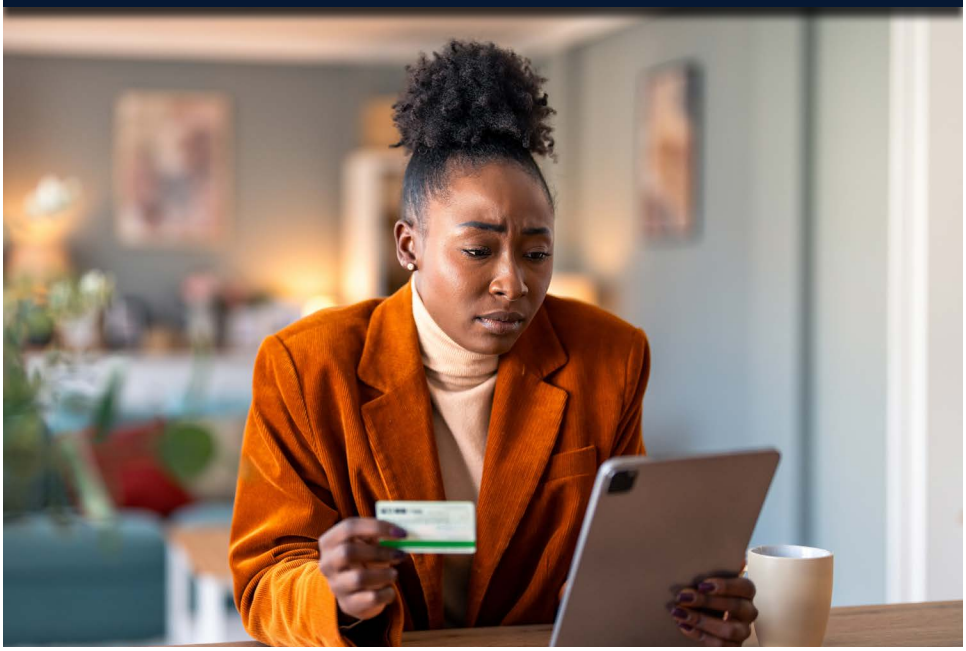
Legal Services

Chinese American Service League

華人諮詢服務處

Identity Theft

• Illinois •



DISCLAIMER: The information in this document does not constitute legal advice. All content herein ("the content") is for general informational purposes and is cited from the U.S. General Services Administration website USA.gov, the Federal Trade Commission website FTC.gov and IdentityTheft.gov, the Federal Bureau of Investigation website FBI.gov, the United States Postal Service website USPS.com, and the Illinois Attorney General's website IllinoisAttorneyGeneral.gov.

DATE ISSUED: October 2024

FAQ's

What is Identity Theft?

Identity theft happens when someone uses your personal or financial information without your permission. For example:

- Names and addresses
- Credit card or Social Security numbers
- Bank account numbers
- Medical insurance account numbers

How does Identity Theft happen?

Scammers can steal your identity in several ways, including in person, online, through social media, and by phone. Scammers may:

- Steal your wallet or purse to get ID, credit, or bank cards
- Go through your trash to retrieve bank statements or tax documents
- Install skimmers at ATM machines, cash registers, and fuel pumps to digitally steal information from your bank card
- Get personal information from your phone when you use public Wi-Fi
- Use "phishing" to get information from you through fraudulent emails, texts, or phone calls
- Look through your social media accounts to find identifying information in posts or photos. Or they may ask you for personal information through online quizzes and surveys

How do I recognize Identity Theft?

You may not know that you experienced identity theft immediately. Beware of these warning signs:

- Bills for items you did not buy
- Debt collection calls for accounts you did not open
- Information on your credit report for accounts you did not open
- Denials of loan applications
- Mail stops coming to or is missing from your mailbox
- Credit score drops
- Credit card charges or bank withdrawals you do not recognize

FAQ's

How do I protect myself from Identity Theft?

- Do not answer phone calls, texts, social media messages, or emails from numbers or people you do not know.
- Do not share personal information like your bank account number, Social Security number, or date of birth.
- Use strong passwords that combine letters, numbers, and symbols.
- Collect your mail every day and place a hold on your mail when you are on vacation or away from your home.
- Review credit card and bank account statements. Watch for and report unauthorized or suspicious transactions.
- Understand how ATM skimming works and how to protect yourself.
- Learn when it is safe to use a public Wi-Fi network.
- Store personal information, including your Social Security card, in a safe place. Do not carry it in your wallet.
- Monitor your credit reports regularly. You can request one free credit report every week from each of the three major credit reporting agencies: Equifax, Experian, and TransUnion.

What do I do if my identity is stolen?

Identity theft can take many forms. This brochure covers two major types: credit/debit card fraud and fraudsters obtaining credit in your name.

The key actions for each type are discussed below. Before taking these actions, keep the following principles in mind:

- Record dates, names, phone numbers, report or file numbers, and notes from any important conversations.
- To confirm, always follow up on a conversation through written communication.
- Send everything by certified mail, return receipt requested.
  Certified mail:
  FAQ.usps.com/s/article/Certified-Mail-The-Basics
  Return receipt:
  FAQ.usps.com/s/article/Return-Receipt-The-Basics
- Keep copies of all letters and documents. Remember never to send originals, only copies.

Procedures

Common Type 1: Credit/Debit Card is Stolen

What should I do if my credit, ATM, or debit card is lost or stolen?

1. Report loss or theft to the card issuer immediately.

Call or get on the mobile app to report the loss or theft to the bank or credit union that issued the card when you first noticed the missing card. The bank customer service representative will lock your card to prevent anyone from using your credit or debit card.

2. Follow up immediately in writing.

Send a letter to the card issuer, and include your account number, the date and time you noticed your card was missing, and when you first reported the loss. Keep a copy of your letter and notes from calls with the bank or credit union.

3. Document the theft on IdentityTheft.gov.

You can create a Federal Trade Commission (FTC) Identity Theft Report by filing a report on IdentityTheft.gov. The report helps prove to businesses that someone stole your identity and makes it easier to correct problems caused by identity theft.

What should I do if I see an unauthorized transaction on my credit or debit card?

1. In general, report the unauthorized transaction to your card issuer as soon as possible.

a. If the authorized transaction is on a debit card, you should notify your issuer as soon as possible, because debit cards offer less protection against fraud than credit cards, and the time it takes for you to report an unauthorized transaction may affect your liability for the charge.

b. For credit cards, you must notify your credit card issuer via customer service number or a mobile banking app of any error you're disputing within 60 days of the date the first statement on which the charge appears was sent to you. 60 days is the legally mandated minimum time limit allowed for disputing unauthorized charges, but some card issuers may allow for a longer time limit such as 90 days. If it has been more than 60 days since the unauthorized charge appeared on your statement, check your cardholder agreement to see if you may still file a dispute.

c. Regardless of card type, keep a record of who you spoke with and when.

Procedures

2. Follow up promptly with a dispute letter to your card company with your name, address, account number, and the unauthorized charges.

a. A template is available on the Federal Trade Commission (FTC)Website: Consumer.FTC.gov/articles/sample-letter-disputing-credit-and-debit-card-charges. Do this within 60 days.

3. If you have an issue with your credit or debit card bank services and cannot resolve it, report it to the Consumer Financial Protection Bureau.

a. Go to ConsumerFinance.gov/Complaint or call (855) 411-CFPB (2372).

How do I limit my losses in unauthorized credit or debit card charges?

Under federal law, you have protections that help limit what you have to pay if your credit, ATM, or debit cards are lost or stolen.

	Credit Card	ATM/Debit Card
You report your card's loss **before** someone uses it	You aren't responsible for any charges you didn't authorize	You aren't responsible for any transactions you didn't authorize
You report your card's loss **after** someone uses it	The maximum you might be responsible for is $50	What you're responsible for depends on how quickly you reported it (refer to the following chart)
Your account number is used, **but your card isn't lost or stolen**	You aren't responsible for any charges you didn't authorize	You aren't responsible for any transactions you didn't authorize **if you reported the loss within 60 calendar days after your statement is sent to you**

If someone uses your ATM or debit card before you report it lost or stolen, what you owe depends on how quickly you report it.

If you report your ATM or debit card lost or stolen:	Your maximum loss is:
Before any unauthorized charges are made	$0
Within 2 business days after you learn about the loss or theft	$50
More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you	$500
More than 60 calendar days after your statement is sent to you	All the money taken from your ATM/debit card account, and possibly more—for example, money in accounts linked to your debit account

Procedures

Common Type 2: Someone Applied for a Credit Card in Your Name

Someone can apply for a credit card using your date of birth, social security number, address, and other sensitive information. They may then use the card and not pay the credit card bill, eventually hurting your credit score. This kind of identity theft is much harder to discover. Most victims discover it months later when they encounter unexpected trouble with opening another credit card, applying for leases, or get bothered by debt collectors. A proactive way to discover such theft is to monitor your credit reports and sign up for a fraud alert, see below for details.

If someone applied for a credit card in your name, please follow the following six steps:

STEP 1
Call the companies where you know fraud occurred.

STEP 2
Place a fraud alert and obtain your credit reports.

STEP 3
Report identity theft to the FTC.

STEP 4
File a report with your local police department.

STEP 5
Close new accounts opened in your name.

STEP 6
Correct your credit report.

Procedures

STEP 1: Call the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze the accounts.
- Change logins, passwords and PINS for your accounts.

STEP 2: Place a fraud alert and get your credit reports.

- Place a free, one-year fraud alert by contacting one of the three credit bureaus.
  - Experian.com/help, (888) 397-3742
  - TransUnion.com/credit-help, (888) 909-8872
  - Equifax.com/personal/credit-report-services, (800) 685-1111
- Get your free credit reports from Equifax, Experian, and TransUnion.
  - Go to AnnualCreditReport.com or call (877) 322-8228.
  - Review your reports. Make note of any account or transaction you don't recognize.
  - As of October 2023, you can check your reports every week for free at AnnualCreditReport.com.

STEP 3: Report identity theft to the FTC.

- Complete the online form at IdentityTheft.gov/assistant or call (877) 438-4338.
- If you don't create an account, you must print and save your Identity Theft Report and recovery plan right away.
  - Note: Once you leave the page, you won't be able to access or update them.

Step 4: File a report with your local police department.

- Go to your local police office with:
  - A copy of your FTC Identity Theft Report
  - A government-issued ID with a photo
  - Proof of your address (mortgage statement, rental agreement, or utilities bill)
  - Any other proof you have of the theft (bills, IRS notices, etc.)
- Tell the police someone stole your identity, and you need to file a report.
- Ask for a copy of the police report.

Procedures

Step 5: Close new accounts opened in your name.

- Call the fraud department of each business where an account was opened.
  - Explain that someone stole your identity.
  - Ask the business to close the account.
  - Ask the business to send you a letter confirming that: (1) The fraudulent account isn't yours; (2) you aren't liable for it; (3) it was removed from your credit report.
  - Keep this letter. Use it if the account appears on your credit report later.
  - Note: The business may require you to send them a copy of your FTC Identity Theft Report or complete a special dispute form. This sample letter can help: IdentityTheft.gov/sample-letters/identity-theft-dispute-new-account.

Step 6: Correct your credit report.

- Write to each of the three credit bureaus. Use certified mail with a return receipt requested.
  - This sample letter can help: IdentityTheft.gov/sample-letters/identity-theft-credit-bureau.
  - Include a copy of your FTC Identity Theft Report and proof of your identity: name, address, and Social Security number.
  - Explain which entry in your report came from identity theft.
  - Ask the following credit bureaus to block that information:

    Equifax.com
    P.O. Box 105069
    Atlanta, GA 30348
    (800) 525-6285

    Experian.com
    P.O. Box 9554
    Allen, TX 75013
    (888) 397-3742

    TransUnion.com
    Fraud Victim Assistance Department
    P.O. Box 2000
    Chester, PA 19016
    (800) 680-7289

- If someone steals your identity, you have the right to remove fraudulent information from your credit report. This is called blocking. If you have an FTC Identity Theft Report, credit bureaus must honor your request to block this information.

Resources

Federal Trade Commission (FTC) Identity Theft Report

- IdentityTheft.gov is the federal government's one-stop resource for identity theft victims.
- If someone is using your information to open new accounts or make purchases, IdentityTheft.gov can help you report and recover from identity theft.
- Your FTC Identity Theft Report helps prove to businesses that someone stole your identity and makes it easier to correct problems caused by identity theft.
- You can create an FTC Identity Theft Report by filing a report with the FTC at IdentityTheft.gov.

National Credit Bureaus

- Contact the national credit bureaus to request fraud alerts, credit freezes (also known as security freezes), and opt-outs from prescreened credit offers.
  - Experian.com/help, (888) 397-3742
  - TransUnion.com/credit-help, (888) 909-8872
  - Equifax.com/personal/credit-report-services, (800) 685-1111

CASL Legal Services

If you have any questions about the contents of this brochure or if you would like to speak to an attorney, contact CASL Legal Services at (888) 764-6125 or request an appointment through our website. Eligibility for services is based on the applicant's household income and residency.

CASLservice.org/Legal

Mail Services

- Sign up for Informed Delivery offered for free by USPS at USPS.com/manage/informed-delivery.htm
  - This service emails you in the morning about incoming mail and packages. The address-side scans of letter-sized mail is also available. Although there are still limitations, the scans of important mailings should prompt you to look for that mailing when you pick up the mail.
- Submit a mail hold request for free online at USPS.com/manage/hold-mail.htm
  - As you place the mail hold request, you will have an opportunity to choose to pick up your accumulated mail or have them delivered after the hold period.

Resources

Understanding ATM Skimming

This article by the Federal Bureau of Investigation is a good guide to skimming: FBI.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming

Public Wi-Fi Network Safety

Look for a "lock" sign (🔒) on your browser's address bar to confirm that your connection to a website is encrypted. Visit the following site for more information: Consumer.FTC.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

Extended Fraud Alert or Credit Freeze

Extended Fraud Alert	Credit Freeze
A company must contact you before granting new credit in your name.	Limits access to your credit report unless you lift or remove it.
Free to place and remove. Available if someone stole your identity.	Free to place and remove. Available to anyone. Parents, guardians, and conservators can place for children under 16 or adults under their care.
Lasts for 7 years	Lasts until you lift or remove it
Set it by contacting one of the three nationwide credit bureaus. The one you contact must tell the other two.	Set it by contacting each of the three credit bureaus.

Credit Bureau Contact Information

- Experian.com/help, (888) 397-3742
- TransUnion.com/credit-help, (888) 909-8872
- Equifax.com/personal/credit-report-services, (800) 685-1111

Legal Services

Chinese American Service League

華人諮詢服務處

CASL | 2141 S. Tan Ct. | Chicago, IL | (312) 791-0418 | CASLservice.org | @CASLmedia