

Protect Your Credit Cards

Cooperative Extension Service
College of Agriculture and
Home Economics



Guide G-244

Reviewed by Constance Kratzer
Family Resource Management Specialist

This publication is scheduled to be updated and reissued 3/08.

Credit card fraud is a growing crime in the United States. It affects everyone—bankers, merchants and consumers. Although consumers have some financial protection from fraudulent use, loss of credit cards can be a time-consuming nuisance. Reporting the loss and getting new cards is necessary. One New Yorker said it took three months to get fraudulent charges off his bill after his wallet was stolen.

The growing use of automated teller machine cards creates more problems. Protections afforded consumers of these services are quite different from credit cards, and potential losses to the card users are much greater.

Stolen credit cards have been a problem for a long time. Now that ordering merchandise by telephone is a common practice, all a thief needs is your name and account number to make charges. He doesn't have to have your card. Counterfeiting is reported to be on the increase. All kinds of schemes are used to get names and numbers, including use of discarded carbons from transaction slips.

Liability of Cardholders

Credit cards. You are liable only for the first \$50 charged to your account by an unauthorized user. You do not have to pay for any unauthorized charges made after you notify the card company of loss or theft of your card. If you act quickly, you may not have any loss. Notification can be made by telephone or in writing. It is recommended that you follow up a phone call with a letter confirming your call.

If your cards have been used illegally and you have had to pay the first \$50 on one or more cards, check your homeowners policy for reimbursement. Most policies provide coverage up to \$500. No deductible applies to this coverage.

For the credit card issuer to hold you liable, they must have provided you with a telephone number, address or both that you can use for notification. In addition, the card issuer must provide some method by

which the cardholder or authorized user can be identified, such as a signature or photograph on the card.

Transactions not involving the card such as phone orders. The cardholder may not be held liable when the card itself (or some other sufficient means of identification) is not presented. Because the issuer has not provided a means to identify the user under these circumstances, the issuer has not fulfilled one of the conditions for imposing liability. For example, when a person orders merchandise by telephone, without authority to do so and using a credit card account number, no liability may be imposed on the cardholder.

Automated teller machine cards. If your automated teller machine (ATM) card is stolen and used, your liability could be much more than the \$50 limit on credit cards.

If you notify the card issuer within two days after you discover the ATM card loss, your liability cannot exceed \$50. If you do not notify the financial institution within two business days after learning of a theft or loss you can be liable for the amount taken from your account, up to a maximum of \$500.

If an unauthorized transfer occurs and you do not discover it until it shows up on your monthly bank statement, you must notify the bank within 60 days after the statement was mailed to you. Your liability is \$50 or the amount of the transaction, whichever is less. If you do not tell the bank within 60 days, you may be liable for all losses resulting from unauthorized use of the card after the 60-day period. This means you could lose all the money in your account.

TAKE PRECAUTIONS WITH YOUR CREDIT CARDS

Examine your statement. Keep your sales slips and check your monthly statement carefully, comparing sales slips with the charges on the statement. If

there are charges you did not make, notify the card company immediately. Examining your statement is the single most important thing to do, says a security expert at the Bank Administration Institute, a banking research group. Be particularly watchful when you have a big bill because of travel or holiday shopping.

Make a list. Set up a record right now of all your credit cards, the account numbers, addresses and phone numbers of the issuing companies. Keep the list in a safe place, but not with your credit cards. This information is vital if your cards are lost or stolen. Note whether there is a free 800 number to call, or a number that can be called collect. This information will be on the disclosure statement that comes with your new card and with each renewal card. It may also be on the back of your credit card.

Travel with care. Do not travel with more credit cards than you need for the trip. Leave the rest at home in your safe deposit box. If your cards are stolen or lost, you will need the card company phone number. Carry this separately from the cards.

Report a loss at once. If your cards are lost or stolen, notify the card issuer immediately. You are not liable for any charges made on your card if notification is made before the card is used.

Keep cards separate from cash. It is best not to carry your credit cards in your wallet. Use a separate card holder or a purse that has inside zipped pockets for credit cards so you will not lose everything if your wallet is lost or stolen.

Treat cards as cash. Do not leave them lying around loose in a coat pocket, in the house or in the glove compartment of a car. Never toss an expired card in the trash without first cutting it up. If you decide to discontinue the use, notify the company to close your account. Do not lend your card to anyone.

Limit the number of cards you own. The fewer you have, the fewer you need to keep track of. Some authorities say one, or two at the most, major all-purpose cards is enough. Also limit gasoline and retail cards.

Get your card back. Be sure your card is returned after each transaction. Also, check to see that it is your card rather than a substitute card.

Watch the salesperson. Present your card only after completion of a sale. Watch how your card is handled during the transaction and see that only one slip is imprinted. Be sure the amount handwritten or imprinted on your receipt is correct.

Be cautious using your card by phone. Beware of anyone who wants your credit card number over the

telephone. Counterfeiters use tricky calls to get valid numbers.

Common sense will be your guide because there may be occasions when you must give your credit card number over the phone, such as to guarantee hotel reservations. Use your credit card number to order merchandise by phone only when absolutely necessary.

Tear up carbons. Large counterfeiting rings in New York and Florida were found to be using the carbons from transaction slips. Some people now tear up the carbon after a transaction so it can't be recovered from a waste basket and used by counterfeiters or dishonest salespeople.

SERVICE PROTECTION PLANS

A number of companies offer a credit card listing service. For \$12 to \$20 a year, the company offers to register your credit cards and, if they are lost or stolen, they will notify all the credit card companies.

Before you decide to sign up for one of these plans, give some thought to whether you really need the service. Remember, federal law provides that the most you can be held liable for is \$50 per card, and this is only if someone uses the card before you notify the company of its loss or theft.

If you carry a large number of credit cards, this could add up if each one was used. If you carry only a few cards, you may prefer to handle notifications yourself rather than paying the annual fee.

PROTECTING YOUR ATM CARDS

Bankers say there is less fraud involving the cards used in automated teller machines, because you need a personal identification number (PIN) as well as the card to get into the system. One of every three losses that banks and their customers suffer from fraudulent use of automated teller machines involves a member of the cardholder's family. According to Visa International, which distributes ATM cards as well as credit cards, the second-most-common fraud pattern involves theft of ATM cards on which card holders have written their personal identification numbers.

Memorize your PIN number. Do not write it on your card. Also, do not write it on other cards in your wallet, such as your Social Security card. Arizona bank officials found the PIN number on 25 percent of

the teller-machine cards they examined in an informal survey.

Choose a random number. If you choose your own teller-machine identification number, stay away from your birthdate, Social Security number, address and phone number. Thieves try these numbers first.

Check your statement. As with credit card bills, check your statement carefully and report any unauthorized charges immediately.

SOURCES

“Credit-Card Holders Can Minimize Losses Due to Fraud by Taking Basic Precautions,” *The Wall Street Journal*, Feb. 26, 1984.

Electronic Fund Transfers, Regulation E, Board of Governors, Federal Reserve System, Section 205.6.

Everybody's Money. Volume 24/No. 1. Credit Union National Association, Box 431, Madison, Wis. 53701.

“Finance Trends,” *U.S. News and World Report*, Feb. 27, 1984.

Truth-in-Lending, Regulation Z, Board of Governors, Federal Reserve System, Section 226.12.

The information given herein is supplied with the understanding that no discrimination is intended and no endorsement by the New Mexico State University or the Cooperative Extension Service is implied.

New Mexico State University is an equal opportunity/affirmative action employer and educator. NMSU and the U.S. Department of Agriculture cooperating.

March 2003

Las Cruces, NM
3C

Guide G-244 • Page 4

Electronic Distribution March 2003