



Identity Theft Worksheet

Developed to assist victim recovery, enhance investigation/prosecution, and inform community.

Protect Your Current Accounts

Contact the fraud department of your banks, credit unions, credit card companies, cell phone company, telephone company, utility companies, and investment firms with whom you currently have accounts. Advise them that your identity was stolen and request that no changes be made to your account such as a change of address, password, PIN, or increase in credit limit. Ask if any charges, changes, or withdrawals have occurred since your last statement.

Put robust PINs or passwords on all of your current financial accounts. Robust passwords are a combination of letters, numbers, and symbols. Do not use the following types of information as passwords or PINs:

- Your mother's maiden name
- Your Social Security number
- Consecutive numbers or letters (example: 5678, vwxy)
- A family member's date of birth
- A family member's name
- Your nickname
- Your telephone number

Never share your account passwords or PINs with anyone. Do not carry passwords or PINs in your purse or wallet.

Cancel all credit cards you do not use. Ask that the accounts be "cancelled at customer request" to avoid the accounts being reported as "lost or stolen credit cards" on your credit bureau reports. Too many reported incidences of lost or stolen credit cards can have a negative impact on your credit score and hamper your ability to obtain credit in the future.

Company and Account Number	Date Contacted	Password/Pin
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Copyright Board of Trustees at Michigan State University. All rights reserved.