identity theft
& what to do

Identity theft affects millions of people every year. These strategies will help lessen the severity of identity theft if it happens to you.

- Photocopy the contents of your wallet and keep them in a secure location.
- Shred papers with personal information with a micro cut shredder.
- Only enter your personal information online from a trusted site with "https" in the address bar - the "s" means secure.
- If you use a public wireless network, do not send information to a website if it is not fully encrypted.
- Use anti-virus, malware protection, and a firewall on your computer.
- Keep all passwords secure and not written down.
- Check your bills and statements for fraudulent activity as soon as they come in the mail.
- If your wallet was stolen, immediately file a police report in that jurisdiction.
- Call Experian, Equifax, and Trans Union to place a fraud alert on your name and Social Security Number.
- Read your credit reports. You have a right to a free credit report every 12 months from each of the three credit reporting agencies.
- If your identity is stolen, file a complaint with FTC at ftc.gov/complaint or call 1.877.438.4338. Then take your FTC affidavit to your local police to file a report.

helpful
contact info

Equifax 1.800.525.6285
Experian 1.888.397.3742
TransUnion 1.800.680.7289

Federal Trade Commission
1.877.438.4338 | FTC.gov | OnGuardOnline.gov

National Do Not Call Registry
888.382.1222 | DoNotCall.gov

Better Business Bureau
1.703.276.0100 | bbb.org

FBI Online Internet Crime Complaints
ic3.gov

Annual credit report
877.322.8228 | AnnualCreditReport.com

Michigan Attorney General
877.765.8388 | Mi.gov/agcomplaints

Amer1can
CREDIT UNION

Boldly Generous. Convenient. Uncomplicated.

american1cu.org | 718 E. Michigan Ave. Jackson, MI 49201 | 888.213.2848

NCUA

Rev. 1/2020

Identity Theft
& Scams

Amer1can
CREDIT UNION

types of **scams**

Lottery and Sweepstakes Scams Emails or letters stating you won a sum of money and instruct you to keep the notices secret and send money for fees. Criminals make money by convincing victims to pay for processing taxes, or delivery, or provide bank account information to verify their identity.

Romance or Sweetheart Scams A new love interest, usually met online, asks for money for many reasons and can never meet in person. Do not give out your online banking credentials to someone you meet online, but have never met in person.

Technology Expert Scams Scammers call and claim to be computer techs employed by well-known companies such as Microsoft or Apple. The caller will state they have detected a virus or malware on your computer. They will diagnose a nonexistent problem and ask you to pay for unnecessary or harmful services.

IRS Scams Scammers will call claiming your taxes need to be paid or you will get arrested. The IRS will not call you and demand immediate payment. They will send you a bill and will never request payment in gift cards.

Grandparent Scams Scammer poses as your grandchild stating they need money to post bail or pay for another emergency event.

Phishing Phishing scams are when you receive an email from a familiar entity such as your credit union, credit card company, or government agency asking you to confirm your account credentials. A legitimate company would never send emails asking for account information because they already have it. Delete the email and do not hit reply.

Card Skimmers Card skimmers are devices that can be attached to a gas pump or ATM in order to steal card information. Look for a security seal at the gas pump or ATM - these are used as a way to prevent tampering. If you notice unauthorized charges on your card, report it to your financial institution.

tips to **protect yourself**

Use these helpful tips to not only protect yourself, but to protect your loved ones and friends as well.

- Do not send money to someone you don't know or have not met personally.
- Do not respond to online solicitations for "easy money."
- Give only to well-known and credible charities. You can go to www.usa.gov/donate-to-charity or www.michigan.gov/agcharities to verify.
- Do not agree to deposit a check and wire money for anyone.
- Do not reply to messages or emails asking for personal or financial information.
- Use caution answering the phone from an unfamiliar number. Let it go to voicemail and call back if needed.
- Phone numbers can be faked. Even if your caller ID shows that a caller is using a number in your area, they could actually be from another state.
- Do not open emails from senders that you do not recognize or click on unknown links in them.
- Use strong passwords with at least eight characters, including letters, numbers, and symbols.
- Do not trust "free" credit report information.
- Never allow strangers to come into your home and take information about you or your assets.
- Never sign contracts that have blank lines in them. Someone can add clauses later that harm you.
- No legitimate company will ask to be paid in gift cards, Apple or Google Play cards.
- You should never have to send money back to someone that sent you a check for lottery winnings, a new job, or the sale of an item. Sending cash back always equals fraud.
- Do not file a false claim with your credit union. By filing a false claim you are a co-conspirator to fraud.
- Treat your mail carefully. Place outgoing mail in a secure collection box and remove mail from your mailbox promptly.
- Only carry what you need in your wallet. Do not carry your social security card - keep it at home in a secure location.
- Only give your social security number to trusted entities such as your financial institution, your employer, government agencies, law enforcement, and insurance companies.
- Protect your PIN number.
  - Memorize your PIN.
  - Do not write it on your card.
  - Never let someone enter your PIN for you.
  - Do not give your PIN to anyone over the phone or internet.