White Paper

Identity Fraud Prevention

How to Detect and Prevent Identity Based Fraud in Government.

June 2012

Author: Andrew Bucholz
Vice President of Market Planning – Government
LexisNexis Risk Solutions

LexisNexis®

Table of Contents

Fraud is on the Rise

Over the past 10 years, government programs have become highly vulnerable to fraud. There is evidence that fraud has permeated virtually every government-based benefit program at the state, local and federal level – but the problem goes beyond social programs. Tax refunds have become a major target and even non-monetary programs like passports and driver's licenses make the list. Fraud is now so pervasive that estimating its cost has become impossible, with suggestions ranging from two-three percent to as high as five percent of total outlays. In light of the current economic climate, agencies across all government branches can no longer be passive when it comes to fraud.

The impact of this theft is far-reaching. Layoffs are now common at all levels, reducing critical services and directly impacting citizens. Unfortunately, the reduction of critical investigators and tax assessors only aids the criminals' ability to remain undetected. In some areas of the country, the economic impact has become so devastating that some jurisdictions have been forced into bankruptcy. While the government has a responsibility to provide for public safety, schools, and those that are in need, there is also a responsibility to minimize the tax burden on citizens by ensuring that refunds and benefits are not sent to ineligible parties or support illegal activities.

The Role of Identity Theft

Today's fraud schemes are largely being perpetrated by widespread identity theft. This should come as no surprise, since many government programs only require four key data-points to confirm identities and distribute funds or benefits:

Name

Address

Date of Birth (DOB)

Social Security Number (SSN)

This hasn't always been the case. Twenty years ago, if you wanted to apply for unemployment benefits you had to go to a government office and sign up in person. Individuals had to show multiple forms of identification – similar to the way the Transportation Security Administration screens the identities of airline passengers today. This presented a barrier to fraudsters who wanted to steal identities, since they would have to furnish hard-copies of fake documents – and would have to show up in person for each instance of fraud. Back then, criminals risked capture each time they perpetrated fraud. As a result, instances of fraud in these programs was low and the fraud that did occur was largely due – not to identity theft – but to legitimate beneficiaries who continued collecting after gaining employment.

With the Internet, government agencies recognized that it made good sense to allow people to register online. This was more convenient and required less man-power from the government agency. Unfortunately, without person-to-person contact, people used stolen identities or the identities of those who were ineligible (e.g., prisoners, deceased persons, etc.) to gain access to these payments. Because many government programs evolved before Internet fraud became pervasive, these organizations now find themselves ill-equipped to mitigate today's unprecedented levels of fraud.

In spring 2008 – before the financial crisis – the irs identified 50,000 cases of taxpayer identity theft. The next year that number had tripled to nearly 170,000.

In 2010, the number of identity theft cases doubled again.

How it Happens

There are widespread misconceptions about the origins of identity theft, both among government managers and the general public. Media reports might suggest that the vast majority of identity theft takes place through computer hacking. Data compromises at a wide range of companies, including banks and online retailers, have perpetuated this stereotype. However, while these breaches do present a threat to those businesses, they rarely represent a meaningful slice of identity theft as perpetrated against government programs.

Yet another misperception is that identity theft is largely the result of online phishing schemes. This occurs when an individual is sent an official-looking email from a trusted source – such as a bank – that asks them to follow a link and enter personal financial information. Phishing remains a powerful tool for criminals and companies continue to innovate to find ways that protect consumers and preserve email as a trusted communication avenue. These schemes do not play a major role in identity theft against government agencies either, since criminals are generally interested in gaining immediate economic rewards through credit card numbers and other sensitive financial data.

A few decades ago, when identity theft was first beginning to make headlines, citizens were availed with widespread reports of criminals' dumpster-diving for sensitive information printed on mail that was thoughtlessly tossed away. The solution many proposed: shredding your junk-mail. But it's been 10 years since companies last sent names, addresses, and SSNs through the mail. Today, the pickings are just too slim – and alternative means too available – for dumpster-diving to represent a viable means for identity-based fraud.

So, how are fraudsters perpetrating identity theft? They are targeting places wherever individuals leave their SSNs. A quick survey yields a surprisingly long list. It includes virtually everywhere a citizen might fill out paperwork or application forms:

Doctor's Offices

Dentist's Offices

Public Schools

Real Estate Offices

Universities

Loan Offices

Car Dealerships

And anywhere that houses employee records. Which is anywhere.

In many of these facilities, sensitive personal information – name, address, DOB, SSN – sit in unlocked filing cabinets which nearly any employee has access to. What's worse, these files are rarely purged, even after an individual severs their relationship with an organization.

Fraudsters plant people at these locations – or take advantage of their current employers – in order to gain access to these identities and file for false tax returns or other government benefits. The examples are growing:

- A report from CNN in March 2012 highlighted how criminals are using laptops and free WiFi connections to file false tax returns with information gleaned from insiders at hospitals, doctor's offices, and car dealerships.
- A report from KVOA.com in November 2011 highlighted how a single community college lost $270,000 in student loan fraud through identity theft.
- A report from CourthouseNews.com in March 2012 detailed how an Illinois woman masterminded a seven year unemployment fraud scheme by filing false claims in the name of undocumented immigrants and using stolen SSNs to amass over $700,000.
- A report from ABC News in April 2012 explained how a manager at the Long Island Head Injury Association stole the identities of 56 patients to file false tax returns.
- A report from the *Salt Lake Tribune* in April 2012 unveiled a disturbing trend: fraudsters stealing the identities of children to perpetrate fraud ranging from unemployment to food stamp programs.
- A report from the *Burlington Free Press* in April 2012 detailed how a fraudster filed false tax returns using the information of 55 current and former employees of a Hampton Inn.

Often times, individuals don't realize that their identities have been stolen until government agencies like the Social Security Administration or the IRS tell them that somebody has already filed in their name. Since fraudsters are typically among the first to file, the IRS tried to curb the trend this year by delaying early tax returns in hopes of curbing abuse. But all returns weren't subject to the same scrutiny. The majority of refund checks are issued before the government has a chance to verify W-2s. In the case of some, that means a quicker path to the bank.

The Climate for Fraud

There are a number of factors that together have created an opportunity for individuals to capitalize on this type of deception:

Technology - Reliance on the Internet to file for benefits or tax returns reduces face-to-face contact and the use of hard forms of identification (like driver's licenses and passports).

Numerous Government Agencies - With multiple paths to filing for benefits, fraudsters can often exploit multiple agencies without being caught.

Parallel Programs - Fraudsters can exploit local, state, and federal authorities, often using the same stolen identities over and over again.

Lack of Data and Data Sharing - Agencies rarely share real-time information across government boundaries and often lack access to other public but non-governmental sources.

Breached SSNs - SSNs are at the heart of most government benefits programs but are becoming easy targets for criminals.

Dependence on Self-Reported Data - Agencies trust citizens to report accurate and timely information. While many do, others exploit this trust to game the system.

All of these factors have contributed to a climate where fraud can easily take root.

How Agencies Try (and often fail) to Catch Fraud

Current methods to fight fraud center on building a system that flags suspicious requests based on rules for matching governmental data against each other. This rules-based method alerts government agencies to fraudulent schemes such as multiple checks going to the same account, suspiciously high dollar amounts, and use of previously-suspicious accounts. There are limits, however, to the effectiveness of these systems in rooting out major fraud schemes.

Rules-based systems cannot see outside of an agency's own historical data repositories. This provides the system with a very narrow view of the citizen. As a result, when a fraudster presents the system with a false SSN, the government agency may mistakenly assume that the SSN represents a new citizen – and therefore provide the applicant with the requested benefit. Fraudsters have learned that to defraud rules-based systems they only need to tell the system a lie it cannot detect.

> "Fraud is always changing, but the thing that stays constant is that it usually takes advantage of a jurisdiction or agency that has a very narrow view of self-reported data."

How to Stop It

Identity-based systems can find those lies. They expand fraud detection significantly beyond the traditional rules-based system by accessing national repositories of identity information. This provides the government agency with a national view of an individual culled from multiple sources. For instance, privately-operated public record repositories combine identity, asset and address information to help agencies assess the validity of self-reported information.

Identity-based detection is powerful because it does not treat self-reported data as the truth. For example, a common rule in many rules-based filters is to match the name, SSN and address from the presented information with the name, SSN and address on-file. This rule ensures that an applicant's self-reported data aligns with the other information held by the agency. But matching data does not confirm an individual's eligibility. Common fraud schemes center on mis-reporting an SSN to avoid the "Do Not Pay List," or involve fabricated or false identities that have been nurtured through multiple filings over the course of years.

Yes, the filer may have provided a valid name and SSN on file, but…

- …the individual is locked in a prison.
- …the individual has been dead for 10 years.
- …the individual has never lived at the requested address.

Rules-based systems do not, and cannot, find these extremely risky and fraudulent returns. Identity-based detection provides insight into these instances by checking data against a broader repository.
Using an identity-based approach, agencies can help flag the following fraud scenarios:

Stolen Identity - A common scheme involves a fraudster obtaining information on recently deceased people, infirm patients, etc. to obtain fraudulent benefits/money.

Providing a False Address - A fraudster will sometimes provide an address that the true person is not affiliated with.

Identity Masking - Sometimes fraudsters will know they owe child support, another type of non-tax debt, or have a tax lien and will mask their identity by altering their SSN to avoid detection via a "Do Not Pay List."

Misrepresentation - A common fraud scheme is for people to misrepresent themselves to gain a payment that they are not entitled to receive.

Fraud Rings - Multiple payments going to the same address; for the same amount of money but to different identities; to prisons; or to the recently-deceased at a common address for similar refund amounts.

Strong results have been seen in several states who have implemented an identity-based fraud system. By employing industry-leading technologies and matching applications and tax filings against state and national public records, agencies are able to accurately identify fraud and improve their effectiveness to the citizen.

Check out our Fraud of the Day Forum at: fraudoftheday.com

For more best practices around identity in the government space, contact LexisNexis:
www.lexisnexis.com/government
888.579.7638

About LexisNexis® Risk Solutions
LexisNexis® Risk Solutions (www.lexisnexis.com/risk/) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity and discovering and recovering revenue. For more information, visit www.lexisnexis.com/government.

LexisNexis®