Colorado Legislative Council Staff

ISSUE BRIEF

Number 02-07 A Legislative Council Publication October 28, 2002

IDENTITY THEFT WITH SOCIAL SECURITY NUMBERS

by Jennifer Moe

Identity theft is one of the fastest-growing crimes nationwide. Identity thieves seek a social security number (SSN) because it is a common link to multiple pieces of someone's personal information, such as financial or medical records. From 1999 to 2001, complaints about identity theft increased by 575 percent, and identity theft complaints related to SSN misuse increased by 67 percent.[1]

Identity theft is a federal felony pursuant to the 1998 Identity Theft Act. While identity theft cannot be prevented, individuals can minimize their risk by understanding the legitimate use of SSNs for business transactions, and by carefully managing their personal information. This *Issue Brief* addresses these matters, and provides resources for those who suspect they are a victim of identity theft.

The Use of Social Security Numbers

According to the Federal Trade Commission, identity thieves generally obtain someone's SSN from an everyday transaction, such as applying for a credit card or writing a check. An SSN is commonly required by entities to conduct specific business, such as:

- wages and tax reporting (an employer);
- tax reporting (a financial institution);
- running a credit check (a lender);
- applying for a driver's license (the Colorado Department of Revenue); and
- applying for a marriage license or a child support order (the Colorado Department of Human Services).

The federal Privacy Act of 1974 requires any government agency requesting an SSN to inform the individual of five things:

1. by what law or other order the SSN is being solicited;
2. whether disclosure is required or voluntary;
3. why the SSN is needed;
4. how the SSN will be used; and
5. what will happen if the person does not provide the SSN.

Government agencies may not deny privileges or benefits to an individual who refuses to provide an SSN, *except under the following circumstances*:

- disclosure is required by federal law; or
- the agency used SSNs for record-keeping prior to 1975.

Although Colorado does not have a statewide policy governing the collection and use of SSNs by government agencies, many state agencies have such guidelines established in statute or by rule. Individuals should inquire about these guidelines when their SSN is requested by a state agency.

Some businesses request an SSN for record-keeping purposes only. To determine whether to give an SSN to a business requesting it, the Federal Trade Commission suggests asking the five Privacy Act questions. In addition, a person should ask whether another identifier may be used. A business may choose not to provide services or benefits if an individual chooses not to provide an SSN.

1. As measured by the Federal Trade Commission hotline and the Social Security Administration Fraud hotline.

Minimizing Your Risk

To prevent identity theft, the Federal Trade Commission advises individuals to only give out their SSN when necessary, and suggests four ways to minimize the risk of identity theft related to SSN misuse.

- Do not use any numbers from your SSN as a password.
- Do not carry your social security card with you.
- Do not give out your SSN on the phone, through the mail, or on the Internet unless you initiated the contact or know who you are dealing with.
- Tear or shred discarded documents that have your SSN printed on them.

Contacts for Victims

A person who suspects that his or her identity was stolen should file a police report in the community where the identity theft occurred, and keep a copy of the report as proof of the crime. In addition, the Federal Trade Commission encourages victims to contact two hotlines to report the crime and obtain assistance in reclaiming their identity. Finally, victims should report the situation to the three main credit reporting bureaus and any affected creditors.

Federal Trade Commission (FTC) Identity Theft Hotline. The 1998 Identity Theft Act made the FTC a clearinghouse for complaints about identity theft. The FTC provides information about identity theft and helps victims resolve problems resulting from the crime. Victims can contact the FTC Identify Theft Hotline at 600 Pennsylvania Avenue, NW, Washington, D.C. 20580; www.consumer.gov/idtheft; or 877-438-4338 (toll-free).

Social Security Administration (SSA) Fraud Hotline. The SSA Office of the Inspector General is one of several federal law enforcement agencies that investigates identity theft. Victims may report stolen or misused SSNs to the SSA Fraud Hotline at P.O. Box 17768, Baltimore, MD 21235; www.ssa.gov/oig/guidelin.htm; or 800-269-0271 or 800-772-1213.

The Three Main Credit Reporting Bureaus. Victims of identity theft should contact the fraud departments of the following credit reporting bureaus to report fraud and obtain a credit report.

Equifax
P.O. Box 74025, Atlanta, GA 30374-0241
www.equifax.com
Report fraud: 800-525-6285
Order a credit report: 800-685-1111

Experian
P.O. Box 1017, Allen, TX 75013-0949
www.experian.com
Report fraud/order a credit report: 888-397-3742

Trans Union, Fraud Victim Assistance Dept.
P.O. Box 6790, Fullerton, CA 92834
www.tuc.com
Report fraud: 800-680-7289
Order a credit report: 800-916-8800

Explain that you are a victim of identity theft, and:

1. request that a fraud alert be placed on your credit file;
2. obtain a copy of your credit file from each credit bureau and review it carefully, looking for additional accounts or unauthorized changes;
3. request that fraudulent accounts opened by a company and listed under the "inquiries" section be removed from your report; and
4. order copies of your report several months later to verify that your requested changes were implemented and that no new fraudulent activity has occurred.

Affected Creditors. Victims of identity theft should also contact the fraud department of creditors for any account in which fraudulent activity has occurred. Close the accounts, and open new accounts with new personal identification numbers (PINs). Follow up any phone conversations with a letter detailing the request.