Conduent Public Sector
Public Services Solutions

Fighting Fraud in Government Benefits Programs

Government benefits programs provide vital assistance to the citizens who need it most. Unfortunately, qualified recipients aren't the only ones who are cashing in.

Every year, these programs lose billions of dollars to fraud, siphoning money away from legitimate recipients and increasing the burden on already-tight government budgets.

In 2011 alone, TANF fraud loss was estimated between $171 million and $684 million, with SNAP losses estimated between $718 million and $2.8 billion. In 2012, fraud loss for unemployment insurance topped $993 million. And those numbers are expected to double over the next five years.

While the threat of fraud is nothing new, technology has changed the game. Back in the day of check-based benefits disbursements, forgery and counterfeiting were the main concerns. As government agencies move from paper to Electronic Benefits Transfer (EBT) and branded debit cards, fraud threats become more sophisticated, fueled by international crime rings as well as local, computer savvy predators.

To compound the problem, fraud, waste and abuse schemes are constantly changing. As fast as you can block today's common culprits, new scams are already in progress. Fighting fraud is a continuum. Today's master plan requires the fluidity and expertise to anticipate and protect against tomorrow's challenges.

The word "fraud" is like the word "disease" – a generic term encompassing a vast range of issues. Just as you wouldn't treat a broken arm with antibiotics or strep throat with a cast, you need different approaches for specific programs and types of risk. The combination of tools that works for one agency may not be the right choice for another. That makes things more complicated.

Then, there's the human element; the reason these programs exist in the first place. As much as we all want to eradicate fraud, if state agencies erect too many barriers, they'll make it difficult for valid recipients, many of whom may have physical or mental challenges, to gain access to the help they deserve.

There's no silver bullet, and there's no one-size-fits-all solution. So, what's the answer?

Although nothing can completely stop fraud in government benefits programs, agencies can reduce it through early detection and deflection. Fraud follows the path of least resistance. Much like a burglar bypasses the house with the locked gate and security system for the one with the open window, criminals will always look for the easy money. The key to protecting benefits funds from fraud without alienating your recipients is remaining vigilant and investing in the right combination of data analytics, fraud prevention tools and expertise required to deflect these ever-evolving threats.

As a starting point, this paper provides a high-level overview of some of the most prevalent types of fraud found in government benefits programs today, as well as strategies for detection and prevention.

New, knowledge-based authorization (KBA) tools use improved techniques to stop fraud.

Authenticating Identity at the Point of Enrollment

It's impossible to talk about fraud without spotlighting identity theft, a phenomenon that occurs in the U.S. every three seconds, and impacts nearly every type of entitlement program, from SNAP to TANF to unemployment and beyond.

While the concept of individuals using stolen credentials for personal gain is nothing new, social media now makes it easier for criminals to obtain all-important proprietary information. Phishing scams lure people into divulging personal information, passwords and social security numbers to what they believe is a legitimate company or familiar organization. Others fall prey to social engineering, where a new Facebook 'friend' is really a criminal looking for a social networker with a propensity to 'share' too much. Whether identity thieves use one of these tactics, spoof a call or take a dumpster dive, they're uncovering treasure troves of personal data – and using it to illegally enroll in or divert funds from your benefit program.

Whereas, in the past, a drivers' license, address verification, and a correct answer to, "What's your mother's maiden name?" might have been enough to validate a person's identity, today, the answers to those questions are one quick web search away.

The best defense is using sophisticated authentication and validation tools to spot the fakes before they make it into the system.

Sophisticated Authentication and Validation Tools

New, knowledge-based authorization (KBA) tools, plugged into government contact centers, on-line enrollment sites and IVR systems, use a different technique to weed out the posers. These tools aggregate data to prompt compliant, non-credit-based, "out of wallet" questions to more accurately verify identity.

As the name implies, "out-of-wallet" questions are specific inquiries that can't be answered very quickly by looking through stolen credentials, and are typically something that only the real John Smith or Jane Doe would know. These multiple choice questions could range from, "What color car did you drive in 1998?" to "Which of the following states have you not lived in?" to "Who was your fourth grade teacher?" In addition to these questions, the KBA often throws in a "red herring;" an inquiry that should elicit a "none of the above" answer, if the applicant is really who he or she claims to be. This technique further weeds out the criminals, who typically guess at the correct response.

Based on answers to these questions, combined with other data, these tools use algorithms to automatically "score" the enrollee. Those who score a high percentage move through the enrollment process, while those in the lower percentiles route through additional authentication functions.

This same methodology is also effective in authenticating suspicious "change of address" transactions, to ensure the real benefits recipient is requesting the change. This extra effort is highly effective in deterring theft by making sure the disbursements don't get rerouted into the wrong hands, without inconveniencing people making legitimate requests.

Automating Eligibility Verification

Every agency knows that verifying identity is only one facet of the process. Step two is validating whether or not the individual is eligible to receive benefits in the first place.

A hosted enrollment system from a trusted provider automates this verification process, aggregating data from multiple sources to verify assets, employment history and other critical information needed to confirm eligibility. It eliminates manual processes and provides agencies with the necessary documentation to validate recipients more quickly and more accurately.

The ability to aggregate and analyze data in real time at the point of enrollment and throughout the disbursement process is the key to effective fraud mitigation.

Keeping Employer and Merchant Fraud at Bay

Of course, benefits fraud isn't limited to the recipient side. Fictitious "employers" set up mock companies, pay just enough into unemployment to cover employees, then, all of a sudden, multiple "employees" – either members of the owners' family or part of a crime ring – start claiming unemployment benefits totaling far and beyond anything the fraudulent company paid in.

SNAP trafficking, in which unscrupulous merchants pay 50 cents on the dollar to record illegitimate SNAP debits, continues to drain program funds. Government-subsidized daycare operators get stand-ins to inflate the reported number of children they serve. The list goes on and on.

Both up-front verification and ongoing monitoring are essential to finding and cutting off the fraudsters. The same eligibility systems used to authenticate beneficiaries can also vet employers, pulling in documentation from other sources to confirm location, identity and number of employees, and the fact that it's a real business at all.

Many agencies are exploring the use of biometric authentication to prevent fraud in eChildcare programs. Instead of relying on written documentation, operators check in children using a fingerprint reader to validate identity and get an accurate daily count of enrolled beneficiaries. With this methodology in place, operators can't claim 50 children when they're actually caring for 10. This fast, accurate methodology doesn't inconvenience parents or children, and improves accounting for childcare operators.

Biometric authentication and fingerprint readers can also be deployed to validate identity at point-of-sale or enrollment application for a variety of other programs.

Using Analytics and Mapping to Detect Suspicious Activity More Efficiently

No matter what precautions you take, some perpetrators will always sneak into the system. The key to reducing loss is recognizing and investigating suspicious behavior as quickly as possible. Although EBT cards and other electronic payment methodologies are rich sources of transactional and behavior data, until recently, this vital information often went unused.

By mining the data produced by benefit card usage every day, and applying analytics to uncover suspicious activity quickly, agencies gain a powerful fraud-fighting weapon.

Whereas in the past, the analytic process took months and extra manpower, new analytic tools use advanced algorithms to monitor behaviors and patterns in real time, sending alerts of suspicious behavior, based on preset parameters, directly to the fraud team's desktops for follow up. Lengthy, overloaded reports are now replaced by streamlined on-screen dashboards that provide a cohesive view of activity for rapid response.

With the right solution, technology partner and online transactional databases, an agency's staff can run reports, queries and slice and dice data instantly – without ever leaving their desks. Not only does this agility enable agencies to identify and follow up on potential fraudulent activity faster, but do it without adding headcount.

For example, let's say an agency wants to investigate a specific merchant on Beach Street in Anywhere, USA. Using an analytics system with a geo-mapping feature, the staff member can pull up a list of every benefits recipient who has purchased something from that merchant in the past five weeks. After extracting this list, he or she can produce a list of items bought, and then rerun the query to identify where the different buyers live.

If everyone's buying the same items, or if multiple recipients are driving an inordinately long way to get to the store, chances are, there's something illegal going on.

Predictive analytics, in which data is modeled based on specific patterns, enable agencies to anticipate problems based on its own history. When similar characteristics arise, the system recognizes the pattern, and flags the activity for further review and action.

Has merchant activity dramatically increased or decreased? Has enrollment spiked beyond preset norms? Are multiple payments for different recipients going to a single bank account? With the right tools, your agency can automatically extract customized reports, identify situations that trigger alerts, and generate a list of cases that warrant further investigation. The important part is that you can do it all fast enough to prevent the theft from escalating.

As fraud increases, agencies are looking beyond their own state boundaries. By collaborating and sharing data with other states, agencies can cast a wider net on fraud prevention and, with their provider's help, identify instances in which multiple state programs paid the same individuals during the same months. This extended use of analytics has already paid off for states in a recent pilot program, pinpointing a multitude of discrepancies and preventing thousands in lost funds.

The net-net? In the case of fraud mitigation, knowledge is power, and the party with the best data wins.

Staying One Step Ahead with the Right Fraud Prevention Partner

But, even with the right mix of technology, most agencies can't effectively tackle ongoing fraud mitigation on their own. The best defense is finding a technology partner who offers a full portfolio of tools, a highly developed analytics practice and a deep understanding of the intricacies of government benefits programs. This team becomes your "man behind the curtain," pulling the levers to enable technology to extract the right data and generate customized reports, and applying dedicated resources to monitor fraud on your behalf.

At Conduent, our fraud team brings proven experience from the world's leading banks, card associations, law enforcement and government programs to benefit our clients. We offer a comprehensive range of internally and externally managed tools, with a dedicated fraud team fully focused on finding, developing and implementing the tools that enable agencies to preserve program integrity and mitigate fraud before it occurs. Proprietary strategies and predictive analytics leveraging Conduent innovation set us apart from the crowd.

Whether we help you employ more stringent authentication practices like biometric verification or apply advanced data analytics to help you stop fraudulent activity faster, we help you take a stronger stand in the war against fraud – both protecting your funding and the people you serve.

And that's worth fighting for.

About the Author

Sheila Hoeppner is the Director, Fraud and Risk Systems for Conduent Public Sector Services. With nearly 30 years' experience in financial payments services, commercial banking and government benefits, she leads a best-in-class fraud and risk team that serves our federal, local and state government benefits payment card programs.

Prior to joining Conduent, Ms. Hoeppner served as Global Fraud Strategy Leader for GE Capital, where she led multi-national teams of strategy managers, decision scientists and business intelligence data analysts to develop, design, implement, monitor and enhance risk/fraud strategies and fraud mitigation tools for the company's private label and bank card accounts worldwide. She is also a Certified Green Belt in Six Sigma and Business Process Management.

CONDUENT™