whole.

In discussing Internet threats, it is important to differentiate between two major threat types:

- **Application threats,** in which the person committing the fraud appears to be a legitimate user of the online banking application, but is instead conducting illegal activities. (Firewalls, proxy servers, network filters and similar products will not protect an institution from application-based threats.)
- **Network-based threats,** such as hacks, site-defacement attacks, denial-of-service attacks, and viruses and worms, which attack the core network and infrastructure but don't directly try to carry out transactions and are not application-specific. (Established tools, such as firewalls, can be used to counter such attacks.)

This paper addresses application threats only; it does not address network issues. However, certain situations cross the boundaries. For example, a hacker may compromise a server database containing online banking user IDs and passwords, which can then be used to commit fraud against legitimate users. In this case a network weakness is used to enable an application attack. Technical personnel and application and fraud personnel must work together to understand the threats and ensure that they are being addressed structurally as well as in response to a known hacking penetration.

Internet fraud risks are present for all financial institutions. The information provided here seeks to minimize the risks and make the Internet a safer, sounder, and more trusted environment for everyone.

II. OVERVIEW OF THE PROJECT

A. Background

As financial institutions increasingly offer online banking services to their customers, they must face issues of consumer confidence in the Internet. Consumers are concerned about identity theft and wonder if the Internet is safe for online banking. The answer is yes—if financial institutions, in cooperation with their customers, make it safe. Therefore, building the best controls to prevent fraud and protect customers is of critical importance.

In order to address online banking fraud, the BITS Fraud Reduction Steering Committee was asked to examine Internet fraud and develop a white paper addressing the operational concerns involved. This paper, a product of the efforts of the BITS Internet Fraud Working Group, reviews the processes financial institutions use when enrolling a customer in online banking and opening an account online. It also outlines successful strategies institutions employ to address Internet fraud, including identity theft, and minimize risk in servicing customers via the Internet. The paper covers the processes involved in enrolling customers in online banking, opening a deposit account, and using bill pay services, as well as key points of employee and customer communication that can help prevent Internet fraud.

The methods explored here may not be used in all institutions—or even in the majority of institutions. Instead, the paper’s intent is to raise awareness of the issues and concerns related to Internet fraud as well as to share some current best practices and successful strategies for preventing its occurrence.

B. Project Organization and White Paper Availability

This white paper was created under the direction of the BITS Internet Fraud Working Group and the BITS Fraud Reduction Steering Committee. Project participants are considered to be specialists in Internet risk management. The paper is being distributed to the BITS membership and will be made available to other interested parties. Because of its value as an educational tool, it is available on the BITS Web site, www.bitsinfo.org, in the public area under Fraud Reduction, Publications.

C. Data Gathering

The data-gathering process to develop the content for this white paper was completed by project teams created from participating organizations within the membership of BITS and The Financial Services Roundtable. The teams volunteered to comment on the issues, controls and tools they use to mitigate risk. Each team’s response was vetted with the entire group of participants who were free to comment on the response. All of the data gathered are included in this document.

III. DEFINING THE PROBLEM

Clearly, Internet fraud is a significant problem for the financial services industry. In the American Bankers Association 2002 Deposit Account Fraud Survey Report, 14.9 percent of respondents cited the Internet as being the number one threat to the industry during the next 12 months.¹ Further, community and mid-sized institutions are more apprehensive about Internet fraud than large institutions.

At the same time, financial institutions are increasingly offering online banking services to their customers. This is especially true at large financial institutions, as the chart below illustrates.

Banks Offering Internet Channel or Transactions

Bank Assets in Million Dollars	Under 500	500 – 4,999	5,000 – 49,999	50,000 or More
Inquiry on account information				
Currently offer	52.4%	85.9%	89.9%	93.8%
Plan to offer	21.7	5.1	---	---
Transfer funds within the bank				
Currently offer	53.4	84.6	88.9	93.8
Plan to offer	19.7	3.8	---	---
Transfer funds outside the bank (e.g., bill pay or wire transfer)				
Currently offer	43.7	73.1	86.1	93.8
Plan to offer	20.1	9.0	2.8	---
Opening new accounts				
Currently offer	10.0	28.2	69.4	68.8
Plan to offer	19.4	21.8	5.6	12.5

Source: ABA Deposit Account Fraud Survey Report

Online banking fraud is divided into three categories, each of which poses a unique threat to customers and institutions. The three categories are:

- **Identity Theft** – The most broadly defined of the three types of online banking fraud, identity theft gets the most attention from the media and is of highest concern to consumers. Identity theft can be very simple or quite complex, as these examples illustrate:
 - A collection agency calls and tells a customer that she owes \$5,000 in credit card debt. After doing some research, the customer finds that her identity was stolen and that the thief opened several credit card and checking accounts at different banks, passed bad checks, and accessed her online account and transferred the money out via bill pay.

¹ American Bankers Association, *ABA Deposit Account Fraud Survey Report* (2002).

- A customer receives a returned check notice in the mail and contacts customer service to find that his account was debited \$1,350 via an electronic check. Research reveals that someone obtained his checking account number (perhaps an identity thief spotted the number in the grocery store) and then used the account number to make purchases through the Internet.
- A customer has all of her savings withdrawn because someone in her doctor's office had a similar name and obtained access to her confidential data. Once the identity thief got the information, he or she depleted the victim's funds by transferring them into a new account and then withdrawing from that account.

Identity theft can be extremely difficult for its victims. It can take months or even years to correct the damage it can cause. If the thief has acquired enough information to satisfactorily answer the questions asked by the financial institution, he or she will be able use the information to commit fraud. Because the level and types of questions asked can determine whether or not an identity theft succeeds, those questions must be crafted so that only the true person will know the answers.

- **Friendly Fraud** – This kind of fraud, also known as “civil fraud” or “family fraud,” refers to fraud committed using information that belongs to a trusted friend or family member. As much as financial institutions, independent organizations and the media communicate to consumers that they should not share confidential data, many people do share their information with close friends and family. A growing number of identity theft cases indicate that some close friends and family members will pretend to be the customer and steal from that individual. These are very time-consuming cases to research, but they can present a lower risk to the institution if the case is referred back to the customer to handle in a civil (rather than criminal) manner.

Because it can be devastating to an individual to learn that he or she has been deceived by a close friend or family member, these cases can be especially difficult for victims. Here are some examples of how friendly fraud occurs:

- A customer calls the financial institution's call center because he can't access his account online. While the call center representative is talking with him, the representative can see someone is accessing the customer's account on the Internet. When the representative asks if anyone might know his password, the customer explains that he shared it with his daughter; the password is the same as his ATM password, which he had given to her so she could withdraw money. It turns out that the daughter just left home, not on good terms, and took all of her father's money.
- A customer calls the call center to inquire about her account, and finds that her soon-to-be ex-husband has transferred all of the funds out of her individual account into the joint account using her online user ID. He then went into the branch and withdrew the money from the joint account. The husband disappears with her money.

The strongest defense against this type of fraud is to emphasize to customers the importance of keeping their passwords completely confidential. If a customer wants a trusted friend or family member to have access to his or her funds, the customer should add that person to the account. If the customer does not trust the person

enough to do that, and wants to give someone money, the customer should withdraw the money personally.

- **Internal Fraud** – This type of fraud is not new, but online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions should require a password or PIN for online banking, and the password or PIN should be stored in an encrypted format. Another option is to truncate account numbers and customer data and limit employee access to the full numbers. Of the three types of fraud, internal fraud can be the most costly to financial institutions.

IV. RISK MITIGATION TOOLS

In order to mitigate risk associated with online banking, financial institution policies and systemic controls should create an environment in which fraud can be prevented, detected, monitored and benchmarked against industry standards. These policies and controls should:

- **Require “reasonable efforts”** to be made to ascertain the true identity of individual customers and/or the stated business purpose of each commercial enterprise with which the bank conducts business.
- **Have a know your customer (KYC) policy** that includes the following for personal account opening:
 - Proper identification of the customer;
 - Validation of the customer’s residence or place of business;
 - Consideration of the source of funds used to open an account; and
 - Checking with a service bureau, if applicable, for undesirable customer behavior such as insufficient funds or check kiting.
- **Have adequate ongoing monitoring systems** in place to identify suspicious transactions, such as structuring, transactions inconsistent with the nature of a customer’s stated business purpose, and unusual wire activities. Various operational controls are available to mitigate fraud risk, including:
 - Monitoring transactions coming in and going out of deposit accounts using reports that identify a certain threshold and history of the activity over a specific time frame;
 - Creating reports that monitor large dollar deposits; and
 - Tracking ATM activity based on dollar thresholds over a certain time frame.

Combining technology and sound banking practices can help maintain the security and integrity of financial transactions. When enrolling online banking customers or opening accounts via the Internet, operational controls and software can be used together to mitigate risk. Because most online transactions occur in real time, validation and monitoring should whenever possible be conducted in real time, rather than overnight or through batch processing.

Financial institutions should establish policies and train call center representatives to recognize customer impersonation or “pretext” calls.² When these types of calls are identified, the representative should deny the caller access to information and report the incident. In establishing policies related to caller identification, financial institutions should consider the impact of denying access to legitimate customers, as well as of granting access to someone impersonating a customer. Each institution must determine how much risk it is willing to accept and establish policies accordingly.

² “Pretext callers” attempt to obtain others’ personal information under false pretenses.

V. BASIC CONTROLS FOR NEW ACCOUNT OPENINGS ONLINE

A. Processes

Financial institutions use a number of processes to mitigate Internet fraud risk when opening online accounts. The chart directly below illustrates the various processes and their frequency of use at institutions of different sizes. The second chart shows how effective each tool was found to be based on organization size.

Approaches Banks Have Taken or Are Planning to Take to Prevent Check Fraud Losses

New Account Reviews – During Account Opening Via the Internet				
	Under 500	500 – 4,999	5,000 – 49,999	50,000 or More
Account screening service				
Currently use	15.4%	34.6%	69.4%	75.0%
Plan to use	2.3	5.1	2.8	12.5
Credit bureau scores				
Currently use	11.1	12.8	69.4	75.0
Plan to use	1.0	5.1	2.8	12.5
Customer authentication online (when customer is online)				
Currently use	10.1	20.5	47.2	37.5
Plan to use	1.3	6.4	2.8	6.3
Customer authentication offline (after the session)				
Currently use	7.2	20.5	38.9	37.5
Plan to use	1.6	5.1	---	---

Source: ABA Deposit Account Fraud Survey Report

Effectiveness of Fraud Prevention Procedures (Average Points Awarded: 1=Extremely Ineffective; 5=Extremely Effective)

New Account Reviews – During Account Opening Via the Internet				
	Under 500	500 – 4,999	5,000 – 49,999	50,000 or More
Account screening service				
Average points	4.05	3.79	3.70	3.58
<i>Number of banks responding</i>	44	24	23	12
Credit bureau scores				
Average points	3.74	3.89	3.86	4.20
<i>Number of banks responding</i>	31	9	14	5

Customer authentication online (when customer is online)				
Average points	4.13	3.69	3.94	4.00
<i>Number of banks responding</i>	<i>30</i>	<i>13</i>	<i>17</i>	<i>6</i>
Customer authentication offline (after the session)				
Average points	3.85	3.92	3.31	3.60
<i>Number of banks responding</i>	<i>20</i>	<i>13</i>	<i>13</i>	<i>5</i>

Source: ABA Deposit Account Fraud Survey Report

New account application fraud poses a serious threat to financial institutions' bottom lines. Fraud techniques are becoming increasingly sophisticated, costing financial institutions millions of dollars each year. In combating application fraud, the goal is to strike an acceptable balance between convenience to the *bona fide* customer and difficulty for the identity thief.

To qualify and authenticate an applicant's identity, financial institutions detect fraudulent attempts by linking names, Social Security numbers, addresses, telephone numbers, email addresses and IP addresses for the fraudulent criminal attempts. This can be done by using proprietary and/or third-party verification databases. Depending on an institution's technology infrastructure, this can be done in real time on the Web or subsequently in batch file processing.

According to the ABA 2002 Deposit Account Fraud Survey, one of the highest-ranked tools for effectiveness in preventing fraud is online customer authentication. A variety of new technologies is emerging that may give rise to more effective means of authentication, including digital certificates, tokens, public-key infrastructure, and other vendor or Internet service provider solutions. Today there are significant challenges to implementation with all of these emerging technologies; however, solutions may become available in the future. BITS is monitoring developments in this area through the BITS Authentication Working Group, which tracks and reviews new authentication technologies.

B. Successful Strategies

The following methods are recommended for use in tandem or individually as part of a comprehensive Internet fraud-prevention strategy that includes deterrents to identity theft:

Application Process

- **Limit timeframes** during which applications must be completed to deter fraud operators from keeping an application open while researching customer data.
- **Provide a secure channel** for receipt of the customer's data to assure that the information is not intercepted.
- **Create an audit trail** or request, which may include capture of IP address and/or date/time information, to assist in authenticating the customer at a later date.

Applicant Authentication

- **Use a real-time process** to determine if the customer is accurately representing his or her identity. A real-time process automates the identity-verification and fraud-detection steps, checking at the moment of application data entry. When a customer fills out an online application, the institution should collect the personal data first and perform the ID verification and fraud checks before allowing the customer to proceed to account funding.
- **Ask “in-wallet” questions** to verify that the data are correct and that the identity exists by comparing various data sources. In-wallet questions ask for the type of information a fraud operator would be able to get if he or she had stolen a wallet, such as name, Social Security number, driver’s license number, or credit card numbers. In-wallet questions are recommended to verify that an individual person’s identity exists. Used alone, however, in-wallet questions cannot verify that the individual applying for a new online account is actually who he or she says.
- **Use “out-of-wallet” questions** to the extent practical. Certain suppliers are including out-of-wallet questions, which are generated dynamically from information in an individual’s credit bureau report. These questions may be presented as four or five multiple choice questions, such as, “Which of the following lenders holds your first mortgage account?” or “How much is your monthly mortgage payment?” Only the “real” person should know the right answers.
- **Use “out-of-credit” questions.** These questions ask for information that cannot be found on a credit report, such as what high school the person attended or what kind of car he or she drives. Using these questions **may** require a vendor who can supply the necessary data.
- **Provide standard field validations** to ensure the customer entered all of the data on the application in the correct format.
- **Verify application data** by providing checks against Social Security number and date of birth, comparing and verifying that the area code belongs with the state of residence, checking the driver’s license format (actual driver’s license number to address and name in states that allow it), and confirming that both the former and current address fields are valid and match the United States Postal Service mailing addresses.
- **Compare all names on the application** with the Specially Designated National (SDN) List of the Office of Foreign Asset Control (OFAC) to determine if the account should be refused or funds should be blocked.

- **Partner with third party suppliers of application pattern recognition services:**
 - **Web system environment tracking** prevents fraudulent overuse in a system. For example, an applicant can be restricted from going through the application process more than twice within a 72-hour period.
 - **False address tracking** monitors the number of times the same address has been recycled with different last names and Social Security numbers.
 - **Various data checkpoints** check data; for example, Social Security numbers can be checked against numbers of deceased persons, persons reported missing and numbers never issued; addresses can be checked against known mail drops, state prisons and national parks, post office boxes, etc.; and phone numbers can be checked to identify cell phones or pagers.
 - **External options** can be used to validate the customer's identity and qualify the applicant. Databases can track ongoing fraudulent attempts by linking name, Social Security numbers, addresses, telephone numbers, email addresses and IP addresses to the fraudulent criminal attempts. Depending on the institution's technology infrastructure, this can be accomplished in real time on the Web or subsequently in batch file processing. There is a growing list of companies entering the fraud mitigation and identity verification marketplace. Shopping for the best solution to meet your needs and budget is recommended. External solution providers include:
 - ChexSystems
 - eFunds – Chexsystems Qualfile and Integreat! Solutions
 - Equifax Secure
 - Experian's Authentication Solution series
 - Trans Union - Achievant

After Applicant Approval

- **Wait for funding prior to opening an account.** Financial institutions can prevent criminals from accessing ATM cards, checks and PINs by requiring a waiting period. A waiting period can also prevent criminals from learning the institution's policies and procedures.
- **Require that a signed application be on file.** An application can be used to compare signatures on checks, payments, ACH authorizations and wire requests. Tools can include signature verification software and use of check images.
- **Require customer authentication to be completed in the branch or by contacting a call center.** Two different scenarios constitute an applicant's agreement to the terms and conditions for deposit or lending accounts that online banking offer: One is waiting for a signed agreement prior to opening the account; the other is accepting an electronic agreement with the online application. Bank policy may dictate that an application be signed in a branch, since branch authentication offers the most security. The process of accepting electronic agreements should also incorporate a real-time systematic authentication process that is reliable and minimizes the risk inherent in online applications.

- **Use the bank’s internal “hot/warm file” systematically.** A hot/warm file can also be a good validation tool against existing confirmed fraudulent applications. Fraud rings that target online banks often use similar application information. Using internal files can help thwart them.
- **Implement manual fraud screening on initial deposits.** This can be done with images captured by check-processing equipment within a very short time after the checks or deposits have been captured by the check-sorting equipment. The review can be based upon dollar amount, high-risk handwriting and other fraudulent check characteristics. While it does require back-office operations review, this type of monitoring can protect the bank of first deposit and mitigate the risk with online banking deposits.
- **Mail account verification to the customer at the address supplied in the online application.** Frequently, identity thieves will use a true person’s demographic information to apply for an online account and subsequently (within a day or two) call in to request a change of address. Mailing verification to the address originally supplied helps to confirm that the customer is the true person that applied for the online account. A number of different scenarios can result, two of which are the receipt of return mail, which would require back-office monitoring and subsequent account restrictions, or a call from an individual who says he or she has not applied for the product.

As stated earlier, financial institutions must strike an acceptable balance between offering convenience to the *bona fide* customer in opening a new account online and deterring the identity thief. By using many, if not all, of the suggestions above, financial institutions can better prevent fraud and detect identity thieves.

VI. BASIC CONTROLS FOR ONLINE BANKING ENROLLMENT

A. Identification and Authentication

Assuming that the customer has been properly verified and accepted at the opening of an account, enrollment for online banking consists of validating that the person attempting to enroll is in fact the same one who opened the original account. This involves verifying the following:

- **Basic identity.** To verify basic identity, the customer supplies an account or customer number that was given when the account was opened. This number must have a PIN associated with it, as described below. An account or customer number is *not* considered to be secret information. It is readily available from trash, mailings, and is visible to employees. Its only value is in ensuring that the correct customer has been located on the bank's system of record.
- **Subsidiary data.** These data may be used to "raise the bar" against a fraudster. The data are not secret in any meaningful way but may at least require a fraudster to spend additional time to obtain it. Analysis of failed enrollment attempts (from insufficient or incorrect subsidiary data) may highlight to fraud departments that there is an attempt being made against a certain person or account, *but subsidiary data should not be relied on in the absence of the correct secret data.* Typical subsidiary data might include a Social Security number, name, address, amount of the latest deposit, or location of the branch where the account was opened. Note that these data must be available on the system of record in order to be verified.

One form of subsidiary data that has more strength is a credit card suffix, such as Visa CVV2. This number is printed on the back of the card but is not part of the imprinted account number. By requiring the CVV2, the bank is reasonably assured that the presenting person at least has the credit card in his or her possession (although it does not prevent using a stolen card from being used).

Business customers are generally required to submit additional data, including company name, TIN, and the employee name in order to enroll. However, this enrollment is just for Web access to the retail system or a version of it. Sophisticated cash-management systems generally will require manual, offline setup.

- **Secret data.** The only secret data that are shared between the customer and the bank is a PIN on an opened account, where the PIN has been delivered out-of-channel, preferably mailed to the statement address of the account or selected in a branch. The PIN should be attached to a specific account, is never visible to any bank employee, and is stored in an encrypted form in the system of record.
- **Systematic lockout.** Systematic lockout by real-time monitoring controls set on the system's parameters locks a person out after two or more invalid attempts to access account information or transfer funds.

The enrolling application, then, requires entry of (1) the basic identity data, (2) some subsidiary data, and (3) the secret data. This information is matched to the system of record's data, verified through outside databases, and, if verified, the customer enrollment is accepted. Remember, at this point the customer should already have passed general account-opening tests, e.g., cross-checking phone number and physical address, and these are not, in general, re-verified here. If enrollment fails, a limited number of retries should be allowed before the attempt is terminated and this failure is logged. If the customer is already enrolled for online banking, the system should prevent re-enrollment without manual intervention and direct customer contact.

B. Post Authentication Setup

Once the customer has been verified, he or she should be required to create an online identity. This is how the customer will log on in the future. This identity should not include any of the data required for enrollment and should consist of:

- A **self-selected user ID** that is used only on the Web site, and is never printed out for statement mailings, etc. Note that this ID is not considered secret since it is generally visible to employees. However, it may raise the bar slightly and pose an additional knowledge or guess requirement against a potential fraudulent entry.
- A **self-selected Internet password**, which should replace the PIN for Internet authentication since the PIN is generally 4 to 6 digits and as such is far too small to resist a brute-force cracking attempt. The more characters used in an Internet password, the more effective it is, so institutions should allow up to 20 characters. Passwords should be stored at the financial institution in an encrypted format and should never be visible to employees, including call-center representatives.

C. Operational Controls After Enrollment

Two final steps should be taken after a customer is enrolled in online banking:

- A **“Welcome to online banking” letter** should be mailed to the statement mailing address. This letter informs the customer to call or email the bank immediately if he or she did not enroll in online banking. (This will be ineffective as a fraud-prevention tool if a hijacker has changed the customer's mailing address recently.)
- **Customer behavior should be tracked** for at least the first 30 days to attempt to identify suspicious or out-of-pattern activities. The customer should be contacted if there is a shift in behavior patterns, while suspicious behavior (e.g., completely draining several accounts into one in a short period of time or attempting to change the account address) should lead immediately to account blocking and customer contact.

Institutions must not only monitor open accounts for suspicious activity and unusual transactions, they must also implement the technological controls that constitute the monitoring and detection processes, such as:

- **Providing back-end controls** that can prevent account takeover scenarios with policies that require user IDs and passwords to be different.
- **Providing a systematic control that can prevent account takeover** with PIN identification (which must be changed on first access) and customer-generated nicknames and passwords.

Finally, the system should have the ability to allow a logged-on customer to change his or her password at any time, and the bank should encourage customers to do so periodically. This may hinder a determined penetration attempt where the fraudster is working over time to guess the password. Resetting the password forces the fraudster to begin the password search all over again. Business customers may be required to change their passwords regularly, typically monthly. The system should prevent some number of previous passwords from being reused (typically 13).

D. Additional Fraud Prevention and Detection

Customized reports and manual monitoring of account activity can provide a safety net to financial institutions for mitigating fraud losses by preventing or reducing the amount of online high-risk transactions. One risk strategy involves monitoring transactions coming in and going out of deposit accounts by developing reports that identify certain dollar thresholds and comparing them to the account activity history over a certain time frame. Other strategies include reviewing a report that monitors large-dollar deposits and subsequent ATM withdrawal activity based upon dollar thresholds over a certain time frame.

The following are a few of the tools institutions use to supplement front-line account authentication and information-verification processes. These tools also provide details on account data that can be investigated and reviewed from a root-cause perspective to track trends month over month and year to year. This can be a control to document improvements with the implementation of new tools and/or strategies.

Supplementary tools include:

- **Reviewing rejected transfers** to determine if there have been unauthorized access attempts.
- **Reviewing employee accounts added to a new or existing account profile.**
- **Reviewing large-dollar (>\$2,500) “unfunded” transfers** (these could be transactions from an overdraft line of credit).
- **Using account-level warnings** to alert the institution of suspicious activity or high-risk transactions like high-dollar transactions or risky deposit activity.
- **Monitoring debit card activity**, i.e., creating a report that examines high velocity and activity of transactions within a certain period of time. This method is highly successful in identifying account takeover activity after an account has been opened.

- **Using the most conservative Regulation CC rules for account opening and large deposits;** this permits the financial institution to investigate the source of funds and provides confidence that there will be sufficient time to be notified of a return deposit.
- **Monitoring bill pay transactions** with high-velocity or dollar amount to detect transactions that may be inconsistent with the nature of a customer's stated business purpose.
- **Reviewing high-dollar transactions** within 30 days of address change on new accounts for potential money laundering or structuring scenarios.
- **Using a vendor** for both money laundering and fraud-transaction monitoring

VII. MONITORING CONTROLS FOR BILL PAYMENT SERVICES

Fraud through bill payment (BP) and electronic bill presentment and payment (EBPP) products can occur on an existing account that has been fraudulently taken over, as well as with a new product opened using a stolen identity. BP and EBPP products offer a faceless environment from which a fraudster can siphon funds from an account. Since BP and EBPP services are often provided by third-party vendors, institutions must monitor enrollment of these services, as well as high-dollar or risky transactions.

BP and EBPP fraud can also occur when the service is enrolled through an outside vendor directly, which allows the person enrolling to use any transaction account at any institution to fund the payments. In these cases institutions have no control over the enrollment and verification process. With this type of fraud the customer usually notifies the institution. In most cases, with timely notification, recovery of the funds is possible through an ACH- unauthorized return. Although the victim's institution is usually able to recover funds by returning the ACH, the customer will likely feel violated and may feel that his or her institution, online banking, and/or bill pay is not secure. (Customers do not always understand that the debit is being initiated from outside of their institution.) A victim may also feel frustrated that the institution didn't protect them and prevent the fraud from occurring.

Establishing a relationship with outside payment providers can be helpful in preventing this kind of fraud, or identifying it in its early stages. These relationships can provide a vehicle for the provider to verify account ownership with the institutions at the time of setup with the provider. They can also be useful when the providers are reviewing their risk reports.

A. BP and EBPP Enrollment

When using a third-party vendor for BP or EBPP, it is important to keep the enrollment process at the institution rather than with the vendor. There are two ways customers can enroll for BP and EBPP:

- **Telephone and Internet enrollment.** Via telephone or Internet, customers can use pre-existing authentication measures similar to the criteria used for enrollment in online banking.
- **In-session enrollment.** Customers can enroll during a secure session initiated with their user ID and password. In-session enrollment in BP and EBPP is preferred because the customer has already been authenticated through the sign-in process (assuming the online banking enrollment is not fraudulent).

B. High or Risky Transaction Review

Institutions may review BP and EBPP transactions and payment schedules that are risky or unusually active. It is best to review this information before the payments are sent. Ideally it should be reviewed between the scheduling and sending of the payment, or as soon after as possible. This way, the institution has a greater chance of preventing a risky payment from being sent, or of placing a stop payment on a paper item that has already been sent.

Some criteria for identifying risky transactions are:

- **Multiple bill payments** that will deplete the balance in the account;
- **Payments of maximum amounts;**
- **Payments made to individuals** rather than merchants; and
- **Payments on an account with a recent change** of address/phone number.

VIII. INTERNAL ORGANIZATION FOR MITIGATING ONLINE BANKING RISKS

A financial institution's overall structure will determine how it addresses online banking risks. However, certain methods of addressing these risks can be applied to all institutions. The guiding principle behind these suggestions is to establish a well-defined process for communication between all areas affected by online banking risks.

A. Address the Risks to be Managed

Before determining how to organize to manage online banking risks, financial institutions must make certain there is a clear understanding of the risks to be managed by the group. Many risks associated with online banking can be found in multiple business units within the institution (call centers, consumer lending, etc.). Therefore, in order to avoid duplication and identify gaps in risk coverage, responsibilities should be clearly defined.

Does the institution **have a policy** for establishing the group that should manage these risks? If not, a policy should be developed that clearly establishes the rights, roles, responsibilities and authority of the group. At a minimum **the policy should:**

- **Establish the scope of the risks to be managed** by the group.
- **Establish the authority** for the group to develop the standards and guidelines necessary to execute the policy.
- **Determine reporting responsibilities** and management authority for the group.
- **Address interactions with other business units** (compliance, consumer lending, privacy, etc.), establishing fixed and dotted reporting lines where appropriate. A means of resolving any real or apparent conflict in the authority of different business units should also be established.

Determining how the group will interact with other business units will help define the composition of the online banking risk management group and identify the extent of resources (human capital and otherwise) that may already be available within the institution to help address these issues.

B. Maximize Existing Investments

In order to avoid duplication of services, institutions can leverage their existing risk management capabilities. Certain business units (e.g., information security, consumer lending) may uncover meaningful information concerning online risks, regardless of whether that is their primary responsibility. If those business units share information, it may not be necessary to include representatives from that area to the online banking risk management group.

Efficiencies can also be achieved by creating internal partnerships. The nature of those partnerships will vary based on the governance and structure of a particular institution; however, at a minimum the online banking risk management group should participate or at least interact regularly in the risk-management, compliance, privacy, legal, and information-security groups.

This kind of participation is essential because it allows the online banking risk management group to ensure that risks that arise in online banking but fall in the purview of other areas of the institution are identified and properly considered. Without this level of participation, these issues may go unnoticed until problems begin.

C. Provide Vision and Visibility Across the Institution

The group responsible for managing online banking risks should participate in the institution's risk management committees, particularly those committees that address compliance with new regulations (such as the USA Patriot Act) and changes in Internet technology. This kind of participation helps members to identify and anticipate changes that may affect online banking.

In addition, the online banking risk management group must have the clear, formal support of senior management. Establishing a policy to support these efforts may be the most effective way to convey this support. Published, internal statements by senior management acknowledging the role all business units have in managing the risks associated with online banking can help reinforce the policy.

D. Facilitate Hiring and Training

Unique exposures should be considered in establishing a fraud/risk management organization for online banking. While online banking is still relatively new, staff experience should not be gained solely through trial and error. **Two major areas should be considered in selecting staff to fill the online banking fraud and risk functions:**

- First, recognize that, unlike other delivery channels, the **Internet delivers products and services without direct personal interaction with the customer.** Depending on how you establish your service, a customer can apply and open an account, including all fulfillment, without a single paper document being exchanged.
- Second, since online delivery of banking products and services is still relatively new, **problems and issues are still evolving.** Knowledge of the fraud patterns and methods are not as well-established as they are in other delivery channels.

Candidates that are able to adapt to this environment may be identified by considering the unique characteristics of online banking. A risk management candidate cannot be assumed to be well-suited to the online environment simply because he or she has previous risk management experience. Financial institutions should seek individuals who recognize the uniqueness of the online environment and can identify new methods of addressing those risks. Institutions that fail to recognize this will likely miss opportunities available through the channel and/or sustain substantial losses. Successful employees will be those that are capable of evolving with the channel. They should be able to stay ahead of the curve as the Internet matures, and be capable of adapting to change as products and marketing seek to meet new customer demands at what seems an ever-increasing pace. Successful employees will also need to adapt to the eventual maturing of online fraud schemes and patterns. Such employees should seek development opportunities by participating in relevant industry organizations and attending seminars.

In addition to these considerations, online fraud/risk management personnel must also fit well with the organization's structure. Online banking can affect virtually all products and services offered by the institution, so online fraud/risk management staff must be able to work well across the entire organization and have exceptional inter-organizational skills. As is the case in any large organization, and quite often in smaller ones as well, the "unofficial" relationships are the most critical ones to success. If your staff is not able to establish effective communications informally, it is unlikely the formal ones will be totally effective. These individuals need to build their visibility and credibility throughout the organization. For example, product managers who are increasingly viewing the Internet as a must-have solution need to understand the value of online risk management. The insights and advice that an effective fraud/risk management group can provide can help ensure online products and services are developed, implemented and delivered effectively.

IX. TRACKING AND REPORTING LOSSES ASSOCIATED WITH ONLINE BANKING

Losses associated with online banking should be tracked in accordance with the ABA's standard reporting categories. However, institutions must capture additional detail in order to understand the nature of the fraud losses and pathways, including account age, account source, and how the money came in and left. These details should then be able to be translated into ABA categories and reported.

The first step is to adopt a consistent and standard definition of "Internet fraud." Customers who use the Internet are often heavy cross-channel users, which complicates loss analyses. For example, a customer may open an account by telephone, move money via the Internet, and then over-withdraw it from an ATM. Or a person may open a credit card via the Internet, charge large sums at merchants, and disappear. The same customer may also open a card by mail and then charge sums through Internet merchants. Which of these would be considered Internet fraud? The following **examples of Internet-related losses** may help clarify the distinction:

- **The account was opened via the Internet.**
- **The bulk of the transaction activity that set up the fraud was conducted on the Internet**, regardless of how the money was ultimately extracted.
- **Account-takeover activities were carried out over the Internet** even though other kinds of fraudulent activities were carried out, e.g., start-fraud on a credit card.

Perhaps because of confusion over how to track Internet-related losses, many institutions find tracking these losses difficult. Some may also be hesitant to report Internet-related losses due to reputation risk concerns. However, organizations should understand that customers are generally aware that losses will occur, and that they should be accurately tracked and reported. Accurate tracking is critical to accurately assess the level of exposure an institution faces, and to determine whether losses are increasing or decreasing. The table below illustrates that electronic banking fraud is often not tracked.

**Banks Having Financial Losses in 2001 from Electronic Fraud
(Percentage of Banks)**

Bank Assets in Million Dollars	Under 500	500 – 4,999	5,000 – 49,999	50,000 or More
Percentage of banks having losses	32.8%	73.9%	93.3%	100.0%
Tracking the loss amount	17.6	47.7	63.3	66.7
Unable to track the loss amount	15.2	26.2	30.0	33.3
<i>Number of banks responding</i>	<i>296</i>	<i>65</i>	<i>30</i>	<i>15</i>

Source: ABA Deposit Account Fraud Survey Report

Standards for classification and reporting are evolving, but institutions can adopt their own rules until industry standards are in place. As part of the BITS Fraud Reduction Initiative, BITS is developing a methodology for capturing and reporting Internet fraud statistics.

X. CONSUMER EDUCATION

Consumer education is critical to preventing Internet fraud. Most individuals will take action if they believe it will decrease their chances of being victimized by fraud, as long as the action does not significantly inconvenience them. By educating customers, financial institutions can decrease their fraud losses.

The following are consumer tips to prevent fraud. Institutions can share this information with customers through various channels, such as postings at the branches, flyers sent with monthly statements, emails, through a Web site, and/or by request to a call center.

CONSUMER TIPS TO PREVENT IDENTITY THEFT AND OTHER FORMS OF FRAUD

- **Ensure you know the person/entity you are giving information** to over the Internet.
- At least once a year, **order copies of your credit report** from each of the three major credit bureaus, ensuring all of the information is accurate.
- **Monitor your accounts and monthly statements thoroughly**, ensuring that all the activity is accurate. If your account statements are late, immediately contact your bank(s) to ascertain if and when they were mailed.
- **Always thoroughly tear or shred personal information**, such as pre-approved credit offers, that may contain account information, Social Security numbers, date of birth, etc.
- **Check merchant privacy policies** and only shop with those who have published privacy policies that you agree with.
- **Only do business with Internet companies that use a secure form** to capture private information, such as an account numbers or credit card numbers. (The key symbol on your browser status bar indicates whether or not a page is secure.)
- **Avoid instant credit offers**, ensuring they are properly shredded/discarded.
- **Ensure your computer(s) are equipped with anti-virus protection and firewalls** to help keep trespassers out. Always back up your data.
- **Never divulge personal information to anyone**, as identity thieves often obtain information through social engineering.
- **Avoid purchasing a product from a merchant or an auction site where the deal looks “too good to be true”** because it usually is.

- **Confirm the legitimacy of an online business by clicking on the solid lock or key symbol on your browser window**, which provides information about the merchant from the server certificate. If the certificate was issued by an independent certificate authority, due diligence has been performed on the business. If someone has cloned a site, the site will not have a certificate. If the certificate name does not match the site, do not use it and notify the institution.
- **Always protect your account information.** Don't write your personal identification number (PIN) on your ATM/Debit Card. Don't write your Social Security number and/or credit card number on a check.
- **When using your ATM, cover your hand when entering the PIN number** to protect the information from shoulder surfers.
- **Carry only those pieces of identification you absolutely need**, and keep them secure.
- **Always log off from your online banking session.**
- **If you suspect your identity has been stolen, contact your financial institution and the authorities immediately.** U.S. consumers should file a police report with their local police department and call the Federal Trade Commission at 1-877-ID-Theft. Complaints can also be reported to the Internet Fraud Complaint Center at www.ifccfbi.gov. Contact the three credit reporting agencies to place a fraud alert on your record. Maintain a log of all contacts you make with the authorities regarding the matter, including the name, title, phone number and police case number, in case future contact is required.

XI. CONCLUSION

Identity theft, “friendly fraud” and internal fraud conducted via the Internet pose significant threats to the financial services industry and our customers. However, while there are certainly a great number of unknowns, many serious threats are known and containable, and can be mitigated with the good banking practices outlined in this paper.

While the Internet offers great opportunity, its pervasiveness also poses a real threat to every business, whether or not it offers online services. In contrast to other technologies, lack of participation in online technology will not protect a financial institution from its dangers. For example, a customer’s account can be compromised if someone fraudulently uses her account for an online transaction, whether or not the institution where the account is held offers online banking. Further, an institution that does not offer certain services, such as online bill payment, will likely find that its customers often look to the institution for help when problems arise with that technology. Financial institutions cannot afford to be uninformed in these situations, nor can they simply be passive players. Instead, all institutions must be vigilant and stay abreast of developments in online banking.

BITS was founded on the principle that the challenges the financial services industry faces can be mitigated when institutions work together to create common solutions. The Internet can be a great benefit to the industry. When financial institutions identify its risks, implement common practices, train employees and communicate with customers, they will be better able to use the technology to their advantage. Further, implementing mitigation practices now can lay the foundation for basic controls to be built upon as the Internet evolves.

There is not, nor will there ever be, a perfect strategy to eliminate Internet risk to financial institutions and our customers. However, the widespread use of mitigation strategies can minimize many risks and make online banking safer for consumers and institutions. When online banking is more secure, and consumers have confidence in the services their financial institution provides, everyone can benefit.