Sign Immediately.
As soon as your card arrives in the mail, sign the back and keep in a safe place.

Memorize Your Pin.
Do not write your personal identification number (PIN) down and carry it with you.

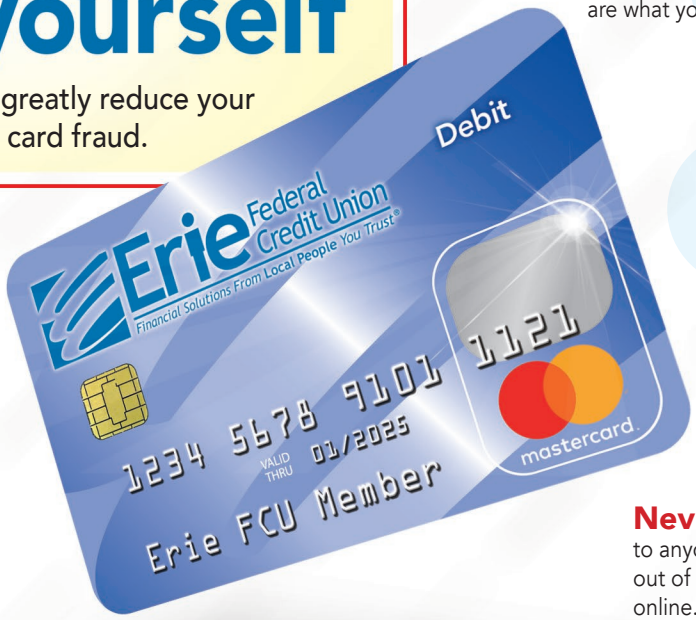
Protect your cards
as if they were cash.

Take your receipt & save it.
Always check sales receipts for the correct purchase amount before you sign them.

Smart ways to protect yourself

Adopt these simple habits to greatly reduce your odds of falling victim to debit card fraud.

Review your account statements
to assure the amounts charged are what you authorized.



Sign up for text or email alerts to help catch debit card fraud attempts early.

Report lost or stolen card immediately.
(814) 825-2436 or **1(800) 480-0494.**
After business hours: **1(800) 523-4175**

Do not volunteer any personal information
when you use your card other than by displaying a personal ID as requested by a merchant (i.e. driver's license).

Never lend your card
to anyone or let your debit card out of your sight and be careful online. Shop and bank on secure websites with private Wi-Fi only.

Don't ignore data breach notifications If you get one of these messages, change your PIN and ask the credit union to change your debit card number. You can also ask one of the major credit bureaus to place a fraud alert on your file.

Inspect card readers & ATMs. Don't use card slots that look dirty or show evidence of tampering, such as scratches, glue or debris. And steer clear of machines with strange instructions, such as "Enter PIN twice."

Cover your card.
When using your debit card or typing your PIN at an ATM, block the view with your other hand. Go to a different location entirely if suspicious people are hanging around the ATM, and if your card gets stuck, notify the financial institution directly rather than accepting "help" from strangers.

Beware of these Classic Scams

Hacking: When you bank or shop on public Wi-Fi networks, hackers can use keylogging software to capture everything you type, including your name, debit card number and PIN.

Phishing: Be wary of messages soliciting your account information. Emails or text messages can look like they're from legitimate sources but can actually be from scammers. If you click on an embedded link and enter your personal information, that data can go straight to criminals.

Skimming: Capturing card information or "skimming" is on the rise at ATM and gas stations. Never use an ATM or card swipe that looks like it has been tampered with as indicated by loose or extra parts attached to the face of the machine, adhesive tape or glue residue. Look for anything that may have a tiny hole or slot for a camera that is aimed at the keypad. If your card is captured inside an ATM or other device, call Erie Federal Credit Union immediately to report the incident. Most skimming devices are installed for short periods of time-usually just a few hours.

Spying: Plain old spying is still going strong. Criminals can plant cameras near ATMs or simply look over your shoulder as you take out your card and enter your PIN. They can also pretend to be good Samaritans, offering to help you remove a stuck card from an ATM slot.

Even if you've taken precautions, debit card fraud can still happen. If your card gets hacked, don't panic. Contact your credit union right away, so you won't be held responsible for unauthorized charges, and file a complaint with the Federal Trade Commission.

(814) 825-2436 • www.eriefcu.org

Erie Federal Credit Union®