c2

Federal Deposit Insurance Corporation

FRAUD Alert

FDIC

Spring, 1999 Volume 7, Number 1

Pretext Calling and Identity Theft

Bank customers are not the only ones gaining access to their account information. Organizations and people who call themselves "account information brokers" have been accessing customers' confidential financial information through "pretext phone calling."

Pretext phone calling is a practice used by an information broker pretending to be a customer. With technological advances making it possible to consolidate disparate pieces of information about a consumer, brokers can obtain personal identifying information, such as a Social Security number. The broker then contacts a financial institution by telephone and uses this information to convince employees to provide additional information over the phone. The account information that the broker obtains from the bank can be sold to third parties, including private investigators or debt collection services.

The federal government has taken notice of this practice and is taking action. Vice President Al Gore has advocated an Electronic Bill of Rights to protect consumer privacy. One element of the proposed bill of rights concentrates on the need for action by the government and the private sector to prevent people from fraudulently obtaining confidential customer financial information from a bank.

Separately, legislation has been introduced and referred to the House Banking Committee that would make it a federal crime to obtain personal financial information from financial institutions under false pretenses. This bill would make it illegal to obtain, or attempt to obtain, or cause to be disclosed, customer information of a financial institution by knowingly making false statements or representations to a financial institution or a customer. The measure also would make it a crime to receive customer information obtained from a financial institution knowing that the information was acquired under false pretenses.

Financial institutions that release information in response to a pretext phone call would not be held liable under the bill. However, financial institutions and their customers who fall prey to pretext phone calling would have the right to sue any person, including an account information broker who obtains customer information in violation of the bill's provisions.

Congress recently passed H.R. 4151, the Identity Theft and Assumption Deterrence Act (Public Law 105-318). The new law makes it a federal crime to fraudulently use another person's means of identification to assist in committing some other state or federal felony. Violations of this statute are punishable by fines up to $250,000 and imprisonment for up to 20 years, depending upon the severity of the crime in which the means of identification is fraudulently used.

For example, a person who uses another person's means of identification in connection with a drug-trafficking crime could receive the maximum sentence. It would be a violation of this statute to use information that provides a means of identification obtained through pretext calling to carry out a criminal scheme.

*See **next page***

Pretext Calling and Identity Theft

Continued from page 1

Financial institution regulatory agencies have also responded to the growing anxiety over the use of confidential financial information. Banking agencies have issued guidance to financial institutions (available at www.fdic.gov/banknews/fils, then click on September 1998) to enhance their awareness of the confidentiality and sensitivity of customer information, while pointing out measures that financial institutions can take to protect information. To avoid the risk of an inappropriate or unauthorized release of information, financial institutions are encouraged to:

- Educate employees about the tactics used by account information brokers;

- Develop policies that establish precisely the types of information and the circumstances under which an employee may release customer account information over the telephone (e.g., limit access to confidential information on a need-to-know basis);

- Train employees about their responsibility to safeguard customer account information;

- Maintain strong internal controls to ensure that customer information is adequately safeguarded from improper disclosure (e.g., provide customers with unique authorization codes); and

- Monitor and audit activity to evaluate susceptibility to unauthorized disclosures (e.g., have the bank staff conduct pretext calling tests).

Financial institutions should file a Suspicious Activity Report and contact regulatory and law enforcement agencies when there is an attempt to obtain customer account information under false pretenses.

Customers can also play a role in preventing unauthorized disclosures of sensitive financial information. Customers should ask their bank about its privacy policies and information practices. They should also ask the institution about the types of security it uses to prevent the improper disclosure of their account information.

Customers should understand what types of personal information the bank will provide over the telephone, to whom it will provide that information, and what forms of identification they will require from a caller before providing the information. Customers who suspect their account information was improperly obtained from the financial institution should report the matter to their bank officials.

Financial institutions are challenged by their desire to provide customers with quick access to their account information and the bank's need to protect that information from unauthorized access via pretext phone calling operations. In the end, banks must take appropriate actions to instill in customers the confidence that their financial information is safe.Δ

The ***Fraud Alert*** is published quarterly by the
Federal Deposit Insurance Corporation,
550 17th Street, N.W.
Washington, DC 20429

This newsletter is produced by the
Office of Corporate Communications, FDIC.

Donna Tanoue,*Chairman*

Phil Battey, *Director*
Office of Corporate Communications

Frank Gresock, *Editor*

Graphics by **FDIC Design Group**

Cyber-Thieves Creating Debit Cards

Thieves that guess debit card account numbers have caused losses to several financial institutions. The thieves use number-guessing computer programs that can be downloaded from the Internet. Number-guessing programs use sophisticated mathematical calculations to determine relationships between the digits in valid account numbers to produce other numbers that also might be valid.

To make fraudulent charges using a number-guessing program, thieves must first steal a valid account number. Stealing debit or credit cards from customers or rummaging through the trash for receipts are the most common ways to get valid account numbers. When a valid account number is obtained, a thief can use a hacker program like "Creditmaster" or "Credit Wizard" to generate other possible numbers. The generated numbers are then used to produce counterfeit cards or to purchase items through mail order. Not all of the generated account numbers will work, but hackers keep trying until they find numbers that do work.

Hacking tools are not illegal and they are plentiful on the Internet. Initially, these hacking tools were used to go after credit cards. But now they are also being applied to the increasingly popular debit cards. Because of the threat to debit cards by hackers, we are bringing it to your attention although the *Fraud Alert* dealt with credit cards and hackers in the Autumn 1996 newsletter. Programs such as "Creditmaster" and "Credit Wizard" can easily be found and downloaded from a hacker's Web site in minutes. These programs can generate hundreds of account numbers for credit and/or debit cards in seconds using a valid account number as well as identify the bank that issues the card. The hits at financial institutions have targeted certain off-line debit cards that allow merchants to deduct funds directly from a cardholder's checking or savings accounts for purchases. Debit and credit cards are convenient for consumers and merchants, but without proper security measures, a financial institution can lose a lot of money quickly.

Law enforcement authorities believe that organized crime groups in Asia are behind several of the number-guessing schemes. These groups appear to be working with corrupt merchants who knowingly accept counterfeit cards.

Financial institutions can protect themselves from this type of fraud with adequate security programs tailored to meet their own needs and including measures such as:

- Using risk-management software to provide early and accurate fraud detection. This type of software is built around specialized risk models.

- Advising their merchants not to print entire account numbers on customer receipts.

- Advising merchants to question a shipping address used by a mail-order buyer that does not match the billing address. (This, however, may not be practical in all cases, such as orders from gift merchandisers.)

- Only issuing cards with encrypted codes on the magnetic strips on the backs of the cards for verification. This code is used to electronically verify card numbers when the card is swiped though a merchant's point of sale (POS) or credit card machine.

Each security measure should be tested to ensure that it is working properly. Smaller institutions may be more vulnerable to the number-guessing scheme because they tend to have fewer security resources. An adequate security program should also include procedures on how incidents involving fraud will be handled if they are discovered at your institution. If fraud is discovered, financial institutions are required to file a Suspicious Activity Report with the appropriate authorities.Δ

Remember: Part III, Box 37, "Other"

Remember: Suspected computer crimes are reported in Part III, Box 37, "Other" on the Suspicious Activity Report (SAR).

Under the banking and thrift regulators' current SAR rules, a financial institution is required to report any known or suspected criminal law violation involving an insider, regardless of amount. A financial institution is also required to report any known or suspected federal criminal law violation that involves $25,000 or more if no suspect can be identified—a threshold that drops to $5,000 if a potential suspect can be identified.

Computer crimes are not among the 17 categories of criminal law violations and suspicious activities specified for Box 37, but fall under the general category "Other." Use this category when the offense or activity does not seem to fit any of the specified types of crimes.

With computers driving the operations of financial institutions, criminals recognize the potential vulnerability of these systems. Consequently, financial institutions should be cognizant of the federal computer crime law, 18 U.S.C. 1030. This statute specifically addresses crimes against computers in banks and thrifts, among others protected by the statute; any computer exclusively for the use of a financial institution; or, if not exclusively for such use, used by or for a financial institution where the conduct constituting the offense affects that use.

Three provisions of the law are of particular importance to financial institutions. These are prohibitions against:

• Obtaining information contained in a "financial record" of a financial institution. A financial record is defined as information derived from any record held by a financial institution pertaining to a customer's relationship with the institution. This prohibition may also apply to anyone who hacks into a financial institution's computer system.

• Using a bank computer without authorization or beyond an authorized level to commit fraud. So, anyone who intentionally uses another person's home banking software and steals that person's password in order to transfer money fraudulently into his or her personal bank account has committed a crime.

• Intentionally accessing a protected computer without authorization that results in damage. Under the law, damage includes any impairment to the integrity or availability of data, a program, a system, or information that causes a loss totaling $5,000 over the course of one year. Examples include a disgruntled former employee who has a "back door" into the computer system and uses it to send a disruptive virus into the system, or someone who causes a system outage by flooding an institution's computer system with e-mail requests for information.

Also important to financial institutions are provisions in the statute that outlaw trafficking in passwords knowingly and with the intent to defraud. Further, the law prohibits transmitting to a financial institution threats of damage to protected computers when the intent is extortion. This prohibition applies whether any damage is caused or the offender had the ability to cause damage.

These violations carry penalties of a fine or imprisonment for up to ten years.

So remember, if you detect a reportable offense involving your computers, check Box 37, marked "Other," and describe as completely as possible in Part VII, the narrative section of the SAR, the nature of the illegal or suspicious activity.Δ

A number of errors are turning up repeatedly on Suspicious Activity Reports. On Page 8, you'll find out what they are and how to avoid them.

SPECIAL ALERTS

The following is a current listing of entities that may be conducting banking operations in the United States without authorization. Proposed transactions involving these entities should be viewed with extreme caution. The listing does not include those entities included on warning bulletins issued by the Office of the Superintendent of Financial Institutions (Canada), the Central Bank of Belize, and the Swedish Financial Supervisory Authority. The warning notice for Canada may be found in FIL-106-98, dated Oct. 2, 1998; the notice for Belize can be found in FIL-140-98, dated Dec. 30, 1998; and the notice for Sweden can be found in FIL-121-98, dated Nov. 16, 1998. (These FILs can be found on the our Web site at www.fdic.gov.)

Future issues of the Fraud Alert will list entities whose fraudulent activities have come to light since the last newsletter was published.

ENTITIES THAT MAY BE CONDUCTING BANKING OPERATIONS IN THE UNITED STATES WITHOUT AUTHORIZATION

(Footnotes explained on page 7.)

Access Bank International (Nauru), Ltd.
629 Second Street, SE
Puyallup, WA

Al-Manaf International Merchant Bank
1819 Pauger Street
New Orleans, LA

Atlantic Bank, Ltd.
1300 Division Street, #200
Nashville, TN

Atlantic Caribbean Bank & Trust Co., Ltd.
St. Johns, Antigua

Banca Populara Ardealul (1)
Bistrita, Romania

Banhofstrasse, Commercial Bank AG
(Melchizedek)
110 East 59th Street
6th Floor
New York, NY

Bank of Business Western Samoa
12-A Nampacia-Center
Apia Upolu, Samoa

Bank of Business Western Samoa
6223 NE 8th Avenue
Portland, OR

Bank of Finance
P. O. Box 770729
Woodside, NY

BANQUE de Petite MARTINIQUE (2)
St. George's
Grenada, West Indies

Caribbean Bank of Commerce, Ltd. (3)
Chase Bank of Las Vegas, Nevada
C.I.A. of Las Vegas
7624 San Mateo Way, Suite #206
Las Vegas, NV

Commercial Credit of New York, LLC (4)
Holding Group Corporation
Commercial Credit of New York Holding Corp.
Commercial Banking Group
Commercial Bank, A.G.
Creditanstalt A.G.
110 East 59th Street (6th Floor)
New York, NY

Commercial Intercontinental Bank, Inc. (NAURU) (5)
8249 NW 36th Street, Suite N-106
Miami, FL

Dominion International Bank, Ltd. (6)
Christchurch
Barbados, West Indies

Dunbar National Bank of Maryland (7)
http://www.ncsinccards.com

European Union Bank (2)
(Address Undetermined)

The Excelsior Bank/The Excelsior (2)
International Bank Corp.
Barbados, West Indies

Fidelity International Bank
520 Madison Avenue
New York, NY

First Americans Trust
211 South Washington Street
Sonora, CA

First Americans Trust Company
"aka First Americans"
Oklahoma City, Oklahoma
Apache Tribe General Bank
of Anadarko, Oklahoma
620 East Colorado
Anadarko, OK

First Lenape Nation Bank
Route 1, Box 174D
Anadarko, OK

First National Bank, FSB
First National Bank National Trust and
Savings Association
First National Trust
2614 Wyoming Ave.
Burbank, CA

First Savings Bank
800 W. Oakland Park Blvd., Suite 306
Ft. Lauderdale, FL

First State Bank of Montana
P. O. Box 278
Fairfield, MT

First Zurich National
P. O. Box 20290
Cheyenne, WY

Focus International, Ltd. (2)
West Indies

Greater International Bank of Nauru (5)
719 E. Bird Street, Suite 444
Miami, FL

Industrial Bank, Inc. (8)
Samoa

Liechetensteinische-Amerikanische Union Bank
Corp.
USA Management Office
545 8th Avenue, Suite 401
New York, NY

London Chartered Bank, Ltd.
(Melchizedek)
28720 Roadside Drive, Suite 178
Agoura Hills, CA

Meridian Merchants Bank, Inc. (Nauru)
1420 Fifth Avenue, 22nd Floor
Seattle, WA

Midland Credit & Guarantee Bank, Ltd.
67 Wall Street
New York, NY

Mitsubishi Trust & Banking Co. Finance
Corporation (9)
(Address Undetermined

Mitsubishi Finance Corporation (9)
(Address Undetermined)

Netware International Bank
136 Stutts Road #2
Mooresville, NC

Panacea Bank & Trust
P. O. Box 30054
Bellingham, WA

Prime Bancorp, Ltd.
82 Wall Street
New York, NY

Richard Jones' Bank
111 South Lewis Street, Apartment B
New Iberia, LA

Royal Meridian International Bank (2)
Nauru, Mid-Pacific

South Atlantic International Bank, Limited
f/k/a Americapital International (6)

Swiss Merchant Bank, AG
1730 K Street, N. W.
Washington, DC

Sunfirst Trust Co., Ltd.
912 Thousand Oaks Drive
Virginia Beach, VA

Sunlight Church World National Bank
2255 West 15th Street, #2
and
777 South Figueroa Street
Los Angeles, CA

United Bank and Trust Company (5)
(NAURU)
13351 Bridgeford Avenue #36
Bonita Springs, FL
and
P. O. Box 9076
Naples, FL

United Funding Bancorporation, Ltd.
318 North Carson Street, Suite 214
Carson City, NV

United Overland Trust & Bancorp
2005 Woodmont
Austin, TX

United Pacific Bank, Ltd.
Port Vila, Republic of Vanuatu
South Pacific

Western Credit Bank, L. L. C.
245 Winter Street, S. E.
Salem, OR

(1)Not authorized by the government of Romania.

(2)Not authorized, supervised or regulated by any U.S. financial institutions regulatory agency.

(3)Stricken from the register in Antigua and Barbuda.

(4)None of these entities are affiliated with Creditanstalt, A.G., Greenwich, Connecticut.

(5)License revoked by the government of Nauru.

(6)Banking license has been revoked.

(7)Not authorized, supervised or regulated by the Office of the Comptroller of the Currency.

(8)License cancelled by the government of Samoa.

(9)Not related to Mitsubishi Trust and Banking Corporation. Δ

Tips on Cleaning up Your SARs

Some recurring errors on Suspicious Activity Reports (SARs) are being spotted by federal bank regulators and the Financial Crimes Enforcement Network. You can help make the SAR system more efficient if you heed the following tips:

- Be sure to list your **primary regulator**. This is the federal agency that examines your institution.
- Use numbers – don't spell out amounts.
- Dollar amounts should be shown to the nearest dollar.
- Use the MM/DD/YY format for dates – don't spell them out.
- Try to fit the activity you are reporting into one of the categories. "Other" should only be used if the activity CLEARLY does not fall within one of the categories.
- Be sure your narrative is clear and fully explains the activity. Busy agents rely on the narrative to make initial investigation decisions.
- Always include the location of the main office or branch where the activity occurred. The law enforcement agencies generally assign investigations to the local office where the violations took place.
- Do not send attachments with the SAR. Documentation should be maintained in the bank for review by law enforcement and regulatory officials.Δ

Attn: Chief Executive Officer

FDIC
Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
Penalty for Private Use, $300.00

BULK RATE
MAIL
Postage & Fees
Paid FDIC
Permit No. G-36