CONSOLIDATED CREDIT®
When debt is the problem, we are the solution.

# *Identity Theft*

**1-800-210-3481**
www.**ConsolidatedCredit**.org

# Letter from the President

*Congratulations on taking this important step to a brighter financial future. Consolidated Credit has been helping Americans across the country solve their credit and debt problems* ***for over 30 years.***

*Our Educational Team has created over forty publications to help you improve your personal finances; and many available in Spanish. By logging on to* ***www.ConsolidatedCredit.org*** *you can access all of our publications free of charge. We have the tools to help you become debt free, use your money wisely, plan for the future, and build wealth. The topics Consolidated Credit addresses range from identity theft and building a better credit rating to how to buy a home and pay for college. On our web site you will also find interactive courses, calculators, video education, and much more.*

*We are dedicated to personal financial literacy and providing a debt-free life for Americans. If you are overburdened by high interest rate credit card debt, then I invite you to* ***speak with one of our certified counselors free of charge*** ***by calling 1-800-210-3481*** *for free professional advice. We also have partnership programs available where groups, businesses and communities can hold financial workshops and received money management guides and workbooks like the one you are reading now.* ***Please call 1-800-210-3481*** *if you would like to discuss pursuing a personal financial literacy program.*

***Sincerely,***

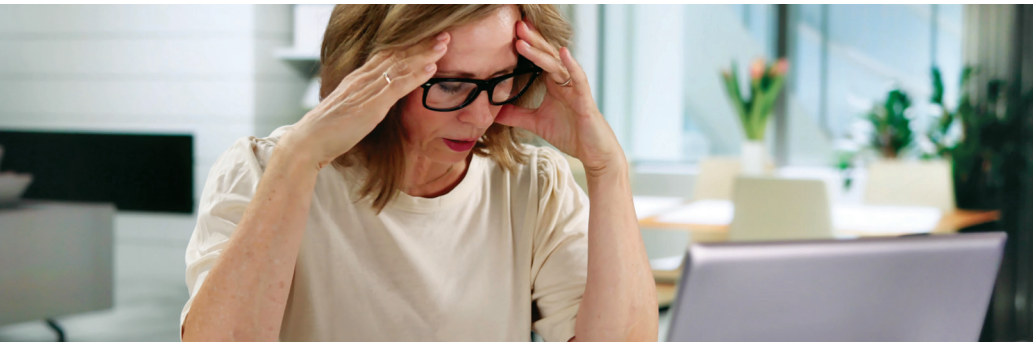
***Gary S. Herman***
***President***
***Consolidated Credit***

# Protecting Your Identity: How to Prevent, Detect, and Recover from Fraud

Identity theft occurs when someone uses your personal information — like your name, Social Security number, credit card data, or even your child's identity — without permission to commit fraud or other crimes. While monetary loss is the most common motivation, the impact can also include damage to your credit, medical records, taxes, and emotional well-being.

**Common types of identity theft include:**

- **Financial identity theft:** Unauthorized accounts, loans, or purchases made in your name.
- **Medical identity theft:** Use of your name or insurance for medical services or prescriptions.
- **Tax identity theft:** Filing false tax returns using your Social Security number to claim refunds.
- **Child identity theft:** Fraudulent use of a minor's personal data, often untracked for years.



**Why it matters:**

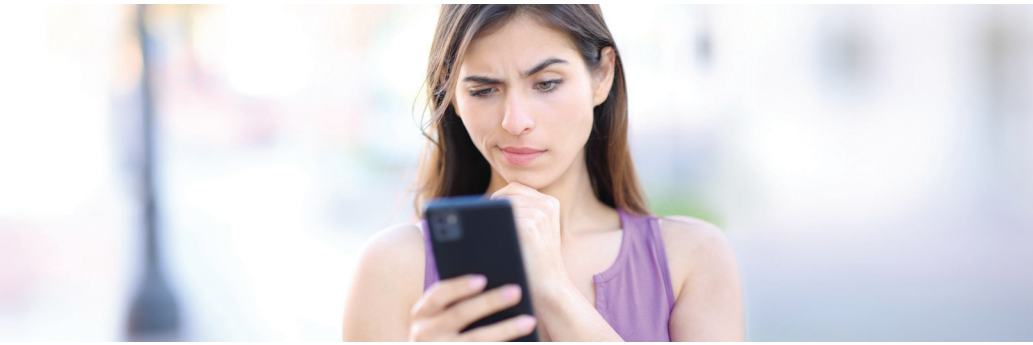
Identity theft is more than just an inconvenience; it's a serious threat. According to the Federal Trade Commission's most recent Consumer Sentinel Network Data Book (2024), more than 1.1 million identity theft reports were filed via IdentityTheft.gov last year.

That accounted for roughly 18% of all 6.5 million consumer complaints received by the agency. In total, consumers reported $12.5 billion in fraud-related losses in 2024. While not all of that stemmed from identity theft, it underscores the growing scope of digital and financial fraud in the U.S.

These are the latest verified figures available from the FTC as of July 2025.

That's why taking identity theft seriously — and acting swiftly if it occurs — is critical. In the upcoming pages, you'll find practical tips for protecting your identity and comprehensive recovery steps in case of theft.

# How identity theft happens



Identity thieves use both high-tech strategies and old-fashioned methods to acquire personal data, and their tactics are evolving constantly. Awareness of these high-risk methods helps you spot suspicious activity before it becomes a problem.

**Some of the most common methods include:**

### Phishing scams

Deceptive emails, texts, or links that mimic trusted sources like banks or government agencies. A notable example: a rash of fake “PayPal” emails directed victims to fraudulent login pages to harvest their credentials.

### Data breaches

Hacking into company systems to access massive sets of personal information. In 2024, high-profile breaches hit institutions such as AT&T (exposing over 86 million customer records, including more than 44 million SSNs), healthcare provider Episource (impacting 5.4 million people), insurance firm Allianz Life (1.4 million customers via vendor breach in July 2025), and the dating app Tea (leaking 72,000 images including ID verification photos and messages).

### Credential stuffing / weak password reuse

Cybercriminals exploit reused or compromised login credentials to gain access to accounts or networks, such as in the 23andMe breach, which affected around 5.5 million users via credential stuffing attacks in recent years.

### Unsecured Wi-Fi networks

Public networks (like coffee shops or airports) may lack strong encryption. Without a VPN, your data — passwords, emails, or financial logins — can be intercepted by cybercriminals.

### Mail theft and card skimming

Thieves may steal paper mail containing sensitive information or use skimming devices hidden at ATMs or gas pumps to capture card and PIN data.

### Social media oversharing

Sharing too much personal data, birthdays, pet names, family connections, can give scammers ammunition to guess password recovery questions or impersonate you online.

### Why it matters:

The Identity Theft Resource Center tracked over 3,200 data breach events in 2024, affecting more than 1.7 billion records, a 312% increase from 2023. Breaches involving stolen credentials, phishing, and ransomware dominated these events.

These methods are real, ongoing, and increasingly prevalent, often leading directly to identity theft.

# Warning signs your identity may be stolen

Sometimes identity theft is obvious: A credit card charge you didn't make or an account you never opened. Other times, the signs are subtle or delayed. That's why it's important to recognize the red flags early, before more damage is done.

**Here are some of the most common warning signs:**

### Bills or credit card statements you didn't expect

If you start receiving mail for unfamiliar accounts — especially credit cards, loans, or utilities — it may be a sign that someone opened them in your name.

### Debt collection calls for accounts you don't recognize

Debt collectors may contact you about unpaid balances that were never yours to begin with. Always ask for written verification and never provide additional personal information over the phone.

### Credit denial, even with good history

If you're suddenly denied for a loan, mortgage, or credit card despite having a solid credit score, it could mean a thief has damaged your credit behind the scenes. A quick check of your credit report may

reveal new accounts or large balances you didn't authorize.

### Strange activity on existing accounts

Small, unfamiliar charges on your credit or debit cards can be a thief testing the waters. Never ignore these; even minor fraud can escalate quickly.

Spotting these signs early can prevent further harm. The sooner you act, the easier it is to stop identity theft before it spreads.

## How to protect your personal information


Protecting your identity starts with protecting your information, both online and offline. With the right habits, you can dramatically reduce the chances of becoming a victim.

### Use strong, unique passwords

Avoid reusing the same password across multiple accounts. Strong passwords should include a mix of letters, numbers, and special characters. Use a password manager to generate and store them securely.

### Enable two-factor authentication (2FA)

Adding a second layer of security — like a code sent to your phone or generated by an app — makes it much harder for hackers to access your accounts, even if they have your password.

### Secure your devices and Wi-Fi network

Install antivirus software and keep your operating systems updated. Always set a password for your home Wi-Fi and consider using a virtual private network (VPN) for added protection, especially on public networks.

### Shred sensitive documents before disposal

Pre-approved credit offers, medical records, and bank statements can all be used to steal your identity. Invest in a paper shredder and use it regularly.

### Lock your mailbox or go paperless

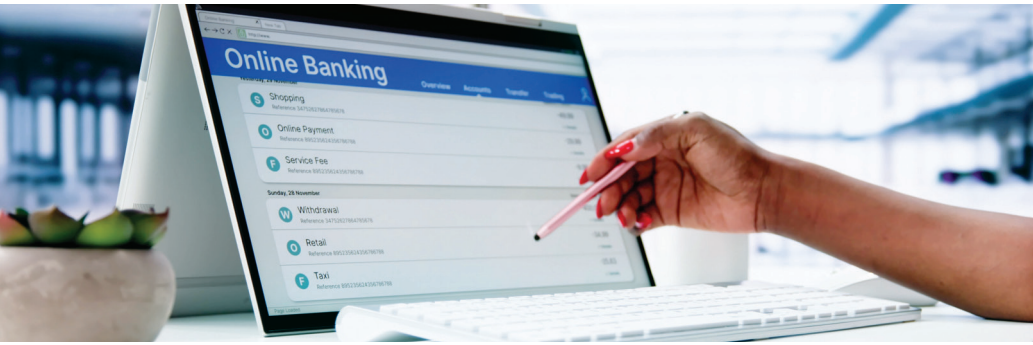
Mail theft is still a common entry point for identity thieves. Use a locked mailbox if possible, or opt for paperless billing and statements when available.

### Be selective on social media and with email

Don't overshare personal details like your birthday, address, or family connections. Be wary of emails asking for personal information or prompting you to click on unknown links — these could be phishing scams.

Every small step strengthens your overall security.

# Protecting your financial identity




Your financial information is a prime target for identity thieves. That's why taking a few extra precautions with your bank accounts, credit cards, and spending habits can go a long way toward protecting your money and your credit.

## Monitor your financial accounts regularly

Review your bank and credit card statements every month, line by line. Look for unauthorized charges, even small ones. Thieves often test stolen account numbers with minor transactions before making bigger purchases.

## Consider placing a fraud alert or credit freeze

A fraud alert notifies lenders to take extra steps to verify your identity before opening new credit in your name. It's free and lasts one year, with the option to renew. A credit freeze, also free, completely blocks access to your credit report unless you temporarily lift it. Both are available through Equifax, Experian, and TransUnion.

## Carry only the cards you need

Don't keep your Social Security card, birth certificate, or rarely used

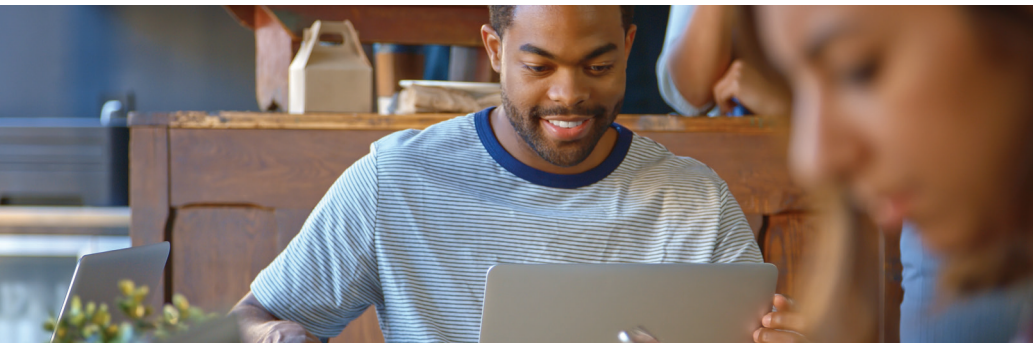
credit cards in your wallet. If your purse or wallet is lost or stolen, fewer items will be at risk, and easier to cancel.

### Watch out for skimming devices

Skimmers are small, hidden devices attached to ATMs, gas pumps, or point-of-sale terminals. They capture your card information during use. Look for loose or unusual parts on a card reader, and if anything feels off, don't insert your card.

By staying alert and limiting exposure, you can make it harder for thieves to access your financial identity.

## Online safety tips



The internet is a daily necessity, but it's also a hunting ground for identity thieves. Practicing smart online habits can help keep your personal information out of the wrong hands.

### Stick to secure websites

Before entering personal or financial information online, check that the website address starts with "https://"— the "s" stands for secure. Also look for a padlock icon in the address bar. If either is missing, don't enter sensitive data.

### Use strong, unique passwords

Each online account should have its own password. Avoid common choices like “123456” or your pet’s name. Combine upper- and lowercase letters, numbers, and special characters. Consider using a password manager to help create and store strong passwords safely.

### Avoid public Wi-Fi for sensitive transactions

Public Wi-Fi networks — like those in airports, hotels, and coffee shops — are often unsecured. Hackers can easily intercept data on these networks. Never log into financial accounts or enter credit card information on public Wi-Fi unless you’re using a virtual private network (VPN).

### Don’t click unknown links or download attachments

Phishing scams often use emails or text messages to trick users into clicking fake links or downloading dangerous files. These can install malware or send your login information directly to a criminal. If you weren’t expecting a message, especially one asking for urgent action, don’t click.

Online safety comes down to vigilance. With a few habits and tools, you can protect yourself against most digital threats.

# Monitoring your credit


One of the most effective ways to detect identity theft early is by keeping a close eye on your credit. Even small changes, like a new account or a sudden dip in your score, can be signs that someone else is using your information.

### Check your credit reports regularly

Federal law allows you to check your credit reports from all three major bureaus — Equifax, Experian, and TransUnion — for free at AnnualCreditReport.com. Through at least the end of 2026, you can access each report weekly at no cost. Reviewing your reports regularly makes it easier to spot suspicious activity before it becomes a major problem.

### Look for unfamiliar accounts or credit inquiries

New credit card accounts, loan applications, or collections accounts that you don't recognize are major red flags. So are "hard inquiries" from companies you haven't done business with. These may indicate that someone is trying to open credit in your name.

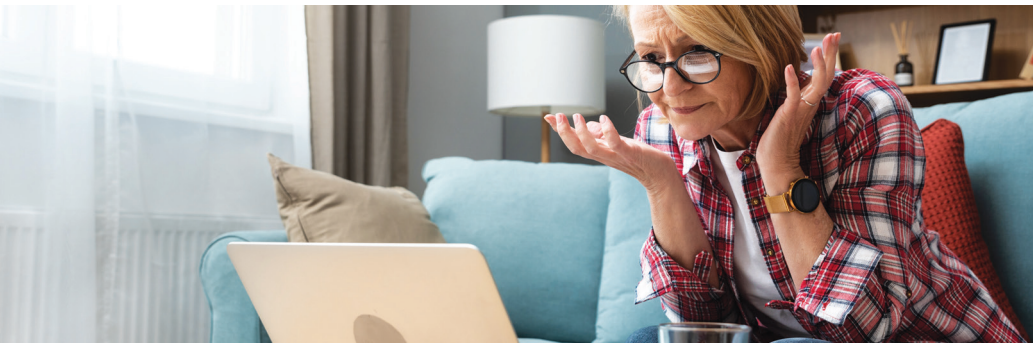
### Consider enrolling in a credit monitoring service

Many credit monitoring services will alert you to changes in your

credit file, such as a new account opening or a significant score drop. Some services are free, while others charge a monthly fee. If you've already been a victim of identity theft or are at higher risk, monitoring can provide added peace of mind.

The sooner you catch unauthorized activity, the easier it is to limit the damage and begin recovery.

## What to do if you're a victim



If you suspect your identity has been stolen, acting quickly is crucial. These five steps can help you limit the damage and begin the recovery process:

### 1. Place a fraud alert on your credit file

Contact any one of the three major credit bureaus — Equifax, Experian, or TransUnion — to request a fraud alert. That bureau will notify the other two. A fraud alert tells lenders to verify your identity before approving new credit. It lasts one year and is free to renew.

### 2. Order your credit reports

After placing a fraud alert, you're entitled to a free copy of your credit report from each bureau. Review all three for unfamiliar

accounts, hard inquiries, or inaccurate personal information. Make note of anything suspicious.

### 3. Report the theft to the FTC

Visit IdentityTheft.gov to file an official report with the Federal Trade Commission. The FTC will help you create a personalized recovery plan and provide pre-filled letters to send to creditors, debt collectors, and the credit bureaus.

### 4. File a police report

Some creditors or agencies may require a police report to investigate fraud or close fraudulent accounts. Bring your FTC report, ID, and any proof of the theft when filing with local law enforcement.

### 5. Contact affected institutions

Call your bank, credit card issuers, or lenders where fraudulent activity occurred. Close or freeze compromised accounts and follow their instructions for recovery.

Prompt action is the best way to stop identity theft from spreading further.

# Fixing the damage

Once you've reported identity theft and taken steps to stop it, the next challenge is cleaning up the mess it left behind. This process can take time, but knowing your rights and staying organized can help make it smoother.

## Dispute fraudulent charges and accounts

Contact any company where a thief opened an account or made unauthorized charges. Explain that you're a victim of identity theft and provide supporting documentation, such as your FTC Identity Theft Report and a copy of your police report. Ask the company to close or remove the fraudulent activity from your records.

## Close compromised accounts and open new ones

If a credit card or bank account was used fraudulently, request that the institution close it and open a new account with new credentials. Change passwords, PINs, and security questions for any affected services to prevent repeat access.

## Replace your identification documents

If your driver's license, Social Security card, passport, or other official ID was compromised, contact the appropriate agency to report the

misuse and request a replacement. Some states may also let you flag your driver's license number to prevent future fraud.

### Create or update your Identity Theft Report

If you discover additional fraudulent activity after filing your initial report with IdentityTheft.gov, go back and update your case. Keeping a comprehensive record will help you resolve disputes with creditors or collectors.

Taking time to follow up thoroughly will protect your credit and your identity in the long run.

## How Consolidated Credit can help

While Consolidated Credit doesn't offer identity theft protection or credit monitoring, as a respected nonprofit credit counseling agency, it offers a range of free and low-cost financial education resources and personalized support to help you recover effectively.

### Certified credit counseling and personalized advice

If identity theft has left your finances in disarray, you can contact Consolidated Credit to speak with a certified credit counselor. A counselor can help you review your income, expenses, and debts to

rebuild a strong financial foundation in the wake of fraud.

### Help interpreting credit reports and disputing fraud

Through their educational tools and coaching, Consolidated Credit can teach you how to analyze your credit reports for suspicious accounts, evaluate fraudulent activity, and understand dispute procedures, even though they don't directly place fraud alerts for you.

### Debt recovery planning with budgeting tools

If identity theft has triggered late payments or increased balances, Consolidated Credit provides budget worksheets, webinars, and counseling to help you manage payments, track essential expenses, and prioritize recovery efforts.

### Educational resources including articles and webinars

Their Identity Theft and Fraud Resource Center features educational guides, on-demand webinars like "Prevent ID Theft & Credit Fraud," and downloadable booklets that explain best practices in both prevention and recovery.

### Getting started

To access support, visit consolidatedcredit.org or call their toll-free number. Counselors are available to discuss your situation confidentially, regardless of your income or credit history.

CONSOLIDATED CREDIT®
When debt is the problem, we are the solution.

# *Financial Knowledge*
# ***is Financial Power***

- *Learn how to manage debt, credit, and money with confidence.*
- *Gain tools that support smarter decisions at every life stage.*
- *Protect yourself from scams, setbacks, and costly mistakes.*

Call **1-800-210-3481**

HUD-APPROVED OFFICE OF HOUSING COUNSELING HOUSING COUNSELING AGENCY

HUD Approved Housing Counseling Agency:

**1-800-435-2261**

Email:
counselor@ConsolidatedCredit.org

5701 West Sunrise Boulevard.
Fort Lauderdale, FL 33313

**www.ConsolidatedCredit.org**