FD COMMUNITY FCU

FRAUD PREVENTION & WHAT TO DO WHEN YOUR IDENTITY IS STOLEN

IDENITY THEFT

SCAMS: CHECK FRAUD

A significant amount of check fraud is due to counterfeiting through desktop publishing and copying to create or duplicate an actual financial document, as well as chemical alteration, which consists of removing some or all of the information and manipulating it to the benefit of the criminal.

Victims include financial institutions, businesses that accept and issue checks, and the consumer. In most cases, these crimes begin with the theft of a financial document. It can be perpetrated as easily as someone stealing a blank check from your home or vehicle during a burglary, searching for a canceled or old check in the garbage, or removing a check you have mailed to pay a bill from the mailbox.

SCAMS: MAIL THEFT

Many important documents are sent through the mail, and can sit in the box for hours or even days before retrieval. Criminals can steal checks, intercept credit or debit cards, or even retrieve documents such as bank statements or medical paperwork if not properly discarded.

How to prevent it: The simplest solution for mail theft is to install a locking mailbox that only you or others with the key can access. Shredding mail you no longer need will help keep private information away from prying eyes. If given the choice, pick up important documents or cards in person rather than risking mail theft. If you've been the victim of mail theft or tampering, you can report it to the U.S. Postal Inspection Service by calling 877-876-8455.

203-753-9201

@fdcommunityfcu

www.fdcommunityfcu.org

FRAUD PREVENTION

RESOURCES & INFORMATION

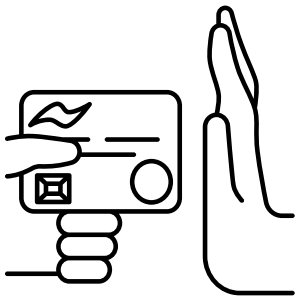
- **FTC's Identity & Privacy Web Site** - The Federal Trade Commission (FTC) is the nation's consumer protection agency.
- **FACTA Free Annual Report** - Information on your right to a free report.
- **Create An Identity Theft Report -** An Identity Theft Report gives you some important rights that can help you recover from the theft.
- **Place an extended fraud alert on your credit report**: Contact the national credit bureaus to request fraud alerts, credit freezes (also known as security freezes), and opt outs from pre-screened credit offers.
  - **Equifax:** Equifax.com/personal/credit-report-services or call 800-685-1111
  - **Transunion:** TransUnion.com/credit-help or call 888-909-8872
  - **Experian:** Experian.com/help or call 888-EXPERIAN (888-397-3742)

STEPS TO TAKE AFTER IDENTITY THEFT OCCURS

1. File a report with your local police precinct or your state's attorney general.
2. File a complaint with the Federal Communications Commission (FCC) or Federal Trade Commission (FTC).
3. Contact close any impacted accounts at your financial institution and open a new account.
4. Contact one of the three credit reporting agencies to place an extended fraud warning or credit freeze.

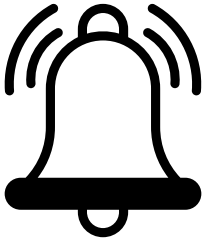
Fraud Prevention

BEST PRACTICES

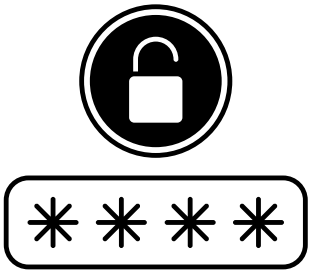


- **Monitor your credit reports and credit score.** Thieves can use your information to set up new credit cards in your name with a fake address. This means you'll never receive bills, so your first clue that something is amiss may be a credit score left in ruins by unpaid bills or delinquent charges on your credit report.
- **Explore putting a lock or a freeze on your credit reports compiled by Equifax, Experian, and TransUnion.** Both a lock and a freeze block access to your credit reports, making it highly unlikely that anyone could open a credit card in your name.

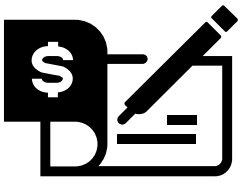
- **Shred or securely store your paper bank statements.** One of the advantages of online banking is that your records are stored securely online. However, if your financial institution sends you monthly statements about your account or another account you have with them, be aware that these statements can include log-in information as well as account numbers that can be used to access your account. You should shred these documents when you are done with them or store them in a secure place.
- **Enroll in e-statements.** Receive your statements electronically. Paper statements can divulge your financial information if stolen from your mailbox.



- **Get account alerts.** Ask your financial institution or brokerage house representative if the institution provides account activity notifications and how to implement them. Alerts will notify you about activity on your account. Review alerts immediately can protect against fraudulent activity on your account.



- **Change Your PINs & Passwords.** Once your computer is free of malware, it's time to change your password. If you've lost access to your account, you may need to contact the company directly, prove who you are and ask for a password reset. Choose a new password that is very different from your old one and make sure it doesn't contain strings of repeated characters or numbers. Your password should be unique for each account, complex (i.e., a mix of letters, numbers, and special characters) and at least 15 characters long.



- **Reconcile or balance your bank account every month.** The beauty of online accounts is that you can monitor them almost in real time. That means you can catch crooks long before a statement arrives in the mail.