How to protect yourself from six common scams:

Corporate Breaches

- Encrypt your physical card: Use chip-based cards, contactless payments, or mobile wallets
- Encrypt transactions online: “Https” over “Http”
- Use credit cards over debit cards

Phishing

- Be wary of urgent communication
- Always call customer service first
- Use two-factor authentication, whenever possible
- Keep your software updated
- Always have your information backed up

Typosquatting

- Avoid “fat-fingering”
- Bookmark your favorites
- Use search engines first
- Keep an eye out for grammatical errors

Telephone Scam

- Never give out information to a cold caller
- Don’t respond immediately
- Wait for a voicemail
- Call the organization

Skimming

- Always inspect card readers
- Use credit cards over debit cards
- Monitor your accounts

Physical Theft

- Keep personal items safe and out of sight
- Destroy unnecessary material that has personal information
- Keep track of incoming material, such as mail

Protecting Your Credit Cards

The Simple Dollar

What to look for if you suspect your identity has been stolen:

- [ ] Unexplained or incorrect expenses
- [ ] A sudden fluctuation on your credit report
- [ ] Missing mail or email
- [ ] Unexpected calls from debt collectors
- [ ] Two-factor authentication alerts
- [ ] Small but consistent “test charges”
- [ ] Letters from the IRS
- [ ] Sudden denial of your credit or debit card

How to recover from identity theft:

Fraud Alert

- Used for stolen financial information
- Requires creditors to verify before opening new accounts

3 different types of fraud alerts:

- Initial Fraud Alert - Lasts 90 days
- Extended Fraud Alert - Lasts 7 years
- Active Duty Alert - For military members only, lasts 1 year

Security Freeze

- Used if personal information is at risk
- Prevents new accounts from being opened in your name
- You must contact each credit reporting company to initiate a security freeze
- You must contact each credit reporting company to lift a security freeze