WSB Winchester Savings Bank
STRENGTH. SERVICE. COMMUNITY.

ATM & Point of Sale (POS) PIN Fraud

ATM/POS PIN (Personal Identification Number) Fraud is when debit and credit card data is stolen from ATMs and POS transactions when a PIN is used. This can happen at an ATM owned by a bank, at a retail store, restaurant or gas station.

How does this happen?

Criminals install devices that capture information from the card's magnetic stripe. The method, called skimming, sometimes also involves a tiny camera that records the cardholder entering a personal identification number. The information is used to manufacture counterfeit debit cards that can be used to withdraw cash at an ATM or make a purchase in a store or online. Thieves can drain a bank account when they have access to cardholder information.

Social engineering scams include sending emails that look like they are from a known sender and request you to click on a link that directs you to a site to verify or input your personal data or that asks you open an attachment. They also include phone calls claiming to be from someone you trust who needs your information right away.

What does the Bank do to help?

The Bank

- sets limits on the amount of money that can be withdrawn each day to help prevent large cash withdrawals from a customer's account.
- monitors ATM/Debit card activity for unusual or suspicious transactions.
- inspects its ATM's to look for any skimming devices or cameras that are not part of the Bank's equipment.
- will never call, text or email you and ask you to provide us with your personal or account information. (In some cases, our Fraud department will call or email you to verify suspicious transaction activity.)
- offers CardValet® for setting up alert notifications and card usage restrictions.

What can YOU do?

- Sign up for banking alerts through Online Banking and the Mobile Banking app. These will inform you when particular changes occur, such as irregular card activity. CardValet® is a smartphone app that lets you turn your debit card on and off in real time.
- Stay away from ATMs that appear dirty or in disrepair. At best, such ATMs may not work when used, and at worst, they may be fake machines set up to capture card information.
- Do not use ATMs with unusual signage, such as a command to enter your PIN twice to complete a transaction.
- Watch out for ATMs that appear to have been altered. If anything on the front of the machine looks crooked, loose or damaged, it could be a sign that someone attached a skimming device.
- Avoid using the ATM if suspicious individuals are standing nearby. Criminals may try to distract you as you use the machine to steal your cash, or watch as you type your PIN.
- Be aware that if your card gets stuck in the machine and someone approaches to help, it may be a scam. A criminal may be trying to watch as you enter your PIN code. Contact us promptly to report the incident.
- As you key in your PIN, cover the keypad with your other hand to block anyone, or a camera, from viewing the numbers you type.
- Do not open any attachments or click on a link in an email that appears suspicious, out of the ordinary or that you were not expecting. Contact the sender using a phone number or other method that is reliable, such as the number on your bank, credit card or account statement. Never use the contact information in the email.

Remember to check your balance on a regular basis and immediately report any discrepancies to your bank.