HORIZON
CREDIT UNION

Identity Theft

PARTICIPANT'S GUIDE

Table of Contents

My Identity

What information do you think could be at risk for identity theft? Fill in the boxes below.

Biographical Data	Medical Data

Biometric Data	Financial Data

Common Identity Theft Scams

Phishing Email Scams Activity

Circle or otherwise note anything you find suspicious.

From: YahooMail
Subject: Change your password

Dear Customer,

We notice that you sign in from a different computer. Please log in using this link to verify your password: www.yahooo.com
If you do not verify this information within 24h your account will be permanently deleted.

Best,
Yahoo Team

Phone Scams Activity

Circle or otherwise note anything you find suspicious in this phone call.

"Hi, I'm friends with your nephew. He's in trouble with the law and needs your help. He got arrested last night and is now in jail. He needs bail money before he can be released. It's a long story but he asked me to call you instead of his parents because he is embarrassed about what happened to him. He needs you to wire money in the next hour from Western Union. It's important that you send this money right away."

Elder Fraud by Power of Attorney Activity

Circle or otherwise note anything you find suspicious in the actions described here.

Mrs. Garcia was 78 years old when she gave her niece, Angela, power of attorney. Recently, Mrs. Garcia has become quiet and sad. She does not leave the house for her daily walk anymore. Her neighbors noticed that Angela bought an expensive new car and claimed it was for her aunt. Angela is also making plans to remodel and expand the guest bedroom and plans to move in. Since it is her aunt's house, she intends to use her aunt's funds to pay for the expenses. When Angela is not around, Mrs. Garcia complains that some of her things are missing.

Red Flags of Identity Theft

Denials

- Denial of credit card application or services
- Denial of services (utility, rent, mortgage, etc.)

Unusual Activity

- Unusual charges on credit card or financial account
- Unusual changes in credit report and credit scores
- Unusual calls from debtors or collection agencies for debts you do not owe
- Unusual bills for services or products that you have not used
- Unusual increases in insurance or interest rates

IRS Reports

- IRS reports indicating that more than one person has filed a tax return using your Social Security number.
- IRS reports indicating wages received from unknown sources.

Medical

- Incorrect medical history information
- Incorrect medical bills

Lost Items

- Lost mail
- Lost bills

Protecting Against Identity Theft

How do you protect your information against identity theft?

Review the list of recommended steps. Put a check by steps that you take already, those you plan to start now, and those you plan to begin doing later.

	Already Do	Start Now	Start Later
Monitor your credit reports and scores*:* Access your credit reports for free at https://www.annualcreditreport.com. You are entitled to one free credit report a year from each of the three main credit bureaus.	☐	☐	☐
Monitor your financial statements: Review financial transactions carefully and correct any errors by contacting the bank or credit card company promptly.	☐	☐	☐
Practice online safety:			
Log in to your email and online banking accounts regularly, and change your passwords every few months.	☐	☐	☐
Use strong passwords that are difficult to guess. Use numbers, punctuation marks, and a combination of capital and lowercase letters.	☐	☐	☐
Do not click on links or download files from unknown senders, especially files that end in ".exe."	☐	☐	☐
Become familiar with the language that scammers use to target victims via email.	☐	☐	☐
Do not use public Wi-Fi to receive or send sensitive documents.	☐	☐	☐
Secure your documents:			
Keep sensitive information in a safe place.	☐	☐	☐
Do not carry your Social Security card with you.	☐	☐	☐
Shred sensitive documents once you no longer need them.	☐	☐	☐
Be aware of your surroundings:			
Cover the ATM keypad when entering your PIN.	☐	☐	☐
Keep an eye out for "shoulder surfers" who may be watching you key in your phone's passcode in public spaces.	☐	☐	☐

Monitoring Services

	Already Do	Start Now	Start Later
Use a credit monitoring service: Credit monitoring services keep a close watch on your Experian, TransUnion, and Equifax scores, reports, and activity. They can send you updates and alerts based on credit report requests by companies or if a bill is late.	☐	☐	☐
Use an identity monitoring service: Identity monitoring services can fill the gaps credit monitoring services may miss. Identity monitoring services can alert you that your personal information is being used to create accounts or to sign up for services or is showing up in records, such as court records.	☐	☐	☐
Use credit freezes: Credit freezes or security freezes protect your accounts by sealing off your credit report from any agency, organization, or individual who wants to access it until you authorize its release. It can take a few days for the freeze to be lifted if you decide to authorize the inquiry. Requesting a credit freeze or unfreeze to the credit reporting bureaus is free.	☐	☐	☐
Use fraud alerts: Fraud alerts are free and available from any of the three credit reporting bureaus, as long as you provide them with proof of identity. Temporary fraud alerts are free and last up to one year. If you are a victim of identity theft, they can last up to seven years. There are also special packages for those who are deployed in the military.	☐	☐	☐

Reporting Identity Theft

If you've become a victim of identity theft, there are a few steps you can take to regain control over your personal information.

Step 1: Collect Information

- Review your credit report and monitor any changes caused by the theft.
- Review the account where the theft occurred and note any changes.
- Review other and connected accounts.

Step 2: Report to Fraud Departments and Federal Agencies

- Report the theft to the fraud department at the organization or company where it occurred. Close all accounts and change all passwords, PINs, and access data to prevent the breach from reoccurring.
- Report the theft to the three nationwide credit reporting bureaus and request a fraud alert:
    - Experian.com/fraudalert: 1-888-397-3742
    - TransUnion.com/fraud: 1-800-680-7289
    - Equifax.com/CreditReportAssistance: 1-866-349-5191
- Create an Identity Theft Report by reporting the theft to the Federal Trade Commission:
    - Complete the online form at https://www.identitytheft.gov or call 1-877-438-4338. Include as many details as possible.
- Create a report with the local police.

Step 3: Repair

- Review the new accounts created by the thief and close them down.
- Review and correct statements and charges on your bills, credit reports, and other financial documents.
- Make a plan of action for monitoring your accounts, or get a paid monitoring service.

The Federal Trade Commission website, https://www.identitytheft.gov, offers free personalized recovery plans.