PROTECTING YOUR IDENTITY:
WHAT TO **KNOW**, WHAT TO **DO.**

First Financial
FEDERAL CREDIT UNION

ID THEFT PROTECTION GUIDE
Information to help you fight back against identity theft.

Identity theft is the fastest growing crime in the United States. It can happen to anyone, anywhere — regardless of how careful you are, your age, income, or where you live. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money, destroy your credit, and ruin your good name. According to TransUnion credit bureau, almost 10 million incidents of identity theft occur each year. In fact, the bureau calculates that every minute, 19 people become victims, and the average cost to the victim is $500 and 30 hours.

Deter identity thieves by safeguarding your information.

- **Shred financial documents** and paperwork with personal information before you discard them.
- **Protect your Social Security number.** Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- **Don't give out personal information** on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- **Never click on links** sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to- date.
- **Don't use an obvious password** like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- **Keep your personal information** in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require your immediate attention:

- Bills that do not arrive on time.
- Unexpected credit cards or account statements.
- Denials of credit for no apparent reason.
- Calls or letters about purchases you did not make.

Inspect:

- **Your credit report.** Credit reports contain information about you, including what accounts you have and your bill paying history.
    - The law requires the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report each year if you ask for it.
    - Visit **AnnualCreditReport.com** or call 1.877.322.8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

Defend against ID theft as soon as you suspect it.

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:

Equifax:	Experian:	TransUnion:
1.800.525.6285	1.888.397.3742	1.800.680.7289

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

- **Close accounts.** Close any accounts that have been tampered with or established fraudulently.
  - Call the security or fraud departments of each company where an account was opened or changed without your permission. Follow up in writing with copies of supporting documents.
  - Use **IdentityTheft.gov** for assistance.
  - Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of your conversations about the theft.
- **File a police report.** File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.

Online: **ReportFraud.ftc.gov**
By phone: 1.877.438.4338 or TTY, 1.866.653.4261
By mail: Identity Theft Clearinghouse,
Federal Trade Commission,
Washington, DC 20580

Initial fraud alerts, credit freezes, and credit locks: What's the difference?

What you should know about	Initial Fraud Alerts	Credit Freezes	Credit Locks
Purpose	Verify your identity before extending new credit	Restricts access to credit file to prevent identity theft	
Legal protections	Based on federal law (Fair Credit Reporting Act)	Based on state law	• Based on consumer's lock agreement with each credit reporting agency (CRA) • Varies by CRA & may change over time
Fees	Free	Free	• Free from Equifax, as part of free credit monitoring service • Otherwise, CRAs may charge monthly fees • Monthly fees may change
Turning them on and off	A fraud alert: • Lasts 1 year	To freeze or unfreeze: • Online or by phone • Requires a PIN	To lock or unlock: • Online only • No PIN required

COMMON WAYS ID THEFT HAPPENS:

Skilled identity thieves can get your information hundreds of different ways. The goal of most identity theft scams is to access your credit card or bank account information directly. If you keep that in mind at all times, it can help you remain more vigilant about protecting your information and your money. Below are just some of the tactics criminals use to steal your identity.

1. Dumpster Diving

They rummage through trash looking for bills or other paper with your personal information on it.

2. Skimming

They steal credit/debit card numbers by using a special storage device when processing your card.

3. Phishing

They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

4. Changing Your Address

They divert your billing statements to another location by completing a "change of address" form.

5. "Old-Fashioned" Stealing

They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access.

First Financial
FEDERAL CREDIT UNION

732.312.1500

firstffcu.com

Your savings federally insured to at least $250,000 and backed by the full faith and credit of the United States Government

NCUA

National Credit Union Administration, a U.S. Government Agency

EQUAL HOUSING LENDER

Insured by NCUA.