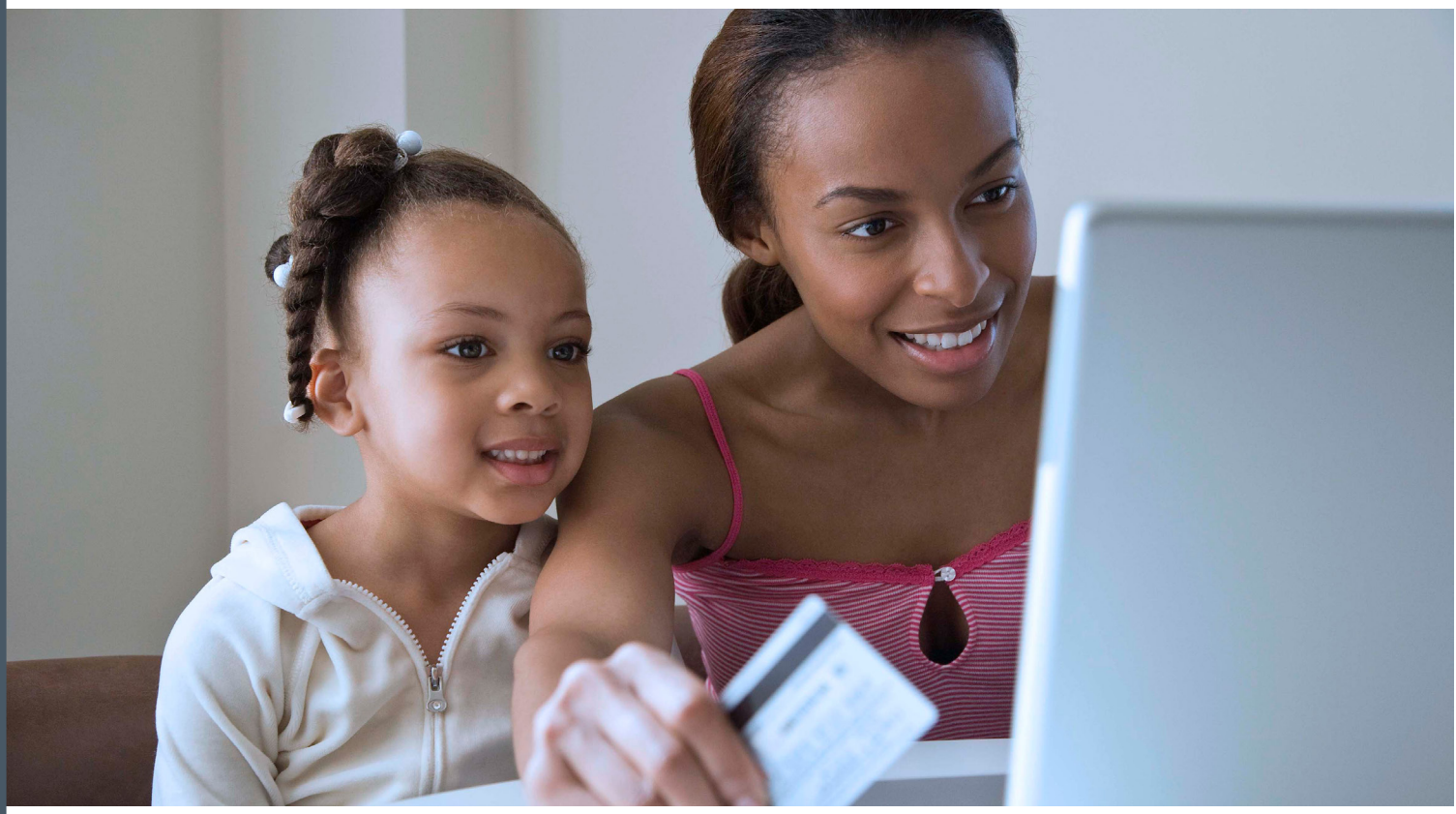
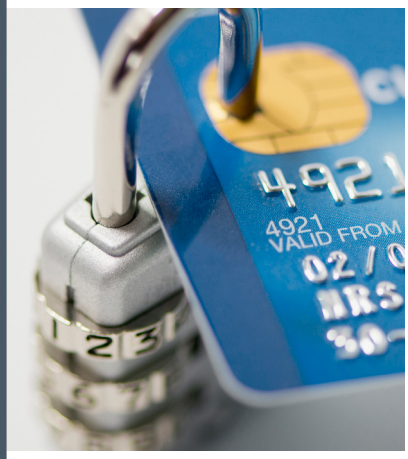
THE BASICS of IDENTITY THEFT



The MHV Guide to Protecting Yourself From Identity Theft



MHV
MID-HUDSON VALLEY FEDERAL CREDIT UNION

THE BASICS of IDENTITY THEFT

What is Identity Theft? Your wallet is missing. Thousands of dollars have been charged to your credit cards, your checking account is empty, and loans you never took out appear on your credit report. What happened? You've become a victim of identity theft – an increasingly common and inventive crime.

Identity theft occurs when someone uses your personal information to commit fraud or other crimes. It may also involve computer fraud, mail fraud, wire fraud, and bank fraud.

Fortunately, there are preventative measures you can take to substantially reduce the chance of identity theft occurring, as well as steps to recover from any damage if you are a victim.

ARE YOU AT RISK for IDENTITY THEFT?

Answer TRUE or FALSE to find out:

1. I shred all pre-approved credit offers, account statements, and financial documents before disposing of them. TRUE ☐ FALSE ☐
2. I never carry my Social Security card. TRUE ☐ FALSE ☐
3. My Social Security and driver license numbers are not printed on my checks. TRUE ☐ FALSE ☐
4. I view each of my credit reports annually. TRUE ☐ FALSE ☐
5. I only carry those credit cards that I use. TRUE ☐ FALSE ☐
6. I carefully review my monthly credit card statements before paying them. TRUE ☐ FALSE ☐
7. When shopping on the internet, I buy only from secure websites. TRUE ☐ FALSE ☐
8. I'm aware of all my creditor due dates, and know immediately if a bill is missing. TRUE ☐ FALSE ☐
9. I know the security procedures at my place of work. TRUE ☐ FALSE ☐
10. I never reveal personal information unless I initiated the contact and know exactly who I'm dealing with. TRUE ☐ FALSE ☐
11. I have up-to-date virus protection software installed on my computer. TRUE ☐ FALSE ☐
12. I never store personal and financial information on my device. TRUE ☐ FALSE ☐
13. I know exactly what to do and who to contact in case my wallet is stolen. TRUE ☐ FALSE ☐
14. I have complete copies of all my credit cards stored in a safe place. TRUE ☐ FALSE ☐
15. All of my account passwords are too complicated for anyone to guess. TRUE ☐ FALSE ☐

If you answered FALSE to any of the above questions you may be at risk. This guide will give you steps you can take to help protect you and your financial future.

PREVENTING IDENTITY THEFT

1 Review Your Credit Report

• Check your credit report, at least annually, from each of the three major credit bureaus for fraudulent activity. If you find inaccuracies on your report, dispute them immediately and contact the involved creditors or other parties.

• Register for a credit monitoring service to be notified of key changes to your credit report. If the change is not something you initiated, such as buying a new car, opening a new credit card or changing your address, you can respond immediately and address the potential fraud.

2 Safeguard Your Personal Information

- Keep all identification and financial documents in a safe and private place.
- Provide personal information only when you know how it will be used, you are certain it won't be shared, and you've initiated contact and know who you're dealing with.
- Make all passwords hard to guess by using a complex combination of numbers, upper and lower case letters, and special characters.
- Request a vacation hold if you can't pick up your mail and deposit outgoing mail in post office collection boxes or at your local post office.
- Be aware of your workplace's security procedures and keep your purse or wallet in a safe place.
- Do not carry your Social Security card or have it or your driver license number printed on your checks. Share this information only when necessary and with those you trust.

3 Monitor Your Cards & Accounts

- Carry only those cards you really need and cancel unused credit card accounts.
- Shred pre-approved credit card offers or opt out of receiving them.
- Photocopy both sides of your credit cards so you have all the account numbers, expiration dates, phone numbers, and keep the copies in a safe place.
- Be aware of people behind you at the ATM or anywhere else you use your card.
- When you give your credit or debit card to someone for a transaction, watch them swipe it and inspect the receipt for accuracy.
- Know your billing cycles and contact the creditor if bills don't arrive on time. Carefully review all statements and shred when no longer needed.
- Know where your checkbook is at all times and be sure to use permanent ink when writing a check.
- Do not give out your credit card or account numbers unless you know the company requesting it and how it will be used.

4 Protect Your Computer, Tablet & Phone

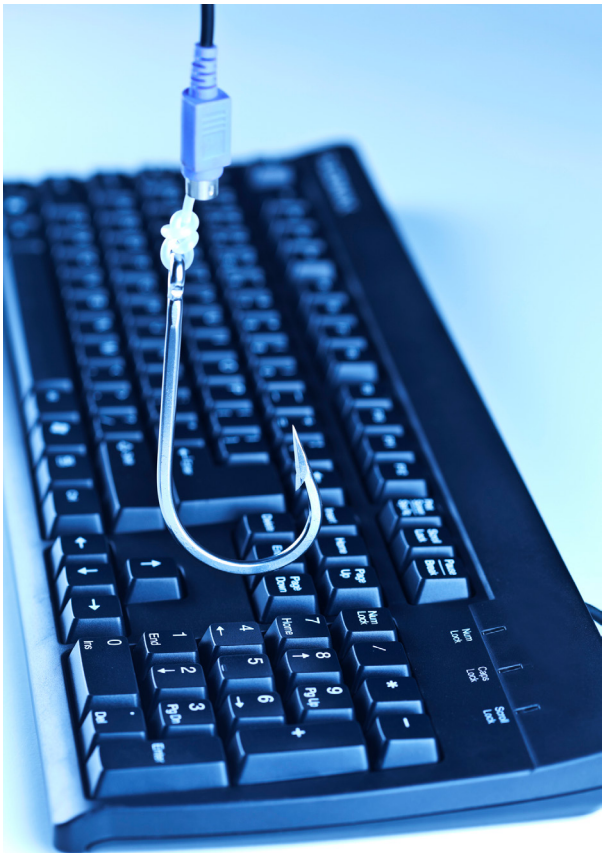
- Update virus protection software periodically, and after every new virus alert is announced.
- Do not download files or open hyperlinks sent from people you don't know.
- Use a firewall program to prevent your computer from being accessible to hackers.
- Use a secure browser to guard the security of your online transactions.
- Enter personal and financial information only when there is a "lock" icon on the browser's status bar and look for the URL to read "https" versus "http".
- Don't use an automatic login feature and always log off when you're finished.
- Before disposing of a computer, delete personal information using a "wipe" utility program to overwrite the entire hard drive.

HOW *is* YOUR INFORMATION OBTAINED?

Thieves use a variety of illegal techniques to obtain identity information.

THEY MAY:

- Take mail from a mailbox
- Divert mail to another location by filling out a change of address form
- Go through trash to find identification and financial documents
- Access credit reports by posing as landlords or employers
- Hack into personal computers
- Steal hard copy or electric files from your workplace
- Pose as legitimate companies or government agencies to request personal information via email (called phishing) or text message (called smishing)
- Stand close to you at the ATM to obtain your PIN
- Use social media to mine personal data
- Use a skimming device at a restaurant, gas station, or other business to steal money or information from credit/ATM/ debit cards



HOW DO THEY USE YOUR INFORMATION?

Once identity thieves have your personal information, they may use it to:

- Charge on existing credit accounts or open new credit accounts in your name
- Use existing or open new checking accounts in your name and write bad checks
- Establish phone or wireless service in your name
- Use your debit cards or counterfeit checks to drain your checking account
- Take out loans to buy cars and other big ticket items

What if IDENTITY THEFT HAPPENS?

If you are a victim of identity theft, understand that minimizing damage will take patience and a systematic approach. However, the sooner and more aggressively you deal with the problem, the faster you will see results.

Creditors and Financial Institutions

If accounts have been used or opened illegally, contact your creditors immediately. For any compromised account, get a new account number and card. You may need to provide the creditor with a police report. Monitor all future account statements carefully for evidence of new fraud. If a collection agency attempts to collect on a fraudulent account, explain (in writing) that you are a victim of identity theft and not responsible for the debt. Ask that they confirm in writing that you do not owe the balance and that the account has been closed. For checking account fraud, contact your financial institution to place stop payments on any outstanding checks that you did not write. Close current checking and savings accounts and obtain new account numbers and passwords. Monitor all future account statements carefully for evidence of new fraud.

Local and Government Agencies

Report the crime and file a police report. Request a copy of the report and keep the phone number of your investigator handy. Notify the U.S. Postal Inspection Service if someone has used your address or in other ways committed fraud through the mail.

Credit Reporting Bureaus

It is very important that your credit report lists only factual information. To know what is being reported, you will need to obtain a credit report from each of the three major credit bureaus. If you are married, your spouse should also check his or her report. Even if the fraudulent information hasn't yet appeared on your reports, be proactive and report the crime now. Call any one of the three credit bureaus to place a fraud alert on your credit report and they will contact the other two to have alerts placed on their reports as well. If you have proof that identity theft has occurred and you have filed a police report, you may request that the fraud alert be placed for seven years instead of the initial time frame of 90 – 180 days. While fraud alerts are in effect, no new credit should be granted without your explicit approval.

RESOURCES

HELPFUL WEBSITES

EQUIFAX:
www.equifax.com

EXPERIAN:
www.experian.com

TRANSUNION:
www.transunion.com

ANNUAL CREDIT REPORT REQUEST SERVICE:
www.annualcreditreport.com

U.S. FEDERAL TRADE COMMISSION:
www.ftc.gov

U.S. POSTAL INSPECTION SERVICE:
www.postalinspectors.uspis.gov

At MHV, we are committed to guiding you to discover your financial possibilities, wherever that may be. Need more advice on protecting your identity? Contact us for more information about our MHV Perks Package with IDProtect™.

MID-HUDSON VALLEY FEDERAL CREDIT UNION

Federally Insured by NCUA