Next Generation Countermeasures for Identity Theft Tax Refund Fraud

A FedCentric White Paper
by
Thomas Van de Merlen
Director of Fraud Detection and Prevention

FedCentric
TECHNOLOGIES, LLC

4511 Knox Road Suite 300 • College Park, MD 20740 • 301.263.0030 (o) • 301.263.0032 (f) • www.fedcentric.com

I. Introduction

Identity theft and identity fraud are crimes in which individuals improperly obtain and use someone else's personal data for economic gain through fraud or deception. Unlike biometrics such as fingerprints or facial images which can't be used by someone else, personally identifiable information such as social security numbers, bank or credit card account numbers, or other identifying data can be used by an impersonator to profit at the victim's expense.

The risk of identity fraud is greatest during online transactions that don't involve face-to-face interactions between the participating parties. The Consumer Sentinel Network is a secure online database of millions of consumer complaints available only to law enforcement. According to Consumer Sentinel Data Book for 2015, identity theft complaints comprised 16% of all consumer complaints. ID theft complaints increased more than 47 percent in 2015 as a result of *a massive jump in complaints about tax identity theft*. At 45% of all identity fraud complaints, tax-or wage-related fraud was the most common form of reported identity theft.

The growth of identity theft (IDT) tax refund fraud is recognized by the IRS and many state tax administrators. The most common response to this threat is the implementation of fraud filters aimed at identifying anomalies and suspicious entries by filers. Once identified as suspicious, filers are subjected to identity authentication measures to ensure that the return is from the true taxpayer.

While often effective, these measures create a new set of challenges including:

- ***Additional costs to create and support filters and identity authentication measures***
- ***The need for increased analyst and taxpayer support to vet the suspicious returns and respond to taxpayer inquiries***
- ***The delay of tax return processing while the filer's identity is authenticated***
- ***Adaptive methods developed by fraudsters to avoid the fraud filters***
- ***Voluminous false positives that ensnare legitimate filers in authentication measures***

Not all states have adequate deterrents in place. State tax administrators lacking effective IDT deterrents are often cognizant of the problem, but taking steps to protect against refund fraud has been challenging for budgetary, technology or other reasons. As the IRS and states with proactive measures decrease their vulnerability, the states without these defenses become more of a target for fraudsters.

A next generation of countermeasures for Identity Theft Tax Refund Fraud that can filter fraud without delaying processing and effectively authenticate taxpayers without creating outsized costs has the potential to benefit state tax agencies both with or without effective IDT defenses.

II. Background

Current countermeasures to IDT Tax Refund Fraud employed by many states incorporate fraud filters returns aimed at identifying anomalies in the return. Once the anomalies have been determined, steps are taken to authenticate the identities of filers captured in the filters. Information on the returns is matched to databases of publicly available information and/or to proprietary information held by the state to identify discrepancies between what is known about the filer and what is entered on their tax return. Returns with anomalies are then subject to identity authentication steps that involve the administration of quizzes also based on known historical information about the filer.

States that have taken these steps experienced an unanticipated high volume of returns that were captured in their filters. One state reported 19,000 returns were still in their review queue in August 2016 as they worked their way through the quizzes and follow-up actions for the large volume of returns captured in their filters. Another state reported it administered over 200,000 quizzes and handled 75,000 related phone calls. Others reported a plethora of false positives that created delays and expense that were beyond acceptable. In all states, the cost of administering the program and the vetting actions and taxpayer support demands on their personnel presented a significant budgetary challenge.

Nonetheless, for the states at the forefront in the fight against IDT tax refund fraud, the amount of fraud avoided through these efforts was initially substantial. However, the effectiveness of their approach had several consequences:

- ***Fraudsters quickly shifted their activity towards states without proactive identity authentication measures.***
- ***Fraudsters began targeting payroll companies and tax professionals for data thefts that would provide them with enough correct personal identifying information to pass through the filters.***
- ***The amount of fraud prevented in states with countermeasures declined precipitously but the costs of administering the anti-fraud program remained constant or increased.***

Current countermeasures often cannot be performed within an acceptable period or in compliance with state guidelines for issuing refunds after a return has been accepted. In some states with these limitations, fraudulent refunds are issued unknowingly. Subsequently, when they are identified as fraudulent, the recovery of the refunds is pursued through a “pay and chase” effort that is often unsuccessful in recovering the funds.

III. Next Generation IDT Tax Refund Fraud Countermeasures

FedCentric has developed a **High Performance Tax Analytics** (HPTA) solution paired with **IdentityX©**[1], a biometric identity authentication mobile application, to identify suspicious tax returns and quickly and efficiently authenticate filers captured in the fraud filters.

HPTA is built upon FedCentric's high performance computing technology that is currently being used effectively for real-time analytics of big data at the USPS:

http://www.enterprisetech.com/2015/05/05/hpc-for-advanced-analytics-at-the-usps/

FedCentric's High Performance Computing (HPC) and memory centric database (MCDB) architecture affords incredible increases in processing speed when compared to conventional methods. These increased processing speeds allow us to perform real-time or near real-time analytics which identify the fraud, prevent improper payment and alert investigative resources. FedCentric solutions feature a total commitment to commodity products and software standards. Your current IT staff is familiar with our environment and we are compatible with your current custom developed codes and third party application software.

Although principally designed for fraud detection, HPTA will also identify taxpayer error and assist in closing the estimated 15% difference between taxes owed and taxes paid known as the "Tax Gap". The fraud filters and the specific output from HPTA can be used **prior to acceptance** to efficiently filter returns to deter fraud, eliminate processing delays and decrease the number of legitimate returns captured by the filters.

IdentityX will enable tax administrators to authenticate taxpayer identities more effectively and at less expense by using forward leaning technologies that are being increasingly deployed throughout banking and other industries. Current levels of authentication are described as follows:

- ***One-factor authentication is "something a user knows" such as password.***
- ***Two-factor authentication adds "something a user has" such as a SecurID token.***
- ***Three-factor authentication adds "something a user is." Examples of a third factor are the user's voice, facial image or fingerprint.***

The strength of authentication is primarily determined by the number of factors used to allow online access. Applications that use all three factors are stronger than those that only incorporate one or two of the factors.

IdentityX (IDX) will provide a quick and reliable three-factor authentication that collects a facial image, voice sample and/or fingerprint directly from the individual during enrollment. IDX then validates their identity each time online access is requested via a mobile application that

[1] **IdentityX© is a product of Daon, a FedCentric partner. More information about Daon can be found at https://www.daon.com/**

collects the same biometric in real-time for comparison to the sample obtained during enrollment. The IDX solution reduces quizzes, visits to websites and call volume to taxpayer support centers while increasing the reliability of the results.

Adoption of these next generation tax fraud countermeasures will reduce excessive costs to administer current anti-fraud measures. Delays and inconveniences to legitimate taxpayers drawn into fraud filters will be reduced as well as revenue loss from fraud and error. The quick resolution of filtered returns will enable auditors, analysts and investigators to concentrate on more complex tax avoidance and non-compliance schemes. And IdentityX will provide a future opportunity for secure online taxpayer accounts by providing a high degree of confidence in taxpayer identity.

IV. HPTA and IdentityX in Detail

HPTA and IdentityX includes the following components:

- ***Binary Matching to detect fraud and error***
- ***Identity Authentication of filers captured in fraud filters***
- ***Advanced Analytics to identify more sophisticated fraud***
- ***Website Support***
- ***Call Center Support***

- ***Binary Matching*** - Increasingly, state tax administrations and the IRS are requiring earlier receipt of information returns such as Forms W-2 and a variety of Forms 1099. Additional information returns such as Form 1098, Mortgage Interest and Form 5498, IRS Contributions are also available for matching. *IRS auditors have reported a much lower tax gap when information returns are available to validate taxpayer entries*[2]*.*

  Additional binary matching opportunities exist beyond information returns including comparison to Social Security Administration databases such as Numident (all names and associated SS#s and DOBs), Death Master, Prison Update and Benefits Paid. In addition, Device IDs, IP Addresses, phone numbers, e-mail addresses and bank or debit card accounts already associated with fraudulent returns can be included in the binary matching process and updated throughout the filing season.

  IDT Tax Refund Fraud can also be deterred by authenticating the filer's identity when the return is from a first time filer, the filer has changed their address, or there have been changes in contact or banking information. In order to be effective against fraud, these

[2] GAO 16-92T pp 39 http://www.gao.gov/assets/680/672884.pdf

occurrences should result in follow-up before a return is processed and a refund is issued. Using HPTA loaded with historical information, these types of incidents can be identified as soon as the return is received.

HPTA can load information returns at the rate of 721 million per hour and process returns at the astounding rate of 5 million per hour. The speed of HPTA can facilitate the daily rerunning of previously filtered returns as additional information returns or other information is received without delaying the processing of returns not captured by the filters. An error database is created to assist with taxpayer inquiries and to support case follow-up and resolution.

When a return is received that contains information that was not received by the state or is different from the information received or known by the state, HPTA will afford identification of such discrepancies prior to acceptance. HPTA will automatically generate alerts to the filer notifying them of an error on their return. The specificity of the error information provides a deterrent to fraudsters and can serve as a corrective message to filers who mistakenly omitted required information such as a missing Form W-2 allowing them to refile without the need for additional support. The alerts will direct taxpayers participating in IdentityX to authenticate themselves via a mobile app and will direct non-participants needing assistance to a website or call center for validation.

- ***Identity Authentication*** – Using IdentityX, FedCentric can facilitate the implementation of biometric identity authentication that uses fingerprint, voice and/or facial biometrics to authenticate the filer via a mobile device and App. This process involves initial enrollment which can be configured to an individual state's requirements. During enrollment, an individual's biometrics are captured once their identity has been established. When their tax return is received, they are contacted via the mobile app and asked to validate their identity by providing a live picture, voice sample and/or fingerprint through their mobile device.

  Many financial institutions and online retailers are moving towards requiring biometric authentication for online transactions. Recently, MasterCard became the latest company to raise their online protocol to three-factor authentication through the use of biometrics:

  http://newsroom.mastercard.com/videos/mastercard-identity-check-facial-recognition-biometrics/

  Forward looking tax administrations are also experimenting with this concept. IdentityX can provide a biometric authentication solution which has already proven to be highly effective in proactively deterring fraud by ensuring that online applications are allowing access to the real individual.

For filers who opt not to participate in IdentityX, specific steps are established in HPTA to authenticate the identities of filers who returns are captured. These include automatically mailing a notification to the filer at their last known address with a reference code and steps to validate their identity via a website or call center.

It’s important to note that contacting the filer through the e-mail or phone number included with the return often puts the state in contact with the fraudulent filer who can in many instances answer the identity questions using publicly available or stolen information. The use of hard copy mail and a reference number greatly diminishes the risk of these occurrences.

Advanced Analytics – Some tax fraud requires more sophisticated analysis to identify. Advanced analytics employs more predictive and less binary analysis to compare taxpayer entries on their current return to previous submissions or third party information. The use of trend analysis to detect suspicious changes in income, interest and dividends, deductions and dependents is effective in identifying risk factors that justify additional due diligence by tax administrations before processing a suspicious return. Using graph databases, FedCentric can make connections between non-obvious fraud characteristics such as the same e-mail or phone number used on multiple fraudulent returns.

FedCentric uses its high performance computing and analytics expertise to process huge amount of data from proprietary and open sources to identify suspicious anomalies and establish fraud risk levels in near real-time. Working with tax administrators, risk scores can be developed and fine-tuned to provide analysts, auditors and investigators with actionable leads. And by eliminating a significant volume of refund fraud via HPTA and IDX, these skilled tax professionals can be focused on the more sophisticated tax frauds that require their level of training and expertise.

- ***Website Support*** – For discrepancies that cannot be resolved through IDX, a website is constructed that provides identity authentication or other validation questions to authenticate filers. Correspondence from HPTA is directed to the last known address of the filer along with a reference number and a link to the website. This approach simultaneously eliminates fraudulent filers who either did not receive the correspondence or cannot correctly answer the questions. This approach will also provide legitimate filers with honest errors on their returns with enough information for them to potentially correct and resubmit their filing without further assistance.

- ***Call Center Support*** – Output from HPTA creates an easily searchable database for taxpayer support personnel to reference and resolve responses from taxpayers who receive ID authentication requests or binary matching error notifications.

• V. Benefits of the HPTA/IdentityX Solution

Implementation of FedCentric's HPTA/IDX solution provides multiple benefits to tax administrations including:

- A smaller tax gap from reduced fraud and loss from taxpayer error
- Reduced cost of administering anti-fraud measures
- Reduced delays in processing legitimate returns captured in fraud filters
- Fewer amended returns
- Enhanced identity authentication using IdentityX and establishment of the groundwork for secure online taxpayer accounts
- Reduced IDT workload for analysts, auditors and investigators allowing greater focus on more sophisticated tax frauds
- Website and Call Center support to enhance timely resolution of filtered returns

VI. Summary

IDT Tax Refund Fraud is a real and persistent threat that is costing tax administrations an alarming loss of revenue while undermining trust in government and proper custody of taxpayer information. The challenges in combatting this fraud include initial acknowledgement and identification of the scope of the problem, implementation of effective and cost-efficient processes to identify tax fraud once the problem is recognized, and sufficient taxpayer support mechanisms to deal with the unavoidable and substantial workload that results from fraud filter and identity authentication leads.

FedCentric's HPTA/IdentityX solution combined with call center and website support can help tax administrators effectively respond to this threat. HPTA can improve on the identification and response to error and fraud while simultaneously reducing costs providing an even greater return on investment from these proactive efforts. And IdentityX can provide the Level 3 taxpayer authentication that will enable secure online taxpayer accounts that offer even greater future savings.

About the Author *– Thomas Van de Merlen has been Director of Fraud Detection and Prevention at FedCentric since 2014. Before joining FedCentric, he worked as an independent fraud prevention consultant for 7 years. Previously, Van de Merlen had a 22-year government career investigating fraud, managing fraud investigatory resources, and building fraud detection systems for the US Postal Inspection Service.*

Tom can be reached at thomas.vandemerlen@fedcentric.com or at 301 263 0030 ext. 115.