Federal Deposit Insurance Corporation

FRAUD Alert

Winter 1994/95 Volume 4, Number 3

A scam in the Philippines that U.S. Bankers Can End

United States banks and thrifts are being victimized by a wire-transfer scam that has become a cottage industry in the Philippines.

While the scheme is not new, U.S. postal inspectors say it is spreading across the country. It is not confined to the West Coast where it was first seen years ago.

Why is it coming back? As one postal inspector put it, "A good fraud scheme never dies."

Here's how this one works. A bank receives a letter from one of its customers, which has been written on an old manual typewriter. The letter states that the customer has been out of the country and has been hospitalized in the Philippines. The letter goes on to ask that a portion—usually a high percentage—of the customer's account balance be wire-transferred to a specified account so he can pay medical or hospital bills. Comparing the signature on file at the bank with the one on the letter would indicate it is legitimate, say postal inspectors.

Unfortunately, the letter is a forgery and the signature has been traced from a stolen check. The customer is probably not out of the country and knows nothing of the request.

The U.S. Postal Inspectors say that in almost all cases, the victim recently mailed a personal check to someone out of the state or the country. This check, however, never arrived and was stolen from the mail, either in this country or in the Philippines. (Thousands of retired United States citizens live in the Philippines.) Also, the victim may have simply paid a bill by check and someone working for the business that was being paid photocopied the front of the check and mailed it to the Philippines.

The front of the check contains the account number and the customer's signature, which will be used in the letter to the bank. Because the perpetrators generally don't know the balance in the account, they will usually ask that a percentage of the balance be wired to them. The U.S. institutions believe the letters are valid requests and wire the money to the temporary accounts set up at a bank in the Philippines or elsewhere in the Orient by the perpetrators to receive the funds. By the time the fraud is discovered the perpetrators are gone.

Why is this scheme flourishing? Simply put: because banks wire the money as requested, without first investigating.

Estimating the loss is difficult, because banks don't necessarily report this sort of thing to the same law enforcement agency, says John J. Sullivan, Jr., a postal inspector in San Francisco. Sullivan, an expert on the scheme, says the only way to bring this scam to a halt is for banks to stop wiring the money. [See page 2 on how banks can protect themselves.]

Why? Because there are no alternative solutions. There is little incentive for a far-flung investigation, Sullivan says, because Philippine law is so weak, "you've got to catch them in the act." At the same time, Philippine bank secrecy laws protect the holders of the accounts into which the money is wired.

Sullivan is trying to work with bank security managers in the Philippines to stem the illegal

*See **Scam**, page 2*

Scam in the Philippines

continued from page 1

wire transfers into the new or temporary accounts set up to receive them. Filipino bankers have been asked by postal inspectors to contact the U.S. bank and suggest it verify that the customer is actually in the Philippines before completing the transfer. The Postal Inspection Service has even volunteered to contact the bank in this country on behalf of the Philippine bank to verify the transaction.

At the same time, when a U.S. bank or thrift alerts postal inspectors to an attempted fraudulent wire transfer, the Philippine bank will be told. "As we identify accounts in the Philippines that we know to be fraudulent, we will promptly notify you and request that you take immediate action against the account holder," Sullivan said in a letter to Philippine bank security managers.

A remailing house in San Francisco that takes mail from Pacific Rim countries and repackages it to be sent on through the U.S. Postal Service, also has been alerted to the scam.

The envelopes used in the scam are always addressed "attention manager," followed by the name and address of the U.S. bank. The remailing firm alerts the postal service to these envelopes. The bank is then warned by the postal service that it may be the target of a fraud. In the past year, the postal service has sent a "hotsheet" warning about the scam to about 150 banks around the country whose names turned up on envelopes at the remailing firm.

The remailing house is only one means of getting the fraudulent letters into this country. Postal investigators point out that the letters can also be coming into the country by express delivery services.

While the Postal Inpsection Service is trying to warn banks here and abroad about the scheme, Sullivan asserts that only U. S. banks and thrifts can bring the scam to a halt.

As Sullivan notes, crooks won't spend the money to send the letters by expensive international courier services once the wire transfers begin to dry up. 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.

Ricki Helfer,
Chairman

Alan J. Whitney,
Director
Office of Corporate Communications

Frank Gresock, Editor

T. W. Ballard, Graphic Designer

Protecting Your Bank From the Letter Scam

The Postal Inspection Service offers the following advice to bankers to avoid being taken by the wire-transfer scheme in the Philippines.

—Tell employees who handle wire transfers about this scheme and to be especially alert to requests from the Philippines.

—Read the letter carefully. Was it written on an old manual typewriter? Is the return address a hospital or medical center? Does it contain abbreviations and phrases an American would not normally use?

— Before anyone acts on the wire transfer, go to the bank records and phone the depositor to confirm the request.

—If you cannot contact the customer locally, request more information by writing to the return address on the letter. Ask for a social security number or mother's maiden name to verify the identity of the customer.

—Any wire transfer request from the Philippines should be viewed as attempted fraud, until you prove it otherwise.

If you suspect your institution is the target of this scheme, contact the U.S. Postal Inspection Service at 415-550-5625 or P.O. Box 882528, San Francisco, CA 94188-2528. Δ

First Conviction in "Certified" Money Order Scam

Federal prosecutors in Dallas have gotten their first conviction and other indictments are expected in Texas and Wisconsin as a result of investigations into the use of fraudulent "certified" money orders.

Allan L. Kramer, a 59-year-old Canadian citizen living in Dallas, was sentenced in late February to 33 months in prison and fined $6,000. He was also ordered to pay his victims restitution of $26,794 by U.S. District Judge Sidney Fitzwater on 14 counts of mail fraud. Kramer used fraudulent money orders distributed by L.A. Pethahiah of Tigerton, Wisc. and OMB J.D. McCall of Waxahachie, Tex., to buy cars, trucks, a boat and real estate from victims who gave Kramer possession of their property. The sellers then mailed the fraudulent money orders to lending institutions, the U.S. Attorney's office in Dallas said. The amount of the bogus money orders topped $500,000.

According to government investigators, Kramer bought the certified money orders in bulk and filled in the amount after he had negotiated a purchase price with the seller of the property. The certified money orders are being sold around the country by groups who say they can be used to pay off loans. These groups, who dismiss currency laws as unconstitutional, argue that banks don't loan money, they loan credit. Further, when the currency of the United States is backed with precious metals, then the money orders can be redeemed by lenders, these groups maintain.

The government's case was built by investigators for the U. S. Postal Inspection Service and the U.S. Secret Service. Prosecutors said that many of the people from whom Kramer purchased property were under stress.

Kramer purchased five houses, which he quickly rented to people who gave him cash deposits and an initial rent payment. When the sellers discovered they had received nothing for their homes, Kramer's tenants were already living in the houses. One conservative estimate is that more than $100 million of the bogus money orders have been written in a nationwide scheme that has been called the biggest scam in more than five years. Δ

FDIC Wins $13.5 million in Contractor Fraud Case

The Federal Deposit Insurance Corporation has been awarded more than $19.4 million and interest in a major civil fraud case in Dallas.

Charged in the case were Jeff Thompson and Jerry Moore, principals in Southwest Management and Development, Inc. Also charged was former FDIC account officer Joseph Moreland.

The jury found that the three men defrauded the FDIC of more than $81,000 and each had filed 908 false claims against the FDIC between 1987 and 1989. Southwest Management had a contract with the FDIC between 1988 and 1989 to maintain FDIC-owned real estate. This included finding tenants, collecting rents and keeping properties in good repair until they were sold.

The case was brought together by special agents and attorneys of the FDIC's Office of the Inspector General working with the United States Attorney for the Northern District of Texas. Evidence in the investigation showed fraud and conspiracy.

Southwest Management failed to turn over rent money to the FDIC, while Moreland served as a confederate by approving payments for at least two thousand inflated invoices or phony invoices submitted by Thompson and Moore for work that was never done. Investigators also found that Thompson and Moore made numerous withdrawals from the FDIC fiduciary account. Moore and Thompson also made many payments to Moreland.

The case was brought under the False Claims Act, which requires damage payments of triple the actual loss from the fraud, and imposes civil money penalties for each false claim submitted to the agency. Δ

INTERPOL-Washington: The link to international law enforcement

INTERPOL-Washington is an information hub linking American and foreign police seeking assistance in criminal investigations which stretch beyond their borders. Unlike most countries that have a national police force, the United States has 18,000 state and local police forces and some 150 federal agencies with law enforcement powers.

INTERPOL-Washington cannot chase down a suspect on the street or make an arrest. But it can perform a more important function: It can rapidly exchange information between American and overseas criminal investigators. INTERPOL-Washington also is known as the U.S. National Central Bureau (USNCB) and is part of the Department of Justice. Each country creates its own national central bureau to interact with its counterparts around the world.

With the technology explosion leading to the internationalization of financial crimes, the rapid dispersal of information and the plotting of trends has become critical. Fraud involving, for example, phony bank securities shows up in the U.S. today and next week in Eastern Europe. A thrift executive, under indictment in Maryland, is tracked down in Paris.

Fraud Alert spoke with Shelley G. Altenstadter, chief of INTERPOL- USNCB. Altenstadter took on her current post in September 1993, after serving as deputy director of the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

Fraud Alert: *How does INTERPOL relate to banking in America?*

Altenstadter: INTERPOL is a communications organization that deals almost exclusively with other law enforcement entities as required by the INTERPOL constitution.

We do, however, have an agreement with the International Banking Security Association (IBSA) to accept reports of suspicious actions or scams attempted on member banks and to let the IBSA know if we have any information that relates to their inquiry. The INTERPOL-USNCB also makes referrals to U.S. law enforcement officers when appropriate.

INTERPOL also will distribute information through its "purple notices" on any unusual modus operandi or bank fraud to all the INTERPOL member countries. We're kind of a switching station, a place through which the leads are transmitted. Sometimes we're called the Western Union of law enforcement.

We don't have our own police force. We have analysts here on the permanent staff and 14 representatives of federal law enforcement agencies. We are unique because most of the other national central bureaus are located in the national police force or the ministry of justice, which do have law enforcement authority. Here in the U.S. we derive our investigative authority from using the detailees from the other agencies or we forward the leads to the appropriate law enforcement agencies.

Fraud Alert: *Can bankers involved in international transactions ask their local police departments to contact INTERPOL if they suspect something might not be right?*

Altenstadter: Yes, they can. The USNCB has a state liaison program which provides the 18,000 police departments in the U.S. with access to the INTERPOL channel.

These state liaison offices can request INTERPOL assistance, including records checks and related information on any suspect in a criminal case, including bank fraud and money laundering. The state liaison can contact us to have the country in question do the investigation.

Fraud Alert: *What information can foreign law enforcement agencies provide American bankers?*

Altenstadter: Foreign law enforcement agencies are under no obligation under INTERPOL regulations to provide information to American bankers.

INTERPOL does receive and provide information to law enforcement agencies about international criminal investigations. We're not at liberty to

see next page

continued from previous page
give out information on specific cases to bankers; that has to be decided by the police agency that asked for the information. But they can, if they deem it appropriate. We have to deal with the police agencies. We will be distributing to the federal interagency Bank Fraud Working Group "purple notices" on criminal trends and methods that we, or our headquarters in Lyon, France, are seeing.

Fraud Alert: *What can financial institutions or their regulators do to help INTERPOL?*

Altenstadter: Financial institutions should report frauds and attempted frauds to the federal, state, or local law enforcement authorities, particularly if these incidents have an international aspect. The reporting should include the methods of operation used by the perpetrators. I would like to work with the Bank Fraud Working Group to be able to exchange information with them. In turn we can pass our information on methods and trends to Lyon; in return Interpol headquarters can then send us their analytical information to share with the working group.

Fraud Alert: *Should financial institutions contact INTERPOL directly?*

Altenstadter: No, the banking institutions should contact the appropriate law enforcement agency.

Fraud Alert: *Is INTERPOL just a network of law enforcement agencies, or does it involve foreign agencies concerned with securities or bank regulations?*

Altenstadter: INTERPOL is strictly a criminal law enforcement organization. Some regulatory agencies attend international INTERPOL forums and conferences as observers and as participants.

Fraud Alert: *Are there any financial scams going on in Europe or Asia that may spread to North America?*

Altenstadter: Well, we are seeing a rise in some scams which started overseas and are beginning to occur here. The "prime" bank guarantee scheme has arrived in the U.S. after some activity in Europe. Scams asking for advance fees for loans also are turning up almost everywhere now.

In addition, solicitation letters from Nigerians continue to arrive in the U.S. in large numbers. The writer claims to be a member of the deposed Nigerian government and requests bank account information, letterhead and other business information. They say they are trying to get access to millions in U.S. banks and they need a legitimate entity to intercede for them. The Nigerians ask for seed money until they can get their money out. And they promise to provide millions of dollars to those who will help keep the money away from the corrupt government of Nigeria.

Fraud Alert: *Has INTERPOL been involved with the fallout from savings and loan failures, such as tracking down off-shore accounts or fugitive S&L executives?*

Altenstadter: INTERPOL working in close cooperation with the U.S. Marshal's Service and the U.S. Postal Inspection Service provided information which lead to the arrest and extradition of Thomas Billman. INTERPOL had a "red notice," which is like an international arrest warrant, out for Billman. [Billman was recently convicted of having been involved in a large scale S&L fraud while serving as the president and chief operating officer of Community Savings and Loan in Bethesda, Md.]

Information on Billman was circulated by INTERPOL and the marshal's service throughout Europe. A Parisian recognized Billman in that city from a picture in the International Herald-Tribune. The French citizen provided information which led to Billman's return to the U.S.

Sometimes we don't know what effect the information we request will have on a case in this country. Often what we see is a little corner of a case and we may not know what the case is about. We may never realize how important the information was, or how the case came out.

Fraud Alert: *Is crime growing more international?*

Altenstadter: Absolutely, because criminals can move the money so quickly and the trail can be obscured so quickly. They also can put it into legitimate transactions. But law enforce-

see ***Q&A****, page 8*

How Much do you Contribute to Fraud?

Fraud is to a large degree caused by the way most banks do business, said a long-time security director at a recent seminar on fraud and security in San Francisco.

William F. Gearin, a former Massachusetts State Trooper who spent 27 years as head of corporate security for Shawmut National Corp., told a group of bankers that "money from fraud is as much stolen as it's given away." The seminar was sponsored by the California Bankers Association.

Warning that fraud loss prevention requires "not Star Wars technology, but good common sense," Gearin recalled a $5 million fraud that could have been prevented:

A senior officer in a bank's loan workout operation had just opened a business account at a neighboring bank. Then, wire transfers started transmitting money from the commercial account in Massachusetts to a personal account in Naples, Florida. All the credits to his personal account were deposits of "starter-kit" checks.

A quick investigation revealed that 34 fictitious accounts had been opened using these fake starter checks. The starter checks used Post Office box addresses and fictitious names and addresses, while other accounts were opened with money orders. The purchaser? The senior officer of the bank's loan workout operation.

A full security audit revealed that $1 million in cash had been deposited in banks in New England and Florida, as well as accounts opened in Swiss banks.

The officer was caught after bank security notified the FBI, U.S. Attorney's Office, and the bank's management. The officer pled guilty to 55 counts of embezzlement. He was sentenced to 40 months in prison. About $4 million was recovered through restitution.

How was the officer caught? His attempts to wire transfer the funds from the commercial account attracted the attention of a valuable resource: A "SID," Gearin said. Short for "suspicious, inquisitive and demanding individuals." This employee notified the officer's employer about the transfers.

Gearin said other red flags could have tipped off staffers sooner: The officer was living well above his means, he exercised dictatorial management techniques at work, and controlled all incoming funds payable to the bank. He also had control over all vendors, attorneys and consultants in his department.

A regular review of the books by security personnel, using forensic accounting methods, and requiring the segregation of duties in the department, could have prevented the fraud. But most simply, verifying the information given to open the accounts would have stopped the embezzler in his tracks, Gearin said.

Verifying the addresses, Social Security numbers, places of business and background information listed on applications goes a long way toward fraud prevention. But it's not done enough.

There are many reasons why fraud can occur in a bank. But most fraud is caused by inadequate security and management controls in the bank. When polled, none of the 75 security managers at the seminar had monthly security training sessions. Most had them annually, which security consultants stress isn't enough.

Gearin outlined the following methods that he says can work to prevent losses:

— Position your security department so it reports directly to top management. Reports should be made to the top, including the board of directors and the CEO. Further, make sure the security staff is involved in drafting banking policy, including the making of loans.

— Train and retrain your people, and include account officers in

see next page

continued from previous page
that training. "It helps to make your training entertaining, and to try to spice up your presentations as much as possible," added David Battle, a consultant in Clayton, Missouri. "If your tape shows people in bell-bottoms and beehive hair, it's time to redo your training materials."

— Work out philosophical differences that probably exist between security and bank managers and other employees.

— Don't rely heavily on the internal auditing department to detect fraud. "I have nothing against internal auditors, but you need fewer layers of authority to have an effective security program," Gearin warned.

— Don't cut corners on due diligence. Verify information before an account is approved.

— Trust your gut reaction when dealing with a potential customer. Don't be shy about using "street smarts," and filing criminal referrals. And don't open accounts for strangers without verifying the information they give you.

Communication with other bankers, to set up a network of "fraud-watchers," is essential to success, he said.

The $5 million fraud described above was detected by just such a network. Working internally with the audit committee, keeping in contact with other banks' security offices and law enforcement agencies are all ways to keep up, and keep fraud out.

Rewarding successful tipsters will also help your cause. Gearin said that the officer who tipped the bank about the suspicious wire transfers was given an award. "It was a push to get it through senior management, but the bank did it."

It also helps to review how your bank uses bonuses and awards. An incentive program based solely on the number of new accounts opened will invite trouble, he warned. "You need to have security somehow review account applications, and you need to discourage bank officers from over-encouraging" the quick opening of new accounts. Δ

David Paul's Sentencing Ends the CenTrust Saga

"If that's what they're looking at to possibly indict him, I'm a little relieved. I keep waiting for them to come up with some serious charges," Sanford Bohrer, David Paul's attorney, told a reporter in response to allegations raised against Paul in 1990.

But, prosecutors, jurors and the judge apparently disagreed with the optimistic assessment.

Eleven years in prison, $60 million in restitution, and a $5 million fine were imposed in December as Paul's sentence following his seven-year high-flying tenure as CEO of CenTrust Federal Savings Bank of Miami, Florida.

Paul was convicted in November 1993 of 68 counts of wrongdoing and pled guilty to another 29 securities manipulation charges.

In 1983, Paul acquired the near-failing savings and loan, Dade Savings. With the aid of junk-bond king, Michael Milken, the thrift under Paul grew to nearly $10 billion in assets in about seven years before it failed.

He received salary and bonuses totaling millions of dollars a year by the late 1980s. He also lived in a posh Miami Beach estate, owned a yacht, had a leased jet at his beck and call, and used his home to house the $30 million CenTrust art collection.

Paul's lifestyle, paid for by CenTrust, rivaled that of other well-known S&L figures. His estate spanned two acres, comprising four waterfront lots on Biscayne Bay. He bought out three of his neighbors and had the houses razed after they complained about the

*see **Paul**, page 8*

Paul Sentencing

continued from page 7

unsightly view of his yacht, the Grand Cru, protruding into the bay. He then made additions to his home and built a teakwood dock for the Grand Cru. CenTrust, of course, loaned the $6.1 million needed to pay for the purchases and alterations.

While Paul claimed to have used his own money to have the $7 million yacht built, CenTrust paid for improvements, fuel, insurance, and the crew.

The boat had everything, from 14–carat gold nails studding the interior, to skeet-launching equipment.

His conviction included multiple counts of bank fraud, making false entries on the bank's books, misapplication of funds, filing false tax returns, mail fraud, wire fraud, conspiracy, obstruction of regulatory proceedings, securities fraud, mail and wire fraud on junk bond trades, and one count each of racketeering and racketeering conspiracy.

In a related case, Donald Anderson, a former CenTrust Vice President, was sentenced to spend weekends and holidays in federal prison for ten months. In addition, he was given three years probation and was ordered to pay $15,000 in restitution.

He was convicted for helping to conceal the diversion of $3.2 million from CenTrust to pay for the construction projects at Paul's estate.

The long-awaited sentencing of David Paul closes another chapter in the S&L cleanup. Δ

Q&A
Interpol-Washington

continued from page 5

ment is playing at a disadvantage. While we go through lengthy government procurement to upgrade our telecommunications, the criminal can afford to go out and purchase state of the art technologies.

It is getting more international and it's partially because criminal don't recognize borders and police still do. That's where INTERPOL plays its role of fostering a free exchange of information across borders. Δ

Attn: Chief Executive Officer

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20429-9990

OFFICIAL BUSINESS
Penalty for Private Use, $300

BULK RATE
MAIL
Postage &
Fees Paid
FDIC
Permit No. G36