



CRIME PREVENTION HANDOUT

ATM Safety and Security

A robbery of a person using an ATM is the most serious concern related to the presence of ATMs. A would-be robber will obviously know an individual using an ATM will usually leave the machine with cash money in their possession after withdrawal of funds. In addition, if an individual is the victim of an ATM robbery, other personal property such as wallets, purses, credit cards and jewelry will often be taken.

According to the Bank Administration Institute, the most dangerous hours for ATM crime are from 7:00 p.m. until midnight, when approximately 40% of ATM-related crimes occur.

The following are a number of ATM safety and security tips.

Approaching the ATM

- At a drive-up ATM, keep all windows closed, except the one you are using, and all vehicle doors locked. Keep the vehicle running and be watchful of the vehicle's front, rear and sides. If someone approaches your vehicle on foot, cancel the transaction and leave.
- If you drive to the ATM and then exit your vehicle to use the ATM, lock all of the vehicle doors after you exit it. Then, keep your keys handy so you can re-enter your vehicle quickly after completing your transaction.
- When approaching the ATM, be alert for anything suspicious, especially two or more people in a nearby vehicle, particularly if no one else is at the ATM, or someone appears to be "hanging" around the area.
- Never approach an ATM if the lights at the site are not working.
- Particularly after dark, take a companion along to the ATM, if at all possible, and park close to the ATM in a well lighted area.
- Avoid using ATM's with obscuring bushes around them, again, particularly after dark.

Using the ATM

- When waiting in line to use the ATM, wait well behind the person(s) ahead of you, and do not approach the ATM until they complete their transaction.
- When you are using the ATM and someone is closer to you than you would like them to be, ask them politely and tactfully to step back a few steps. If they do not do so, cancel your transaction and wait in your locked vehicle or other safe location until that person leaves — or possibly go to another ATM.
- Before you approach the ATM, have your card ready, know your code and if anything such as a deposit slip needs to be filled out, have it completed. If making a deposit and you do not have a deposit envelope, obtain one from the storage section of the ATM and fill it out in your locked vehicle or other safe locations before you return to the ATM.
- Protect your Personal Identification Number (PIN). Memorize your PIN. Do *not* write your PIN on your ATM card or carry your PIN in your wallet or purse.
- Select a PIN that is different from other numbers noted in your wallet or purse, such as your address, birth date, telephone or social security number.
- When using the ATM, stand directly in front of the keyboard, blocking the view of others.
- Do not enter the PIN if anyone else can see the screen.
- As remote as it may seem, criminals can use high-powered equipment to visually capture cardholder's PIN's as they are punched into keypads. By picking up discarded ATM transaction receipts, criminals can match up PIN's and account numbers and have all the information they need to manufacture false ATM cards and gain access to consumer's money. This is referred to as "shoulder surfing."
- Never accept offers of assistance with the ATM from strangers. If you are having problems, contact your financial institution.
- When your ATM transaction is completed, immediately take your property — card, receipt, money, etc., put them in your pocket, wallet or purse and leave immediately. *Never stand and count your money.* You can count it later. If your transaction is inaccurate, you cannot discuss it with the machine. Thus, there is no need to count your money at the ATM and risk exposing yourself to a would-be criminal.
- ATM robberies often occur after the patron has completed their transaction. Always have your head up and be aware of your surroundings when you leave an ATM. If you feel or sense someone is following you, walk or drive to the nearest open business or where there are a lot of people and call the police.

- **Never** tell your access code or PIN to *anyone!*
- **Never** lend your ATM card to anyone; treat it like cash or a credit card.
- If you lose, misplace or have your ATM card stolen, notify the card issuer *immediately*. If you report an ATM card missing before it is used without your permission, the Electronic Fund Transfer Act (EFTA) says the card issuer cannot hold you responsible for any unauthorized withdrawals. If unauthorized use occurs before you report it, the amount you can be held responsible for depends upon how quickly you report the loss to the card issuer. 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 \$50.00 for unauthorized use. If you do not notify the card issuer within two business days of its loss, you could be held responsible for up to \$500.00 for unauthorized use. If within 60 days after your bank statement is mailed to you, you do not report an unauthorized transfer or withdrawal, you risk total loss of funds.
- Consider buying a card registration service. Many companies offer card registration and protection services that will notify all companies where you have credit and ATM card accounts in case your card is lost or stolen. With this service, you make only one telephone call to report all card losses instead of calling each card issuer individually. Also, most card registration services will request replacement cards on your behalf. Registration services usually cost \$10.00 to \$35.00 annually.

Reference "The Complete Campus Crime Prevention Manual" by The AEGIS Protection Group.