

# WHAT IS IDENTITY THEFT?

Identity theft occurs when a thief obtains personal information about you, such as your name, address, Social Security Number, account number, or driver's license number.

## UNFORTUNATELY, CASES OF IDENTITY THEFT ARE ON THE RISE

Thousands of people are facing the inconvenience of reclaiming their identities and sorting out their financial lives. If you believe you're a victim of identity theft or you simply want to know how to avoid becoming the next statistic, Eli Lilly Federal Credit Union is here to help.

Here you will find the answers to many of your questions and step-by-step advice about what to do and where to turn next. We're glad you've come to your credit union for support.

You'll also find a helpful Identity Theft link on our website under the Security Center. There you will find several security tools to help you. For starters, ELFCU recommends these services, all available at [elfcu.org](http://elfcu.org):

- **eBranch:** You can regularly monitor account activity with our online banking system.
- **eStatements:** Enroll via eBranch by clicking on eStatements under Account Access; then follow the steps. eStatements eliminate paper and clutter, and they're free!
- **Verified by Visa®:** Register any of your Visa® cards with this service to ensure that only you can use your Visa card to shop online.
- **AlertMe:** Monitor your Credit Bureau file regularly with this service. When credit activity occurs under your name, the service will alert you by email.
- **Annualcreditreport.com:** You can review your credit file annually at no cost via this site. We provide a direct link for your convenience.

Consider updating your credit union telephone security word, as well. Simply contact Member Service to make these important changes, **317.276.2105** or **800.621.2105**.

For further information and guidance from an expert please call **317.524.5031**.

## WHAT ARE THE RED FLAGS OF IDENTITY THEFT THAT REQUIRE IMMEDIATE ATTENTION?

- Stolen wallet, purse or records that contain account numbers or confidential information
- Suspicious requests for confidential information over the telephone or computer
- Unexpected credit cards, utility or account statements
- Bills that do not arrive as expected or denials of credit for no apparent reason



# WHAT SHOULD I DO IF MY PERSONAL INFORMATION IS LOST OR STOLEN?

## CONTACT THE NATIONAL CREDIT BUREAUS.

Call the national credit bureaus to place a fraud alert on your file. It is best to contact all three of them: Equifax, Experian, and TransUnion. (See **Important Identity Theft Resources & Contact Information**) If you call only one, it could take up to 30 days for the bureaus to share the information.

Ask for a free copy of your credit report from all three credit bureaus. Review the reports carefully and look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. In a few months, order new copies of your reports to verify all corrections and make sure no further fraud has occurred.

Credit grantors may not always consider fraud alerts and victim statements when extending credit. You should continue to check your credit reports regularly, especially during your first year of discovery. You want to be sure no new fraudulent activity is taking place.

## CONTACT YOUR CREDITORS' FRAUD DEPARTMENTS.

- You will need to get in touch with all your creditors, including financial institutions, credit card issuers, utilities, and phone companies to tell them about the identity theft. It's important to follow up verbal notification in writing, so follow up with a letter or affidavit (Example of affidavit at [FTC.gov/idtheft](http://FTC.gov/idtheft).) Use this resource to dispute unauthorized credit, goods or services.
- To report a lost or stolen CU CheckCard or CashCard to ELFCU after-hours, call 888.241.2510 or 800.621.2105.



## FRAUD WARNING

If you can answer **YES** to any of the following questions, please notify the teller before completing your transaction.

- Have you been told you are the winner of a sweepstakes or lottery?
- Did you receive this cashier's check or official check for selling merchandise?
- Did your transaction or sale originate over the internet or sales ad?
- Did the buyer overpay the purchase price?
- Were you instructed to wire the excess funds to the buyers?

## AND IF YOU ARE THE VICTIM OF A CRIME SUCH AS A STOLEN WALLET OR PURSE, HOME ROBBERY OR BURGLARY, DO THE FOLLOWING:

### FILE A POLICE REPORT.

Call your local police department or the police department where the theft took place and file a report. Be sure to ask for a report number and copy of the report in case you're asked to provide proof of the crime. Also, ask for information on how to reach the investigator and give this information to all the companies you contact about getting your credit cleaned up.

### FILE A COMPLAINT WITH THE FTC.

The Federal Trade Commission (FTC) will provide you with information and refer your complaints to appropriate credit-reporting agencies and law enforcement agencies. They're true experts in handling identity theft and fraud. To learn more, visit [FTC.gov/idtheft](https://www.ftc.gov/idtheft).

### TAKE CONTROL.

Your next steps will depend on how you think the identity theft happened. Here are the advised responses to common circumstances:

- **A thief has tampered with your account, checks, ATM, debit or credit card.** Report lost or stolen cards or checks to the issuer immediately.
- **Your mail has been stolen or the thief issued a change-of-address to redirect your mail.** File a report and change of address with the U.S. Postal Inspection Service.
- **A thief used your driver's license number as false identification.** Call the state office of the BMV to see if another license was issued in your name. Put a fraud alert on your license and request a new driver's license number. To initiate a fraud investigation, fill out a BMV complaint form and send it, along with supporting documents, to the nearest BMV investigation office.
- **Your Social Security Number was stolen.** Report the suspected theft at the nearest Social Security Administration office. Ask for verification of the accuracy of the earnings reported on your SSN, and request a copy of your Social Security Statement.
- **Your contact with Identity Theft or Fraud was via the Internet.** File a complaint with the Internet Crime Complaint Center, [www.ic3.gov](https://www.ic3.gov).



## WHAT DOES ELFCU DO TO PROTECT ME FROM IDENTITY THEFT?

ELFCU is committed to safeguarding your personal financial identity. Here are some of the measures we take to protect you:

- **Privacy Policies.** ELFCU strictly enforces privacy policies approved by the federal government, and employees are regularly trained to keep your financial information safe.
- **Internal Confidentiality.** Access to nonpublic information about you is limited to employees who need to know that information to provide products and services to you.
- **Password Protection.** Your account information, by phone and online, is secured by personal passwords that only you know.
- **Computer Security.** When you are accessing your accounts online, your transactions and personal information are secured by powerful encryption software that scrambles the information into secure code.
- **Notification of Major Check Verification Companies.** If your ELFCU checks have been stolen or misused, we will ask retailers who use these databases not to accept your checks on the old account: Tele-Check, Certegy, Inc., CheckCare Systems and SCAN.

## WHAT CAN I DO TO PROTECT MYSELF IN THE FUTURE?

There are precautions you can take to protect your personal information from identity thieves. Moving forward, be sure to establish these habits:

- Review your accounts regularly on eBranch at [elfcu.org](http://elfcu.org)
  - Reconcile your check and credit card statements in a timely fashion. Immediately challenge any purchases you did not make.
  - Review your credit reports periodically for fraud. (Note: Military personnel who are serving away from their usual duty station can place an active duty alert with any of the three major consumer reporting agencies.)
  - Do not carry your extra credit cards, Social Security card, birth certificate, or passport in your wallet or purse. Consider making a copy of both sides of any item in your wallet or purse so you can quickly call the issuers to inform them about missing or stolen cards.
  - Never leave your purse or wallet unattended at work or in church, restaurants, health fitness clubs, parties, or shopping carts. Never leave your purse or wallet in your car, even when your car is locked.
- When creating new passwords or PINs, don't use any part of your Social Security number, personal information or anything that could be easily deciphered by a thief.
  - Use virus protection on your computer and don't open email from unknown sources. Verify an organization's website by typing its URL in the address line, rather than cutting and pasting it into your browser or clicking on links within emails.
  - Use a secure browser when banking or shopping online. When submitting your purchase information, look for the "lock" icon on the browser's status bar or for a website that begins "https:" which indicates the site is secure during transmission.
  - When you are writing checks to pay your credit card accounts, DO NOT put the complete account number on your check. Instead just use the last four numbers. Better yet, use the credit union's free bill pay service.



## IMPORTANT IDENTITY THEFT RESOURCES & CONTACT INFORMATION

To place a free 90-day fraud alert please contact the following credit bureaus.

### Equifax

PO Box 740241

Atlanta, GA 30374

[equifax.com](http://equifax.com)

800.525.6285 (to report fraud)

800.685.1111 (to order a credit report)

### Experian

PO Box 9532

Allen, TX 75013

[experian.com](http://experian.com)

888.397.3742

### TransUnion

Fraud Victim Assistance Division

P.O. Box 6790

Fullerton, CA 92834

[transunion.com](http://transunion.com)

800.680.7289 (to report fraud)

800.916.8800 (to order a credit report)

### Other Helpful Links

- Federal Trade Commission, [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or 877.438.4338
- Social Security Administration, [www.ssa.gov](http://www.ssa.gov) or 800.269.0271 (Fraud Hotline)
- U.S. Postal Inspection Service, [postalinspectors.uspis.gov](http://postalinspectors.uspis.gov) or 800.372.8347