F D I C

FRAUD ALERT

Summer 1993 Volume 3, Number 1

Food Stamp Fraud: A Growing Problem Bankers Can Spot for Federal Investigators

In May of this year one-in-ten Americans was on food stamps. If Congress goes along with the Clinton Administration's request the program will cost $27 billion, up from the $22 billion for the budget year that began October 1. Food stamps have become a second currency.

With the increase in the program's size, the level of fraud is also expected to rise. The sophistication of the criminals and the dollar amounts involved are also on the rise. The cases of food stamp fraud are no longer counted in the thousands of dollars, they are now multi-million dollar cases. The *Fraud Alert* discussed food stamp fraud with Brian L. Haaser, director of the program investigations division of the U. S. Department of Agriculture's office of inspector general.

FA: Has there been an increase in the trafficking in food stamps?

Haaser: Yes, food stamp fraud has never dropped off.

FA: Can you explain some of the food stamp scams and how they involve banks?

Haaser: In some cases recipients will sell their food stamps as soon as they receive them at an issuing center. They walk out the door and immediately sell their food stamps to people we call "runners." These runners will then take the food stamps to a store that has a license from the USDA Food and Nutrition Service (FNS) and sell them. The store will redeem them at a bank for the full value. So, a runner may buy them from a recipient for 50 cents on the dollar, sell them to the store for 75 cents on the dollar, and then the store gets its cut when they are turned in at the bank for full value.

Ultimately the federal government is out its money and the food stamps didn't meet their purpose of buying food. So you have kids going hungry who need the food.

FA: And the retailer pays the runner 75 cents on the dollar, without the runner having purchased anything?

Haaser: Yes, the normal mark-up on merchandise in a grocery store is two to five percent. So, if you can go out and buy food stamps and immediately make 25 percent on the money you invest, it's a pretty good deal.

FA: What are some of the other scams?

Haaser: The recipient will know a store in the area and will trade the food stamps for cash, cutting out the middle person.

There are people who don't own stores, but have managed to get a license from the Food and Nutrition Service. About 220,000 stores are licensed to redeem food stamps. But the FNS doesn't have enough staff to check all of those stores. So, if they lie when filling out the forms they might get licenses. They have no stores, they just buy and sell food stamps. "Phantom stores" is what we call them.

FA: How are the food stamps handled by the criminals at banks so that cash transaction reports are not triggered?

Haaser: Food stamp deposits don't fall under currency transaction reports. So you can deposit any number of food stamps without triggering the requirement to fill out the form. However, if you take the cash back out and it's over $10,000, a CTR must be filed.

What the crooks do is deposit, say $40,000 in stamps, and then structure their withdrawals so they are always below the $10,000 reporting requirement.

Stores that are not legitimate will have an account that is used to wash stamps. It is not a normal business account. They deposit the stamps and immediately take it right back out in cash, cashiers' checks or money orders, and all in one visit to the bank.

FA: Is bank employee collusion the key to making some of these scams work?

Haaser: No, several of our cases were provided to us by alert bank employees. They notice a pattern of structured deposits and withdrawals by a retailer, which tips them off that something is funny and they call us. Bank employees have triggered some of our big cases. In fact one case in Los Angeles worth $9 million came to us because a bank official noticed the structured withdrawals.

FA: How can bankers tell if their bank is being used?

Continued on page 2

Food Stamp Fraud: A Growing Problem Bankers Can Spot for Federal Investigators

Continued from page 1

Haaser: First, look for accounts where deposits had been going along at a steady rate, but then there is a sudden huge jump in deposits.

Or, look for a change in the pattern of a customer's redemptions. Somebody who came in once or twice a week to make deposits is suddenly coming in every day to make food stamp deposits. Or they make more than one deposit of food stamps a day.

Third, regular deposits usually involve several thousand dollars in food stamps. But as soon as they put the stamps in, they take out the cash.

Fourth, they usually make deposits of what we call "marching soldiers." They are very clean stamps that look like nobody has used them. When somebody comes in with a stack of food stamps that look like they just came from the printer, there is a good bet that they've been recently purchased on the street.

FA: How can bankers spot it?

Haaser: Generally from their own experience in dealing with retail customers. Bankers know what a storekeeper needs in banking services. If they don't ask for the normal banking services or they don't use them like a normal retailer, then they are probably laundering food stamps. If they do any of the things I've mentioned, it's pretty obvious.

FA: To whom do bankers report suspected food stamp fraud?

Haaser: They can find us in the federal government section of the phone book: the USDA Office of Inspector General. We also have a hotline number they can use: 800-424-9121.

FA: Who investigates food stamp fraud cases?

Haaser: Our office investigates them. We have a staff of 300 criminal investigators, who spend about 40 percent of their time on food stamp fraud.

FA: What can bankers do to protect themselves?

Haaser: There are no losses to the bankers in these cases, because the food stamps are sent through the system automatically. Even when we are involved in an investigation and we know a person is fraudulently redeeming stamps.

What bankers can do is cooperate with us when they come across these cases. When the investigator goes to the bank he will want to look at the suspect's deposit activity. If the bank has a camera, we'll want to look at the films so we have evidence that the person was in the bank. We'll want to interview tellers: Do they recognize the person making these deposits?

FA: Whose help is critical in shutting down these scams? Who is likely to spot it first?

Haaser: Tellers, because they will immediately spot strange activity. If somebody in the bank reviews patterns of deposits and is checking for CTR requirements, he or she will spot it. If a banker suspects that something is strange, he or she should call us right away.

For example, a case in Sacramento came to us by a tip from a bank. The store had been in operation for only three months. The bank noticed a pattern of food stamp deposits and then structured withdrawals of cash. It took us six months to develop the evidence to shut the operation down. That store was in business for nine months and took $1 million from us.

The sooner a bank employee calls us, the quicker we can shut these people down.

The food stamp program is heading toward electronic benefit transfer. In Maryland and Pennsylvania, recipients are given a credit card-like device. They go into a store with a point-of-sale terminal and they run the card through the terminal to buy groceries.

The funds are then taken out of the recipient's account and transferred electronically to the store account. At the end of the day the bank credits the merchant's account and then the bank gets its money from the Fed. So the typical trafficking problem isn't there.

The recipients can still go to the store and sell their benefits, even with the electronic transfer system. If the person who owns that bank account is coming in and getting out cash in structured amounts, that's the key that they are trafficking. The electronic benefit transfer system is small but other states are looking at it.

FA: How much of the food stamp program is getting washed or laundered?

Haaser: No one has set a value on it. We know it's probably in the hundreds of millions of dollars.

FA: So it's a big business and bankers are being used as the conduit?

Haaser: Right, and we have multi-million dollar cases around the country. In New York we have at least three cases that are worth up to $100 million. In Southern California we have cases in the $20 million range. In the Midwest we've had multi-million dollar cases.

FA: What could banks do to help you most?

Haaser: They can be alert to signs of fraud, and if they suspect anything call us and we'll look into it. ■

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.

Andrew C. Hove, Jr., Chairman
Alan J. Whitney, Director, Office of Corporate Communications
Frank Gresock, Editor

The Secret Service's Quest for "White Plastic"

Call it a modern day bank robbery: The U.S. Secret Service's Financial Crimes Division does.

The criminals in this case used electronics to rob customers and financial institutions of vital information that may have put up to 3,000 deposit accounts at risk. The thieves got the information by using a portable automatic teller machine (ATM) installed in a shopping mall in Manchester, Conn.

The thieves jammed a real ATM near where they had installed theirs. The customers walked over and deposited their ATM cards, which were read by the portable machine. Once the ATM had captured the personal identification number (PIN) and account information, it rejected the ATM cards.

The thieves are still on the loose, threatening to drain the cash from ATMs up and down the East Coast, where they have been operating since May, when the scheme in the mall was uncovered.

Agents in the Financial Crimes Division say bankers need to act quickly if they think something may be amiss with any of their cash machines. And by "quickly," the Secret Service agents mean within hours of the discovery.

The people involved in this case operate between 9 p.m. and midnight and early in the morning, after 5 a.m.

First, a banker in a small town who normally sees a dozen overnight transactions but discovers 200 transactions in one night should be prepared to call law enforcement authorities immediately; unless a carnival in town or another plausible situation explains the unusually high number of transactions.

Second, a banker who discovers what agents call "white plastic" in an ATM should immediately call the Secret Service or local police. White plastic means any counterfeit card that may only have some embossed numbers and a magnetic stripe on it. Generally the white plastic does not have a hologram, the logotype of the two major credit card companies, or the overall design of a legitimate card. Often it is just that, a white piece of plastic cut in the shape of a credit card, but it can be any color.

In either situation mentioned above, speed is of the essence. If law enforcement agencies learn about the transactions early in the morning, they can alert neighboring jurisdictions by afternoon to be on the lookout for unusual activity at ATMs in their communities.

After phoning law enforcement authorities, the federal agents say bankers should then save the film from the ATM's cameras. Put it safely away and label it. The pictures on the film may be the best evidence law enforcement officers have in identifying the criminals and the route they are traveling.

Continued on page 4

How to Handle Hot Cards

The U.S. Secret Service's Financial Crimes Division offers bankers these pointers on dealing with counterfeit credit cards that turn up in ATMs or at tellers' windows:

—If an unusually large number of ATM transactions from an equally high number of accounts occur overnight, immediately call the police or Secret Service.

—Likewise, if a "white plastic" counterfeit card with only a magnetic stripe and perhaps some embossed numbers is captured by an ATM, handle it by the edges and store it in an envelope until law enforcement officials arrive. Notify them immediately.

—Do not mail counterfeit cards to Master Card or Visa International; it will only delay the investigation by the Secret Service.

—Label and store the film from the ATM's cameras immediately. This may be the most helpful evidence you can provide.

—Warn tellers to be on the lookout for cards that have an incorrect hologram, lack the logo of either MasterCard or Visa International, or that do not have the overall pattern of standard credit cards. Criminals will also attempt to get cash advances at the tellers' windows.

—Remind tellers who reject counterfeit cards to remember to write down all information about the person who tried to use the card, the license numbers of motor vehicles and descriptions of them.

— The Secret Service wants any counterfeit cards your tellers or ATMs capture. The agency's forensic technicians can use them to develop a file on where and how these counterfeit cards are being made and the areas of the country where they are being circulated. Forward the bogus cards to your local Secret Service office with all pertinent details on how the counterfeit card was used.

—Remember that speed is of the essence.

The Secret Service's Quest for "White Plastic"

Continued from page 3

If you find that a white plastic counterfeit card has been captured by the ATM, handle it by the edges. It is important that evidence not be destroyed. Handing it around to bank employees will destroy fingerprints.

Put the phony card in an envelope to protect it until law enforcement officials arrive. Do not cut the card in half or snip off the corners as the card companies may have instructed. This will destroy vital information on the magnetic stripe.

Do not send the counterfeit card to MasterCard or Visa International. They will only notify the Secret Service, and it will be several days too late to help agents who are trying to discern the pattern of the criminals' activities.

The agents say the most serious part of this scam is that the thieves have the account information that will permit them to produce counterfeit cards that ATMs may reject, but retailers won't. The cards can be used to buy expensive jewelry and watches that are easily fenced.

Authorities are asking bankers to alert merchants and mall managers to the possible criminal activity. Businessmen, like tellers, need to be aware of bogus cards on which the hologram can be scraped off with a fingernail, instead of a genuine hologram that is imbedded into the plastic. They should be aware the counterfeit cards can also carry the wrong holograms, like the Statue of Liberty or a turkey.

Bankers should also tell mall managers to be alert to anyone asking to install a portable ATM. Bankers can verify if the would-be tenants represent a bona fide financial organization.

In the Connecticut case, a mall manager with 19 years of experience mistakenly believed the criminals represented a financial institution. As the Secret Service agents pointed out, these are very sophisticated thieves, who will provide phone numbers, routing numbers and codes that are very convincing. Closer to home, bankers can educate their tellers to be more diligent in examining the cards they accept for cash advances. Bankers should also check their ATMs to make sure the cameras are working.

The photos of the thieves electronically robbing your bank may be the best evidence you can provide the Secret Service.

If you have any questions about cards that may have been captured or seized by your bank's ATMs, call the nearest Secret Service office. ■

FDIC
Federal Deposit Insurance Corporation
Washington, DC 20429-9990

OFFICIAL BUSINESS
Penalty for Private Use, $300

BULK RATE MAIL
Postage & Fees Paid
FDIC
Permit No. G3b

ATTN: Chief Executive Officer