Federal Deposit Insurance Corporation

FRAUD Alert

Summer, 1995 Volume 5, Number 1

Reporting Suspicious Transactions Electronically

Replacing Paper Will Reduce Regulatory Burden

A new system for reporting suspicious financial transactions is due to go into effect later this year that will allow depository institutions to file information faster and easier.

The system, which would replace the often confusing criminal referral forms, also is designed to reduce the burden on banks of unnecessary reporting. The Treasury Department's Financial Crimes Enforcement Network (FinCEN) said this reporting amounted to more than 150,000 forms filed by over 10,000 United States banks each year. For law enforcement agencies, FinCEN pointed out, it meant a struggle to correlate the multiple filings and avoid overlap and confusion in their investigations.

Cooperative Effort

This new reporting process is the result of a joint effort by the Federal Deposit Insurance Corporation, the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Reserve System, the National Credit Union Administration and FinCEN.

The banking and thrift regulators' share of the project involved meeting two goals. First, to improve the criminal referral process by reducing excessive reporting by depository institutions. Second, to eliminate the confusion that resulted from duplicative reporting of suspicious transactions via criminal referral forms and currency transaction reports (CTRs).

At the same time, FinCEN analyzed the need to revise the procedures used by financial institutions to report suspicious financial transactions.

Ease of Filing

The result of these efforts is the new referral process that centers around the Suspicious Activity Report or SAR, which is a shortened and simplified version of the agencies' various criminal referral forms.

As a result, several notable changes are being proposed to the agencies' rules on reporting criminal referrals.

They include the following:

• Raising the dollar thresholds for the mandatory reporting of criminal offenses;

• Filing only one form with a single repository—FinCEN— rather than submitting multiple copies to several federal law enforcement and banking agencies; and

• Clarifying the filing requirements to eliminate the duplication and confusion over the filing of referrals related to suspicious financial transactions of less than $10,000.

Under the new system, banks will be able to file the SARs in several ways. These include submitting the original form on paper, including use of a photocopy of the form; or filing by magnetic means, such as by a computer disk.

New Software

The agencies are working with FinCEN to develop computer

*See **Reporting**, page 2*

Reporting Suspicious Transactions Electronically

continued from page 1

software to assist banks in preparing and filing SARs. The software will allow a bank to complete an SAR and save it on its computer, and to print a paper copy for its own records.

The software will also allow a bank to file an SAR using various forms of magnetic media, such as computer disks or magnetic tape.

The FDIC will provide the software to all of its supervised institutions without charge when it becomes available.

New Database

Once the institution has completed the SAR and mailed it to FinCEN, the information will be added to the newly created database at the Internal Revenue Service's Detroit Computing Center.

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*

This process will meet the regulatory requirement that a bank refer any known or suspected criminal violation to various federal law enforcement agencies

The information on the SAR will then be made available by FinCEN to the appropriate law enforcement and regulatory agencies as quickly as possible. The database will make it easier for federal agencies to track, investigate and take action against those suspected of violating federal criminal laws.

The new reporting rules also raise the dollar thresholds for filing SARs. They are:

• $5,000 instead of $1,000 in situations where a bank has a substantial basis for identifying a suspect who is not a bank employee; and

• $25,000 instead of $5,000 in cases of known or suspected criminal activity where the bank has no substantial basis for identifying the suspect.

When to File

Further, regardless of the dollar amount involved, an institution must file an SAR for any transaction when the bank:

• suspects the money involved was derived from illicit activity or the transaction is aimed at hiding or disguising ill-gotten gains or violated the money laundering statutes;

• thinks the transaction was designed to evade the reporting or record-keeping requirements of the Bank Secrecy Act; or

• believes for any reason the transaction is suspicious.

Keeping Records

The new procedure requires a bank to keep a copy of the SAR and the original documents related to it for 10 years, which corresponds to the statute of limitations for most federal criminal statutes. This ensures federal law enforcement agencies and regulators will have access to the documents needed to prosecute a violation or pursue an administrative action.

In addition, the FDIC will keep an SAR and the information it contains confidential.

If you have any questions on this proposal you may direct them to your primary federal regulator. Δ

Please note:

The Treasury Department says that beginning October 1 financial institutions should use the new CTR, but suspicious transactions should be reported on the existing criminal referral forms until SARs are available. Δ

Two Sentenced in Burritt Fraud Case

The FDIC assisted the United States Attorney's New England Bank Fraud Task Force in obtaining a guilty plea and the sentencing of Robert M. Pawloski, former senior vice president for commercial lending at the failed Burritt Interfinancial Bancorporation, New Britain, Conn.

Pawloski engaged in a pattern of fraudulent lending to Richard W. Kelly, Jr. A real estate developer, Kelly, was one of Burritt's largest borrowers. Pawloski accepted $25,000 cash and other gratuities from Kelly in exchange for approving and disbursing numerous loans to Kelly and Kelly-related projects, including some in Florida. Pawloski, who pleaded guilty, was sentenced to two years probation. Kelly also pleaded guilty and was recently sentenced to 10 months in federal custody and to pay $58,000 in restitution.

Burritt was a Connecticut-chartered bank with total assets of $517 million when it was declared insolvent and closed on Dec. 4, 1992. The FDIC was appointed receiver of the bank's assets.

Because Kelly and Pawloski provided information to federal bank-fraud investigators, prosecutors in turn asked for more lenient sentences for the two.

On May 11, 1995, the FDIC filed a lawsuit in the U.S. District Court for Connecticut against St. Paul Fire & Marine Insurance Company. Burritt had purchased fidelity bond insurance from the company, which was intended to indemnify the bank against losses resulting from the dishonest and fraudulent acts of the bank's employees. Burritt had purchased a $3 million policy from St. Paul. St. Paul has refused to pay the FDIC's claim against the policy for losses caused by Pawloski's loans to Kelly.

The FDIC alleged in its complaint that Pawloski's fraudulent conduct resulted in losses in excess of the $3 million limit of the bond. It is further alleged that Pawloski approved and disbursed more than $4 million in loans to Kelly that resulted in losses to Burritt.

In exchange for the loans, Pawloski received the following financial benefits from Kelly: $25,000 in cash, time aboard Kelly's yacht in Key West and Nantucket, many trips to Atlantic City with Kelly and at his expense, and a 35mm camera. In addition, Pawloski approved and concealed the true nature of a loan made to Kelly, but used by Pawloski to secretly purchase a residence in Connecticut.

As a direct result of Pawloski's fraudulent activities, the FDIC alleged that Burritt sustained losses of more than $4 million. Δ

Californian to Pay FDIC $3.3 Million

The FDIC is expected to collect full restitution on $3.3 million in illegally obtained loans. On March 14, 1994, U.S. District Judge Robert M. Takasugi ordered Alan Robbins to pay full restitution to the FDIC, plus interest, for losses resulting from the loans obtained at the failed Independence Bank, Encino, Cal.

In November 1992, Robbins pleaded guilty to three counts of making false statements on loan applications. Robbins made these false applications to obtain the approval by Independence of personal, unsecured loans totaling $3,380,000. Independence failed on January 30, 1992.

After more than a year of negotiations with Robbins and his former business partners, and with the assistance of the United States Attorney's Office for the Central District of California, Robbins agreed to pay the FDIC the full amount owed less interest, with an immediate payment of 50 percent. On June 23, 1995, Robbins settled with the FDIC, providing for complete satisfaction of the restitution obligation by March 1996. He has already paid the FDIC $1.6 million and is expected to make additional payments totaling $114,000 by the end of 1995. Δ

FTC Moves to Disconnect Phony Telemarketers

Consumers talking on the phone with a telemarketer often can't distinguish a legitimate sales pitch from a con game. Likewise, bankers presented with a draft from a telemarketer to debit a customer's checking account can't always tell a legitimate transaction from one that is based on fraud or deception. Given mounting complaints and concerns, federal officials are taking new steps to save consumers billions and to save banks from potential liability and other dangers.

The major decision: a Federal Trade Commission regulation issued in August that will require telemarketers to obtain clear proof that a consumer has authorized a payment for goods or services via direct debit of his or her checking account.

Also significant: a Federal Reserve System task force report detailing the potential problems banks face when handling drafts and suggesting ways institutions can protect themselves and their customers against fraud.

"Every year, millions of consumers enjoy the convenience of ordering and paying for products by telephone," said Jodie Bernstein, director of the FTC's Bureau of Consumer Protection. "But there is also a dark side to telemarketing... which accounts for about $40 billion in consumer losses, or 10 percent of those sales, every year."

This dark side of telemarketing includes persuading consumers to divulge their checking account number and then either debiting the accounts without permission or misrepresenting the goods or services to be delivered. The new FTC rule, which goes into effect January 1, 1996, will combat this fraud with measures that include:

- Requiring a telemarketer to disclose the total costs of goods or services and the terms and conditions of any refund before asking the consumer for credit card or bank account information or before sending a courier to pick up a payment;

- Prohibiting a telemarketer from debiting a consumer's checking account without first getting one of three forms of "verifiable authorization" to pay (two in writing, the other by tape recording);

- Banning a telemarketer from seeking up-front payment before making certain loans, providing credit repair services or offering to recover money the consumer lost in a scam; and

- Outlawing "credit card laundering," or situations where a telemarketer who is not authorized to accept credit card payments will recruit another company to accept the payments for it.

Telemarketers are subject to fines of $10,000 per violation of the FTC rule. David Torok, an attorney with the FTC in Washington, told *Fraud Alert* that depository institutions are not directly subject to FTC rules and therefore are not required to obtain written or taped authorization of a consumer's permission to have an account debited. However, he said, "if a bank is concerned about whether it should honor a particular draft, it can ask to see the verifiable authorization required by the rule."

The Federal Reserve report covers the problems depository institutions face when presented with preauthorized drafts, also commonly known as demand drafts, telephone drafts or phone checks. These checks are imprinted with the consumer's checking account number, supposedly with the consumer's authorization to debit the account. Even though the consumer's signature is not on the actual draft, according to the report, these checks can be perfectly legal under the Uniform Commercial Code because the signature (i.e., the authorization) can be given verbally. Telemarketers aren't the only organizations that issue preauthorized drafts. Charities and "catalogue" sales houses, for example, often offer the option to pay by preauthorized draft instead of by check.

Banks typically pay these drafts if properly encoded with the account number and dollar amount, if the amount is below a level that would trigger an inspection of a signature, and if there are

*See **next page***

Continued from previous page
enough funds to cover the withdrawal. But who is liable if funds are withdrawn but the draft was not authorized by the account holder, or if the consumer claims that the authorization was obtained by fraud or deceptive promises? What if, for example, the consumer claims to have authorized a draft for a small amount but the telemarketer issued one or more drafts in larger amounts? The report says that ordinary laws governing checking and various other rules provide some guidance, but even so, "the liability of the paying bank to its customer cannot be defined with any precision; the rights of the paying bank against the bank of deposit are even more uncertain."

Robert D. Mulford, vice president and general counsel of the Federal Reserve Bank of San Francisco and chairman of the Fed's task force, told *Fraud Alert* that even though the Reserve Banks have not found many cases of fraud against banks, "we have received numerous calls and questions about preauthorized drafts and the potential for fraud, so we decided to develop guidance on the topic."

The report details various ways a bank could or should investigate a particular draft or telemarketer (a brief summary appears in the box below). One additional bit of advice from the report that could strengthen a bank's protections against lawsuits and losses: Warn customers about the risks of giving out their bank account numbers to people they don't know or fully trust.

For more information about the Federal Trade Commission's rule, you may contact Mr. Torok at: FTC, Washington, DC 20580 (202-326-3075). For a copy of the Federal Reserve task force's report, write or call the Law Department of the San Francisco Fed at: P.O. Box 7702, San Francisco, CA 94120 (415-974-2847).

Bankers who suspect telemarketing fraud should contact their primary federal regulator. They also can contact the FTC's Division of Market Practices (202-326-3128) or the state attorney general. Δ

Pulling the Plug on Bogus Drafts

The following recommendations from a Federal Reserve task force could help depository institutions protect themselves and their customers from fraudulent "preauthorized drafts" against consumer checking accounts by telemarketers and others.

If you receive a preauthorized draft for payment...

- Carefully investigate an accountholder's claims that he or she didn't provide an account number or otherwise authorize the draft. Make use of new evidence that the Federal Trade Commission will require telemarketers to supply to banks upon request, starting January 1 (see *Telemarketers*, page 4), and consider similar forms of proof from other issuers of drafts.
- Consult with bank counsel if the accountholder did provide an account number or authorize a draft but claims this was prompted by fraud or deception.
- If an account was debited incorrectly, promptly recredit the account and refund any returned check fees triggered by the initial transaction. Contact the bank where the draft was deposited and work out arrangements for having the draft and the funds returned.

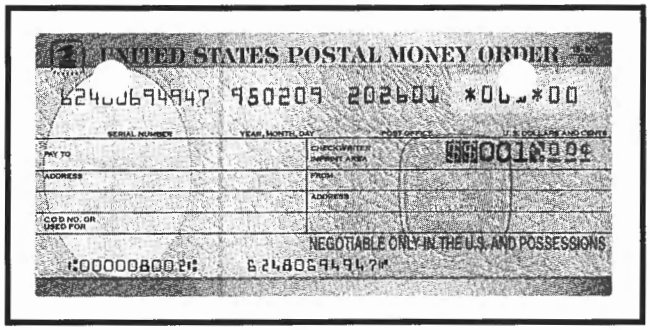
If you receive a preauthorized draft for deposit...

- Investigate the background and creditworthiness of any company that informs you of its plans to deposit preauthorized drafts. Consider having the company agree in writing to comply with the FTC's rules, to return funds challenged within a reasonable period (preferably at least 90 days), and to keep a reserve large enough to cover returns.
- Carefully monitor the transactions of a company that starts depositing preauthorized drafts without telling you in advance. Consider entering into the same written agreement mentioned above. Δ

Putting the Brakes on Smurfing at the Post Office

The domestic Postal Money Orders coming through your institution now have a new look, aimed at reducing money laundering.

The Postal Service changed its domestic money orders (see illustration) because about $200 million a year in drug money was being laundered through their use. The new domestic money order has an endorsement in bold red on the lower right face and in black on the reverse that reads: "Negotiable Only In The U.S. And Possessions." These two endorsements are the only change to the appearance of the money order.



The Postal Money Orders meant for international use are unchanged, points out Postal Inspector Al Gillum.

Drug traffickers hire people, called "Smurfs," who go out each day with about $70,000 to $100,000 in cash, which they turn into negotiable instruments. They purchase money orders, and travelers checks, which are later shipped out of the country.

The Post Office has documented that illegally purchased domestic money orders have been deposited into bank accounts in nearly every country in Europe and Asia.

Now when a foreign bank sends the domestic money orders back to its U.S. correspondent bank for payment, Gillum said, they will be returned as a charge back, because the money orders were intended only for U.S. domestic sale and use. The Postal Service is meeting with the 10 U.S. banks that do nearly all of the international correspondent business to explain the change and smooth the transition to the new money order.

The Postal Service projected that the stock of old money orders would be depleted by about the end of September. Δ

OCC Warns on "Blocked Funds" and Cook Island Guarantees

The Comptroller of the Currency has issued alerts on "blocked funds deposits" lending schemes and guarantees issued by the government of the Cook Islands.

"Blocked funds deposits," as promoted by various individuals and their entities, are not known to exist in the legitimate banking community. But many inquiries have been received by the OCC concerning "blocked funds deposits" relative to proposed brokered loan schemes.

Under the scheme, a loan broker claims to have on deposit in a bank millions of dollars that are purportedly "blocked" for him to lend. Furthermore, several banks have confirmed such blocked funds deposits even though no such deposits exist. Such confirmations expose banks to possible civil litigation initiated by innocent third-party victims. The promoters of such programs cite funds in the hundreds of millions of dollars. The OCC recommends that banks use extreme caution when approached to become involved.

The Cook Islands government issued a number of guarantee instruments in $50 million and $100 million amounts. The instruments are dated between May 11, 1994, and October, 24, 1994, and indicate they are payable to the order of Hanworth Securities Limited, 55 Frederick St., Nassau, Bahamas, or to Hanworth Securities Limited, incorporated in Western Samoa. The government of the Cook Islands has advised the OCC that these instruments were cancelled between September 1994 and December 1994. It has not been ascertained if any unauthorized instruments are in circulation. Δ

Five Indicted in $25 million Loan Scheme

Five men have been indicted in Texas on bank fraud charges involving a series of loans totaling more than $25 million.

Among those indicted were David B. McCall, Jr., and Jack C. Harvard, both former mayors of Plano, Tex. McCall was charged in five counts, including conspiracy, false entries and misapplication of savings and loan funds, *The Dallas Morning News* reported. Harvard was named in five counts in a scheme that allegedly removed a troubled loan from the books of Plano Savings and Loan Association and netted him $250,000. McCall is the former chairman of the failed S&L.

Also indicted were former Plano real estate brokers James R. "Rick" Fambro, Michael J. Barr, and Richard F. Armstrong, the former president of the failed Heritage Savings and Loan Association of Elk City, Okla.

The grand jury, in its 11-count indictment, alleges that the five created a web of transactions designed to transfer troublesome loans from one institution to another, the newspaper reported. The purpose allegedly was to hide difficulties from bank examiners and relieve borrowers of the need to repay the loans.

Fambro, Barr and Armstrong are charged in connection with transactions involving loans that benefitted an insider at Heritage, which had a loan office in Plano.

Harvard, the newspaper reported, was convicted in May on six counts relating to bank fraud in another case. That case involved transactions conducted while Harvard was chairman of Willowbend National Bank of Plano, which he founded. Δ

Former Bank Employee Pleads Guilty to $1.2 million Fraud

A Massachusetts man pleaded guilty recently to a $1 million bank fraud perpetrated against his employer, Saugus Bank & Trust (now Eastern Bank) of Saugus, Mass.

Jeff F. Buckley was charged with defrauding Saugus of $1.2 million. Buckley was a loan officer and vice president of the bank until July 1994, when his fraud was discovered. Buckley entered his plea in July with U.S. District Judge Reginald C. Lindsey, before the case went to trial.

The U.S. Attorney's office said, in a press release, that in early 1993 "Buckley embarked on a scheme to essentially 'donate' the bank's money to a construction company so that the company could generate revenues that would be used to pay off prior, legitimate loans that had been extended by the bank through Buckley.

"Buckley executed the scheme by issuing bank treasurer's checks to and for the benefit of the construction company (payable to its subcontractors or employees), and concealed his actions within the bank by 'offsetting' the amounts of the treasurer's checks by causing deductions to be made from the accounts of other bank customers."

These deductions were unauthorized and were generally unknown to the other customers because Buckley intercepted the customers' monthly statements, prosecutors said. All told, Buckley gave the company over 200 treasurer's checks, ranging from several hundred dollars to $15,000 and totaling $1,213,782.59.

In a separate case, Peter J. Janeczyk of Marlboro, Mass. recently pleaded guilty to his involvement in a scheme to defraud two failed Massachusetts banks of more than $25 million.

Janeczyk admitted to his part in separate schemes in which First Service Bank for Savings in Leominster and New England Allbank for Savings in Gardner were duped into providing loans to Janeczyk and his co-conspirators. He and the others in turn helped arrange for fraudulently obtained real estate development

*See **Saugus,** page 8*

Saugus

Continued from page 7

and mortgage loans for potential condominium buyers in New Hampshire, reported the *Telegram & Gazette* in Worcester, Mass.

However, prosecutor Russell Jacobson of the New England Bank Fraud Task Force asked the judge to delay sentencing Janeczyk until late February, because Janeczyk is cooperating in a number of complex issues in an investigation.

Janeczyk played a leading role in getting $17 million in loans from First Service, which failed in March of 1989. At Allbank, which failed in December 1990, fraudulent loans of about $10 million were obtained. Δ

Californian to Pay RTC $250,000

A Las Gatos, Cal., real estate developer will pay the Resolution Trust Corp. $250,000 as part of his sentence for bank fraud in connection with the failed HomeFed Bank.

Fred N. Sahadi also was put on probation for three years, ordered to pay a $50 fine and agreed to pay extensive back taxes. Federal prosecutors asked for the sentence because Sahadi had provided information that would help substantially with the prosecution of other HomeFed officials, the *San Diego Union and Tribune* reported.

The collapse of HomeFed in 1992 has been followed by criminal indictments. Also a $70 million government lawsuit was filed in July against top bank officers, including Kim Fletcher, the former chairman of the failed S&L, and Robert Adelizzi, its former president, the paper said.

In December, Sahadi pleaded guilty to aiding and abetting in a $2.3 million fraud against the bank. Sahadi admitted during his disposition hearing that he had schemed with bank officers in 1984 to sell HomeFed a $2.3 million condominium, with the stipulation that he would repurchase it two years later.

HomeFed's purchase agreement, however, did not mention the buyback deal, which prosecutors said opened the way for Sahadi and unnamed bank officials to obtain money under false pretenses, the paper reported. Sahadi never bought back the condominium. Δ

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