University of Nebraska - Lincoln
DigitalCommons@University of Nebraska - Lincoln

Historical Materials from University of Nebraska-Lincoln Extension

Extension

1982

EC82-875 Checks, Money and Credit Card Fraud

Wanda M. Leonard

Follow this and additional works at: http://digitalcommons.unl.edu/extensionhist

Leonard, Wanda M., "EC82-875 Checks, Money and Credit Card Fraud" (1982). *Historical Materials from University of Nebraska-Lincoln Extension*. 4383.
http://digitalcommons.unl.edu/extensionhist/4383

This Article is brought to you for free and open access by the Extension at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Historical Materials from University of Nebraska-Lincoln Extension by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

S
85
E7
82-875
c. 1

Nebraska Cooperative Extension Service
EC 82-875

CHECKS, MONEY AND CREDIT CARD FRAUD

Wanda M. Leonard
Extension Community Resource Development Specialist

Frauds using checks, credit cards and cash have increased in recent years and most experts place the total amount lost in excess of $40 billion annually.

Most of these frauds occur late in the year (70% from October to December).

Technological advancements have contributed to success of these frauds. The color-copying machine, invented in 1977, has been responsible for millions of dollars of color-copied checks, counterfeit bills, false credit cards, and false identification. A drivers license can be color-copied as is or can be altered by changing the picture to match the "new" user. When the copy is laminated between two pieces of plastic, it's accepted almost anywhere.

Easily operated, inexpensive printing equipment has also contributed to growth of money fraud schemes. Until recently, forgery was considered a sophisticated crime that involved the "giants" in the criminal world. That's not true today. The inexperienced individual can readily purchase, rent, lease, or use printing equipment.

Another contributing factor to the increase in fraud is the low arrest and conviction rate. Many money fraud criminals are not arrested, and of those who are, only 8% are convicted. The fault cannot always be placed with law enforcement or the courts. Much of the fault remains with individuals who accept the forged or illegal instruments of payment.

Cashiers have been known to accept advertisements pasted up to look like travelers checks, checks written on "sample checks," checks bearing a signature reading "U.R. Stuck," and pieces of paper written in the form of a check but bearing no bank name, address, or bank number.

What Can Be Done?

Business owners and managers need to: 1) become familiar with methods used by the con artists, 2) make sure that employees receive training that will help them recognize fraudulent money schemes and risky checks, and 3) inquire about new or additional methods of detection that can enhance the security of their business.

Cashiers should learn, practice, and use techniques established to identify the con artist's tactics and money fraud schemes. Here are some techniques that can help prevent being a victim of a money fraud scheme.

CHECKS

A cashier is vulnerable in three ways by accepting checks: 1) the check may be drawn on an overdrawn or insufficient funds account, 2) the check may be drawn on a closed or non-existent account, or 3) the check may be a forgery.

Insufficient funds checks can result from intent to deceive, error, or oversight, but non-existent or closed account checks and forged checks are planned, illegal crimes.

Hot Checks

Insufficient funds and closed account checks are called "hot checks." Ninety percent of them are low numbered (101 to 150), and come from new accounts. Not all checks from new accounts are bad. But, when a customer repeatedly writes insufficient funds checks, the bank usually closes the account and the customer opens a new one with a different bank. A high numbered check may indicate that the customer has had the account for a long period of time. You can estimate the age of an account, using as a rule of thumb that a person writes about 250 checks per year. Thus, a check numbered 350 usually comes from an account above one year old; one numbered 600 from a two-year-old account, and so forth.

Some banks use a date code that shows the date on which the account was opened. In this code the number "782" means the account was opened July, 1982; "1061" means the account was opened October, 1961. When the check you're accepting has a date code, use it. It is printed in small type, and is unnoticeable in many cases. It's usually located in the upper left portion of the check—near the individual's name and address, or in the lower right portion, an inch or so above the signature line.

Forged Checks

There are several observations that a cashier can make when accepting a check that will aid in identifying a forged item. With a little practice, these can become a part of the routine of accepting a check.

Issued in furtherance of Cooperative Extension work, Acts of May 8 and June 30, 1914, in cooperation with the U.S. Department of Agriculture. Leo E. Lucas, Director of Cooperative Extension Service, University of Nebraska, Institute of Agriculture and Natural Resources.

The Cooperative Extension Service provides information and educational programs to all people without regard to race, color, national origin, sex or handicap.

Bank Routing Numbers. Learn to interpret bank routing numbers located near the bottom of a check. These are found on all personal checks, money orders, payroll checks, cashiers checks, travelers checks, and government checks. They are found within the bar brackets. Numbers outside the brackets, but on the same line, represent the check number and/or the individual account number.

The first two numbers of the bank routing number identify the Federal Reserve Banking District (Figure 1). A common practice is to alter or change one or both of the first two routing numbers. Always be certain that the check offered for payment bears the Federal Reserve District number that corresponds with the location of the bank on which the check is drawn. Changing one or both of these gives the forger a "get-away time" of a week to ten days. For example: A check written on a Nebraska bank should read "10" because Nebraska is in the Tenth Federal Reserve District. If that "10" were changed to read "11," the check would be directed to the Eleventh Federal Reserve District with headquarters in Dallas, Texas. The forged check would not correspond to an Eleventh District member bank and the check would be returned to the bank where originally cashed or deposited.

Many large company checks are issued on banks located away from the employee's place of employment. For example, an employee of the local plant of the "A" Corporation may receive a payroll check drawn on a San Francisco bank issued from "A" Corporation's headquarters in Minneapolis. Remember, the first two routing numbers correspond to the location of the bank, not the company address, and not the address of the employee.

A cashier who regularly accepts out-of-state checks, or company checks, should keep a reference such as Figure 2 near the cash register for easy referral.

Some Savings and Loan companies (S & L's) offer checking services with NOW accounts. S & L's have different Federal Reserve Districts than commercial banks. Figure 3 shows the Savings and Loan District numbers and their member states. Use the same process to identify a forged routing number as for a commercial bank check.

If you suspect the routing number has been altered, or if it has been torn or mutilated, check the fraction number in the upper right-hand portion of the check (Figure 4). The numbers in the bottom of the fraction should match the first four numbers of the bank routing

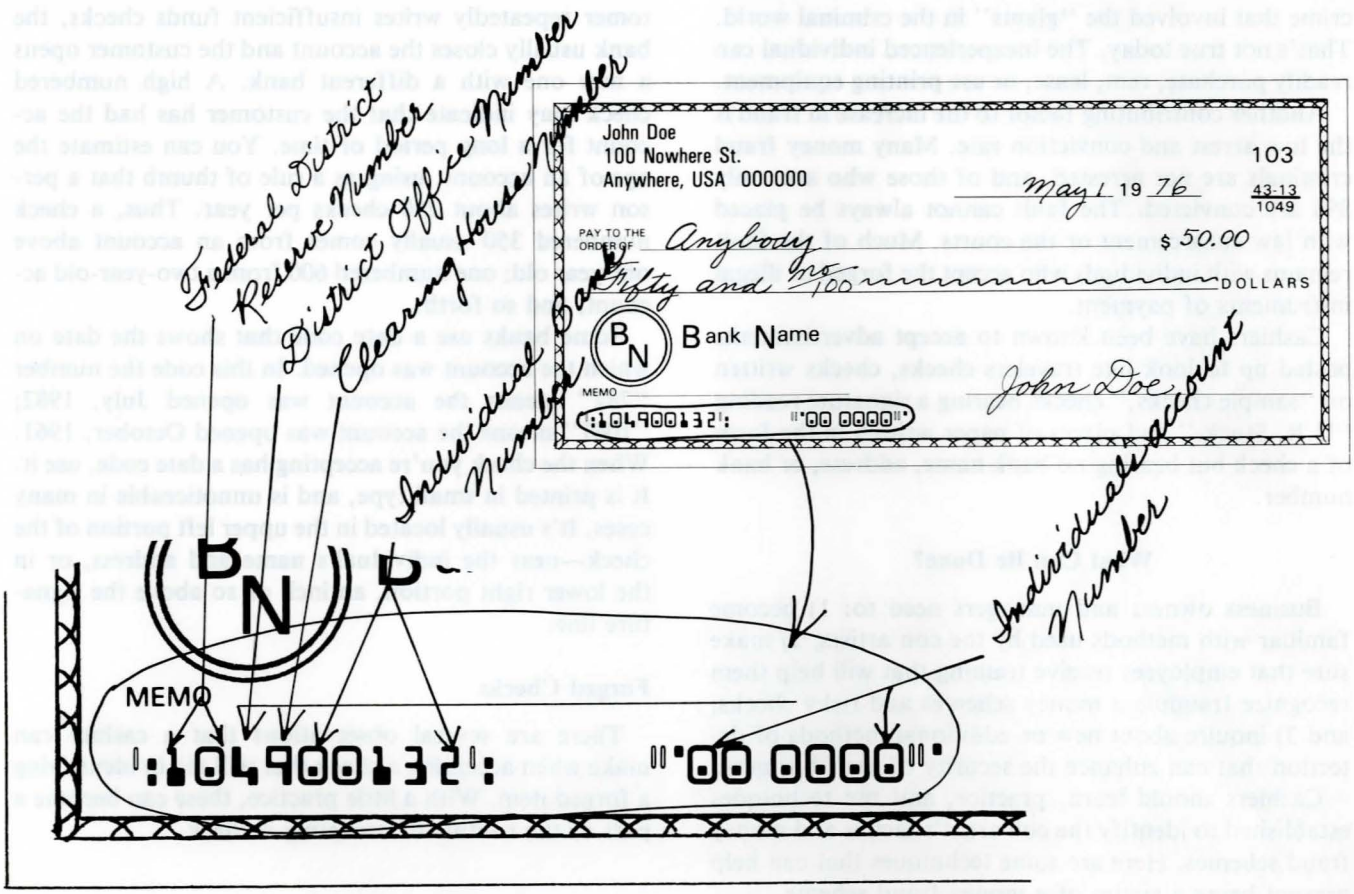
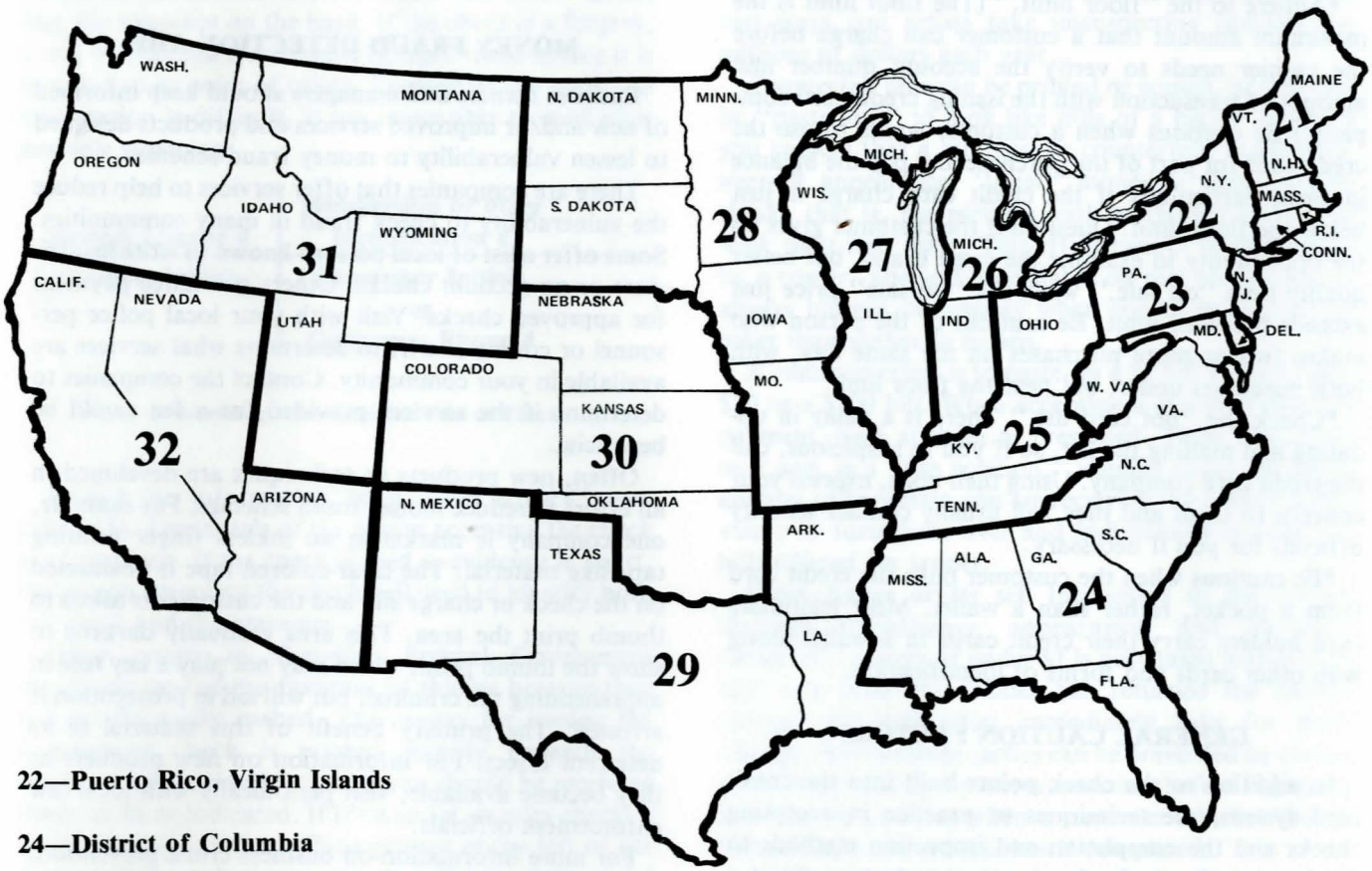


Figure 1. An Explanation of the Bank Routing Number

01-Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont
02-Connecticut, New Jersey, New York
03-Delaware, New Jersey, Pennsylvania
04-Kentucky, Ohio, Pennsylvania, West Virginia
05-Maryland, North Carolina, South Carolina, Virginia, West Virginia, Washington, D.C.
06-Alabama, Florida, Georgia, Lousiana, Mississippi, Tennessee
07-Illinois, Indiana, Iowa, Michigan, Wisconsin
08-Arkansas, Illinois, Indiana, Kentucky, Mississippi, Missouri, Tennessee
09-Michigan, Minnesota, Montana, North Dakota, South Dakota, Wisconsin
10-Colorado, Iowa, Kansas, Missouri, Nebraska, New Mexico, Oklahoma, Wyoming
11-Arizona, Lousiana, New Mexico, Oklahoma, Texas
12-Alaska, Arizona, California, Hawaii, Idaho, Nevada, Oregon, Utah, Washington

Figure 2. Federal Reserve District Numbers and Areas Served



22—Puerto Rico, Virgin Islands

24—District of Columbia

32—Alaska, Hawaii, Guam

Figure 3. Federal Home Loan Bank District Numbers and Corresponding Areas Served

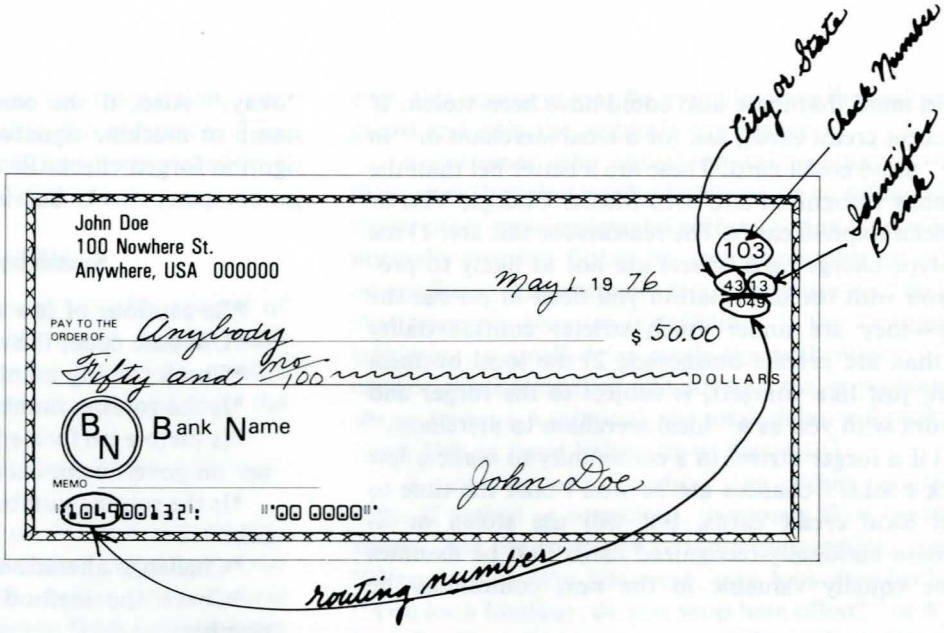


Figure 4. The Fraction Can Be Used to Identify Correct Federal Reserve District Number.

number. Forgers can change the bank routing number, but have difficulty changing the fraction, so they usually leave it unchanged.

Government checks have routing numbers beginning with the number "0000." All travelers checks begin with a routing number "8000."

Position of Routing Numbers. Routing numbers must be located exactly 5 5/8 inches from the right edge of the check. A measuring tape located on the counter or the cash register can be used for quick verification.

Perforated Edge. Most checks are torn from a book. Thus, a legitimate check is usually perforated on at least one edge. Many company checks are perforated on two edges—the edge torn from the book, and the edge torn from the withholding information statement. Forgers often find it too difficult or time consuming to perforate their forged check so they cut the checks smooth on all four sides.

Government Checks Are Not Perforated. These checks are printed on IBM index cards and are smooth on all sides with the upper left corner cut at an angle.

Sheen of Magnetic Ink. Used to print bank routing numbers, magnetic ink is dull and its use is very restricted. Tipping the check will show if there is any sheen to the magnetic numbers. *Remember,* forgers cannot obtain magnetic ink, and *all other inks have a sheen.* If you doubt the ink, try smudging it with a damp finger. Magnetic ink will not smudge. Color-copied ink will smear and turn a different color.

Alterations and Erasures. Alterations and erasures are often used in forgery. A $5.00 check may be converted to a $50.00 check by adding a "0" in the written number and writing over the written "five" to make it read "fifty." Look closely at the written numbers and words. Challenge any check on which numbers or words appear to have been altered or added. Look carefully at the number and letter spacings, style of writing, subtle variations in color of ink or strength of impression.

Check Numbers. Check numbers should always be machine printed and not written, typed, or stamped. Forgers find it difficult to consecutively machine-number checks, so they add the number after the checks are printed, or print many checks bearing the same number. A machine-printed number isn't proof that the check is legitimate, but a typed, stamped, or written number is questionable.

Forgers like to make their illegal checks look legitimate by embossing the written amount of the check by using a common "check protector® " or "pay master® " machine. Many company embossing machines imprint the company name with the amount of the check. When this is done, the check will read, "A Corporation seventy-five dollars." However, do not assume that *all* checks with the company name and dollar amount embossed are good. Blank checks are sometimes taken in a business burglary, and the burglar will use the company embossing machine to put the amounts on the blank checks at the same time the checks are stolen.

Identification. Always ask for identification bearing a picture of the individual presenting the check, such as a driver's license. Is the picture on the I.D. the person before you? Does the birthdate correspond with the age of that person? Has the I.D. expired?

A second identification is a good idea, but be selective in what you accept. A social security card or employee card could have been stolen at the time the other identification and checks were stolen. Ask for another identification with a picture, such as a student I.D. or a check cashing I.D. If the customer does not have a second I.D. with a picture, ask for a local department store credit card, or a local user or membership card, such as a library card, zoo membership card, health club card, or similar organization cards. Most thieves will discard this type of card.

Many businesses accept credit cards as a form of I.D.

Keep in mind that these also could have been stolen. If you accept credit cards, ask for a local merchant or "in house" store credit card. These are a better bet than the nationally recognized and used Master Charge, Visa or American Express cards. The reasons for this are: 1) the bank-type charge card issuers are not as likely to provide you with the information you need to pursue the forger—they are under much stricter confidentiality rules than are private businesses, 2) the local business person, just like yourself, is subject to the forger and can work with you as a "local merchant to merchant," and 3) if a forger arrives in a community to make a few "quick bucks," chances are he won't take the time to obtain local credit cards, but will use stolen or illegitimate nationally-recognized cards that he assumes will be equally valuable in the next community he "hits."

Always check the signature on the membership or credit card with the one written on the check. Determine that they were written by the same individual, and that there have been no erasures.

Recording Identification Information. Always record the identification information on the face of the check, near the top—not on the back. If the check is a forgery, it will be stamped a minimum of eight times before it is returned to its point of origin. Located on the back, the information is difficult, if not impossible to read after multiple stampings.

Drivers License #	**Membership or other Identification #**
Cashiers Initials	**Supervisor Initials or Customers Phone #**

Figure 5. Recording Information on Face of Check

Record the information on a "four square" area (Figure 5). The initials of the person accepting the check are important. If the check is used as evidence in court, the person accepting the check will need to identify both the check and the presenter.

Other points to Consider. Federal Government checks are one of the favorites of thieves because they are usually easily cashed. The reason for issuing the government check is printed directly beneath the amount. Ask yourself if that person should be receiving the benefits as indicated. If it's a social security check, a social security number will be printed at the left of the amount box. Ask the person to tell you their social security number. If it's stolen, chances are the thief will not have memorized the number. If the honest person hasn't memorized his/her number, it will usually be available in the wallet.

Forgers like to use company names in the upper left corner that cashiers recognize and assume to be "okay." Also, if the company is large, it will use a stamp or machine signature. A forger will often hand sign the forged check. Be cautious when accepting major company checks bearing a hand written signature.

Summary Check List

*Be cautious of low numbered checks.
*Use date code, if available.
*Check routing number with bank location.
*Is the routing number in the correct location?
*Is there a perforated edge? Or, a trimmed corner on government checks?
*Is the routing number printed in dull, magnetic ink?
*Challenge alterations or erasures.
*Check the method of imprinting the check number.
*Ask for one or more I.D.s with a picture and signature.

MONEY FRAUDS

Passing counterfeit bills and short-change tactics are two ways con artists take unsuspecting cashiers for millions of dollars each year.

Counterfeit bills can be printed or copied, or they can be "pasted-up" to look like bills of a higher value. If you suspect that a bill may be counterfeit, examine its over-all appearance. "Real" money is three dimensional, that is, the pictures look as though you could walk right into them. This effect cannot be duplicated by a copier. The seal is readable on real money, but is always blurred or smudgy when copied or printed by other than authentic means.

A common crime is to paste-up a $1 bill to look like a $20 or a $100 bill. When accepting a group of bills for payment, look at them as presented. Then, turn them over and, in a "fan position," visually count the dollar amount to be certain you are receiving the correct dollar value; or turn them over and individually recount the bills offered for tender.

Short-change artists sell themselves to the cashier through friendliness, appearance, and sincerity. Generally, an item of under $1 is purchased with a large bill, and after the cashier has returned the correct change, the con artist immediately asks for more change. Short-change tactics can be prevented by always completely closing out one transaction before beginning another. Be cautious when a customer asks for change before the initial transaction is completed.

Another practice to be alert for is the customer who insists that a larger bill was presented for payment, and therefore, more money is needed in return change. To prevent being "taken-in" on this, make it a practice to lay the presented bill(s) across the cash register ledge or across the compartment of bills, and leave it there until change has been counted back to the customer. Then, if

the customer challenges you on the transaction, you have the presented bill available for reference. This would not be the case if the bill had been placed in a compartment upon receipt.

CREDIT CARDS

Credit cards are often the most valuable reward of common street crime. There are "check points" built into the credit card system that cashiers should use as a routine. There are other factors that should alert the cashier to be cautious.

*Always check the expiration date. If the card is expired, don't accept it.

*Always check the signature on the card with the signature on the charge slip. Look at the basic shape of the noncapital letters. (Forget the capital letter, people often change them.) Size proportion from letter to letter is a good check. Also check the end strokes of their signature, that is, the place where the pen leaves the paper. The ending strokes tend to be very consistent regardless of where, when, how or with what the signature is made.

*Adhere to the "floor limit." (The floor limit is the maximum amount that a customer can charge before the cashier needs to verify the account number and amount of transaction with the issuing credit card company.) Be cautious when a customer wants to use the credit card for part of the purchase and pay the balance in cash, particularly if the credit card charge is just below the floor limit. Question if the customer gives up the opportunity to examine the same brand, but better quality item "on sale," when the "on sale" price just exceeds the floor limit. Be cautious of the person who makes two or more purchases on the same day, with both purchases under, but near the floor limit.

*Check the "hot card list." There is a delay in updating and mailing the list, so if you're suspicious, call the credit card company. Using their code, express your concern to them and they will usually contact security officials for you if necessary.

*Be cautious when the customer pulls the credit card from a pocket, rather than a wallet. Most legitimate card holders carry their credit cards in a wallet along with other cards and forms of identification.

GENERAL CAUTION FACTORS

In addition to the check points built into the credit card system, the techniques to practice in accepting checks and the completion and inspection methods to use in accepting cash, there are other factors about a customer's behavior that should cause a cashier to be suspicious.

Be cautious of

...an excessively talkative customer. Some are talkative by nature, so don't use this as the sole reason to doubt the credit card user or the check presenter. However, this customer may be trying to place the cashier off guard and gain the cashier's confidence.

...a customer who insists on taking clothing with them even though it needs alteration, or on taking clothing or other wearing apparel without trying it on when it normally requires fitting or, one who insists on taking an appliance that normally requires delivery; or an item that normally requires installation. If the customer is legitimate, a small delay while the authenticity of the card or check is verified will not be a major problem. If the customer is a criminal, the small delay will probably cause him to leave before he is discovered.

...a customer who "rushes" the cashier at closing time. If rushed or suspicious, purposely slow the transaction. Ask the customer an innocent question, such as "Were you in here last week, you look familiar?" or "You look familiar, do you shop here often?" or "You look familiar, do you use your credit card a lot?" or "I don't recognize you, but the name looks familiar, does your wife (or husband) use the card a lot?" An honest customer usually will not be offended by your question; a criminal customer will become nervous and anxious, and may leave the store for fear of being discovered.

MONEY FRAUD DETECTION AIDS

Business owners and managers should keep informed of new and/or improved services and products designed to lessen vulnerability to money fraud schemes.

There are companies that offer services to help reduce the vulnerability to check fraud in many communities. Some offer a list of local persons known to write insufficient or no-account checks. Others guarantee payment for approved checks. Visit with your local police personnel or county sheriff to determine what services are available in your community. Contact the companies to determine if the services provided for a fee would be beneficial.

Often, new products or techniques are developed in an effort to reduce money fraud schemes. For example, one company is marketing an inkless finger printing tape-like material. The clear-colored tape is positioned on the check or charge slip and the customer is asked to thumb print the area. This area gradually darkens to show the thumb print, which may not play a key role in apprehending the criminal, but will aid in prosecution if arrested. The primary benefit of this material is its deterrent effect. For information on new products as they become available, visit periodically with local law enforcement officials.

For more information on business crime prevention, visit your Cooperative Extension Service Office for the publications available on robbery, burglary, shoplifting and internal theft.