



PROTECT YOURSELF FROM IDENTITY THEFT

If you think your identity has been stolen, here's what to do:

1. Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge.
2. Close the accounts that you know or believe have been tampered with or opened fraudulently.
3. File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
4. File your complaint with the Federal Trade Commission (FTC). The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.

-Source: *The Federal Trade Commission*

Tim's Work on Identify Theft:

During Tim's time in Congress, and as a member of the Senate Banking Committee, he has worked hard to provide sufficient consumer protections to South Dakotans and fight the growing crimes of identity theft and fraud.

The Fair and Accurate Credit Transactions Act (FACT Act), which he helped lead through the Senate, passed into law in 2004. This legislation will create a number of new programs to stem the tide of identity theft and protect the billions of dollars that victims, as well as the banking and credit industries, lose to ID theft each year. The FACT Act ensures that every consumer can receive one free credit report each year. By reviewing credit reports annually, consumers can determine whether there are any inaccuracies, regardless of whether they are accidental or result from identity theft.

Additionally, Tim sponsored the Identity Theft Penalty Enhancement Act (S.153) to increase criminal penalties for identity theft. Tim was invited to the White House when the new bill was signed into law by the President on July 15, 2004. The bill increases prison sentences for committing identity theft in order to commit other serious crimes by two years, and adds five years to the prison terms of anyone who commits identity theft in order to commit an act of terrorism.

For more information on Identity theft, visit:

The FTC's Identity Theft Home Page
Security through the FTC
The National Do Not Call Registry
Cross Border Fraud
Children's Online Privacy Protection Act

<http://www.consumer.gov/idtheft/>
<http://www.ftc.gov/bcp/online/edcams/infosecurity/index.html>
<http://www.ftc.gov/bcp/online/edcams/donotcall/index.html>
<http://www.ftc.gov/bcp/online/edcams/crossborder/>
<http://www.ftc.gov/bcp/online/edcams/coppa/index.html>

*To receive your credit report, contact:

Equifax - www.equifax.com
To order your report, call: 800-685-1111
To report fraud, call: 800-525-6285
Experian - www.experian.com
To order your report, call: 888-EXPERIAN (397-3742)
To report fraud, call: 888-EXPERIAN (397-3742)
Trans Union - www.transunion.com
To order your report, call: 800-888-4213
To report fraud, call: 800-680-7289

Tim advises people to get their annual credit report. Free credit reports will be available in January 2005.

U.S. Senator Tim Johnson (D-SD)

1-800-537-0025

<http://johnson.senate.gov>

Last Updated: July 16, 2004

Caution and Prudence

Here are a few simple things to keep in mind to help minimize your risk of identity theft:

1-Accessing your personal information

Avoid using easily available information, such as your date of birth or your mother's maiden name, as your pin number or password. Secure personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home. Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that your records are kept in a secure location. Ask about the disposal procedures for those records as well.

Check your credit report from all three of the credit reporting agencies to check for any inaccuracies. Also check bank statements and credit card statements to review them for any unauthorized charges.

2- Everyday Diligence

Don't give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact or are sure you know who you're dealing with.

Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail from your mailbox promptly. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to ask for a vacation hold.

Keep your Social Security card in a secure place and share your SSN only when absolutely necessary. If your state uses your SSN as your driver's license number, ask to substitute another number. If someone asks for your SSN, ask the following questions: Why do you need it? How will it be used? How do you protect it from being stolen? What will happen if I don't give it to you?

Limit the identification information and the number of credit and debit cards that you carry to what you'll actually need. Keep your purse or wallet in a safe place at work.

3- Consider Your Computer

Your computer can be a goldmine of personal information to an identity thief. Here's how you can safeguard your computer and the personal information it stores:

- Update your virus protection software regularly. Look for security repairs and patches you can download from your operating system's Web site.
- Don't download files from strangers or click on hyperlinks from people you don't know.
- Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. Without a firewall, hackers can take over your computer and access sensitive information.
- Use a secure browser — software that encrypts or scrambles information you send over the Internet — to guard the safety of your online transactions. When you're submitting information, look for the "lock" icon on the status bar. It's a symbol that your information is secure during transmission.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a "strong" password — that is, a combination of letters (upper and lower case), numbers, and symbols.
- Avoid using an automatic log-in feature that saves your user name and password; and always log off.
- Delete any personal information stored on your computer before you dispose of it. Use a "wipe" utility program, which overwrites the entire hard drive and makes the files unrecoverable.

U.S. Senator Tim Johnson's **IDENTITY THEFT FORUM PANELISTS**

July 17, 2004

ROLANDO BERRELEZ

Assistant Director, Midwest Region – Federal Trade Commission

Rolando Berrelez is the Assistant Director of the Federal Trade Commission's Midwest Region in Chicago, a position he has held since December 1999. The Midwest Regional Office covers the 11 states of Illinois, Indiana, Iowa, Kansas, Kentucky, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin.

Rolando Berrelez joined the FTC in Washington, D.C. in 1985 as a staff attorney in the FTC's Division of Financial Practices, where he enforced compliance with consumer credit protection statutes, including the Truth in Lending Act, Equal Credit Opportunity Act, Fair Debt Collection Practices Act, and Fair Credit Reporting Act. He served as a lead attorney on a wide range of complex credit and leasing cases. Among his accomplishments, Rolando has coordinated joint FTC and state enforcement actions against automobile manufacturers; filed lawsuits against a variety of fraudulent businesses engaged in deceptive credit practices; and negotiated orders against advertising agencies and computer companies. Rolando also spearheaded enforcement actions against lenders engaged in predatory lending practices.

AARON SIMON

Inspector – United States Postal Inspection Service

As a Federal Agent with the Postal Inspection Service, Aaron Simon works on "External Crimes" in South Dakota. He attended the University of Iowa and received a Bachelors degree in 1992 in Sociology. He worked for the Kansas City, Missouri Police Department from 1993 through 1995 and was assigned to Metro division where he worked in the patrol division. He then moved back to Iowa and worked as an Iowa State Trooper from 1995 through 2002, until accepting a job as Federal Agent with the Postal Inspection Service in 2002.

KEVIN STREFF

Director for the Center for Information Assurance -- Dakota State University

Kevin Streff is the Director for the Center for Information Assurance at Dakota State University, a national Center of Academic Excellence in Information Assurance Education through both the National Security Agency and the Department of Homeland Security. Streff has fifteen years of experience implementing and supporting technology in the banking and finance sector, and currently teaches Risk Assessment, Compliance, Security Management, and Security Policy courses for the university in both the undergraduate and graduate Information Assurance programs. Streff also does a lot of work with banks both large and small to improve the security posture of the banking sector.

SERGEANT ROBERT THOMPSON

Detective Division Fraud Unit Supervisor – Sioux Falls Police Department

Sgt. Bob Thompson is a lifelong Sioux Falls resident. Thompson has been a police officer in Sioux Falls for more than 29 years and has served as the Detective Division Fraud Unit supervisor for the past 7 years. He has worked in all areas of the department, including patrol, investigations, training, records, and community services.

LANEIL BARTELL

Project Manager – First PREMIER Bank

LaNeil Bartell is a project manager at First PREMIER Bank and has worked with the company's Identity Theft education and awareness program, reacting to customer concerns and providing tools to combat identity theft. Ms. Bartell's 20 years of experience at First PREMIER Bank are invaluable in helping customers combat identity theft. In 2002, Ms. Bartell received her AAP (Accredited ACH Professional) designation. AAPs work with financial institutions to plan their payments strategies and manage other payment services. In 2001, 2002, and 2003, First PREMIER Bank was recognized by the ABA Banking Journal as the top performing financial institution of its size in the country.