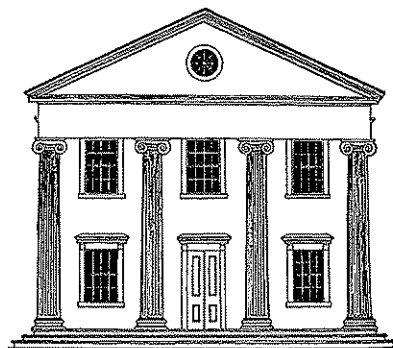


PARKING LOT SECURITY

- Be alert to your surroundings and other people around you.
- Never display cash in a financial institution parking lot ... if possible, not even a "bank bag."
- When you conduct banking business during the hours of darkness, have someone accompany you.
- Park as near as possible to your destination, e.g., branch entrance, automatic teller machine or night depository.
- Establish your banking relationship with a financial institution that provides an obviously safe and secure environment, including the parking lot. Look for the following characteristics:
 - well lighted parking lot and exterior
 - landscaping or other objects which do not provide "hiding places" for robbers
 - located on a well traveled street
 - unobstructed visibility in all directions



Safety and Security Tips for Financial Institution Account Holders

Don't be a Victim!

This pamphlet contains many common-sense, precautionary measures to help you avoid being victimized.

Customers are often victims of crimes which involve their financial institutions. Depending on the type of crime, the customer and/or financial institution can sustain losses of varying severity, and it is conceivable that physical harm may occur during the commission of certain crimes. It behooves you to be aware of such crimes and assume a protective attitude in order to avoid becoming a victim. Following are some of these categories of crime, along with safety and security tips that can be helpful to you in attempting to avoid the situations that may cause you to be vulnerable.

Credit Cards may look like plastic

DO

- Sign your credit cards.
- Exercise care in protecting your bank cards. Remember, they are very valuable.
- Check your cards regularly to ensure you have them.
- Report a lost or stolen card to the bank immediately. The longer you delay, the more time the thief has to run up charges.
- Record your bank card number and keep it where it will be safe but easily available to you.
- Open your credit card bills immediately—even if you intend to pay the bill later. Review the charges to see that they were for purchases YOU made. If you find unauthorized charges, promptly call us.
- Watch carefully (where possible) as clerks fill in credit card slips to prevent a dishonest clerk from making a second slip and submitting a phony charge later.
- Ensure that it is your card that is returned to you after each purchase.
- Carry your cards secured safely in your wallet or purse.
- Retain card receipts and carbon copies which carry your account number.
- Be aware of those around you in crowded places such as malls and entertainment or sporting events.

...but they're really money

DON'T

- Carry credit cards that you use infrequently. Keep them in a safe place.
- Give credit card numbers to "telephone survey" people claiming to work for credit card companies, or to any unknown caller.
- Leave your credit cards anywhere in your automobile, even if it's locked.
- Leave your credit cards unsecured and unattended anywhere, even at work.
- Leave your credit cards unsecured and unattended in a hotel or motel room.
- Treat your credit cards casually. They are worth money, so make sure they are returned promptly by clerks.
- Be fooled by "Good Samaritan" callers who say they have found your credit cards and promise to mail them to you right away. This just gives thieves time to run up charges. **CALL THE ISSUER IMMEDIATELY.**
- Ever lend your credit cards to anyone.



National Association
for Bank
Security



National Association
for Bank
Security

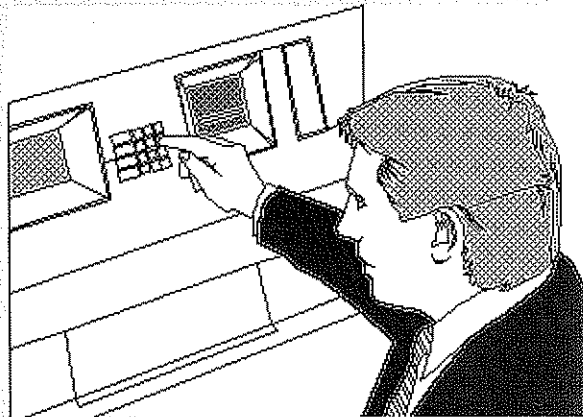


IF IT SEEMS TOO GOOD TO BE TRUE



A significant number of check fraud losses that occur involve customer accounts. In order to avoid becoming an unwitting victim of fraud schemes, you need to know about the existence and consequences of fraud, proper check issuing, and timely statement reconciliation. Following is a brief list of checking account protection tips.

1. Guard your checkbook and extra (new) checks.
2. Never give your account and routing numbers to people you do not know, especially to anyone over the telephone.
3. Never use your deposit slip for "scrap" paper or notes and then give it to someone. Guard your deposit slips.
4. Properly store or dispose of canceled checks.
5. If your checkbook is lost or stolen, immediately inform us.
6. When traveling for a period of time, it is wise to leave your checkbook at home, locked away, and purchase traveler's checks.
7. Always write checks using ink pens or typewriters — never pencil.
8. Write the payee name, and the dollar amount in both numbers and letters, as far to the left in the allotted space as possible and draw a line through the unused space to the right of the letters and numbers to prevent additions.
9. Balance or reconcile your checkbook register with your monthly bank statements.
10. When writing the payee name on the "Pay to the Order of" line, make sure the name is spelled out so it cannot be altered (e.g., I.B.M. could be changed to I.B. Maroney).



A T M S E C U R I T Y

- If possible, avoid using ATMs during hours of darkness. If you must do so, try to have another person accompany you.
- If an ATM facility must be used at night, try to select one in an area that is well lighted.
- When possible, try to choose a facility that has limited foliage and is well-trafficked.
- Familiarize yourself with security devices in place at the ATM you elect to use.
- Thoroughly observe the area around the ATM before approaching and using the machine. . . look for suspicious persons loitering nearby, especially people who remain in parked cars.
- Be cautious of anyone who engages you in conversation as you approach the ATM, while you are using it, or immediately thereafter.
- Be suspicious of anyone who closely observes you while you are using the ATM; protect your PIN from view.
- Spend as little time at the ATM facility as possible.
- Don't count or needlessly expose cash at the ATM. It should be counted in a secure place away from the machine.
- Don't leave your receipt at the ATM because it may contain account information.
- Don't reveal your PIN to anyone in person or over the telephone for any reason, even if the individual represents himself as a bank employee. This is especially important if you have recently lost or had your card stolen.

BUNCO SCAMS

Please be aware that swindlers attempt to commit crimes by having customers of financial institutions withdraw funds from their accounts with the promise that they will be paid a fee or receive some type of immediate windfall. Sometimes the customer is asked to show good faith by matching the amount to be gained by him or her, or the customer may be told that the money will be immediately redeposited in order to test the honesty of a bank employee. Be extremely wary about withdrawing large sums of cash, either to show the funds to a stranger or to give the money, even for a few minutes, to someone you do not personally know.

BANK EXAMINER SCHEME

The phony examiner scheme is a popular swindle usually perpetrated against elderly customers. One variation of the scheme involves the con artist impersonating the financial institution's auditor or a law enforcement officer, such as an FBI agent, rather than an examiner. The elements of the scheme are:

1. The customer (victim) is confronted in person or by telephone by a stranger who claims to be a federal/state bank or savings and loan examiner.
2. The stranger claims an employee of the financial institution is altering deposit records and stealing the funds.
3. The stranger asks the customer to withdraw funds, mark the money and give it to him. He says that he will then redeposit it, creating a trap if the employee alters the deposit slip and attempts to steal the money. The customer never sees the stranger — or his or her money — again.

PIGEON DROP SCHEME

This fraud will generally consist of the following:

1. A stranger engages the customer (victim) in idle conversation.
2. A second stranger joins them, purporting to have found an envelope containing a large amount of money. Something about the envelope indicates it was lost by a criminal.
3. Ultimately, it is decided that the money will be held for a period of time, then shared by each of them. The customer is asked to hold the money.
4. The strangers then show distrust of the customer, with feigned, apparent fear that the customer will spend the money.
5. The customer is convinced to withdraw funds in order to "show good faith" that he has enough personal money and, therefore, has no need to spend the found money until it is to be divided among the three of them. This is the last the customer sees of his or her money.

**Strangers Are Not Always Crooks
But Crooks Are Usually Strangers!**