GOVERNING INSTITUTE

Issue Brief

Cracking Down on Identity Fraud in Public Benefits Programs

True Identity, Data Analytics and the Quest for Better Program Integrity

Identity Fraud in the Age of Online Access

Public benefits programs are a frequent and lucrative fraud target for criminals who use stolen or false identities to illegally obtain, trade or sell government benefits. The losses are staggering. The federal government conservatively estimates $17.5 billion of improper payments (6.7 percent improper payment rate) in the Medicaid program, $5.6 billion (11.6 percent) in the Unemployment Insurance (UI) program and $2.4 billion (3.2 percent) in the Supplemental Nutrition Assistance Program (SNAP) annually. Other assistance programs have similar improper payment rates.[1]

Identity fraud has increased dramatically since the advent of online services, which removes the barriers to fraud created by face-to-face contact. But that doesn't mean the best solution is to revert back to waiting in long lines for in-person appointments. To prevent identity fraud and improve program integrity in public benefits programs, this issue brief from the Governing Institute recommends:

- A multi-layered approach for verifying and authenticating beneficiary identity
- Integration of external data into existing enrollment processes for a broader view of applicants and beneficiaries
- Advanced identity analytics to supplement traditional overpayment recovery techniques

Who Are You, Really: Identity Fraud Prevention

To verify an identity, most government programs require applicants to self-report their names, addresses, birth dates and Social Security numbers. Using data matching technologies, states cross-reference this information with known government data; if they match, the identity is considered verified.

But in the world of online services, it's far too easy to fraudulently obtain or falsely create credentials. Traditional identity verification only confirms an identity exists, not that it is being presented by its true owner. Multi-factor authentication is a more advanced model for identity fraud prevention that applies a layered approach to identity authentication to determine if the identity exists and if it actually belongs to that person. A variety of proven technologies have been used extensively in the financial, insurance and other industries for fraud prevention, and are now beginning to migrate to the public sector.

For example, after the initial verification, agencies can use advanced technologies to automatically conduct a risk assessment of each identity and either pass through those with low-risk indicators or route those with high-risk indicators for further authentication. Risk can be established using identity analytics in combination with self-reported, agency and public records data, and IP address, geolocation and device identification from visiting devices.

Another method is to text or email a time-sensitive password to a previously established phone number or email address. The agency might also require the applicant to submit a photo of his or her driver's license, Social Security card or other identity document via a smartphone app, or even request in-person authentication.

> **"Predictive analytics helps us sort through fraud referrals by identifying which ones are most likely to be fraud so we don't waste our time on fruitless investigations."**
>
> – **Saratu Grace Ghartey,** Chief Program Accountability Officer, New York City Human Resources Administration

More is Better: Integrating External Datasets

These advanced, multi-layered identity verification approaches require agencies to expand beyond traditional verification data, i.e., name, address, birth date and Social Security number. Instead they must use data from other state and federal agencies and integrate third-party public and private data into their verification processes.

By leveraging national repositories of identity information, amassed over the lifetime of the applicant, agencies can ensure the person applying for benefits is indeed who they claim to be.

For example, the state of New Jersey combats unemployment insurance fraud with multi-layered authentication using a database with billions of public records to verify a broad range of personal information and prove applicants' identities. In 17 months, the Garden State thwarted nearly 650 identity fraud attempts and prevented $4.4 million in improper payments.[2]

External data also reveals a more nuanced, multi-dimensional view of the applicant and reduces dependence on self-reported information that may be false or inaccurate. It can help benefits programs confirm applicant eligibility by uncovering intentionally or unintentionally unreported information that may impact benefits eligibility, including:

- Hidden bank accounts, property or other assets
- Undisclosed earner in household
- Changes in family and household composition
- Relationships to known criminals, other recipients and care providers

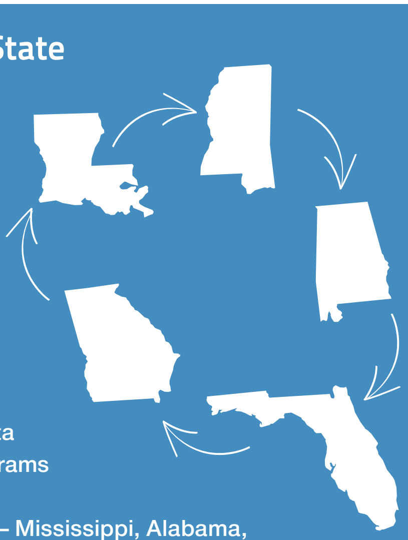
Beyond Pay and Chase: Advanced Program Integrity

Upfront identity proofing through multi-factor authentication improves program integrity, allowing agencies to focus on preventing instead of investigating fraud. In this model, program integrity is no longer dependent on the payment recovery process known as "pay and chase." Instead, agencies can follow a more proactive approach based on the individual's true identity and how it evolves over time.

External data serves as the backbone of predictive analytics technologies, which apply advanced computational algorithms to program data and flag unusual patterns, trends and behaviors that help states anticipate potential fraud. For example, the New York City Human Resources Administration (HRA) adopted upfront identity management and a predictive analytics solution to identify fraud patterns among Medicaid, SNAP and cash assistance recipients. HRA combined its data with public records data and applied a predictive scoring model to determine which cases to investigate, says Saratu Grace Ghartey, HRA's chief program accountability officer. "Predictive analytics helps us sort through fraud referrals by identifying which ones are most likely to be fraud so we don't waste our time on fruitless investigations," she explains.[3]

According to Ghartey, analysts designed a study to test the predictive value of various "red flags" that indicate potential fraudulent activity among Medicaid enrollees. "We found that ownership of luxury vehicles and ownership of more than one property are the strongest indicators of fraud," she says. "This leads to more successful investigations with less investigation time."

Trending Now: Multi-State Data Sharing



When multiple states share applicant data, they can better identify fraudsters who move their criminal activities from one state to another. The National Accuracy Clearinghouse (NAC), a data repository that supports the SNAP program, is a working model for national data sharing to protect benefits programs against dual participation.[4]

A consortium of five states — Mississippi, Alabama, Florida, Georgia and Louisiana — contributes beneficiary data to the NAC repository. When a person applies for SNAP benefits in participating states, applicant information is compared to NAC data to verify they are not currently receiving benefits in another state.

The NAC has revealed thousands of matches indicating dual participation of SNAP recipients across the five participating states, resulting in millions of dollars in estimated savings.[5]

Conclusion

As identity fraud in public assistance programs increases, states can maintain program integrity by using multi-layered identity authentication tools to verify and authenticate identities, and by expanding beyond traditional departmental data to leverage information from other government agencies and third-party external sources.

This strategy validates identity, ensures the presenter is its true owner, and provides a broader view of program applicants and participants, which enables an agency to advance beyond identity verification into the realm of fraud detection and prevention. Identity analytics offers a more efficient way to prevent and investigate fraud than long waits, busy tip lines and ad hoc investigations. This proactive approach enables states to gain a better understanding of the citizens they serve, thereby improving both program integrity and service delivery.

Endnotes

1. paymentaccuracy.gov/high-priority-programs
2. www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1403105422705112
3. Information from Saratu Grace Ghartey taken from phone interview conducted on August 10, 2015.
4. www.youtube.com/watch?v=4ZWhl8GN5Yc
5. www.fraudoftheday.com/2015/03/24/winning-the-war-on-public-assistance-fraud/

Underwritten by:

LexisNexis® RISK SOLUTIONS

LexisNexis Risk Solutions is a leader in providing information that helps customers predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we address evolving client needs in the risk sector while upholding the highest standards of security and privacy. Our government solutions assist agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increase program integrity, and discover and recover revenue.

Discover more at IdentityGov.com