

As we approach the end of the year, we want to share some helpful tips to protect yourself and your finances from potential fraud and scams. This includes important information on **safeguarding your debit card, preventing identity theft, and staying safe when conducting transactions at ATMs/ITMs.**

## Protect Yourself from Fraud

Fraud is intentional deception for personal or financial gain. At Velocity, we're committed to protecting you. Here's how you can stay safe:

Action	Why?
Guard your online information	Keep your security software updated. Look for HTTPS in website URLs before logging in or sharing data, especially for banking and shopping.
Monitor your accounts	Check your financial accounts daily via online or mobile banking. Set up alerts for transactions and account changes.
Shred sensitive data	Keep ATM/ITM receipts, deposit slips, and mobile check deposits until reconciled, then shred. Store monthly statements securely until tax filing, then shred unless needed. Consider eStatements.
Check your credit report	Regularly review credit reports for unauthorized activity through providers like Experian or Equifax. Set up alerts for changes to your business credit score.
Think before sharing information	Be cautious of unsolicited calls or emails requesting sensitive details. Scammers use phishing tactics to impersonate trusted sources via email, text, or phone.
Report suspicious activity	If you suspect fraud, contact your financial institution immediately to improve the chances of recovering funds.
Use fraud detection tools	We offer tools to identify fraud early, such as monitoring payments and flagging suspicious transactions for review.
Business Email Compromise	Be wary of emails with financial changes, attachments, links, or unusual requests. Always confirm changes by phone with a trusted contact.

## Recognizing a Scam

A scam is a deceptive scheme to steal money or personal information. Velocity works to protect you, but we need your help. Always report any scam involving your money. Here's how to identify and protect yourself from scams:

What a Scammer Will Do ...	How They Do It ...
Scammers impersonate trusted organizations	They may pose as officials from the IRS, Social Security, or familiar companies like banks or credit unions, using fake names or pretending to represent someone you know.
Scammers create a problem or offer a prize	They fabricate urgent issues or promise prizes to trick you into sharing personal information or making payments.
Scammers pressure you to act quickly	They create a sense of urgency, claiming immediate action is needed to avoid consequences or secure rewards.
Scammers dictate payment methods	They insist on specific payment methods, claiming they're necessary for urgency or security, to manipulate victims into transferring money or sharing financial details.

## How to Protect Yourself from Scams

- Block unwanted calls and texts.
- Never share personal or financial information in response to unexpected requests.
- Don't rush; resist pressure to act immediately.
- Be aware of how scammers ask for payment.
- Take a moment to consult with someone you trust.

## Protecting You and Your Money

### Protecting Your Debit Card at a Velocity ATM/ITM

ATM/ITM security is a top priority at Velocity.

- Be aware of your surroundings. If the ATM/ITM is poorly lit or obstructed, choose another one.
- Shield your PIN and transaction amount from others.
- Immediately put away your card, cash, and receipt. Count your money later.
- If something feels off, cancel your transaction and leave. If followed, go to a busy, well-lit area and call the police.
- Be cautious of "skimming" devices. If the card reader seems altered, report it.
- Don't let strangers follow you into enclosed ATMs/ITMs.
- For drive-up ATMs/ITMs, lock all doors and raise windows.
- Never leave your car unlocked or running while using the ATM/ITM.

### Protecting Your Debit Card and PIN

- Treat your card like cash—always protect it.
- Report a stolen card immediately.
- Avoid exposure to magnetic objects.
- Never share your card number, PIN, or personal info.
- Choose a hard-to-guess PIN and memorize it.
- Never write down your PIN.

### Receipts & Transactions

- Don't leave receipts behind.
- Verify transactions by matching receipts with statements.
- Shred receipts and personal info before disposal.

### Online Security Tips

- Use wired internet or secured WiFi for transactions.
- Look for "https" or a closed padlock icon when shopping online.
- Always type URLs directly into your browser.

### Beware of Scams

- Velocity will NEVER ask for your username, password, card number, PIN, or account details via phone, text, or email.
- If you call us, we may ask for identity verification.

Any concerns regarding suspicious activity or suspicious attachments should be immediately reported to law enforcement and/or Velocity.

### Report lost or stolen cards immediately:

- Review transaction history for any unauthorized items.
- Call 512.469.7000 to inform Velocity.
- Call us or visit a Velocity Credit Union branch for card replacement.

All Velocity Credit Union ATMs meet Texas Administrative Code standards.