White Paper

Identity Risk Framework

A new perspective on how to protect government programs against identity fraud in today's digital world.

April 2014

Author: Steve Lappenbusch, Ph.D.
Government Strategic Market Planner
LexisNexis Risk Solutions

LexisNexis®

Identity theft is the fastest growing crime in America. To protect government programs against identity-theft related fraud by assessing the risk of an identity, you have to understand the identity risk outside of government data.

Executive Summary

This document tells a story that affects every one of us. Every day, our personal identities are being sought by criminals. In fact, identity theft is the fastest growing crime in America today. On average, an identity is stolen every 3 seconds – about 27,000 per day. In 2012, over 12 million Americans were victims of identity theft. Furthermore, there have been a record number of security data breaches in recent years that have exposed some 822 million records, compromising individuals' personal information such as name, Social Security number (SSN) or bank account. The likelihood that – at some point in our lives – each of us will fall victim to a data breach or identity theft is alarmingly high. This opening story describes fraud committed against the government on a daily basis. These fraud schemes often begin with tax fraud, but then also lead to benefits fraud and fraud against the justice system. No sector of government is immune for the simple reason that the government cannot possibly know all there is to know about a person's identity footprint and this is advantageous to identity thieves. Identities are always bigger than the government. Criminals are also taking advantage of the vast quantities of confidential personal data that is transmitted online and are using this information against us – and they are winning.

Three Important Facts

There are three critically important things LexisNexis has learned that can help government stop the current epidemic of identity fraud. All three things challenge current assumptions in every government system.

1) **Everyone's identity has already been compromised.**
2) **Government programs cannot possibly know all there is to know about a person's identity. Identities are always bigger than the government.**
3) **To assess an identity for risk, you have to understand identity risk outside government data.**

A Story of Identity Fraud against the Government

To provide context to these three facts, I will begin with a story about tax refund identity fraud. But the costs to our nation do not end there, however. This is not a true story per se, but a collection of all the different identity fraud schemes LexisNexis has seen perpetrated by criminals using our own identities against us. Every single fraud in this story has happened in government systems, and is almost certainly still happening right now. All costs are based on average costs publicly reported by the respective government agencies. It is a story of systemic identity risk beginning with tax refund fraud.

This story begins with a man named Sam. Sam walks into a roofing company to get a job. He presents an identity to Gladys, the office manager. He looks like a nice young man who is willing to work hard. Because his documents look good to Gladys, she makes copies, completes his I-9 and starts his withholding with the federal Electronic Federal Tax Payment System (EFTPS). Except Sam lied to Gladys – she's not aware that he's skipping out on a $6,000 per year child support order and a $10,000 tax lien. However, Sam now has a perfect W-2 using a false identity through multiple channels, including XYZ Roofing, EFTPS for federal withholding and the state labor department. These kinds of false identities in government withholding happened over 9 million times last year according to the Social Security Administration (SSA)[1]. Since the federal program known as Temporary Assistance for Needy Families (TANF)

fills the void when child support is unpaid, the unpaid child support (about $100 billion per year nationwide[2]) and unintercepted tax liens ($135 billion at the federal level alone)[3] are just the first costs to taxpayers before a single fraudulent refund is even issued.

Next, Sam does the same thing a dozen times around town, a new fake identity with each employer. He makes sure to quit or get laid off. He's only in it for the fraudulent W-2s. With those W-2s and 200 more identities he bought off a Russian website for $200, he files hundreds of fraudulent tax returns, loaded up with refundable credits like Earned Income Tax Credit (EITC) and four fake children. Sam files 212 returns, and 112 returns get paid the average 2012 EITC amount, for a total of $600,000.[4]

Sam calls into XYZ Roofing to get his fake W-2 sent to his real address. Gladys, the office manager, tells Sam that XYZ Roofing is in financial trouble. Sam goes to talk to the owner, and tells him he can save XYZ Roofing and it won't cost the owner a dime. Sam teaches the owner tax refund fraud, and they file fraudulent returns using identities from former employees. That's another $1 million stolen from taxpayers.

Fraud Type	# of IDs	Average Payment $	Annual Total $
Tax Refund Fraud w/ EITC	112	$ 5,372	$601,664
Tax Refund Fraud via Employer	200	$ 5,372	$1,074,400
UI	50	$ 300	$180,000
SSI	10	$ 1,130	$135,600
Child Care Stipend	20	$ 552	$132,480
SNAP	312	$ 275	$514,800
TANF	50	$ 428	$256,800
			$2,895,744

Next, they use XYZ Roofing employee tax identities to steal unemployment insurance. The business owner uses E-verify to find 50 former employees that do not verify with the Social Security Administration (SSA) and reactivates withholding, fully knowing they are fraudulent tax identities and no one will complain. He puts the fake workers on minimum payroll for the minimum time and then "lays off" the pretend workers. Sam and the owner then collect unemployment insurance for each pretend worker for 99 weeks. That's another $180,000.[5]

Next, they defraud Social Security Disability (SSI Disability). Sam and the owner report 10 of the fake workers as "injured on the job." Sam visits 10 sympathetic doctors under 10 false identities to claim back pain and the inability to work, or just pays off one doctor. Each SSI payment is worth approximately $14,000 per year, paid monthly.[6] That's another $135,000. The total cost to the taxpayers is now over $2.2 million.

1 http://seniorsleague.org/2013/growth-of-the-social-security-earnings-suspense-file-points-to-the-rising-potential-cost-of-unauthorized-work-to-social-security-2/
2 http://money.cnn.com/2012/11/05/news/economy/unpaid-child-support/
3 Fiscal Year 2011 Report to the Congress. U.S. Government Receivables and Debt Collection Activities of Federal Agencies. Dept. of the Treasury, June 2012.
4 http://www.irs.gov/Individuals/Preview-of-2012-EITC-Income-Limits,-Maximum-Credit--Amounts-and-Tax-Law-Updates
5 http://www.cbpp.org/cms/index.cfm?fa=view&id=1466
6 http://www.ssa.gov/policy/docs/quickfacts/stat_snapshot/

All of these fake identities are below the poverty line. They qualify for social assistance, and if you are on SSI Disability, you are almost guaranteed food stamps and child care stipends. The government's Supplemental Nutrition Assistance Program (SNAP) does not even require a SSN to apply. Sam and his accomplice get SNAP for all 312 identities, Child Care for 20 and TANF for 50. The SNAP gets cashed out at a 50% discount at unethical convenience stores. Combined taxpayer costs from TANF, SNAP, and Child Care from these fraudulent tax identities are over $900,000.[7][8][9]

In case you've lost count, the total cost to taxpayers is now almost $2.9M, ($1.7M of it from tax fraud), and this all occurred within 12 months.

Now imagine Sam goes out and gets drunk to celebrate. While intoxicated, he gets in his car to drive home and rams a parked car. The police show up. Sam gets belligerent and punches the police officer. Sam goes to jail. Sam has never been fingerprinted before. Most people haven't. Sam has no ID on him, but he claims he is the individual from his fake identity, the one he presented to Gladys at Roofing XYZ.

The police interrogate Sam, asking about the cash and SNAP debit cards in his trunk. Sam rats out his employer at XYZ Roofing in exchange for a plea bargain. A full investigation unfolds, and the detectives take all the records from XYZ Roofing, which reinforces, in W-2 records, that Sam is who he fraudulently claims to be.

Sam spends 12 months in jail under his fake XYZ Roofing ID. When he's paroled, as a matter of policy, the state DMV issues Sam an official, authentic identification card for the identity he just served time under. Sam now has convinced the government to create an actual, authentic new identity for him.

While the specific details described are fiction, the scenario is very true. It is a form of identity fraud that happens across the country as identity criminals use our own identities, and the assumptions of systems, against us.

The financial impact that often begins with tax refund fraud is startling. This is because the government cannot see enough of our identities or analyze them expertly enough to keep Sam, or larger transnational criminal enterprises, from using our own identities against us.

With the context of this identity fraud story, each of the three facts can now be explored in turn: 1) Everyone's identity is already compromised, 2) Identities are always bigger than the government, and 3) To assess an identity for risk, you have to understand identity risk beyond government data.

All Identities are Already Compromised

Your identity, my identity, everyone's identity is already compromised and/or is being relentlessly sought after by criminals. All of the discussion and effort amongst governments to prevent identity theft is laudable, but too late. Identities can be bought online for as little as 9 cents - Name, SSN, DOB, and Driver's License included. Trying to protect identities will not stop the exploding epidemic of identity fraud perpetrated against the government, particularly in tax evasion and tax fraud. The raw identity material is a mouse click away. That is the only safe assumption given the vast amount of personal data available online.

7 http://www.americanprogress.org/issues/labor/news/2012/08/16/11978/fact-sheet-child-care/
8 http://www.fns.usda.gov/pd/19SNAPavg$HH.htm
9 http://www.cbpp.org/cms/?fa=view&id=4034
10 http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/

Since 2005, according to the Privacy Rights Clearinghouse, over 660 million identity records have been exposed.[11] **The Open Security Foundation cites over 822 million compromised identities in 2013 alone.**[12] Those are just the publicly reported breaches, and according to the government, an estimated 40 percent of identity breaches are never detected.[13] The true number of private breaches is unknown as many businesses do not even know they have been breached. And even for those publicly reported in the much lower Privacy Rights Clearinghouse figure, almost half do not list how many records were exposed. If you multiply those reported without a total by the average number of records exposed in the other reports, you get over 1.1 billion identities exposed since 2005. Even subtracting Asian and European identities, with 318 million Americans that means the most conservative numbers available indicate that **on average, every American's identity has already been compromised in some fashion at least three times**. The higher Open Security Foundation figure indicates that this has occurred within a time frame of the last 12 months. Increasingly, the perpetrators who are after our identities are organized crime and transnational criminal organizations.[14][15][16] What this means for stopping identity fraud in government is that protecting our identities from criminals is not enough, and it is not the right focus. **We must focus instead on protecting ourselves from criminals who are using our own identities against us. Because they will not stop until they have them all**.

Simply put, we are losing the war on identity theft. Our identities are freely available for pennies a piece on the Internet. It is time to start defending ourselves against identity crime where the fraud weapons used against us are our own identities. This is a fundamental change in the assumption around identities in government systems. Self-reported data must all be suspected, as all identities are compromised. Once the identity is assumed to be stolen, a whole new approach in identity risk analysis must be used. Proceeding from the new, data-driven assumption that all identities are already stolen enables the government to think outside the traditional box of identity protection and begin thinking in terms of risk – identity risk. Specifically, how do tax agencies control the risk of all those stolen and synthesized identities hitting their tax systems – tax systems never originally designed for a world where you could not depend on the identity presented?

This identity risk analysis, rather than data matching, approach has proven effective at the state level. Primarily this means analyzing input tax identities against identity information far outside the tax system, or any government system, and against analytics derived from decades of identity risk expertise. Mitigating that risk and controlling those costs requires realizing one very important fact. Government records, specifically tax records, are not an identity. That brings us to the second fundamental thing to remember.

People's Data and People's Identities Are Not the Same

Our identities are much bigger than what the government really knows about us. Any government agency, no matter how large or small, sees only a tiny fraction of your identity. Think of all the bits and pieces of your identity you leave behind during the day or week, and how little of it any government agency, or even the entire government, can see. What's more, our identity information is messy, meaning it changes rapidly (i.e., people move, get married and change names, use nicknames, etc.) and some people lie. Governments attempt to cope by matching data and assuming an identity is not stolen until proven otherwise.

11 http://www.privacyrights.org/data-breach
12 http://datalossdb.org/incident_highlights/62-over-822-million-records-exposed-in-2013
13 http://freebeacon.com/report-4-in-10-government-security-breaches-go-undetected/
14 http://www.fbi.gov/losangeles/press-releases/2012/armenian-power-member-and-three-armenian-power-associates-convicted-in-los-angeles-for-roles-in-identity-theft-ring
15 http://www.fbi.gov/newark/press-releases/2013/eighteen-people-charged-in-international-200-million-credit-card-fraud-scam
16 http://www.businessweek.com/articles/2014-01-09/tax-refund-fraud-fake-returns-net-gangsters-millions

Criminals understand this outdated and dangerous assumption, use it to their advantage, and as a result the last few years have seen an explosion of identity fraud in government, especially in tax and revenue.[17]

The only logical conclusion is that our assumptions are wrong. The prevailing view of identity theft as the problem costs money and increases risk. Identities are not what we think they are, and identity theft is only a fraction of identity risk. This white paper describes and explains the true nature of tax filer identities and by extension, the identities of all citizens. It introduces a plain language framework to improve identities in various systems. The framework allows for direct, immediate action. The framework is also built on the reality that everyone's identity is already stolen and so identities should become facts only when we agree on them. Agreeing on identities entails risks – identity risks that should be fully assessed against the entire identity. LexisNexis customers have proven that embracing this view on identities reduces costs and increases revenue.

Criminals know identities are bigger than the government's knowledge of us individually and they're using our identities to steal public money.

The framework leverages your existing knowledge to map your agency's identity assumptions, highlights the resulting identity risks across your system and explains how to avoid those risks. Overall, avoiding these risks requires reimagining what an identity is in a government system. Reimagining people's identities in tax systems decreases fraud, increases revenue and enhances service. This is because reimagining tax filer identities allows us to design systems for what records really are – people.

People have free will. Both data and people can change, but data can't change itself. People can. People do. People use free will to make themselves look different to governments when it suits them. What's more, they can make themselves look differently, or create multiple identities for themselves, rapidly. People can and often do use multiple identities concurrently and rapidly. People use identities to lie.[18] This white paper explains how to mitigate these costly identity risks in your system.

Moving (especially out-of-state)

- Over 40% of movers never notify the post office (at least 16M annually)
- Per US Census, 6M out-of-state moves annually
- 69% of out-of-state movers are under 34 years old (the population ignoring the US Postal Service)

Identities are always bigger than what the government actually knows.

Different names, divorcing, marrying

- Over 3,000,000 times per year

17 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission
18 A Third of Americans Say They Like Doing Their Taxes, Pew Research Center, April 11, 2013

Jobs

• As many as 21,000,000 job changes this year

Phone numbers

• USA has 321,000,000 active cell numbers (more than the US population)

Multiple residences

• Over 5,000,000 homes sold in 2011

Multiple vehicles

• Average American home has 2.2 cars

Licenses and registrations in multiple states

Per US Census, 35M Americans moved in 2011; all those people changed their driver's license, voter registration, etc.

Incarcerated

• Over 1,600,000 incarcerated; Almost 4,000,000 on parole

Non-existent addresses

• Rampant use of imaginary secondary addresses

Being alive or dead

• Over 2,500,000 die annually; Over 3,900,000 births

• Not all are reported to SSA

Are who they claim to be or even existing at all

• ID fraud against governments up 11%

As an example, in tax refund identity fraud, tax agencies share identity data self-reported by filers. However, with identity fraud at an all-time high, and criminals filing for both state and federal refunds, many of the filings are fraudulent identities and many agencies filings will falsely verify each other, even though those filings are from the same criminal. Two lies will match. Data matching cannot solve this.

The highly variable and fast-changing nature of Americans' personal identity information will only increase. Criminals will continue to use this to their advantage until we assess identity risk more fully and differently. That's why the third thing to remember is so important, because it allows the government to better and more fully analyze identities for risk.

Current State of Identities in Government

To analyze identities in government systems for identity risk, we must first admit that identities are a persistent and pervasive problem in governments, perhaps tax agencies especially, because tax systems traditionally needed to take identities as they were given. Until now, governments had little choice but to accept a tax filer was who he said he was. People sent tax returns and the identities were put into the system. While in the past this may have been reasonable, governments losing billions of dollars each year to identity risk can literally no longer afford to believe people.[19] Businesses routinely reject customers based on identity risk, but governments must take all-comers. The government cannot generally refuse to process someone's tax return. Other government agencies face similar well-intentioned public-facing constraints designed to ensure equal access to government programs. This "all-comers" reality means government systems must cope with severe identity risks. These far-reaching risks create costly impacts to governments.

LexisNexis is Already Succeeding in Preventing Identity Fraud

LexisNexis understands these costs first-hand, because we have already partnered with many government agencies to mitigate identity risk and reduce fraud costs. The three governments below are excellent examples of how assuming all identities are stolen, and expertly mitigating risk, can save millions while simultaneously protecting taxpayers:

- Over the last two tax seasons, 2012 and 2013, the State of Georgia Department of Revenue has stopped over $32M using LexisNexis identity risk technology.
- The Florida Department of Children and Families (DCF) has saved more than $12 million in cost avoidance by preventing fraud and creating increased efficiencies within its first five months rolling out a statewide program to verify and authenticate the identities of customers accessing public assistance benefits.
- The Louisiana Department of Revenue avoided $5 million to $7 million in tax losses in 2013 utilizing the LexisNexis identity solutions.

The reason for these successes is not simply admitting all identities must be treated as stolen or fabricated. These governments also understood they needed LexisNexis to help them move past the historical assumption that matching their records against other government records was enough to fight identity fraud.

Matching Data is Risky, or Worse

Traditionally, governments have combatted the costs of poor identities by matching data. The limitations of matching people's self-reported data are highlighted by the recent dramatic increase in identity crime against government - just as governments are sharing more data than ever. Logically, if data matching stopped identity fraud then this increase in identity fraud would not be occurring. Instead, matching self-reported data either from the same or other government agencies means taking on others' identity risks and faults without knowing what those risks are or how to mitigate them. When you match data, you actually compound identity risks.

This is costly for three reasons. First, because governments lack the resources to resolve a nationwide identity, matching data may unknowingly match an incomplete, dishonest, or outdated identity. The insurance and finance industries routinely employ LexisNexis solutions because these companies know they cannot see identity risks the way LexisNexis does. Second, governments are the last to be told when law-abiding people change their identity information. For example, the US Postal Service admits they see no more than 60% of address changes, and for younger citizens that number drops dramatically[20]. Third is the fact that people are messy, change rapidly and lie.

19 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission
20 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission

If governments match these self-reported half-truths and deceits to each other, it does not make them true, just consistent lies. For this reason, while LexisNexis sees some utility in data-matching, it is crucial to separate data-matching from sophisticated identity risk analysis.

Data matching will validate two fraudulent identities. Two lies will match.

Defining Identity Risk: Identities Do Not Add Up, They Are Agreed To

If you agree on an identity that is not real or is not useful, it costs you. This is identity risk. The fundamental identity risk difference between data matching and identity analysis is the underlying assumption. Matching self-reported data assumes identities are reliably composed facts. It assumes self-reported data are objective, scientific facts - real people. Seeing identities this way entails huge identity risks. Treating identities as stable facts creates identity risks because identities are not objective facts. Identities become facts only when parties agree the identity is genuine. The amount of identity information needed to agree and the acceptable risks depend on what is at stake. Thus, identities are social facts created when two or more parties agree the identity is real and useful, and agreeing on an identity is more or less risky depending on what you do with it. The amount of identity risk determines the threshold for agreement.

Identities become facts when agreed upon.

More importantly, you should only agree on an identity if you can mitigate the risk. You can only mitigate identity risk if you can see more of an identity than matching allows. This is how LexisNexis sees identities - across agency siloes, geographies and decades. We see an entire identity going back over 40 years from all corners of a person's life. This allows governments to intelligently agree to identities and to mitigate the three identity risks LexisNexis sees in customer data. These three identity risks are detailed below, complete with real-life examples of customers realizing and mitigating identity risks.

Three Identity Risks in Government – Examples from Tax & Revenue Agencies

Three identity risks come directly from treating identities as objective facts and matching data, instead of treating identities as variably composed, highly contingent social facts which are agreed upon. Every government record and data match suffer from three costly identity risks: owned identity risk, matched identity risk and identity integration risk. I define and provide examples of each risk below.

Owned Identity Risk

This is the risk of having poor identities and not knowing it. If your agency owns identity information that is false, incorrect, incomplete or outdated, then matching becomes problematic, costly or pointless and no amount of matching can correct for the wrong identity. Passing time only makes

owned identity risk worse. The older your owned identities are, the riskier they are. Fortunately, this is the risk most easily mitigated. LexisNexis can independently assess an agency's identity data to see how current, complete and trustworthy it is. LexisNexis has numerous proven identity solutions which quickly and drastically reduce owned identity risk by helping governments see the rest of the identity the person has declared to the world, and determine if the identity even exists, is fabricated, or stolen.

Why match data for a fraudulent identity? No amount of matching can correct a fraudulent identity.

Owned Identity Risk Example: Property Tax Fraud

An example of owned identity risk in government is homestead exemption fraud. Counties and states own property data on people containing out-of-date, incomplete, or dishonest identities. This costs even small governments millions each year through fraudulently granted homestead property tax exemptions given to people who have multiple exemptions or do not live in the home. LexisNexis identity analysis reduces this risk by showing which property owners have multiple exemptions or homes. A handful of counties have made millions of dollars and corrected their tax rolls going forward by using LexisNexis to mitigate their owned identity risk.

Matched Identity Risk

This is the risk stemming from an identity so poor a match fails, even though the real person represented in both datasets is the same person. Even if your agency is certain your identities are perfect, no agency can afford to simply trust matching. Other agencies will have wildly different identity risk tolerances. Worse still, agencies routinely compile their identity data from other agencies two or three degrees removed. These "Franken-data" quickly make data matching an exercise in the lowest common, but highest risk, identity denominator. This means that the more data silos you match against, the more you create matched identity risk. Data matching occurs with risky identities and in turn produces unreliable or costly identities.

Data matching will make a fictional person look like a real person.

Matched Identity Risk Example: Uncollectable Debt

An example of matched identity risk in government is uncollectable debt. Tax agencies routinely have billions of dollars of debt deemed "uncollectable" because they cannot find the debtor. They cannot find the debtor because of matched identity risk. Their debtor identity is wrong, outdated, or a lie, and as a result does not match even though the real person underneath the matching data is the same person. This results in tens of billions of tax debt going uncollected every year.

Instead of comparing two static or dated records, LexisNexis breaks the identity down and compares the uncollectable identity against our nationwide identity database going back 40 years or more. We are then able to improve locate rates for a newly corrected debtor identity. A southeastern state agency used proprietary LexisNexis solutions to mitigate this matched identity risk, improve their debtor identities, and reactivated over $4.2 million in previously uncollectable debt.

Identity Integration Risk

Identity integration risk is incredibly important and hugely costly, but less obvious than owned or matched data risks. Identity integration risk is best illustrated with a simple question.

Why match data for an identity that does not really exist?

Identity integration risk comes from not knowing who the data really represents: one person, many people, or perhaps no real person at all. When data matching against external records, you rely on that other agency's ability to prevent identity risk and resolve disparate identity records to a real person. Worse still, identity integration risk will interact with owned and matched identity risks. As a result, you have the risks of bad identities on either side of the data match, and even if both sides match perfectly, you have the over-arching risk of poor identity integration. Even if it matches, you still don't know if the identity is a real person. In other words, if I tell you a lie, and your neighbor tells you the same lie, that does not make it true. Data matching compounds identity integration risk.

To review, owned identity risk is the risk of having poor identities and not knowing it. Matched identity risk happens when an identity is so poor a match fails, even though the real person represented by both records is the same person. Identity integration risk is much worse, because not only will you reinforce erroneous identity data by matching dishonest, incomplete or outdated records, you will inadvertently agree on the identity of a person that does not really exist. Matching two errors on a fictional person will make that false identity look like a real person. Data matching compounds identity integration risk by verifying errors and lies as real people in your data.

Identity Integration Risk Example: Tax Refund Fraud

An example of identity integration risk in government is tax refund fraud. Criminals use stolen or fake identities to submit and receive fraudulent tax refunds. In the past, many fraudsters used fake wage data, but the criminals are becoming more sophisticated, using the actual wage withholding system against us. Unfortunately, tax agencies routinely treat wage and withholding records as undeniably real people. The facts demonstrate otherwise.

The largest example of this is the SSA Earnings Suspense File (ESF). The ESF has over $1 trillion dollars in withholdings submitted from W-2 identities that do not exist in the SSA system.[21] Despite repeated contact from the SSA, these "people" do not correct their earnings. The ESF has doubled to over 9 million reports per year; growing in tandem with identity-based refund fraud which has also more than doubled[22] [23] Wage data and tax returns are a perfect example of identity integration risk. Though the match is exact between W-2 and tax return, the identity itself is fraudulent. This is a perfect vector for tax refund fraud, which has increased 650% since 2008.

A specific example is the "nanny scam." Now seen in multiple states across the country, LexisNexis detected this identity integration risk in February 2012. In the tax refund nanny scam, organized crime uses the W-2 identities of previously employed nannies from other countries to file for fraudulent refunds. The nannies come to the United States, work for one year, and then go home. The mafia-controlled business continues to report very minor withholdings after the nanny goes home. Organized crime uses these fraudulent (but official) identities to submit for large refunds, including refundable credits like EITC and because it all matches, are paid quickly. Multiple tax fraud prosecutions and convictions prove the costly reality of this identity integration risk.[24] [25]

21 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission
22 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission
23 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission
24 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission
25 Consumer Sentinel Network Data Book for January-December 2012, Federal Trade Commission

To prevent this risk through tax refund fraud, agencies employ the LexisNexis® Tax Refund Investigative Solution (TRIS). LexisNexis analyzes the input tax identity against our historical and massive identity database to determine identity risk for each filer. We compare the self-reported tax data not against other self-reported data (W-2s) but against the rest of the world. In just two years, LexisNexis customers have stopped $40M in fraud, which other data-matching systems missed.

The LexisNexis Identity Risk Framework Mitigates Identity Risks

Cost-effectively mitigating these identity risks requires more than data matching (e.g. "data hygiene"). Mitigating identity risk requires a framework for action to define and mitigate your identity risks. The framework must be simple, based on real lessons-learned in identity analysis, and relevant to your system. LexisNexis has that concrete, customer-centered framework.

No matter how large or small your system, it has identities and edges. These identities and edges are the basic components of the LexisNexis Identity Risk Framework. Your agency stores human data internally (identities) and it connects with other systems, and likely the public (edges). Even for the largest government systems, most IT departments can readily provide a diagram of your system. This framework allows you to use that diagram to determine identity risk exposure and assess identity risk. The following four steps are a high level overview of implementing the LexisNexis Identity Risk Framework.

Step #1: Owned Identities

Determine where your system stores identities. You should include all local identity stores, not just the data warehouse. This is an inventory of all the places you keep identities. In this example, the Department of Revenue (DOR) has internal identity risks in their data warehouse, a mail database, an audit database, a call center application, and even a photocopied list shared and pinned to the cubicles of call center workers (ad hoc documents).

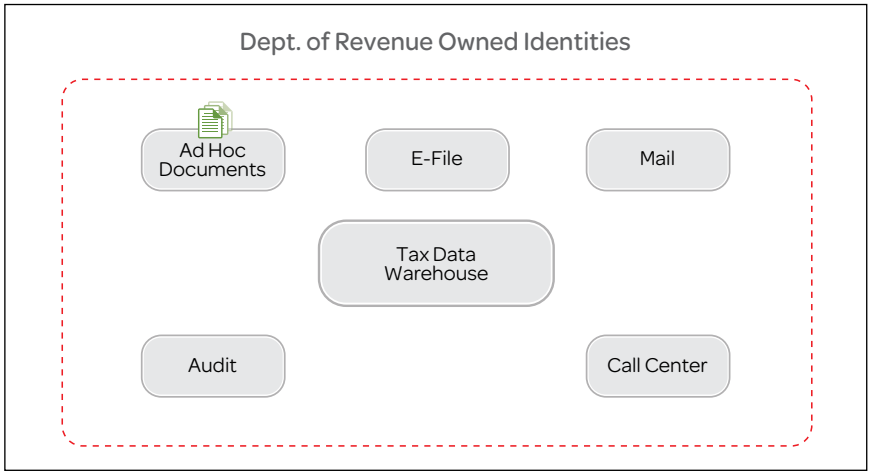

Figure 1. Owned Identities.

Step #2: Matched Identities

Comprehensively assess all the external agencies or partners from which you import identity data. This list will be longer than you think, and each entry on that list exposes you to all the identity risks you assume from external sources. Identity risk compounds with each data match. In this example, the DOR assumes unknown identity risks from four external sources: their Labor Department, Department of Motor Vehicles, the federal government, and their mail processing vendor.

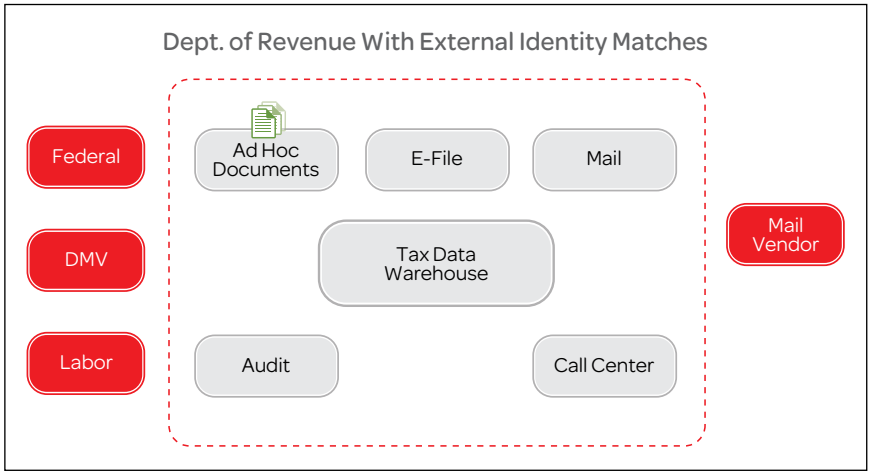

Figure 2. Matched Identities.

Step #3: Identity Paths

In this step, you trace the paths of identity sharing within and without your agency. Basically, connecting the dots between all identity sources both internal and external to see how identities move through, into and out of your agency.

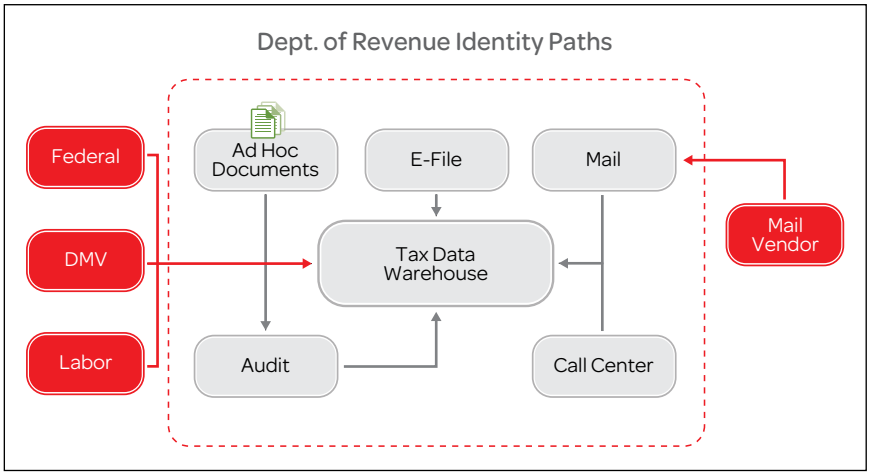

Figure 3. Identity Paths.

Step #4: Publicly Created Identities

Finally, document your public-facing identity edges – where people can directly create your identity data. This could include electronic filing, payments made online or over the phone, or customer accounts on your website. Wherever people (not other agencies or systems) create new identities for your system, that's this list.

Expertly integrating a whole identity automatically mitigates identity risks.

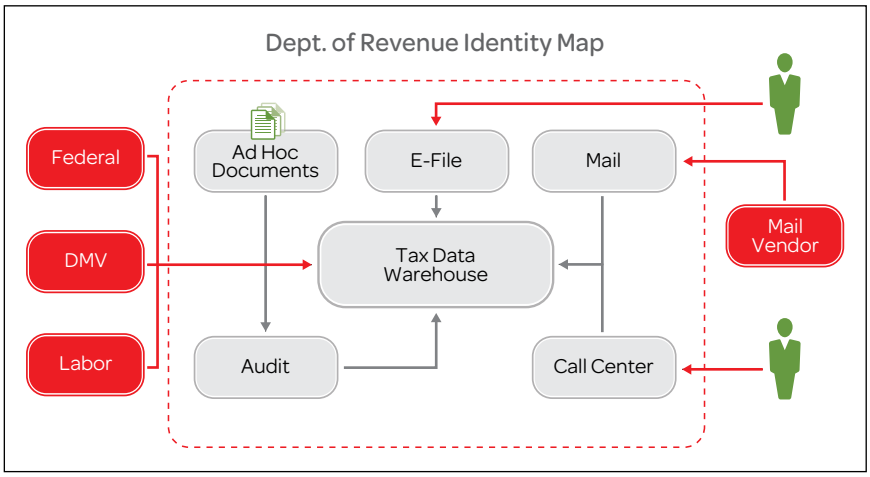

Figure 4. Edges - Publicly Created Identities.

Mitigating Identity Risk with the LexisNexis Identity Risk Framework and Solutions

By mapping identity sources, identity paths, and public-facing edges across your system, you can quickly breakdown where identities are agreed upon, the paths identities take, and your identity risks. More importantly, it literally creates a map of all the places your agency must manage identity risks and suggests the risk thresholds your agency should impose for new identities. Risk thresholds are dictated by tracing the path of the identity to see impacted tasks.

You should only agree on an identity if you can mitigate the risk.

For example, if a customer goes online to open an account and check the status of their tax refund, many agencies may see the identity risk of the new account as minimal since there is no financial activity. However, if in tracing the identity path you find that those online account identities are stored in the data warehouse, and in turn cascade throughout the system for mailing, customer contact, policy research or audits then the potential costs are high and the identity risk must be managed accordingly.

These sorts of subtle or hidden identity risks occur throughout systems as necessarily complex as a tax system. The LexisNexis Identity Risk Framework will help tax agencies perform a basic assessment of their owned, matched and identity integration risks. Mitigating those risks, however, and turning identity risk into increased revenue and decreased costs, requires both

expert identity analysis and the ability to analyze your internal identities against the identities presented to the rest of the world. LexisNexis is eager to discuss how we can do this in partnership with the professionals in your agency, and help your agency discover and prevent fraud, recover lost revenue, and increase taxpayer service by mitigating identity risk.

Summary: Assess Your Identity Risks and Mitigate Them

Everyone's identity is already stolen, so the only rational assumption is to gauge each identity presented to the government for risk. At the same time, people exercise free will to extend their identities beyond data-matching assumptions. As a result, identities are always bigger than the government. Reimagining identities and mapping how identities are used in your system allows you to avoid severe identity risks.

Avoiding costly identity risks requires reconsidering what an identity really is, carefully cataloging and mapping your identities, and leveraging a unique combination of expertise, patented identity integration technology and a massive, unmatched, nationwide repository of identities going back more than 40 years. This allows you to take into account the complex, dynamic and rapidly changing nature of tax filer identities. It can also solve both owned and matched identity risks simultaneously by allowing identity integration.

LexisNexis is simply the best at identities, especially in tax and revenue. We have analyzed hundreds of millions of identities across dozens of local, state and federal systems for identity risk, and are the global leader in mitigating identity risks for the Fortune 500. For government revenue agencies, LexisNexis employs a dedicated team of consultants and architects focused exclusively on identities in tax and revenue agencies. If you have questions on how to deploy this framework, or want an assessment of your identity risk, please contact us.

For More Information

Check out our Fraud of the Day Forum at: fraudoftheday.com
For more best practices around identity in the government space, contact LexisNexis:
www.identitygov.com
Email: identitygov@lexisnexis.com
Phone: 844-IDT-YGOV

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®