BALANCE℠
FINANCIAL FITNESS PROGRAM

Identity Theft Solutions

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 been 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 financial institution 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.

Identity Theft Risk Assessment

How secure is your personal information against identity theft? To find out, answer Yes or No to the following questions.

1.	I shred all pre-approved credit offers, account statements, and financial documents before disposing of them.	☐ Yes	☐ No
2.	I never carry my Social Security card.	☐ Yes	☐ No
3.	I have a locked, secured mailbox.	☐ Yes	☐ No
4.	My Social Security and driver license numbers are not printed on my checks.	☐ Yes	☐ No
5.	I review each of my credit reports annually.	☐ Yes	☐ No
6.	I only carry those credit cards that I use.	☐ Yes	☐ No
7.	I carefully review my monthly credit card statements before paying them.	☐ Yes	☐ No
8.	When shopping on the Internet, I buy only from secure websites.	☐ Yes	☐ No
9.	I am aware of all my creditor due dates, and know immediately if a bill is missing.	☐ Yes	☐ No
10.	I know the security procedures at my place of work.	☐ Yes	☐ No
11.	I never reveal personal information unless I initiated the contact and know exactly who I'm dealing with.	☐ Yes	☐ No
12.	I have up-to-date virus protection software installed on my computer.	☐ Yes	☐ No
13.	I never store personal and financial information on my laptop.	☐ Yes	☐ No
14.	I know exactly what to do and who to contact in case my wallet is stolen.	☐ Yes	☐ No
15.	I have complete copies of all my credit cards stored in a safe place.	☐ Yes	☐ No
16.	All of my account passwords are too complicated for anyone to guess.	☐ Yes	☐ No

(For maximum identity theft prevention, all of the answers should be Yes. Have a few (or more) No's? Review the Identity Theft Prevention section for safety measures.)

Common Practices

How Your Information is 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
- Pose as legitimate companies or government agencies to request personal information via email (called phishing) or text message (called smishing)
- Steal hard copy or electronic files from your workplace
- Stand close to you at the ATM to learn your Personal Identification Number
- Attach a skimmer to an ATM to capture your card number and PIN

How Your Information May Be Used
Once identity thieves have your personal information, they may use it to:

- Charge on existing credit accounts
- 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 or other big ticket items

Preventing Identity Theft

There are many ways to protect your private information from fraud. Though some tasks take a bit of effort, be aware that cleaning up the mess identity thieves leave behind is far more difficult and time-consuming.

Credit Reports
- Periodically check your credit report from each of the three major credit bureaus. You can obtain a copy of each report free once a year from the Annual Credit Report Request Service
- Dispute inaccurate information immediately

Personal Identity 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
  - You initiated contact and know who you're dealing with
- Make all passwords hard to guess by using a complex combination of numbers and upper and lower case letters
- Request a vacation hold if you can't pick up your mail
- Deposit outgoing mail in post office collection boxes or at your local post office
- Remove mail from your mailbox promptly
- Keep your purse or wallet in a safe place at work
- Be aware of your workplace's security procedures
- Memorize your Social Security number rather than carrying your Social Security card
- Do not have your Social Security or driver's license number printed on your checks
- Review your Social Security annual statement for accuracy
- Provide your Social Security number only when necessary and to those you absolutely trust

- Before revealing your Social Security number, ask:
    - Why your number is needed
    - How your number will be used
    - What happens if you refuse

Credit Card and ATM/Debit Cards

- Carry only those cards you really need
- Shred all statements and pre-approved credit card offers with a crosscut shredder
- Opt out of receiving pre-approved credit offers *(see Resources on page 23)*
- Photocopy both sides of your credit cards so you have all the account numbers, expiration dates and phone numbers, and keep the copies in a safe place
- Cancel unused credit card accounts
- Be aware of people behind you at the ATM, or anywhere else you swipe your card
- If 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 creditors if bills don't arrive on time
- Examine the charges on your credit card statements every month

Checking Accounts

- Know where your checkbook is at all times
- Print firmly and use indelible ink when writing checks
- Check your account statement for fraudulent activity
- Do not give out your checking account number unless you know the company requesting the information and understand why the information is necessary

Computer

- 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"
- If you must store personal and financial information on your laptop:
    - Use a strong password – one that is a hard-to-guess combination of upper and lower case letters and numbers
    - Don't use an automatic log-in feature
    - 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

Credit Monitoring & Protection

If you are especially concerned about the possibility of identity theft, you may consider paying for added protection or a monitoring service – but do so only after carefully reading the fine print and weighing the cost against the benefits. Some of these businesses are scams themselves. Research the company's history and check the Better Business Bureau's complaint log before signing an agreement.

- Each of the three major credit bureaus offers a fee-based credit monitoring service. They typically provide regular credit report updates about fraudulent activity, new inquiries, new accounts, late payments, and sudden changes in your credit card balances. These plans often include a specific number of credit reports being mailed to you automatically or at your request, and access to specialized customer service.
- Credit protection is offered by private companies and some financial institutions, and the price and service varies considerably. Most will reimburse victims of identity theft for out-of-pocket expenses (up to a certain dollar amount) and help you through the process of contacting creditors, writing affidavits, and filing reports.

Consumer Rights & Responsibilities

Since thieves prey on those who have not taken preventative measures, it is up to you to be careful with all of your identification and financial information. For maximum security, make safety a family affair. Limit and monitor children's access to the Internet and online transactions, have a designated person collect the mail, and establish guidelines for when telemarketers call and ask for information.

If you have children, you can – and should – safeguard their identity as well as your own. Some companies have mistakenly sent pre-approved offers for credit to those too young to actually have a credit card. Once your child has received one offer, he or she may very well receive others. Monitor the mail carefully and check your child's credit report. Unfortunately, even when you have done all the right things, you may still be a victim of identity theft. While consumer protection laws give you rights, it is your responsibility to take action if fraudulent activity occurs. If someone has used your identity or financial information, it is imperative that you act swiftly and treat the matter seriously. This means, in many cases, dedicating time to letter writing, telephone calls, credit report monitoring, follow-up, and log keeping. Turning from victim to victor takes effort. However, as frustrating as it may be to have to spend the time and energy fixing damage, no one but you can do it.

There are many federal laws that help in the fight against identity theft, both before and after the law is broken.

The Fair Credit Reporting Act
The Fair Credit Reporting Act (FCRA) ensures that the financial data contained in your credit report is not only correct, but private. Only those with a need recognized by the FCRA may access your credit report – usually a creditor, insurer, landlord or other business.

It is the credit reporting agency's responsibility to report only accurate information, so if you discover a false item, file a dispute. The credit reporting agency has 30 days to investigate your claim (45 days if you obtained your report from the Annual Credit Report Request Service).

Fair and Accurate Credit Transactions Act
The Fair and Accurate Credit Transactions Act (FACT Act) amends the FCRA and provides increased protection against identity theft. This law guarantees consumers the right to access their reports at no charge once every 12 months. The credit bureaus only provide the free reports via Annual Credit Report Request Service, not through their individual websites, telephone numbers, or addresses.

Additional protections under the FACT Act include:

- Consumers may receive additional free reports if identity theft is suspected
- Identity theft victims who file police reports may block fraudulent information from appearing on their credit reports
- Active duty military personnel may place special alerts on their files when they are deployed overseas
- Only the last five digits of a credit card number may be listed on receipts

The Fair Credit Billing Act
The Fair Credit Billing Act provides consumers with a legal dispute process to help with fraud committed on open end credit accounts. It limits your responsibility for unauthorized charges to $50 and stipulates that you won't be charged for goods and services you didn't accept or weren't delivered. To take advantage of the law's consumer protections:

- Write to the creditor at the address given for billing inquiries and include your name, address, account number and a description of the billing error.
- Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you.
- Send your letter by certified mail, return receipt requested. Keep a copy of your dispute letter.

The Fair Debt Collection Practices Act
If you have been a victim of identity theft, and a debt that you did not incur has gone to a collection agency, you have rights under the Fair Debt Collection Practices Act.

Write to the collector within 30 days of receiving notice of the fraudulent debt. The collection agency will conduct an investigation, during which time the collector must cease communication. Only if the debt is determined to be accurate, will collection activity resume.

The Electronic Fund Transfer Act
The Electronic Fund Transfer Act provides consumer protections for ATM, debit card, and other electronic account transactions, including fund transfers.

Report lost or stolen ATM and debit cards immediately to the financial institution, since the amount you can be held responsible for is time sensitive:

- If you report loss or theft within two business days, your liability is limited to $50
- If you report loss or theft after two business days, but within 60 days after a statement showing an unauthorized electronic fund transfer, you can be liable for up to $500
- If you wait more than 60 days, you could lose all the stolen money

Note: You may have additional protection if your ATM/debit card has the VISA or MasterCard logo on it. In most instances your liability for unauthorized use is $50 per card, no matter how much time has elapsed since the discovery of the loss or theft.

If you discover a fraudulent transaction, call your financial institution immediately, then follow up with a letter that explains your dispute. Send it certified mail, return receipt requested, and keep a copy of the letter for your records.

Recovery Guide

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.

To start, commit yourself to becoming and remaining organized. Since you will be communicating with a lot of people and have many tasks to complete, use the Action Logs *(pages 24-27)* to keep track. Keep copies of all letters, file paperwork promptly, and store everything in a safe and accessible place.

Creditors and Financial Institutions
- If accounts have been used or opened illegally, contact your creditors immediately. Ask for fraudulent transaction documentation. You may use a uniform affidavit form, available on the Federal Trade Commission's website *(see Resources on page 23*), as you may need it to file a police report. Add "non-guessable" passwords to replacement cards and all existing accounts.
- 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 cancel your debit card and place stop payments on any outstanding checks that you did not write. Report the crime to check reporting agencies *(page 23)*. Close current checking and savings accounts and obtain new account numbers and passwords. Monitor all future account statements carefully for evidence of new fraud.

Legal 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. For additional documentation, you may also report the crime to the Federal Trade Commission.
- If your mail was stolen or your address was used fraudulently, contact the U.S. Postal Inspection Service *(see Resources on page 23)*.

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. The company you contact will notify the other two, who will then place alerts 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.
- If you feel like a fraud alert will not provide you with enough protection, you can place a security freeze on your credit report. When a freeze is placed on your report, no creditor or other business that does not have a pre-existing relationship with you can access your report.
- You may also write a victim's report – a brief statement describing the details of the crime – and send it to all three bureaus to be added to your reports.
- The first reports with the fraud alert are free and will be sent to you automatically. Check your credit report for accuracy every three months for a year, then at least annually after that.

Resources

Credit Reporting Bureaus/Accessing Credit Reports

- **Equifax**
  To order a credit report call: (800) 685-1111
  To report fraud call: (888) 766-0008
  Equifax Credit Information Services, Inc.
  P.O. Box 740241, Atlanta, GA 30374
  www.equifax.com

- **Experian**
  To order a credit report and report fraud, call: (888) 397-3742
  Experian, P.O. Box 2104, Allen, TX 75013-2104
  www.experian.com

- **TransUnion**
  To order credit report call: (800) 888-4213
  To report fraud call: (800) 680-7289
  TransUnion, 2 Baldwin Pl, P.O. Box 2000
  Chester, PA 19022
  www.transunion.com

- **Annual Credit Report Request Service**
  To order a credit report call: (877) 322-8228
  Annual Credit Report Request Service
  P.O. Box 105281, Atlanta, GA 30348-5281
  www.annualcreditreport.com

Government Agencies

- **U.S. Federal Trade Commission**
  The FTC oversees the operation of credit bureaus and maintains a database of identity theft cases used by law enforcement agencies for investigations.
  Consumer Response Center: (877) 382-4357 or online at www.ftc.gov
  ID Theft hotline: (877) 438-4338, or online at www.ftc.gov/idtheft

  FTC Identity Theft Affidavit Instructions and Form: www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf

- **U.S. Postal Inspection Service**
  (877) 876-2455
  Criminal Investigations Service Center
  Attn: Mail Fraud
  222 S Riverside Plaza, Suite 1250
  Chicago, IL 60606
  http://postalinspectors.uspis.gov

Checking Account Fraud

In addition to reporting checking account fraud to your financial institution, you can report it to these agencies that monitor checking account transactions:

- **ChexSystems**
  (800) 428-9623
  ChexSystems, Inc., Attn: Consumer Relations
  7805 Hudson Rd Ste 100, Woodbury, MN 55125
  www.consumerdebit.com

- **TeleCheck**
  (800) 710-9898
  TeleCheck Services, Inc.
  Attn: Forgery Department
  P.O. Box 4451, Houston, TX 77210
  www.telecheck.com

Miscellaneous

- To opt out of receiving pre-approved credit offers:
  (888) 567-8688
  www.optoutprescreen.com

Action Log: Financial Institutions

Financial Institution	Action	Yes/ No	Date	Contact Person	Notes (phone, email, extension, etc.)
	Stop payments				
	Report check fraud				
	Cancel accounts				
	Change account #s and passwords				
	Stop payments				
	Report check fraud				
	Cancel accounts				
	Change account #s and passwords				
	Stop payments				
	Report check fraud				
	Cancel accounts				
	Change account #s and passwords				

Action Log: Credit Accounts

Creditor	Action	Yes/ No	Date	Contact Person	Notes (phone, email, extension, etc.)
	Report fraud				
	Send affidavit				
	Change account #s and passwords				
	Report fraud				
	Send affidavit				
	Change account #s and passwords				
	Report fraud				
	Send affidavit				
	Change account #s and passwords				
	Report fraud				
	Send affidavit				
	Change account #s and passwords				
	Report fraud				
	Send affidavit				
	Change account #s and passwords				
	Report fraud				
	Send affidavit				
	Change account #s and passwords				
	Report fraud				
	Send affidavit				
	Change account #s and passwords				

Action Log: Bureaus & Agencies

Bureau	Action	Yes/No	Date	Contact Person	Notes (phone, email, extension, etc.)
Equifax	Obtain report				
	Fraud alert				
Experian	Obtain report				
	Fraud alert				
Trans Union	Obtain report				
	Fraud alert				

Agency	Action	Yes/No	Date	Report #	Notes (phone, email, extension, etc.)
FTC	Report crime				
	File Report				
Police Dept.	Report crime				
	File Report				
USPIS	Report crime				
	File Report				
DMV	Report crime				
	File Report				

Action Log: Other Contacts

Organization	Contact Person	Date	Notes (phone, email, extension, etc.)

Glossary

Account takeover – When an identity thief uses your personal information to convince a financial institution to give him or her full control of your account.

Affidavit of factual innocence – A legal document issued by a court, stating that you're innocent. You may need one of these if you've been wrongfully arrested as a result of identity theft.

Affidavit of forgery – A legal document that states that a certain signature is not yours, but a forgery.

Check washing – A method identity thieves use to commit check fraud. They dip a check in acetone, which washes the ink off so they can write it for a higher amount.

Credit repair agency – A company that offers "cleanup" services to remove accurate information from your credit report. Often illegal and expensive, they are sometimes called credit clinics.

Credit reporting agency (CRA) – Commonly known as credit bureaus, they keep track of credit records, and issue credit reports to those who have a legitimate reason for accessing your credit history.

DL stop (driver license stop) – A DL stop is a system that puts a flag on your driver license in the Department of Motor Vehicle's database, to show that your license has been lost or stolen.

Fraud alert – A fraud alert is put on your credit report at the CRAs if you become an identity theft victim. It lets potential creditors know that someone may be trying to obtain new credit in your name, so the process will be very closely scrutinized.

Permissible purposes – Guidelines set out in the FCRA that outline the allowable reasons for requesting a copy of a credit report. One of those reasons is if you're a victim of identity theft.

Truncated credit card number – When all the digits of your credit or debit card number, except for the last four or five, are "x'd" out on a receipt or other document. This is done to protect you from identity theft.

Victim's statement – A statement that is attached to your credit report when you think you may be a victim of identity theft. It asks creditors to contact you before opening any new credit accounts, or making any changes to existing ones.