



ATM/DEBIT CARD SECURITY

Tips to Electronic Banking Safety

REMINDER: First State Bank will not send a text asking you to verify a purchase or your credentials.

Always use good judgment and be conscious of your surroundings when using an ATM. These tips are helpful suggestions, but the best advice is simply to not use an ATM if you feel uncomfortable. We want our ATM and night deposit facility to be safe and convenient for you.

The following tips are meant to make you aware that although rare, an ATM crime or debit card fraud can happen. Preventing such a crime must be a cooperative effort between you and your bank. Here are some reminders:

1. Have your card ready and in your hand as you approach the ATM to reduce the time spent at the ATM.
2. To keep your account information confidential, always take your receipts or transaction records with you.
3. Don't leave your card lying around. No one should have access to the card but you.
4. Never give any information about your ATM Card, Debit Card, or PIN over the phone. If you receive a call (for example from someone claiming to be your bank or the police) wanting to verify your PIN, do not give out any information. Only provide information about your card over the telephone or Internet if you initiated the transaction with a merchant you trust.
5. When making a purchase on the Internet with your card, protect against Internet fraud by logging out of the website instead of just closing the web browser when you are finished with the transaction.
6. Make sure that no one can see you enter your PIN information. Use your body to 'shield' the keypad as you enter your PIN.
7. Report a lost or stolen card immediately to your bank, this will reduce the chance that it will be used for the wrong purposes. Prompt notice to the bank will limit your liability for unauthorized transactions. Use the FSB Mobile App to turn off your card if lost or stolen until it is found.
8. Inspect an unmanned ATM machine before use for possible tampering, or the presence of an unauthorized attachment that could capture information from the access device or your personal identification number.
9. Never allow a cashier or another person enter your PIN for you, even if they are helping you with the transaction.
10. Do not count or visually display any money you received from the ATM. Immediately put your money into your pocket or purse and count it later.
11. Promptly review your monthly statement and compare your ATM receipt against your statement.
12. If you are using a drive-up ATM, be sure the passenger windows are rolled up and all doors are locked. If you leave your car and walk to the ATM, lock your car. Before rolling down your car window to use the ATM be sure to observe the entire area.
13. Be aware of your surroundings. Look out for suspicious activity near the ATM or night deposit facility. If you observe any problem, go to another ATM or night deposit facility. At night, be sure that the facility is well lighted. Please report any problems with the ATM/Night Drop facility to us and suspicious activity or crimes to both the bank and the local law enforcement officials immediately.

SIGNATURE BASED VS PIN TRANSACTIONS

- Signature based transactions provide a means of making purchases without the hassle of having to remember a PIN number. When making a signature based purchase always select CREDIT. Signature based transactions have 0% liability for unauthorized use of a consumer debit card.
- When making a PIN based purchase always select DEBIT and enter your PIN number. PIN based purchases carry a greater consumer liability in the event of unauthorized transactions. PIN based transactions at POS and ATMs have 0% liability for unauthorized use of a consumer debit card.

Refer to our Electronic Fund Transfers section in the consumer new account disclosures for all terms and conditions.