Federal Deposit Insurance Corporation

FRAUD Alert

Spring, 1995 Volume 4, Number 4

Con Artists Targeting Checking Account Information

The FDIC has seen an increase in recent months in the number of banks reporting telemarketing schemes directed at getting checking account information from bank customers in order to debit their accounts.

The last time con artists went after checking account numbers was about four years ago, and later they switched back to seeking credit card information. But now it seems they are back, using a variety of ploys to convince people to give them checking account numbers.

In this new round, telephone solicitors tell the consumers anything that is necessary in order to obtain the checking account information. Once that information is obtained, the telemarketers issue drafts to debit the checking accounts of unsuspecting consumers.

The draft processing companies claim to have each consumer's authorization to process the drafts, but the banks have received no written authorization from the consumer, and the consumer has not signed the drafts. Since funds are transferred out of the draft processor's account as soon as the bank will allow it, banks that carry the account and those that debit customer accounts without the proper authorization may suffer substantial losses.

The schemes being used are not new, and some have been around for years. Following is a sampling of some of the ruses being employed to get the consumer's checking information:

The VISA and MasterCard Scam—The consumer receives a postcard offering one of the two credit cards, with a low interest rate and no annual fee. The person must, however, call within 48 hours. But when they do they are told they must pay a one-time fee for the card, which will be debited from their checking account. If the consumer gets anything at all, it may be a list of banks that offer lower interest rate credit cards.

The Prize Scam—A postcard tells the consumer he or she has won a prize. When the consumer phones, he or she is told they have won a trip, a fur, or a car, for example. All he or she has to do is pay shipping charges or taxes, which of course, can be debited from a checking account. The operator is extremely skilled at extracting the checking account information and will debit the account, even if the consumer doesn't authorize it.

The "Let us Sell Your Car" Scam—The consumer, who has placed an ad in the paper to sell his car, receives a call from a telemarketer. The telemarketer offers to market the car around the country for, say, a fee of $349. When the consumer hesitates, the telemarketer assures the customer that all the information can be taken over the phone, but nothing will be charged to the checking account until the customer approves the papers. Of course the account is debited without authorization.

The amounts of these debits generally range from $60 to less than $400.

If you are seeing evidence of this sort of checking account debiting, please call your nearest FBI office. Δ

A Way for Banks to Fight Some of the Oldest Confidence Games

Some confidence schemes have been around for decades and even centuries.

They endure because the con artists involved in these scams are persuasive, determined, and highly mobile. Most important, their schemes work often enough to be highly profitable.

Although these schemes can be tried on any age group, the most susceptible seem to be the elderly, fraud investigators say. Why? A number of factors: they are often lonely, they respect authority figures, they may be affluent, and they are generally too embarrassed to admit to having lost money through a confidence game.

Investigators believe that fraud involving older citizens is increasing and will be with us into the next century, because the population is aging

Let's look at some of these perennial confidence crimes, which require the victims to make large cash withdrawals from their banks:

The Phony Bank Examiner—A depositor is called by someone claiming to be a bank examiner (or a policeman). The victim is asked to help uncover a suspected crime at the bank. In some cases they are told to call 911 to verify the caller's identity, but the call is picked up by the scamster, not the police. This is done by the conman not disconnecting from the call or, investigators believe, by tapping into the phone service. The victim is asked to withdraw thousands of dollars and turn it over to the caller—and instructed not to discuss the transaction with bank employees. The victim is convinced to withdraw the money so that the swindler can mark the bills and catch the dishonest bank employee. Sometimes a second withdrawal is made, with the phony investigator perhaps promising a reward for helping with the investigation.

The Pigeon Drop—One of the oldest con games. This involves befriending the victim, then convincing the victim that a package of currency has been found and should be shared equally. The victim is then convinced to make a large bank withdrawal in order to put up earnest money that will be returned along with one-third of the found money. The victim is then instructed to go to an office building to meet with an authority figure, like an attorney or a broker, only to discover the person doesn't exist and the suspects have fled with the victim's money.

Bogus Home Repairs—There are many variations on this scam. Essentially the homeowner is convinced of the need for some type of home repair or improvement. However, the workmanship and materials turn out to be inferior or dangerous and the cost is far above the estimate. The victim is then coerced into paying the bill, either in cash or by check, which is immediately cashed at the victim's bank.

The Recovery Game—After a victim has lost money in a scam, his or her name may be sold. The victim is then approached by someone claiming to be an investigator who wants to help recover the money. But first he will need some money...

John Bordenet is a senior program specialist in the Criminal Justice Services section of the American Association of Retired Persons. He estimates that only about 3 percent to 10 percent of the fraud against the elderly, like the types described above, is reported.

Jon Grow is the executive director of the Baltimore-based National Association of Bunco Investigators, which is an information network of law enforcement officers who deal

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.
Ricki Helfer, *Chairman*
Alan J. Whitney, *Director*
Office of Corporate Communications
Frank Gresock, *Editor*
T. W. Ballard, *Graphic Designer*

The Milwaukee Program

Below is the generic customer cash withdrawal document developed by bankers and police in Milwaukee to thwart con artists.

CASH WITHDRAWAL ALERT

FOR YOUR OWN PROTECTION: BEFORE YOU WITHDRAW $_____IN CASH FROM YOUR ACCOUNT, PLEASE READ AND SIGN THIS FORM.

Consumers lose millions of dollar each year to con artists. Many scams involve the withdrawal of large amounts of cash from the customer's account. Before you withdraw money, consider the following:

—Have you received a call or met with someone claiming to be an FBI agent, bank examiner, police officer, detective or financial institution official? Do they want you to withdraw money to help in an investigation? Have they promised to return or redeposit money for you?

—Has anyone befriended you, then asked you to put up "good faith" money in order for you to share unexpectedly found money or valuables?

If the answer to any of these questions is "yes," you may soon be the victim of a swindle. You may never see your money again. No financial institution conducts investigations by asking customers for help. No one will share money with you after getting your "good faith" dollars. However, these are common stories given by swindlers who mainly target older customers as victims.

REMEMBER, swindlers are nearly always friendly and have honest faces or pleasant, authoritative voices. This is how they gain your trust.

I have read and understand the above statement. By signing this form, I direct this financial institution to complete my request for cash withdrawal.

Teller_____ Customer_____

Financial Institution Officer_____ Date_____

For more information, you may write to: Det. Dennis M. Marlock, Milwaukee P.D., 749 W. State St., P.O. Box 531, Milwaukee, Wisconsin 53201.

---

with con games. The key to any scheme to defraud, he said, is "controlling the victim."

And in some cases it means the con artist will go to the bank and speak on behalf of the victim.

But the police in Milwaukee have found a way to break that control and give the victim a chance to think about what is going on. Dennis M. Marlock, a Milwaukee Police Department detective, worked with banks there to create a simple program that has cut the number of successfully completed frauds by 85 percent.

Tellers are trained in the steps to take when a customer asks to make a large cash withdrawal. [See page 8.]

The customer also is given a form that warns that they may be a victim of a swindle. The customer, the teller, and a senior officer all sign the form after the bank officer speaks with the potential victim. [See above for details.]

The Milwaukee program is used in Wisconsin and Illinois as well as by some banks around the country. The appeal, said Marlock, "is that it is nearly 85 percent effective and costs nothing." Δ

FDIC Advises Banks with 'Payable-Through' Accounts: "Know Your Customers"

The FDIC has recently warned U.S. banks about the risks of "payable-through" accounts.

Properly supervised, "payable-through" accounts — also known as "pass-through" or "pass-by" accounts — are a useful way for banks to expand services to their customers. The problems arise when banks enter into a pass-through arrangement, usually with a foreign bank, without knowing anything about the institution or its customers.

Under normal circumstances, payable-through accounts enable institutions such as credit unions and investment companies to offer customers services — checking accounts are the most common example — usually available only from full-service commercial banks. That's not where the problems have been. Recently, U.S. banks have been offering pass-through services to foreign banks. This usually means the U.S. bank is providing checking account services to a foreign bank.

Typically, the foreign bank will provide its customers, referred to as "sub-account holders," with checks that enable those customers to draw on the bank's account with the U.S. bank.

The problem with this otherwise innocent-sounding arrangement is that many U.S. banks aren't exercising the same care with the pass-throughs as they are with their domestic accounts. That group of sub-account holders, which may number several hundred for one pass-through account, all become signatories on the foreign bank's account at the U.S. bank. This means that individuals and businesses who may not be subject to the same requirements that U.S. banks impose are nonetheless free to draw on U.S. bank funds.

When U.S. banks allow users of unsupervised pass-through accounts to have access to the bank's funds, those banks can end up inadvertently facilitating unsafe, unsound or even illegal activity. Experience has shown that some U.S. banks simply collect signature cards that have been completed abroad and submitted to them in bulk by the foreign banks.

The U.S. banks then process thousands of checks issued by the sub-account holders. The U.S. banks make little or no effort to verify independently the information about the persons and businesses who use their accounts. This can be dangerous.

Unless a U.S. bank is able to identify the ultimate users of the foreign bank's accounts — most or all of which are off-shore — there is a serious potential for illegal conduct. Recent law enforcement reports confirm that money laundering and similar illegal schemes have involved the use of foreign banks' payable-through accounts at U.S. banks. In those cases, the U.S. banks could be exposed not only to serious damage to their reputations around the nation and the world, but also to significant risk of financial losses resulting from asset seizures and forfeitures when law enforcement authorities move against the illegal activity.

The FDIC has recommended that a U.S. bank terminate its payable-through arrangement with a foreign bank as expeditiously as possible whenever:

1) adequate information about the ultimate users of the payable-through accounts cannot be obtained;

2) the U.S. bank cannot adequately rely on the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers; or

3) the U.S. bank is unable to ensure that its payable-through accounts are not being used for money-laundering or other illicit purposes.

Every safe and sound U.S. bank understands the importance of knowing its customers and understanding their transactions. The wisdom of that principle should be applied to foreign customers using payable-through accounts just as diligently as it is applied to domestic customers.

An institution with questions about payable-through accounts should contact its primary regulator. Δ

New CTRs Available for Oct. 1 Use

The Internal Revenue Service has revised its Currency Transaction Report (CTR) form that banks and other institutions are required to use to help law enforcement agencies detect and prevent money laundering and other illegal activities. The revised form is now available for distribution; however, banks may not begin using the new form until October 1, 1995. The FDIC has sent an advance copy of the form to banks it supervises so that it can be used for training purposes, and so bank employees can become familiar with differences between the old and new forms prior to the effective date.

The new form can be ordered without charge by calling the IRS Forms Distribution Center at 1-800-829-3676. Simply follow the voice prompts, press Option #1 (for ordering blank forms) and make your request by form number (IRS Form 4789). Orders should be placed in time to allow for delivery prior to the effective date. Questions concerning the new forms should be directed to the Financial Crimes Enforcement Network (FinCEN) at 1-800-949-2732. Δ

Heads of Failed S&Ls Indicted for Fraud

A federal grand jury in Chicago indicted two former chief executive officers of failed S&Ls for fraud that caused the loss of hundreds of thousands of dollars to their institutions, *The Wall Street Journal* reported. Indicted were John R. O'Connell, the founder and former chairman and CEO of Skokie Federal Savings and Loan Association, Skokie Ill., and E.M. Huitt, Jr., the former chairman and CEO of Bay City Federal Savings and Loan Association, Bay City, Tex.

Skokie Federal, with assets of $960 million, was declared insolvent and taken over by the government in 1989. Bay City Federal was declared insolvent in 1988.

O'Connell and Huitt were each charged with conspiracy, mail fraud, and wire fraud.

The two are charged with involvement in three related fraud schemes during the 1980s in which they and other S&L executives allegedly did each other favors that damaged their institutions or deceived regulators about their financial condition, said the Justice Department in an *American Banker* story.

In the first alleged scheme, O'Connell and Edwin T. McBirney, III—currently serving 15 years in prison for his S&L dealings—are charged with planning a way to increase Skokie Federal's net worth to appease regulators in 1981.

McBirney would buy $735,000 of Skokie Federal assets using Skokie Federal loan funds, booking a profit for the institution, *American Banker* reported. But because regulators would not have approved of such a transaction, Huitt's Bay City Federal allegedly agreed to be a "nominee purchaser," meaning that some of the money Skokie Federal lent McBirney was passed on to Bay City, which made the purchase, the indictment said.

Related deals for McBirney to buy back the assets from the Texas thrift caused more than $300,000 in losses to Bay City, the indictment said. Subsequent deals between McBirney and Huitt brought Huitt $440,000 in bonuses related to loans that at first earned Bay City fee income but later were delinquent or in foreclosure, the indictment said.

In the second alleged scheme, the newspaper said, O'Connell is charged with arranging in 1982 for McBirney to buy $999,500 of Skokie Federal assets with a Skokie Federal loan using another nominee purchaser, Texas S&L executive Jarrett Woods. The indictment said Woods later transferred the assets to McBirney.

However, one of McBirney's loans was secured by an apartment complex that later defaulted, giving Skokie Federal about $1 million in losses, the newspaper said.

In the third scheme, the paper said, O'Connell allegedly earned $800,000 for doing almost no work through a fraudulent employment contract after McBirney bought a Skokie Federal subsidiary. Δ

Trial Set for Three Wisconsin Men at the Heart of Bogus Money Order Scam

Three Wisconsin men are scheduled to go on trial in August for their roles in a scheme to sell the public phony money orders that are used in attempts to pay off mortgages and other large bank loans.

U. S. Postal Inspectors say the flow of the bogus instrument, called a "Certified Money Order," appears to have ended. But new phony instruments to pay off debts recently began turning up at financial institutions.

The Wisconsin trio was charged in March with operating a nationwide scheme to defraud individuals and financial institutions by distributing bogus money orders. Named by a grand jury in the seven-count indictment were Leonard A. Peth, Thomas Stockheimer and Mark Van Dyke.

The indictment said the three men operated an entity known as "Family Farm Preservation," which mailed out more than 900 packets that included the bogus money orders and instructions on their use. The indictment alleges that the three men received from $50 to $500 for each packet.

Financial institutions and other creditors who received the "Certified Money Orders" were instructed to mail them to L. A. Pethahiah (an alias used by Peth) at a post office box in Tigerton, Wisconsin, for redemption.

The creditors, in return, received a bogus "Certified Banker's Check." The Milwaukee U. S. Attorney's office said that when the creditor tried to return the phony instrument, the defendants merely sent it back marked "paid in full" along with a letter.

"This ended the payment process and the creditor did not receive money or anything else of value," prosecutors said in a press release. The indictment alleges seven cases involving losses of $200,000 or more by creditors.

Bogus money orders bearing the name "L. A.. Pethahiah" have been used around the country for more than a year. Investigators estimate that $65 million in bogus money orders have been written in attempts to get out of debt.

The flow of money orders "seems to have ended, hopefully," said Robert Bauman, a postal inspector in Milwaukee involved in the investigation.

But while the "certified money orders" have faded, there are other bogus instruments related to the scam that purport to satisfy all debt owed the bank by the senders. Worthless instruments labeled "Constructive Notice & Demand" and "Securities Draft" are also turning up at financial institutions.

In addition, new names and addresses to which financial institutions are to mail these phony instruments are being added to the list. They include:

"Constructive Notice & Demand"
Darrell Frech
c/o Route 1, Box 102
Jet, OK 73749

"Certified Money Order"
signed by Mike Loomis
Capital Resources
P.O. Box 1012
Buckeye AZ

"Securities Draft,"
signed by Mike Loomis
Capital Resources
P.O. Box 741
Boonville, IN

Should your institution receive one of these fraudulent instruments, contact federal law enforcement agencies or your primary regulator. Δ

FDIC gets a Record $104.5 Million in Sunrise S&LA Settlement

The FDIC, after a record 10-year effort, received $104.5 million to settle its claims against 25 former officers and directors of the failed Sunrise Savings & Loan Association, Boynton Beach, Fla.

The $104.5 million, which was paid by North River Insurance Company, is the largest settlement ever reached by the FDIC in a suit brought against the officers and directors of a failed bank or thrift.

When Sunrise failed on July 18, 1985, the Federal Home Loan Bank Board said that the thrift grew too fast in the five years since it was chartered. Its asset base climbed to $1.5 billion from $4.7 million. The failure is now estimated to cost taxpayers $440 million.

The Bank Board blamed Sunrise's insolvency on poor underwriting; high risk direct investments; and acquisition, development and construction loans which should not have been made.

In the wake of the failure, several officers and borrowers have been convicted on fraud charges as have three attorneys from the thrift's outside law firm. Recently, the conviction of one of the lawyers was overturned by the trial judge.

The FDIC's $104.5 million will come from an overall settlement of $110 million, which also provides $5.5 million to shareholders of the failed institution. The FDIC's case against the institution's officers and directors was consolidated with a class-action suit brought by shareholders.

This final settlement brings the total amount collected from professional liability claims by the FDIC in connection with Sunrise's failure to $159 million. This figure includes $40 million paid from the malpractice insurance of the outside law firm of Blank, Rome, Comisky & McCauley of Philadelphia, PA. Sunrise was started by senior attorneys at Blank, Rome.

The remaining $14 million came from a global settlement reached by the FDIC, Office of Thrift Supervision and the Resolution Trust Corp. to settle claims against the accounting firm of Deloitte & Touche. Δ

SEC: Shun Phony "Sapphire Bonds"

The Securities and Exchange Commission said that a new type of worthless security called "Sapphire Bonds" has been offered for sale to broker-dealers.

The stated issuer of the bonds is a fictitious firm, Precious Metals Holding Corporation, Brisbane, Australia. These bond certificates are issued as 15-year, non-interest-paying bearer bonds to be paid off at maturity in gemstones, the SEC said.

The SEC said that of the approximately 30 sapphire bond certificates that have come to its attention, all are denominated in face amounts of $1 million. Each bond certificate is accompanied by selling documents that include official-looking endorsements from prominent banking institutions and accounting firms.

These documents, among other things, attest to the value of gems allegedly being held on deposit in bank vaults as the security underlying the bonds.

Financial institutions should exercise extreme caution in accepting any form of bonds that they do not normally handle, especially bonds allegedly backed by gemstones, the SEC warned. If any sapphire bond certificates should come to your attention, the SEC asks that you contact either Ester Saverson, Jr., special counsel, or Thomas C. Etter, Jr., senior counsel, of the Division of Market Regulation of the Securities and Exchange Commission at (202) 942-4187. Δ

Instructions for Tellers under the Milwaukee Plan

Police and bankers in Milwaukee developed the following steps for tellers in financial institutions to follow when a customer wants to make a large withdrawal.

Procedures for Bank Tellers

CONFIDENCE CRIMES

Any teller confronted by a customer, especially a senior citizen customer, who wants to withdraw a substantial amount of money from his or her account should:

1. Try to convince the customer to take a cashier's check or traveler's check.
2. Inquire as to their reason for the cash withdrawal, especially if this transaction does not adhere to their usual pattern of banking.
3. Provide the customer with a "confidence crime" alert form and ask him or her to read and sign this document. Take the time to answer any questions they might have concerning this document. Be sure to point out the purpose of this document.
4. Call on one of the senior officers and request that they speak with the customer concerning this transaction.
5. Always activate the surveillance cameras when you suspect that a confidence crime is in progress.
6. Ask the customer, "Did someone from the bank, or someone claiming to have found a lot of money, ask you to make this transaction?"

If this procedure is adhered to, we may be able to save our customers from becoming the victims of a confidence crime. We have a responsibility to our customers in protecting them against these types of crimes whether they are young, middle-aged, or elderly.

Source: Milwaukee Police Department

Attention: 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