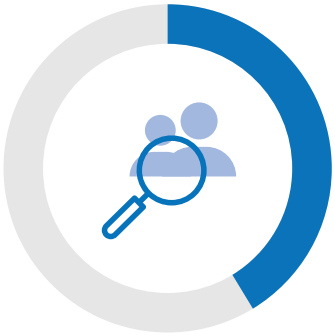
Five steps to combating income tax refund fraud

What every agency should look for when detecting tax refund fraud based on identity theft

Billions of dollars issued in fraudulent state and federal tax refunds siphon millions of dollars from important public assistance programs. During the first nine months of 2016, the IRS flagged roughly 787,000 fake returns claiming $4 billion in refunds, and 237,750 taxpayers filed affidavits saying they, too, were victims of tax identity theft.

Despite widespread government crackdowns, fraudsters are finding new and creative ways to defraud the government and legitimate taxpayers. For example, some individuals and groups acquire personally identifiable information (PII) from the deceased, dumpster dive, hack financial systems, buy information from someone not filing a return or otherwise steal it from legitimate sources such as a doctor's office. This PII is then used to fill out tax returns, add fraudulent income information and request false deductions.

According to a May 2014 Governing Institute research study of 129 state and local government officials, 43 percent of respondents cited identity theft as the biggest challenge their agency faces regarding tax return fraud.* Nationwide, stealing identities and filing for tax refunds is one of the fastest-growing nonviolent criminal activities. These activities burden government agencies and rob taxpayers by preventing returns from reaching the right people.



Almost half of state and local government survey respondents cite identity theft as the number one challenge their agency faces regarding tax return fraud.

But **more than half** of those surveyed also said their agency has not budgeted for any type of fraud initiative.

**All survey data from Governing Institute Tax Return Analysis Platform℠ Survey, May 2014, unless otherwise noted.*

An age-old problem

While revenue offices have existing tax return review protocols in place, tax fraud continues to rise. Unfortunately, simply relying on business rules based on past behaviors and conducting internal database checks do not stem the tide of tax fraud. By relying on singular customer information categories such as public records and demographic data, many agencies struggle to stop fraudsters. Furthermore, because identity thieves often use legitimate taxpayer information to commit crimes, revenue offices may have to wait until the legitimate taxpayer files before detecting a duplicate filing under the same name and Social Security number.

It's time for a multifaceted approach to detect tax refund fraud, where agencies augment current review processes with third-party data and analytics to detect the highest possible number of fraudulent returns. Some revenue agencies are adopting antifraud techniques such as issuing each taxpayer a unique personal identification number, but thieves often circumvent these controls. This is not only ineffective in reducing fraud, waste and abuse, but it gives agencies a false sense of security. With more than half (53 percent) of respondents to the Governing Institute survey indicating their agency has not budgeted for any type of fraud initiative, revenue agencies must incorporate easy-to-implement and cost-effective strategies that show an immediate return on investment and continue to pay for themselves over time by preventing tax fraud.

Almost half of agencies surveyed rely on manual review to identify and flag potentially risky or fraudulent tax returns.

However, 36 percent of respondents cited **lack of staff** as the biggest challenge to detect fraud.

A new approach

Agencies can strengthen their verification processes by augmenting existing systems with a risk-based authentication process that focuses on the following:

1. Identity proofing

According to the Governing Institute survey, nearly 50 percent of respondents rely on manual review to identify and flag potentially risky or fraudulent tax returns. But 36 percent of respondents cited lack of staff as the biggest challenge to detect fraud.

With tax fraud resources at a premium, revenue agencies must use new fraud detection techniques to improve results and manage costs. This means an increasing number of revenue agencies are exploring outsourcing for their identity proofing activities. Comprehensive identity proofing involves a multifaceted approach that not only includes existing internal database checks and the use of business rules, but also provides access to unique data sets and analytics that strengthen the identity proofing process. When using third-party data to authenticate a tax filer and ensure refunds reach only the legitimate taxpayer, agencies must consider the veracity of the source data used in the identity proofing process. Most authentication protocols are based on aggregation of public records data to verify the elements associated with identity. However, public records can contain errors and information reported is not independently verified before use. Additionally, because public records comprise aggregated data from a variety of sources, the profile of the consumer is not based on any long-standing relationship. Rather, the profile relies on the ability to follow name and address changes throughout a consumer's lifetime to justify the connections to the identity being authenticated.

Because of this, tax revenue offices should consider a vendor that has a long-standing relationship with a consumer and relies on the information collected and verified over years to sustain its core business. Credit reporting agencies rely on their need to authenticate consumers accurately on a daily basis as part of mitigating risk for billions of dollars' worth of customer transactions.

Using information compiled on a legitimate consumer over years of financial transactions provides the most accurate data available on the identity attributes of that legitimate consumer and increases the ability for agencies to detect red flags. By combining credit history attributes and historical applications with traditional information categories such as public record assets, a third-party provider can match information it knows to be accurate with the PII a filer submits.

When identity theft forms the basis of fraud, fraudsters attempt to use stolen credentials in as many financially beneficial transactions as possible before someone detects the identity theft. However, credit reporting agencies are already collecting information to detect all kinds of financial fraud that may be occurring with stolen identity credentials. Having access to millions of financial and credit transactions for customers who are applying for credit cards or lines of credit allows for fraud detection in the use of identity credentials outside of the tax submission process.

2. A focus on where the refund is going

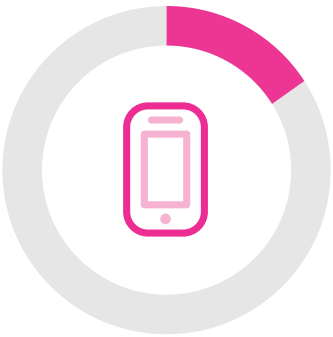
While practices such as refunding money through direct deposit and debit cards create convenience for the consumer, fraudsters can exploit these processes as well. Once a refund is directly deposited into a bank account, an individual can withdraw it instantly. Once money is withdrawn, the account can be closed and the money is no longer traceable. Similarly, if revenue agencies place refunds on a debit card, the card can be used immediately without traceable transactions.

Because of this, a highly effective tax refund fraud detection practice is to focus on where refunds are delivered. It should raise a red flag if the same address or bank account receives multiple refunds. While one address or bank account might receive refunds for up to four individuals, agencies should investigate any more than this. But 49 percent of Governing Institute survey respondents said they don't determine how many refunds are deposited to the same bank account.

3. Device intelligence

More than 80 percent of tax filings occur online, and that number is increasing. While many tax fraud detection protocols focus on authenticating information on the application itself, virtually no attention is given to evaluating the device used to submit that information. Typically, individuals committing tax fraud will use the same device when engaging in other fraudulent online activity, such as applying for credit or opening accounts to gain information. However, while individuals who commit tax fraud often perpetuate multiple financial crimes using the same device, revenue agencies rarely have the tools and resources and analyze devices. In fact, in the Governing Institute survey, a mere 16 percent of respondents said their agency screens devices to evaluate and verify a tax return.

Individuals who commit tax fraud often perpetuate multiple financial crimes using the same device.



However, revenue agencies rarely recognize and evaluate devices. Only 16 percent of survey respondents screen devices to evaluate and verify a tax return.

Beyond device identification and reputation, the key is to enable further investigation of the device against multiple and past events to link cooperating criminal enterprises and predict and guard against future events. By analyzing the devices submitting tax returns, agencies can not only examine a device's compatibility with the user, but also use the device to link seemingly unrelated activities to a common impersonator. In addition, device-based assessment adds another level of screening when identities are stolen. Because device assessment looks for malice rather than mere anomaly, false positives are typically low, leading to significant improvement in both detection and productivity. For example, one online aggregator that deployed intelligence was able to handle triple the volume of transactions with half the staff and still reduce fraud by 50 percent.

Finally, since fraudsters consistently attempt to make their Web movements untraceable, it is critical agencies employ a device intelligence protocol that does not simply rely on cookies to capture device attributes but allows capture simply through connection to the web page.

4. Automation of authentication on returns that need further investigation

Selecting the right third-party provider with the required data and analytics is crucial in combating tax fraud. This provider should not only have experience working with state and federal government agencies, but should have a fraud detection platform that is easy to implement and does not require additional time or resources to manage on top of the existing tax fraud detection process.

Every tax fraud detection process is intended to flag suspect returns for further follow-up. However, that additional follow-up may include a high degree of manual work, and while legitimate fraudulent returns will be detected, the process will invariably flag false positives.
It is essential that these suspect returns and false positives, while reviewed thoroughly, are examined as quickly and efficiently as possible.

If executed correctly, the integration of third-party data and analytics should ensure the continued quick turnaround for legitimate refund release while simultaneously providing increased confidence that refunds are being provided to the legitimate taxpayer.

As a complement to the traditional identity proofing process that uses various data sets, business rules and analytics, revenue offices should do further authentication via the web. For example, if filers need further authentication before a refund is released, the agency can direct them to a government website and ask them to answer a series of questions to further authenticate before releasing the refund. Most fraudsters will not respond even if such a request reaches them, because they don't want further scrutiny. Challenge-response question technology is used to formulate questions that only a true taxpayer would know, sourcing from both public records and financial data, and adjusting questions depending on previous answers. The process is entirely automated, quick to implement and can be combined with device authentication to complete the verification process.

5. Mitigation services

While not part of the tax return fraud detection process, revenue offices should consider offering possible victims of tax refund fraud access to services that will protect their identities in future transactions. For example, offering individuals flagged as potential victims access to an identity theft detection service can ensure they are alerted automatically if a fraudster attempts to open a line of credit or apply for a credit card using their personal information. As a result, agencies can outpace criminals by proactively detecting, avoiding and managing fraud activity on behalf of their constituents.

The key is to complement, not replace

Revenue offices need to process returns and provide refunds as quickly as possible. In fact, most tax returns are processed and refunds released within a few days or weeks. To maintain this quick turnaround, any addition to the existing tax fraud detection process should not add significant time to an agency's current tax return review process.

Revenue agencies can't afford to completely overhaul their existing verification systems and processes. They need a service that can complement their current tax return evaluation process. An easy-to-implement platform should fit seamlessly into any existing tax return evaluation process, adding little or no time to the existing process. Whether offered as a standalone product or one customized to integrate with existing processes, it also should provide batch scrubs that can be completed within 24 to 48 hours. Moreover, web-based authentication and device proofing should be implemented together with minimal setup time and minimum impact on current process timelines. If executed correctly, the integration of third-party data and analytics should ensure the continued quick turnaround for legitimate refund release while simultaneously providing increased confidence that refunds are being delivered to the legitimate taxpayer.

The same assurances apply to security. The Governing Institute survey indicates that 56 percent of respondents consider security in the decision-making process when determining whether to share tax return data with a third party. However, with the right third-party provider, the security of the information provided is already paramount, especially among organizations that work with sensitive financial and credit information daily and take great measures to secure the information and access to it.

A platform for protection

With identity theft reaching unprecedented levels, government agencies need new technologies and processes in place to stay one step ahead of fraudsters. In a world where most transactions are conducted in virtual anonymity, it's difficult — though not impossible — to keep pace with technological advances and the accompanying pitfalls. A combination of existing business rules based on authentication processes and risk-based authentication techniques provided through third-party data and analytics services creates a multifaceted approach to income tax refund fraud detection, which enables revenue agencies to further increase the number of fraudulent returns detected.

To learn how Experian can help your agency, visit www.experian.com/publicsector or call 1 888 414 1120.

**All survey data from Governing Institute Tax Return Analysis Platform℠ Survey, May 2014, unless otherwise noted.*

GOVERNING
INSTITUTE

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 414 1120
www.experian.com

06/17 • 2000/1242 • 1084-DA