How To **Protect** *Your* **DEBIT, CREDIT and ATM CARDS**

ATM SAFETY

Protecting Your Cards

The best protections against card fraud are to know where your cards are at all times and to keep them secure. For protection of ATM and debit cards that involve a Personal Identification Number (PIN), keep your PIN a secret. Do not use your address, birthdate, phone or Social Security number as the PIN and do memorize the number.

For Credit and ATM or Debit Cards:

- Be cautious about disclosing your account number over the phone unless you know you are dealing with a reputable company.
- Never put your account number on the outside of an envelope or on a postcard.
- Draw a line through blank spaces on charge or debit slips above the total so the amount cannot be changed.
- Do not sign a blank charge or debit slip.
- Tear up carbons and save your receipts to check against your monthly statements.
- Cut up old cards - cutting through the account number - before disposing of them.
- Open monthly statements promptly and compare them with your receipts. Report mistakes or discrepancies as soon as possible to the special address listed on your statement for inquiries. Under the Fair Credit Billing Act (FCBA) for credit cards and the Electronic Funds Transfer Act (EFTA) for ATM or debit cards, the card issuer must investigate errors reported to them within 60 days of the date your statement was mailed to you.
- Keep a record (in a safe place seperate from your cards) of your account numbers, expiration dates, and telephone numbers of each card issuer so you can report a loss quickly.
- Carry only those cards that you anticipate you will need.

For ATM or Debit Cards:

- Do not carry your PIN in your wallet or purse or write it on your ATM or debit card.
- Never write your PIN on the outside of a deposit slip, an envelope, or other papers that could be easily lost or seen.
- Carefully check ATM or debit card transactions before you enter the PIN or before you sign the receipt; the funds for this will be fairly quickly transferred out of your checking or other deposit account.
- Periodically check your account activity. This is particularly important if you bank online. Compare the current balance and recent withdrawals or transfers to those you have recorded, including your current ATM and debit card withdrawals and purchases and your recent checks. If you notice transactions you didn't make, or if your balance has dropped suddenly without activity by you, immediately report the problem to your card issuer. Someone may have co-opted your account information to commit fraud.

Automated Teller Machine Safety

1. Be aware of the surroundings when using an automated teller machine, particularly during the hours of darkness.
2. Be accompanied by another person when using an automated teller machine during the hours of darkness.
3. Refrain from displaying cash, place cash in a pocket as soon as a transaction is completed and count cash in the safety of a locked enclosure such as a car or home.
4. Use another automated teller machine or return at a later time if anything suspicious is noticed when using or considering using an automated teller machine.
5. Limit your time at the machine. Prior to arriving at the ATM site, have your card out to avoid any delay of going through your purse or wallet to find it.
6. Cover your transaction with your body by blocking the keyboard from view. By doing this, you will prevent someone from learning your Personal Identification Number (PIN).
7. Always keep your Personal Identification Number a secret. Never give the number to anyone or write it down anywhere. Memorize it or use a secret code if you must write it down.
8. Notify us immediately if your ATM access card or secret PIN is lost or stolen.
9. Never let anyone use your card or access code. Law enforcement officers or financial officials will never ask for these items. Be suspicious if anyone does ask for these items.
10. Report all crimes immediately to the operator of the automated teller machine or to local law enforcement officials.

Electronic Funds Transfer Act

Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss. If you report an ATM or debit card missing before it is used without your permission, the EFTA says the card issuer cannot hold you responsible for any unauthorized transfers. If unauthorized use occurs before you report it, your liability under federal law depends on how quickly you report the loss.

For example, if you report the loss within two business days after you realize your card is missing, you will not be responsible for more than $50 for unauthorized use. However, if you do not report the loss within two business days after you discover the loss, you could lose up to $500 because of an unauthorized transfer. You could also risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you. That means you could lose all the money in your bank account and the unused portion of your line of credit established for overdrafts. However, for unauthorized transfers involving only your debit card number (not the loss of the card), you are liable only for transfers that occur after 60 days following the mailing of your bank statement reflecting the unauthorized use and before you report the loss.

Fraudulent Charges or Transfers - Fair Credit Billing Act

Your maximum liability under federal law for unauthorized use of your credit card is $50. If you report the loss before your credit cards are used, the FCBA says the card issuer cannot hold you responsible for any unauthorized charges. If a thief uses your cards before you report them missing, the most you will owe for unauthorized charges is $50 per card. Also, if the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use.