F D I C

FRAUD ALERT

Spring 1992

Volume 1, Number 4

The Secret Service Increases the Pressure on Financial Institution Fraud

Most people equate the United States Secret Service with the protection of the current and former Presidents and the Vice President; it actually was formed in 1865 to suppress counterfeiting. The Banking Act of 1933 charged the Secret Service, a division of the Treasury Department, with protecting the assets of the FDIC. In 1990 the Secret Service was enlisted by Congress in a broad effort to go after fraud in the savings and loan and banking industries. The ***FDIC Fraud Alert*** talked to Robert H. Rasor, the Secret Service's special agent in charge of the financial crimes division, about the agency's efforts.

FA: How many agents do you have working on financial institutions fraud?

We dedicated 100 of our senior investigative positions to attack the problem. We developed a program in the Secret Service to train the agents and support personnel in a very short time. We had agents and trained personnel working on the cases three months later.

The proof is in the pudding. We thought we would be successful in the first year if we could do 100 arrests. In the first year we went over 200 arrests. Of the initial 200 arrests, more than half resulted in guilty pleas with no trials. And it's not the result of case selection. Under the referral system, we are dependent on what is given to us. Right now, banks and regulatory agencies refer their cases to the FBI and the United States Attorneys' offices. From that they then give us cases to work. That's the traditional referral process.

We currently have in our inventory about 450 cases. And our arrests are up.

FA: Would a banker call the Secret Service if he or she suspected fraud or would they call the FBI first?

They could call either. We have a working relationship with the FBI so we don't do anything without telling the other, so we don't have a duplication of effort.

FA: What percentage of cases come through referrals from the FBI and the Department of Justice, and from bankers simply calling the Secret Service?

Probably a third come through the referral process, a third come from the industry, and a third come through informants or from cases that already exist in the credit card area.

FA: In a related area, would you explain the West African Task Force?

Fraud is being committed in an organized fashion, and the people involved in these activities are for the most part Nigerians. The West African Task Force is the result of congressional and law enforcement interest in the fact that there is an organized structure out there attacking the economy. It's done through bank fraud, it's done through telecommunications, computer and credit card fraud. Those are all areas where we are actively involved. What makes it so difficult to attack the problem is that these are perpetrated by a very closed and concentrated group of people. Infiltration in undercover capacities is a difficult problem.

FA: How have banks felt the impact?

Banks have felt the impact in the credit card side of the business. It is not uncommon for these groups to get the large volumes of genuine credit card numbers that a bank or a business has. They get into the system and use those numbers on either counterfeit or altered cards. They can take a bank's base of customers who use its credit card and duplicate their credit lines. And in less than a month it can severely affect your business, if not put you out of business. People are hired in low-level positions, either in the cleaning crew or the security force. (Federal agencies have also been victimized.) They can get into the books and the records of the bank. Once they have those numbers, they can counterfeit a credit card or take an existing credit card they've stolen and melt it down. Because the cards are plastic, a heat process can take the numbers off. And an embossing machine puts on new numbers. The card is now good for at least one billing cycle for the card's line of credit. In most instances the crime is not discovered until the customer gets the bill or the line of credit has been used up.

FA: Are the people the task force is aimed at involved in multi-million dollar crimes or are they involved in crimes that net $5,000 or $10,000 ?

It's a cumulative organized effect. We have an ongoing case in the Southwest—so I can't get into details—but the loss in that case was $12 million. That was a medium-size operation. The $12 million in losses was done in maybe seven or eight months.

You take that one and others around the country and it's big, big money.

FA: How long has this group of criminals been operating in this country?

It has been a significant problem for us for the past few years. It's been highlighted in the last two or three years with the large volume losses and the fact that we've discovered this structured format.

Most of the cases we work operate by a pattern, whether it's West African or Asian gang activity. What we see is a structure where they get the list of account numbers, the fake credit cards, and they put them together. They will then organize teams of three-to-five people and will send those people out day after day around the country with 20 or 30 credit cards to hit banks in the Midwest or the South. They don't go to the big cities, they go to the heartland of America. They hit all of the banks in a small town for $2,000 or $3,000 until they've used up these cards. They then bring all of the money back to the source in a big city.

FA: How can bankers protect themselves against these people?

They can instruct their tellers on how to get proper identification from people, how to size people up, and work to make sure that the employees of the bank are aware that there are people trying to get the bank's money.

FA: It could also be a threat to the bank from a scheme involving counterfeit checks?

We had a case, but this group was Palestinian. They were originally picked up on a $5,000 problem. We were able to investigate and the case turned into a $1.5 million loss to 62 banks across the United States over five years.

It was a pretty simple scam. It involved opening two accounts, and taking a check from one account and depositing it into another account. They did it after hours using the night deposit and would check "cash" instead of "check" on the deposit slip. They then got to the ATM in the morning and pulled the money out before the bank figured out that it wasn't a cash deposit. They would do that in small amounts, maybe $1,500 to $2,000.

So the problem is the system itself. The way we look at it, the Secret Service should be directing our efforts at protecting the integrity of the system.

Our philosophy is that you should manage the crimes you investigate. In managing the crimes you investigate you come up with recommendations for fixes in the system, or five years from now you are going to have the same problem.

Give me an example of the changes you recommend?

I can tell you this: We are constantly in touch with telecommunications agencies, credit card agencies and the banking agencies to say: "This is why you're getting beat."

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

This newsletter is produced by the Office of Corporate Communications.

William Taylor, Chairman

Alan J. Whitney, Director, Office of Corporate Communications

Frank Gresock, Editor

Hackers Invade Credit Card Files

San Diego police say that computer hackers worked their way into the data bases of credit card reporting agencies to obtain valid credit card numbers that may have led to millions of dollars in purchases.

The actions of the computer rogues in San Diego and elsewhere in the country could put the entire credit card industry at risk of losses from the elaborate electronic fraud, San Diego police told the ***American Banker*** *.*

"Any bank that issues a credit card could be a victim of this," said Dennis Sadler, a detective leading the investigation.

While the scope of the electronic theft is not known, police say the rogues may have made millions of dollars of purchases using the credit card numbers stolen from Atlanta-based Equifax Credit Information Services Inc. The computer criminals also reportedly made fraudulent long-distance telephone calls, and may have broken into automated teller machines, the ***American Banker*** *reported.*

Although Equifax is the only company that has confirmed that its systems were violated, police said that other credit reporting agencies may have also been victims.

Several hackers appear to be involved in the scheme, either by sharing tips or by committing fraud. The San Diego group may have been involved with two hackers arrested in the Dayton, Ohio, area and with others being investigated in New York City, Philadelphia, and Seattle.

Atlanta-based Equifax said that the San Diego incident was not the first violation of the company's computers.

Tom Robb, an Equifax senior vice president, said the most recent case involved a computer hacker in Cincinnati who invaded the company's computers in February.

Computer break-ins are rare, Robb contends. Equifax is upgrading its security to further limit fraud, he told the newspaper.

FDIC Warns Banks About Cancelled Securities Certificates

Recent reports to the Securities and Exchange Commission indicate that some domestic and European banks and broker-dealers (and their insurance companies) have suffered losses by accepting cancelled securities certificates as collateral for loans and for deposit in trust and custodial accounts. The certificates were worthless because they had already been cancelled on the books of the transfer agent. Although the FDIC is unaware of any FDIC-supervised banks that have suffered such losses, the agency is warning institutions about this fraudulent activity and reminding them about procedures that should help detect fraudulent securities certificates.

Banks can guard against this scam by inquiring about securities certificates before they are accepted for collateral or for trust accounts. The chief resource is the Securities Information Center (SIC), a firm contracted by the SEC to operate a database of information on lost, stolen, counterfeit and recovered securities certificates.

Under SEC Rule 17f-1, every insured bank must be registered with the Securities Information Center. SIC registrations may be either direct or indirect. A direct registrant may telephone the SIC to inquire about certificates. An indirect registrant must route all inquiries through a designated direct registrant, usually a correspondent bank.

In general, Rule 17f-1 requires an FDIC-insured bank that receives from a customer a certificate worth $10,000 or more to verify its validity through the SIC. Banks complying with this rule should be able to protect themselves against significant losses from fraud.

Rule 17f-1 also generally requires an insured bank to report to the SIC lost, stolen, counterfeit or recovered securities certificates worth $10,000 or more for which the bank is owner, fiduciary or transfer agent.

An institution that is the transfer agent for its own securities is advised to ensure that securities certificates are properly and prominently cancelled. The same protections also need to be afforded to outside issues of stocks and bonds transferred by a trust department. In addition, a bank that uses an outside certificate destruction or recycling service should be sure that the certificates actually are destroyed and should have verifying documentation.

A bank that suspects that a fraudulent securities certificate is being presented is encouraged to immediately report the information to the local office of the Federal Bureau of Investigation.

For further information about rules and procedures for preventing losses, contact John F. Harvey, trust review examiner, in the FDIC's Division of Supervision (202-898-6762), or the Division's Special Activities Section (202-898-6781).

Fraud in New England Banks tops $1 billion

The Federal Bureau of Investigation is looking into fraud cases totaling more than $1 billion in four New England states.

Boston, the financial hub of the region, is where most of the largest cases are centered, agents told reporters last month.

"The numbers are astounding in New England... the number of cases, the amount of lost money and the exposure, and it is so tied to real estate speculation," John C. Eckenrode, a supervisory agent told the *Boston Globe.*

The FBI's Boston division has the second-highest number of cases involving fraud of more than $100,000 among all of the divisional offices in the country. Only the Los Angeles office has more major fraud cases under investigation. The Boston office covers Massachusetts, Rhode Island, New Hampshire and Maine.

Agents said that unlike California and Texas, where much of the fraud involved junk bond speculation or small S&Ls, many of the Boston investigations involve large financial institutions. Also unusual is the number of lawyers, bankers, mortgage brokers and accountants under scrutiny.

In some cases, the officers of financial institutions are under suspicion, while in others, the institutions were defrauded, agents said.

The number of cases has been growing steadily. By March, the FBI said, 153 investigations dealt with $100,000 or more and 79 were for $1 million or more.

"There has been no leveling effect yet," Thomas A. Hughes, special agent in charge of the Boston division said. "The trend is continuing to go up and we are monitoring it to see if we need more agents." The FBI already has more than 50 of its 259 agents in Boston working on bank fraud cases.

Almost all of the investigations involve real estate and many involve false loan applications, hidden second mortgages and straw borrowers.

Because of the volume and similarity of the cases, the agents are working on a profile of those who may be a target or a witness in an investigation. "We're looking for individuals who would have borrowed heavily or leveraged borrowing between 1983 and 1990," Eckenrode said. "They are on the verge of bankruptcy or in bankruptcy already."

"They supplied information which inflated their assets or reduced their liability and they left spaces blank on loan applications or financial statements and they were assisted by loan brokers," said Thomas Powers, supervisory agent.

The number of cases in which fraud played a significant role in a bank's failure has increased from only three in January 1991 to 20 in March 1992.

Forfeiture: The Route to Quick Recovery

Congress has extended the use of forfeiture, which has been a powerful tool in the attack on drugs, to bank regulators as one means of recouping property obtained through fraud.

Forfeiture is seen by law enforcement officials and bank regulators as a boon because, they say, it is easy, quick, cheap and it works.

Forfeiture is easy because it is handled by the U.S. Attorney's office and federal law enforcement agencies. The cases grow out of referrals and investigations by financial institutions and federal banking regulators.

The process of forfeiture can be carried out in a matter of weeks or months.

The process is also inexpensive because everyone involved in carrying out a forfeiture is a government employee. Unlike other methods of recovery, which involve retaining outside counsel and contractors, forfeiture does not cost taxpayers anything extra. Uncontested forfeitures can be resolved in a matter of weeks, meaning less resources are used.

The Department of Justice has thus far seized and forfeited cash, cars, real property, jewelry, bank funds and a luxury yacht. Under provisions of the Financial Institutions Reform, Recovery, and Enforcement Act a mortgage servicing company was forfeited.

The goal of forfeiture, of course, is to seize and forfeit assets, both real and personal property, that are traceable to bank fraud, and transfer those assets to open financial institutions or the FDIC or RTC.

There are two types of forfeiture, administrative and judicial. Administrative forfeiture is the easier to carry out. Usually the FBI or the IRS as the seizing agency obtains a seizure warrant from a U.S. magistrate, after showing probable cause that the asset sought by the government was obtained through bank fraud. After seizure, potential claimants are given notice and are provided an opportunity to contest the grounds of the seizure. If no one makes a claim within 20 days, the property is automatically forfeited.

A judicial forfeiture is initiated if the claimant of the property does come forward or in a case involving real property, with the U. S. Attorney filing a complaint in federal court. The action is then handled like other civil matters until either a settlement is reached or a court order is issued.

At the end of the administrative or judicial proceeding, the forfeited cash and the title to the real or personal property is turned over to the financial institution as restitution or to the regulator responsible if the bank has failed.

FDIC
Federal Deposit Insurance Corporation
550 17th Sreet N.W., Washington, D.C. 20429

Official Business
Penalty for private use, $300

BULK RATE

U.S. Postage PAID

PERMIT No. G-36

Attention: Chief Executive Officer