An ATM is simply a **data terminal** with two input and four output devices. Like any other data terminal, the ATM has to connect to, and communicate through, a **host processor**. The host processor is analogous to an [Internet service provider](#) (ISP) in that it is the gateway through which all the various ATM networks become available to the cardholder (the person wanting the cash).

Most host processors can support either **leased-line** or **dial-up** machines. Leased-line machines connect directly to the host processor through a four-wire, point-to-point, dedicated [telephone](#) line. Dial-up ATMs connect to the host processor through a normal phone line using a [modem](#) and a toll-free number, or through an Internet service provider using a local access number dialed by modem.

Leased-line ATMs are preferred for very high-volume locations because of their **thru-put** capability, and dial-up ATMs are preferred for retail merchant locations where cost is a greater factor than thru-put. The initial cost for a dial-up machine is less than half that for a leased-line machine. The monthly operating costs for dial-up are only a fraction of the costs for leased-line.

The host processor may be owned by a bank or financial institution, or it may be owned by an independent service provider. Bank-owned processors normally support only bank-owned machines, whereas the independent processors support merchant-owned machines.

Parts of the Machine
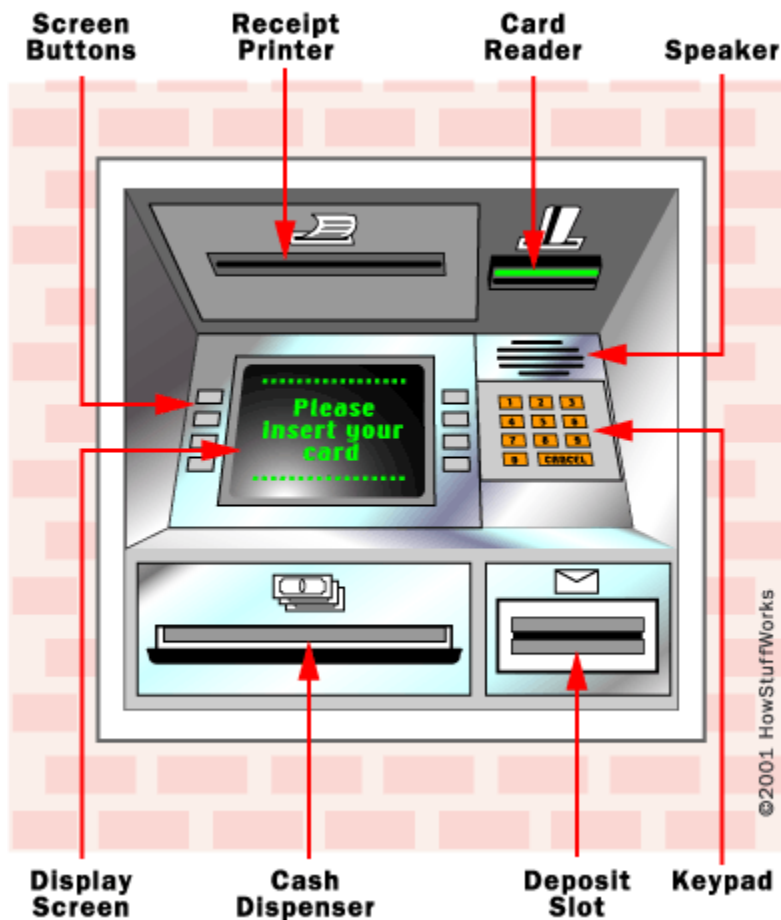
You're probably one of the millions who has used an ATM. As you know, an ATM has two input devices:

- **Card reader** - The card reader captures the account information stored on the magnetic stripe on the back of an ATM/debit or credit card. The host processor uses this information to route the transaction to the cardholder's bank.
- **Keypad** - The **keypad** lets the cardholder tell the bank what kind of transaction is required (cash withdrawal, balance inquiry, etc.) and for what amount. Also, the bank requires the cardholder's personal identification number (**PIN**) for verification. Federal law requires that the PIN block be sent to the host processor in encrypted form.

And an ATM has four output devices:

- **Speaker** - The speaker provides the cardholder with auditory feedback when a key is pressed.

- **Display screen** - The display screen prompts the cardholder through each step of the transaction process. Leased-line machines commonly use a monochrome or color CRT (cathode ray tube) display. Dial-up machines commonly use a monochrome or color LCD.
- **Receipt printer** - The receipt printer provides the cardholder with a paper receipt of the transaction.
- **Cash dispenser** - The heart of an ATM is the safe and cash-dispensing mechanism. The entire bottom portion of most small ATMs is a safe that contains the cash.

Sensing Bills

The cash-dispensing mechanism has an **electric eye** that counts each bill as it exits the dispenser. The bill count and all of the information pertaining to a particular transaction is recorded in a **journal**. The journal information is printed out periodically and a hard copy is maintained by the machine owner for two years. Whenever a cardholder has a dispute about a transaction, he or she can ask for a journal printout showing the transaction, and then contact the host processor. If no one is available to provide the journal printout, the cardholder needs to notify the bank or institution that issued the card and fill out a form that will be faxed to the host processor. It is the host processor's responsibility to resolve the dispute.

Besides the electric eye that counts each bill, the cash-dispensing mechanism also has a **sensor** that evaluates the **thickness** of each bill. If two bills are stuck together, then instead of being dispensed to the cardholder they are diverted to a **reject bin**. The same thing happens with a bill that is excessively worn, torn, or folded.

The number of **reject bills** is also recorded so that the machine owner can be aware of the quality of bills that are being loaded into the machine. A high reject rate would indicate a problem with the bills or with the dispenser mechanism.

Settlement Funds

©2001 HowStuffWorks
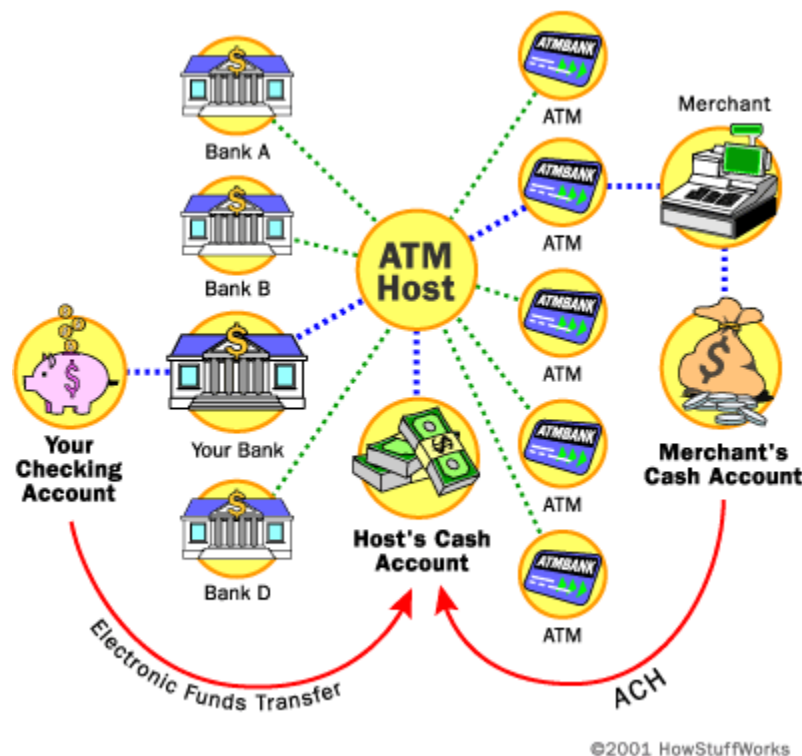
When a cardholder wants to do an ATM transaction, he or she provides the necessary information by means of the card reader and keypad. The ATM forwards this information to the host processor, which routes the transaction request to the cardholder's bank or the institution that issued the card. If the cardholder is requesting cash, the host processor causes an **electronic funds transfer** to take place from the customer's bank account to the host processor's account. Once the funds are transferred to the host processor's bank account, the processor sends an **approval code** to the ATM authorising the machine to dispense the cash. The processor then ACHs the cardholder's funds into the merchant's bank account, usually the next bank business day. In this way, the merchant is **reimbursed** for all funds dispensed by the ATM.

So when you request cash, the money moves electronically from your account to the host's account to the merchant's account.

ATM Security

It's important to use a well-lit, public ATM machine at night.

ATMs keep your personal identification number (**PIN**) and other information safe by using encryption software such as Triple DES (Data Encryption Standard). But there are lots of things that you can do to protect your information and your money at an ATM.

Many banks recommend that you select your own **PIN**. Visa offers the following PIN tips:

- Don't write down your PIN. If you must write it down, do not store it in your wallet or purse.
- Make your PIN a series of letters or numbers that you can easily remember, but that cannot easily be associated with you personally.
- Avoid using birth dates, initials, house numbers or your phone number.

Visa also recommends the following tips for safe ATM usage:

- Store your ATM card in your purse or wallet, in an area where it won't get scratched or bent.
- Get your card out BEFORE you approach the ATM. You'll be more vulnerable to attack if you're standing in front of the ATM, fumbling through your wallet for your card.

- Stand directly in front of the ATM keypad when typing in your PIN. This prevents anyone waiting to use the machine from seeing your personal information.
- After your transaction, take your receipt, card and money away. Do not stand in front of the machine and count your money.
- If you are using a drive-up ATM, get your vehicle as close to the machine as possible to prevent anyone from coming up to your window. Also make sure that your doors are locked before you drive up to the machine.
- Do not leave your car running while using a walk-up ATM. Take your keys with you and lock the doors before your transaction.
- If someone or something makes you uncomfortable, cancel your transaction and leave the machine immediately. Follow up with your bank to make sure the transaction was cancelled and alert the bank to any suspicious people.

Many retail merchants close their store at night. It is strongly recommended that they pull the money out of the machine when they close, just like they do with their cash registers, and leave the door to the security compartment wide open like they do with an empty cash-register drawer. This makes it obvious to any would-be thief that this is not payday.

For safety reasons, ATM users should seek out a machine that is located in a well-lighted public place. Federal law requires that only the last four digits of the cardholder's account number be printed on the transaction receipt so that when a receipt is left at the machine location, the **account number** is secure. However, the entry of your four-digit **personal identification number** (PIN) on the keypad should still be obscured from observation, which can be done by positioning your hand and body in such a way that the PIN entry cannot be recorded by store cameras or store employees. The cardholder's PIN is not recorded in the journal, but the account number is. If you protect your PIN, you protect your account.