First Friday Fraud Facts+

May 1, 2015

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 synthetic identity theft.

Synthetic Identity Theft

We all know how identity theft works (also known as "true-name" identity theft). Someone steals your social security number and other personal information and masquerades opening new credit card accounts and loans, filing fictitious tax returns, or receiving medical benefits in your name (see the April 2014 First Friday Fraud Facts+ newsletter). However, fraudsters have put a new spin on identity theft called *synthetic identity theft*.

Synthetic identity theft occurs when someone steals your social security number but then uses bogus or other people's identifying information to create a person who does not exist. With a new identity, a thief opens new credit card and bank accounts or gets a job and slowly creates a legitimate-looking credit history. In the meantime, the fraudulent activity goes unnoticed because all of the disparate pieces of information confuse computer programs designed to match a person's information to a dataset - name, address, Social Security number, and birthdate. Instead, the system sees what appears to be a legitimate "person". The Social Security number may match someone else's, but the name, address, and birthdate are all different.

As this new identity's credit history grows and strengthens, so also do credit limits and the trust of creditors. The thief then performs a "bust out" by taking out a significant cash advance, making some very large purchases or a lot of smaller purchases of items that can be re-sold very quickly (gift cards, electronics), or simply walking away from a loan. This creates two significant problems: 1) Creditors find it extremely difficult, if not impossible, to track down the thief, and 2) the person whose Social Security number is stolen now has a tainted credit history, which, ironically, will make it very difficult for the person to legitimately obtain credit.

Synthetic identity theft has increased exponentially over the last five to seven years. One estimate puts synthetic identity theft responsible for 20 percent of credit charge-offs and 80 percent of losses from credit card fraud.[1]

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
Synthetic Identity Theft	1
Difficult to Catch, Difficult to Overcome	2
What Can I Do?	2
Fraud Cases	2
Announcements	3

Difficult to Catch, Difficult to Overcome

There are several reasons why it is difficult to detect and overcome synthetic identity theft:

- Synthetic identity theft cases are difficult to identify with any one person. "Reviewing credit data may not reveal accounts created by synthetic identity theft because of the mixture of real and false information leveraged to construct the identity."[2]
- Fraudsters will typically use social security numbers of children and senior citizens, two groups who do not typically use credit very often. If the Social Security number of a newborn child is used, it could be 18 years or longer before anyone realizes what has happened. During this time the child's Social Security number could be fraudulently used repeatedly by the same person or by multiple people.[2]
- The Social Security Administration began issuing SSNs in random order in 2011 to help protect people against identity theft. However, this has allowed for the propagation of synthetic identity theft, making it much more difficult for antiquated anti-fraud tools to detect false identities.[2]
- Thieves use creditors' current security measures against them. For instance, hackers can cross-reference stolen credit card numbers with Social Security numbers obtained from another source. They then call the issuing bank requesting to change the credit card PIN. The bank requires the person to provide a name and Social Security number; once provided by the hacker, the bank changes the PIN.[3]

What Can I Do?

1) Review your annual Social Security Statement ensuring your reported income is not overinflated.
2) Be suspicious of mail sent to your home addressed to someone else.
3) Review credit reports annually, looking for inaccurate information and unauthorized accounts.
4) If a creditor denies you credit, review the denial letter and question the creditor to validate that the lender based its decision on your identity.
5) Consider subscribing to an identity theft protection service.[4]

Fraud Cases

In August 2006, James J. Rose was indicted for devising a scheme to defraud multiple financial institutions issuing credit cards. He and his partner used a small consumer reporting agency to steal valid Social Security numbers to create synthetic identities. One of his synthetic frauds included using a person's real Social Security number to apply for a credit line under a fabricated name. He and his partners obtained over 250 credit cards from 15 different banks, charging roughly $760,000 to these synthetic identities.

In February 2013, federal agents arrested 13 people for creating roughly 7,000 fake identities to steal approximately $200 million from multiple lenders. The perpetrators found unused Social Security numbers sourced through Craigslist listings that solicited individuals who were not credit active to willingly offer up their credentials. The fraudsters used "drop addresses"

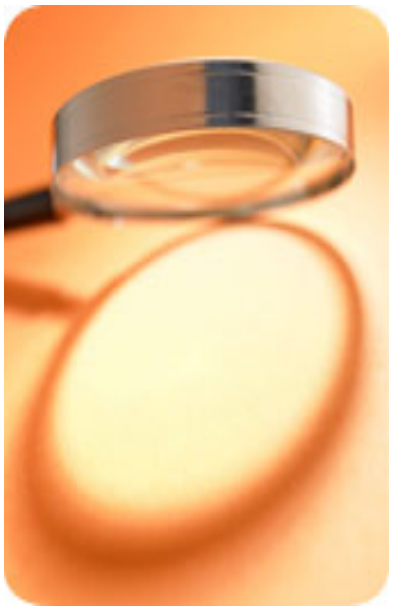
as mailing addresses for the false identities and created sham companies that accepted credit card payments. After obtaining the cards, the fraudsters made small charges and paid off the cards to raise their credit limits and create a strong credit history. With the help of a strong credit history, the thieves secured a large loan, which they then defaulted on leading to a significant financial loss for the lender.[5]

1. Synthetic Identity Fraud A Fast-Growing Category. http://www.darkreading.com/synthetic-identity-fraud-a-fast-growing-category/d/d-id/1316830. Accessed March 30, 2015.
2. Money Talk: Synthetic identity theft causing big headaches. http://www.dallasnews.com/business/columnists/pamela-yip/20140831-synthetic-identity-theft-causing-big-headaches.ece. Accessed March 30, 2015.
3. Spike in Fake ID Schemes Confounds Banks' Fraud Filters. http://www.americanbanker.com/news/bank-technology/spike-in-fake-id-schemes-confounds-banks-fraud-filters-1072377-1.html. Accessed March 31, 2015.
4. Synthetic Identity Theft. http://www.protectmyid.com/identity-theft-protection-resources/types-of-fraud/synthetic-identities.aspx. Accessed March 31, 2015.
5. The Long Con: An Analysis of Synthetic Identities. http://www.idanalytics.com/media/WP_Synthetic-Identities_FINAL-WEB_101714.pdf?mkt_tok=3RkMMJWWfF9wsRokv6zMZKXonjHpfsX56uovXKO2lMI%2F0ER3fOvrPUfGjI4ATMFqI%2BSLDwEYGJlv6SgFT7TEMblz07gKXhE%3D. Accessed March 31, 2015.

ANNOUNCEMENT

Annual Closing Package Training held at the State Controller's Office:

- ⇒ 13 May - Intermediate training (8:30am-10:30am)
- ⇒ 14 May - Beginning training (8:30am-10:30am)
  Intermediate training (1:00pm-3:00pm)

The beginning session is intended for those new to the reporting process and includes a comprehensive tour of all GAAP closing packages, changes made to the packages, challenges encountered in prior years, and review of new accounting standards.

The intermediate sessions are intended for those who are experienced with the reporting process and include a review of changes to the GAAP closing packages, challenges encountered in prior years, and review of new accounting standards.