

First Friday Fraud Facts+

April 4, 2014



QUESTIONS OR COMMENTS:

Chris Floyd, CPA
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8814

Fax: (208) 334-3415

E-mail: cfloyd@sco.idaho.gov

Inside this issue:

Welcome	1
Identity Theft	1
Tax-related Identity Theft	1
Child Identity Theft	2
Medical Identity Theft	2
Prevention	3
Announcements	3

The Idaho State Controller's Office distributes this newsletter as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.

Welcome to First Friday Fraud Facts+ (F4+). This edition will discuss identity theft.

Identity theft has become a rampant form of life-altering thievery. We live in a world that is very much dependent on communications connectivity, which in turn creates an abundant number of opportunities for fraudsters to get their hands on personal information other than their own. Identity theft wreaks havoc on people's finances, credit histories, and reputations. And while it seems as if the thievery happens just that quickly (snap your fingers here) and easily, trying to put your life back in order can take a lot of time, money, and patience.

According to the Federal Trade Commission (FTC), there are three specific types of identity theft:

- Tax-related identity theft
- Child identity theft
- Medical identity theft ¹

Tax-related identity theft

Under the auspices of the New Deal, President Franklin D. Roosevelt signed the Social Security Act in 1935, and the first Social Security Number (SSN) was issued the following year^{2,3}. Today, in order to access government services (at any level), apply for a job, get a credit card, or gain access to any number of products and services a person must have an SSN. This 10-digit personalized number has risen to great prominence and notoriety.

The Internal Revenue Service (IRS) uses your SSN to ensure your tax filing each year is accurate and complete and that you receive the appropriate refund. If a person with malicious intentions obtains your SSN, they can file a tax return in your name and receive the refund intended for you.

Someone can use your SSN to apply for and get a job. Employers use



your SSN to report payroll information to the Federal government. If you receive a notice that you did not disclose all of your income after filing your annual tax return, you may be a target of tax-related identity theft. Another employer, besides the one you work for, is reporting additional income that you did not earn.

Red Flag: You receive a letter from the IRS indicating they have identified a problem.

What can I do?

- Contact the IRS as soon as possible and work with a specialist to rectify the situation.
- Place a fraud alert on your credit reports.
- Order credit reports to identify suspicious activity.
- Submit an *Identity Theft Report* to the FTC.

Child Identity Theft

Fraudsters can be unscrupulous. A fraudster can use a child's SSN to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live.

Red Flags:

- Your child is turned down for government benefits.
- You receive a notice from the IRS stating your child did not pay income taxes.
- You receive collection calls or bills for products or services you did not receive.

What can I do?

- Check to see if your child has a credit report.
- Contact each credit reporting agency and business where your child's information was misused to remove and close accounts.
- Place a fraud alert on your child's credit report.
- Submit an *Identity Theft Report* with the FTC.

Medical Identity Theft

A thief can use your name or health insurance numbers to visit a doctor, receive prescription drugs, or file claims with your insurance provider. This could cause problems with receiving treatments for yourself, your insurance and payment records, and your credit report.

Red Flags:

- The names, dates, and services provided as annotated on your *Explanation of Benefits* do not accurately match reality.
- You receive a call from a debt collector for medical debt you do not owe.

- You receive a notice from your health plan stating you have reached your benefit limit.
- You are denied insurance because your medical records show a condition you do not have.

What can I do?

Send certified letters, asking for “return receipts”, to your health plan and medical providers to explain which information is incorrect. Send copies of supporting documentation.

PREVENTION

- Lock your financial documents and personal records in a safe place.
- Limit what you carry. Leave your Social Security card at home.
- Before sharing personal information, find out why the person needs it, how it will be safeguarded, and what will happen if you do not share it.
- Shred it if you do not need it any more.
- Destroy labels on prescription bottles.
- Beware of phishing emails.
- Remove memory and SIM cards from mobile devices to be discarded.
- Do not share passwords.

¹ Identity Theft, <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>. Accessed February 13, 2014.

² Social Security FAQs, <http://www.ssa.gov/history/hfaq.html>. Accessed February 13, 2014.

³ The First Social Security Number and the Lowest Number, <http://www.ssa.gov/history/ssn/firstcard.html>. Accessed February 13, 2014.

ANNOUNCEMENTS

Annual Internal Control Training held at the State Controller’s Office:

a) Tuesday, April 15, 2014, from 10:00 a.m. — 12:00 p.m.

OR

b) Wednesday, April 16, 2014, from 8:00 a.m. — 10:00 a.m.

Learn why internal controls are important to your organization and who is responsible for ensuring they are practiced. The training will cover the objectives of internal controls, including the COSO’s 17 principles, and a round table style discussion, which will provide participants an opportunity to share their internal control concerns, insights, and receive feedback.

CPE: 2 Free

Registration details coming soon.

