TransUnion

WHITE PAPER

Fight identity-theft tax fraud with integrated layers of authentication

JEFFREY HUTH
Vice President, Product Strategy
TransUnion Government Information Solutions

Executive summary

Identity-theft tax fraud–or fraudsters impersonating citizens to redirect tax refunds–is on the rise[1].

To combat this threat, you need a layered authentication approach that takes a closer look at the identities and devices involved in the tax refund process. By analyzing the risks associated with particular identities and devices, you can tailor the identity-authentication process to effectively offset a projected threat.

In this white paper, we describe how to achieve a layered authentication approach that takes into account the risks associated with identities and devices and help you examine the costs and benefits involved. With multiple layers of defense working together, you can minimize fraud risk and improve the taxpayer experience.

Our solution: TransUnion ID Manager combines identity verification, device verification and identity authentication into a comprehensive platform that can help prevent identity-theft tax fraud and streamline the tax refund process for the average citizen.

This solution, delivered as a service, significantly shortens implementation time and costs to finally make risk-driven identity authentication a reality.

The challenges of identity-theft tax fraud

A recently released General Accountability Office (GAO) study[2] shows that in 2013 the Internal Revenue Service (IRS) blocked what would have been about $24.2 billion in identity-theft-related refunds. However, in the same study, the IRS found that about $5.8 billion was paid in identity-theft-related tax refunds.

Keep in mind that these numbers reflect only the fraudulent tax returns that the IRS knows about. So, while the GAO recommends that the IRS improve its fraud estimates, in this white paper we focus on reducing the number of identity-theft-related returns overall.

To that end, this white paper outlines how ID Manager analyzes the risks associated with identities and devices and uses that information to automatically authenticate taxpayers in a risk-appropriate manner. Delivered as a service, this integrated platform not only helps prevent identity-theft-related returns, but, at the same time, works to streamline the process for the average citizen.

1. Wood, Robert W. "IRS Paid $5.8 Billion In Fraudulent Refunds, Identity Theft Efforts Need Work." Forbes. Feburary 19, 2015. http://www.forbes.com/sites/robertwood/2015/02/19/irs-paid-5-8-billion-in-fraudulent-refunds-identity-theft-efforts-need-work/ (accessed June 3, 2015).

2. United States Government Accountability Office. "Identity Theft and Tax Fraud: Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks." GAO.gov. January 20, 2015. http://www.gao.gov/products/GAO-15-119 (accessed June 3, 2015).

A tax fraud example

Let's take a look at an example of a real, detailed, successful instance of identity-theft tax fraud[3].

The victim in question was attempting to file his tax return when he discovered that a return had already been filed for the current year using his information. Knowing he could obtain a transcript of a prior tax return from the IRS website, the victim attempted to secure a copy of the fraudulent return. Unfortunately, the victim discovered that someone had already registered through the IRS website using his information.

The victim then used another mechanism, a paper-based form, to request the transcript of his return. This method was successful. Through the transcript, the victim discovered that the fraudsters used the IRS website to request his return from the previous year. Using his W-2 information, the fraudsters changed the income and withholdings slightly and submitted a tax return for the current year using the IRS's free e-file website. The fraudulent return indicated a refund of $8,936, which the IRS paid directly to the fraudster's bank account.

Analysis: How something like this can happen

To begin with, the fraudster had to obtain the victim's personal information, including his Social Security number (SSN). Sadly, this isn't as difficult to do as it might seem. The GAO report states that "the sources of stolen identities are limitless." While significant attention is paid to the breaches that have resulted in hundreds of millions of identities being exposed, the fact remains that criminals are increasingly obtaining more detailed personal data.

Let's highlight a few salient issues from this real-life example:

1. The fraudster was able to authenticate himself or herself using the Knowledge Based Authentication (KBA) on the IRS portal. Arguably, this was the most important breakthrough in the process, for without the ability to view the victim's prior tax return, the fraudster would not have been able to proceed. Analysis of the incident showed that the process for requesting transcripts is vulnerable, as it uses only static KBA, which can be easily thwarted with illegally obtained information.

2. It is unlikely that the fraudster had prior knowledge that the victim filed for a refund in the previous year. The fraudster clearly wanted a specific taxpayer's profile, one with a refund from the previous year that they could alter slightly so as to not trigger any alerts. Therefore, it is likely that the fraudster requested transcripts of multiple tax returns to find one with a relevant refund. What's more, they most likely followed the same process many times with countless other stolen identities.

3. The tax return submission failed to identify and reject a tax return filed under a stolen identity. In truth, it is very difficult to identify a stolen identity, but, at some point, the fraudster had to alter attributes and exhibit other signs of anomalous behavior in order to direct funds from the return to his or her account.

3. Krebs, Brian. "Sign Up at irs.gov Before Crooks Do It for You." Krebs on Security. March 15, 2015. http://krebsonsecurity.com/2015/03/sign-up-at-irs-gov-before-crooks-do-it-for-you/ (accessed June 3, 2015).

Solution

Preventing this type of scenario need not be overly complex. At a high level, agencies need to adopt a solution that delivers these outcomes:

- **Balance security and convenience**: Many agencies attempt to combat fraud by introducing security measures that increase friction for fraudsters. However, these solutions will often increase friction for citizens as well. The right solution will both enhance authentication to more effectively limit identity-theft tax fraud and streamline the process for honest citizens.
- **Adapt to changes and accommodate various levels of risk**: Not all transactions carry the same level of risk, and the threat landscape is ever changing. Consequently, to be effective, an authentication solution needs to be able to adjust to various risk levels and must have the flexibility to stay ahead of emerging fraud threats and trends.
- **Implement at low cost**: As with every IT system, the business case must support the project. In any business case, the cost of implementation is a main concern, as it represents a capital outlay in the first year. Therefore, the implementation and operations costs need to be minimized.

The ID Manager platform

ID Manager is a fraud detection platform that offers tax agencies a risk assessment of the individuals initiating a transaction, as well as the devices used in the process. It can both reduce fraud and enhance the citizen's online experience.

Balancing citizen experience and fraud detection enables an agency to:

- **Say 'yes' quickly and with confidence**: Using complementary layers of invisible defense lets agencies quickly approve good applications and foster a positive citizen experience
- **Reduce fraud**: Moving beyond tools designed to verify data (which fraudsters can easily steal) to powerful analysis of consumer and digital behavioral patterns lets agencies spot even the most sophisticated threat
- **Improve operational efficiency**: By more effectively recognizing good tax filers and finding fraudulent ones, agencies can spend less time and money on back-office reviews

Provided as a service, ID Manager requires no on-site installation or hardware or software purchases. Since ID Manager is already operational, users merely have to implement it via integration with ID Manager's XML-based web-services interface. Implementation costs are restricted only to the integration.

At its core, ID Manager combines device verification and identity verification with dynamic consumer authentication for a layered process that balances convenience and security. All three components can be used individually or as part of a hierarchical, holistic system. These three components provide answers to three important questions needed to ensure certainty in digital transactions:

1. Who is this?
2. What are they doing?
3. How am I sure?

3. Krebs, Brian. "Sign Up at irs.gov Before Crooks Do It for You." Krebs on Security. March 15, 2015. http://krebsonsecurity.com/2015/03/sign-up-at-irs-gov-before-crooks-do-it-for-you/ (accessed June 3, 2015).

Layer 1: Identity verification– who is this?

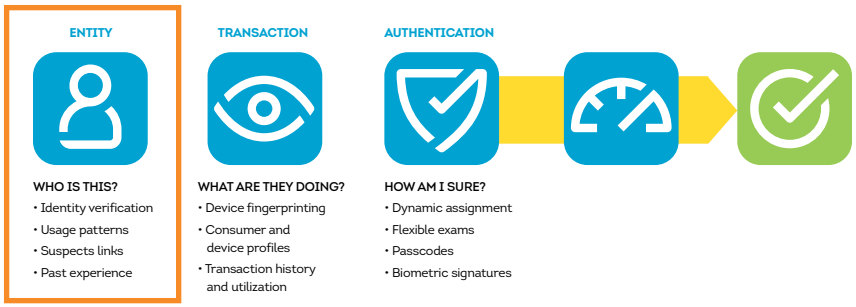
Identity verification checks citizen-provided information against multiple sources across a predictive network of consumer and fraud data. A matching summary reveals discrepancies between the information provided by the tax filer and the information found in an industry-wide network of consumer activity.

ID Manager's algorithms go beyond simply comparing supplied attributes to known data. They deliver the level of insights needed to truly understand the risks associated with any one identity.

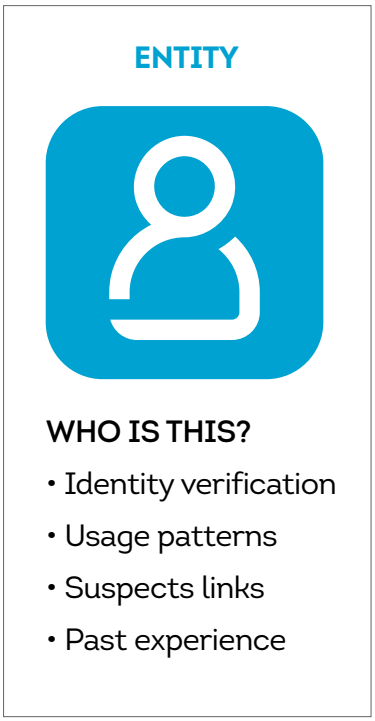
- Analyzing how an identity is being used across industries and sectors at any given moment shows patterns of suspect behavior
- Cross-referencing identity elements will reveal unusual linkages between identities, which is especially powerful when a criminal may have altered just one or two elements of an identity

FIGURE 1.1

TransUnion ID Manager has three core functional components organized into an integrated platform for risk-based assessment: identity verification, device verification and identity authentication.



LAYER 1



TransUnion

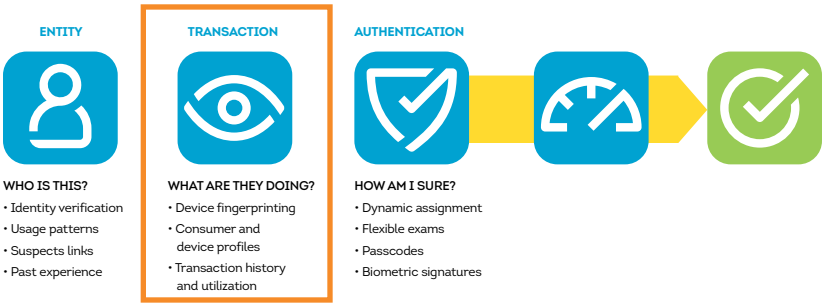
Layer 2: Device verification– what are they doing?

A solid identity decision must look at the devices and digital behaviors of an identity for additional signs of risk or assurance. With so much stolen data available, how the identity is being used is just as important as the details of the identity itself.

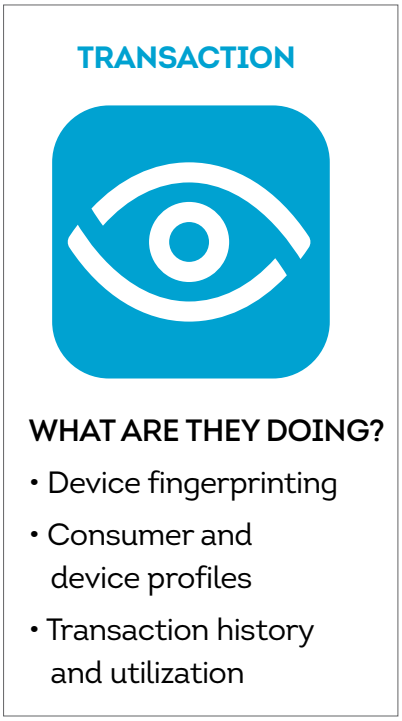
ID Manager goes beyond simple IP checks or comparing a device to a database of known suspect devices to provide a comprehensive view of digital risks.

- Advanced device profiling and geolocation use hundreds of device attributes to pierce layers of obfuscation, providing a near-instant analysis of risks associated with the device in use.
- Digital fingerprinting compares the way a site is being navigated to normal patterns of behavior, and interrogates digital data ranging from wireless to email to social presence in order to tell the difference between legitimate citizens and those who might impersonate them.
- Device reputation accesses cross-industry negative lists to identify known bad devices, as well as positive lists to minimize customer frustration. More specifically, if a device has been used to conduct fraud against a bank, that device, despite never having been used for tax fraud, will have a negative reputation.

FIGURE 1.2



LAYER 2



TransUnion

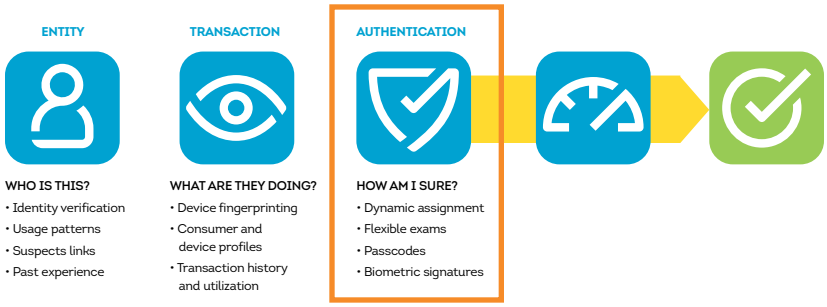
Layer 3: Identity authentication–how am I sure?

Depending on the risk of the transaction, the degree of risk posed by the identity, or other factors, agencies often need some kind of virtual interaction–or authentication–with the applicant to ensure they are who they say they are. This has most often been accomplished by presenting a series of questions that only the applicant should be able to answer.

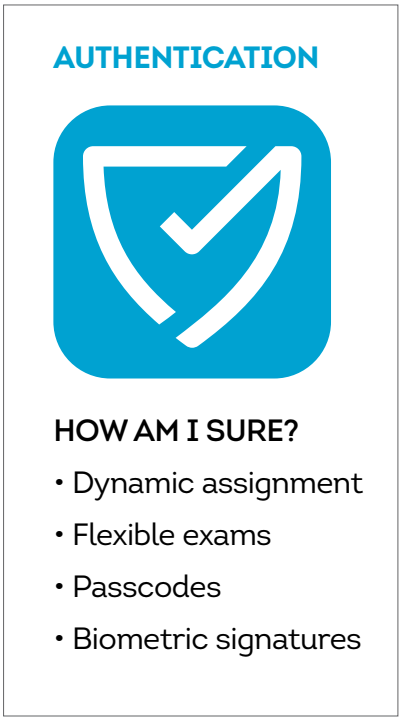
As an alternative to exams, citizens may supply a phone number that can be verified electronically through a passcode or voice call. This physical authentication provides greater certainty and is less intrusive than answering a series of personal questions.

When phone-based authentication is not possible, agencies still have the option to use an exam. Unlike traditional exams, though, ID Manager tailors the complexity of the exam to the risk of the transaction: low risk citizens may be able to miss more questions and still pass, while higher risk transactions get a more difficult exam.

FIGURE 1.3



LAYER 3



TransUnion

Three functions working together

Figure 2 further explains how these three functions work together. Along the left-hand column are the three core functions of ID Manager.

	APPLICANT	JOHN DOE Chicago	MARY SHAW Portland	SUE FOX New York	JANE SMITH Miami
IDENTITY VERIFICATION	IDENTITY VERIFICATION	ID elements match	Low risk	Multiple ID element mismatch	Low risk
	IDENTITY ALERTS	Low risk	Low risk	Input SSN linked to unusual number of phones	Low risk
DEVICE INTELLIGENCE	GEO LOCATION	-	Chicago	Las Vegas	Proxy geo: Miami True geo: Ukraine
	REPUTATION	No negative hit	Positive hit	Negative hit	No negative hit
	DEVICE BEHAVIOR	Phone verified	No anomalous behavior	Wrong screen size Distance traveled alert	Hidden proxy Velocity alert
AUTH	KBA	2 out of 3 exam (Credit and Non-Credit)	3 out of 4 exam (Credit and Non-Credit)	No exam	No exam
	FINAL DECISION	PASS No red flags	PASS IP/Geo flag mitigated by other factors	REVIEW Both consumer and device verification risk	REVIEW Significant device anomalies

FIGURE 2: Identity verification, device verification and identity authentication working together.

Now let's take a look at how these four scenarios played out.

John Doe is an example of a good citizen. He has no identity-element mismatches, his identity doesn't have any behavior alerts and his device is clean. With John Doe, because his risk is low, he is given an easier KBA exam, and ultimately his transaction is approved. We are able to assess the risks associated with John prior to presenting his KBA questions, and, because he is low risk, he is given questions he can answer easily and doesn't have to research. Appropriately, friction is very low for John

Mary Shaw is registering online and claims to be in Portland, Maine, on her registration. At first she appears low risk, based solely on initial identity verification and identity alerts. When ID Manager examines her device, however, it finds that although she says she is in Portland, her device is located in Chicago. This could be legitimate if she is traveling, for instance, but it is still a bit of a concern. As ID Manager moves through the rest of the device verification, we don't see any negative reputation hits on her device or any other device anomalies. Because of the geolocation discrepancy, ID Manager will give her a slightly harder exam and require more correct answers (three out of four), which she passes and ultimately gets approved. For Mary, the risk is slightly higher, and the friction is commensurately increased.

Sue Fox claims to be in New York on her application. From the beginning, ID Manager assesses multiple identity-element mismatches, and several identity alerts surface. ID Manager also sees many negative hits and anomalies on her device. Based on this, ID Manager is configured to forego a KBA exam and immediately fail the transaction. Instead it requests that she contact the agency directly. Sue is actually an amateur fraudster, but, in reality, even the simplest kind of identity verification would have caught her.

Jane Smith is an example of a more sophisticated fraudster. (She's actually taken directly from our real-life example above.) As ID Manager first assesses Jane, she appears to be low risk–nothing looks questionable on either her identity verification or identity alerts. However, as ID Manager conducts device verification, it finds that she is hiding her true location. She appears to be in Miami, but ID Manager is able to pierce the proxy and see that her true geolocation is in Ukraine. Her device doesn't appear on the reputation database, but there are several anomalies with the device that also raise concern. ID Manager has seen her device identity before, and she has triggered a velocity alert on the device. Based on these significant device anomalies, ID Manager will fail the transaction and request that the applicant call the agency directly. Jane is a great example of a transaction that probably would have been approved if only initial identity verification had been conducted, but by adding device verification to the mix, the true risk of the transaction is revealed.

Conclusion

Let's go back to the example of tax fraud provided above and see how ID Manager could have helped.

TAX FRAUD ISSUES	HOW TRANSUNION ID MANAGER HELPS
The fraudster was able to authenticate himself or herself via KBA at the IRS portal to begin the process.	Even before the authentication questions were presented, ID Manager would have developed an overall risk score based on the identity information and the device. It is possible that the identity attributes would not match completely. For example, an email address would have been associated with this identity for the first time. Given that this was obviously a stolen identity, it is highly likely that there would have been identity alerts, as attempts may have been made to use the identity elsewhere. It is also likely that the device itself was not located in the same location as the stolen identity. Additionally, it might have been used in other fraud schemes. As a result of scoring identity and device risks, the KBA questions would be very difficult or may not even be offered as an option.
The fraudster would likely have requested transcripts of multiple tax returns to find one with a refund and would probably have followed this same process many times with many different stolen identities.	Assuming the fraudster was still able to reach the KBA questions and answer with enough accuracy on enough profiles, ID Manager would have quickly detected multiple attempts to create accounts with different identities from the same device.
The tax return submission failed to identify and reject the fraudster's filing a tax return under a stolen identity. It is very difficult to identify a stolen identity versus a fabricated identity, but at some point the fraudster would have had to use different attributes in order to direct funds from the return to his or her account.	In this situation, there is quite a bit of personal information on the tax form. Since it was copied from previous years, very little would have been changed. Identity verification alone likely would not have caught it. Identity alerts would have raised concern as the stolen identity was used elsewhere. Furthermore, the device used to submit the return likely would have had location and behavior issues and would maybe even be on a bad-reputation database. This alone could be used to flag the return as a possible identity-theft-related return.

In sum, ID Manager from TransUnion not only stops fraudsters, but also recognizes that even honest citizens can raise a few flags. Oftentimes an honest citizen can initially appear to be bad, and a fraudster can initially appear to be good. Therefore, agencies should consider a layered approach to identity management to tell the difference.

GETTING STARTED

Contact your TransUnion representative to arrange a live demonstration of ID Manager, and consider a proof of concept to see the ease of implementation and positive impact it can have on your authentication process.

For more information about TransUnion's solutions for government, please visit transunion.com/government or email us directly at government@transunion.com to speak with a team member.

TransUnion

TransUnion