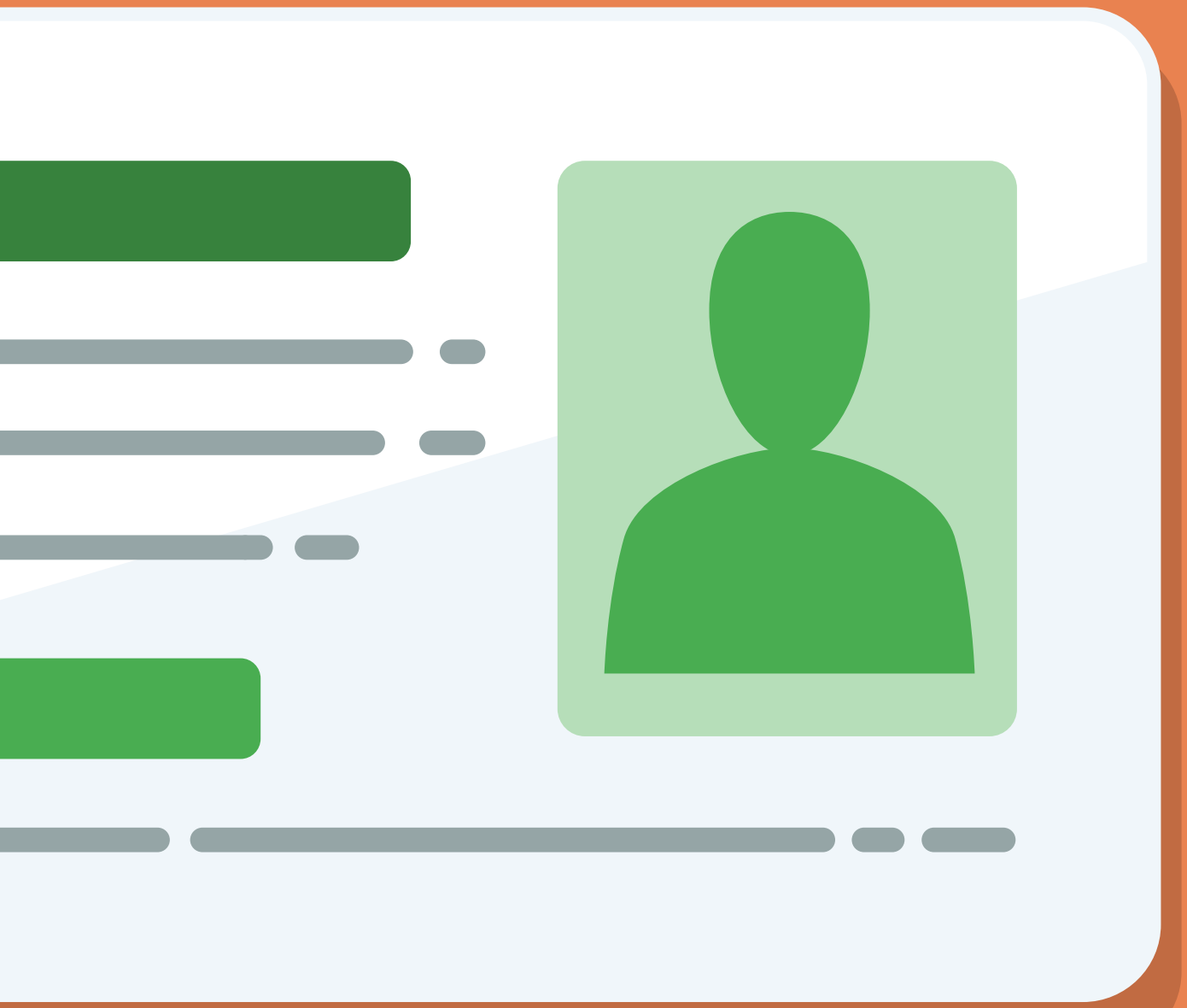

Modernizing Identity Proofing in Government

INDUSTRY PERSPECTIVE

Executive Summary

The rate of fraud perpetrated across the public sector is significantly on the rise. In 2015 alone, the Office of Management and Budget estimated 10.1 percent of all federal welfare payments to be fraudulent, totaling $71.5 billion. According to Javelin research, there were 15.4 million US victims of identity fraud in 2016. That's a 16 percent increase in victims over the previous year.

Billions of compromised or exposed identity records across thousands of data breaches annually create a rich market for nefarious use. And the bad actors are now well-organized and intelligent criminal organizations. Additionally, financial accounts are no longer the primary target in fraud schemes. Identity theft tactics are much more lucrative as they can yield multiple account access points and perpetrations across various marketplaces, both in the private and public sector.

To detect and fight fraud, government relies on identity proofing. The National Institute of Standards and Technology (NIST) defines identity proofing as a means "to establish the uniqueness and validity of an individual's identity to facilitate the provision of an entitlement or service." Proper identity proofing includes verifying identity documents, biographic information, biometric information and knowledge of personally relevant information or events.

Typical identity proofing techniques have traditionally included a series of personally identifiable information checks including name, address, Social Security number and date of birth. These checks have been paired with layered risk assessment, such as high risk conditional checks as well as one-time-passwords or tokens.

Most fraud prevention systems in government are similarly designed. Static processes can degrade over time in the face of more dynamic identity fraud threats. Escalating costs and labor needed for operations and maintenance, however, also weaken them over time. Additionally, communicating between a number of siloed datasets increases complexity. It then becomes harder to keep up with change, creating blind spots in government that fraudsters can easily exploit.

In order for government to keep up with the threat environment, agencies need to modernize their identity proofing strategies by applying more holistic, risk-based approaches. These approaches incorporate more sophisticated identity fraud methodologies.

GovLoop sat down with Keir Breitenfeld, Senior Business Consultant from Experian Fraud and Identity Solutions, to discuss the modernization of identity proofing in the public sector and how companies like Experian can help. Experian specializes in identity management and fraud detection across all markets including public sector.

In the following pages, you will also learn the primary challenges of identity proofing in the public sector, what modernization of identity proofing looks like and some best practices to improve identity proofing and management in your agency.

Challenges of Identity Proofing

As government agencies at all levels look for better ways to detect and mitigate fraud, there are a number of significant barriers to overcome.

First, the sheer range of fraud tactics can impede agencies from achieving security. There are a number of types of fraud, including account takeover, where fraudsters use malware, social engineering, or other data access scams to take over service accounts; first-party fraud, committed by an individual or group by opening an account with no intention of payment or legitimate use; identity theft, where fraudsters steal an identity using personal information; and synthetic identities which aren't real but are falsely 'verifiable' via data sources that have been cultivated to support their creation. These threats must be met with a variety of identity-proofing and management tactics. Without monitoring, performance assessments, and tuning, a singular and static identity proofing strategy can be exposed by evolving schemes and the usage of high quality compromised identity data. Traditional verification and validation parameters alone are simply too obtuse and can be easily circumvented by those with criminal intent.

Additionally, the number and diversity in the population of identities maintained by government is overwhelming. Unlike private-sector institutions that can be more selective about whom to provide services to, government must provide services to everyone that is deemed eligible. As Breitenfeld noted, "Agencies don't have the luxury of risk-based approvals or declinations of service requests that large financial institutions enjoy. They have to service a variety of users and citizens with rare exception and with varying degrees of data available."

"Since public sector identity proofing guidance and standards are more rigid, the challenges are two-fold really," Breitenfeld said. "First, there's positive identity proofing for the vast majority of legitimate applications and access requests. Then, government has to effectively segment fraud without impacting those legitimate users. The creation of standardized levels of assurance for use in identity proofing has been a positive step forward over the years. The difficulty, however, lies in achieving higher levels of assurance in populations that are often lacking in data availability or the tech-savvy to fulfill those requirements."

"Given the expanded guidance around identity assurance levels with 800-63-3, the presentation and verification of identity information is now coupled with the assessment of multiple pieces of evidence ranging in category from weak to fair or adequate to strong or superior. While this allows for more flexibility in accommodating various pieces of evidence in the identity proofing process as well as various ability for populations to present such evidence, it also demands that identity proofing platforms employ orchestrated workflows to determine sequential activities. These activities are designed to reach identity assurance as quickly and seamlessly as possible," Breitenfeld said.

Failing to comply with standards, however, can have devastating consequences. For one, agencies risk their reputation and accountability with the public and businesses they serve. Additionally, agencies with already tight budgets stand to lose a lot of money. "For many agencies, if you get it wrong or allow fraud to invade your processes, there's substantive risk of financial loss combined with unwanted attention from auditors, oversight committees and media," Breitenfeld said.

Lastly, when it comes to identity security and fraud prevention, one tool is rarely enough. A deadbolt lock makes a home safer, but doesn't protect a house from burglars as well unless paired with an alarm system or security camera. The same principle applies to organizational security.

Static rules based on overly simplistic verification and validation checks can easily be circumvented by intelligent fraudsters," Breitenfeld said. "Conversely, those same static rules must also have built in mechanisms to accommodate true name users that may not initially meet that criteria for identity proofing."

Vast and diverse populations, heavy regulations and operational as well as data silos all pose significant challenges for government.

But even as fraudsters' strategies continue to modernize, there is hope for government to modernize identity proofing as well.

To compound these challenges, government has stringent regulations and standards with which it must comply. Such standards include NIST's special publication 800-63-3, which defines electronic authentication as "the process of establishing confidence in user identities electronically presented to an information system." This document also provides requirements by which applicants can both identify proof and enroll at one of three levels of risk mitigation in both remote and on premise scenarios:

LEVEL 1 only requires self-asserted authentication

LEVEL 2 requires the need for either remote or physically present identity proofing

LEVEL 3 requires physical presence for identity proofing where physical attributes have to be authorized by trained representatives

Modern Fraud & Identity Strategies

Identity proofing standards and guidance continues to evolve in response to both fraud threats and the accommodation of vast user populations and applications they seek to access.

In many cases, the standards do allow for various techniques and decisioning workflows to be implemented. However, modernized identity proofing also requires balancing fraud risk mitigation, user experience and the need to provide services to the vast majority of those eligible.

"Today's identity proofing has to be multi-faceted," Breitenfeld said. "Organizations have to understand that certain individuals or identities have more information available than others. You can't just rely on credit profiles or public record data sources anymore. Those are siloed data sources and they're simply not enough."

There are many emerging trends and best practices for modern fraud and identity strategies, including:

- **Applying right-sized fraud and identity proofing solutions.** To reduce user friction or service disruption and appropriately manage fraud risk, agencies need to apply fraud mitigation strategies. Such strategies reflect the cost, measured risk and level of confidence as well as compliance needed for each interaction. This is called right-sizing the fraud solution. For example, agencies can cater a fraud solution that ensures seamless experience when a citizen is calling a service center vs. an online interaction vs. a face to face one.
- **Maintaining a universal view of the user.** Achieved by employing a diverse breadth and depth of data assets and applied analytics, this tactic is the core of modern fraud mitigation and identity management. Knowing the individual user extends beyond a traditional 360-degree view. It means having knowledge of a person's offline and online behavior, not only with your agency, but also with other agencies with which that user has a relationship.
- **Expanding user view through a blended ecosystem.** Increasingly, agencies are participating in a blended ecosystem — working with vendors, peer agencies, and partners. There exists a collaborative culture in identity and fraud management that doesn't exist in more competitive commercial environments. Fraudsters easily share information with one another, so those combatting it need to as well.
- **Achieving agility and scale using service-based models.** More agencies are adopting service-based models that provide greater agility and response to dynamic fraud threats, diverse population changes, and evolving compliance requirements or guidance. Service-based identity proofing provides government agencies the benefit of regularly updated data assets, analytics and expertise in strategy design. These assets are designed to respond to fraud or identity intelligence observed across various markets and industries, often protecting proactively rather than reactively.
- **Future-proofing fraud solution choices.** Technical and operational resources are always in relatively short supply compared to demand. Agencies need the ability to "code once" in order to expand and evolve their fraud strategies with ease. Future proofing solutions must also be combined with an ever changing set of identity proofing requirements and best practices, powered by a robust and innovative marketplace of service providers.

"Modernization is about making data more available and painting a more holistic picture of identities at both onboarding and user account management process points," Breitenfeld said. "You need tailored workflows within an identity-proofing platform to determine potential identity risks at all points in the customer or user lifecycle. Identity risk changes over time, so an identity that may have verified well with a low risk profile at onboarding can certainly become compromised later. It's critical that the identity proofing and management be ongoing rather than a single point in time activity. "

The future of identity proofing in the public sector is more than just verifying individual identities. Government must now use risk-based approaches and mitigation strategies to quickly identity threats and determine the type of fraud before damage is done.

"Modernization is about making data more available and painting a more holistic picture of identities at both onboarding and user account management process points," Breitenfeld said. "You need tailored workflows within an identity-proofing platform to determine potential identity risks at all points in the user lifecycle. Identity risk changes over time, so an identity that may have verified well with a low risk profile at onboarding can certainly become compromised later. It's critical that the identity proofing and management be ongoing rather than a single point in time activity."

Applying Risk-Based Approaches Via Identity Management Pillars

With fraud threats becoming more multi-faceted, identity-proofing solutions should encompass a variety of capabilities across the user lifecycle.

A comprehensive strategy across three primary pillars of identity relationship management can help. These pillars include identity proofing, authentication and identity management. Identity proofing provides checks and decision making with immediate access or prior to the issuance of user credentials for initial users. Authentication consists of supporting account access/login along with password resets and credential re-issuing for existing users. Lastly, identity management is the continuous monitoring of the user population via passive identity management diagnostics. These tactics are designed to isolate identities that have significantly shifted in identity proofing confidence or fraud risk.

Incorporating a true-risk-based approach with these identity management pillars will help agencies better customize tactics and workflows for each of the operational channels most likely to appeal to fraudsters. These areas include in-person, online, mobile, and telephone access or application points. Additionally, a risk-based approach allows agencies to apply the most effective controls for their unique applications and user populations.

The risk-based approach assumes that no single rule or even set of rules provides a comprehensive view of a user's identity and associated fraud risk. Instead, a risk-based systematic approach uses a process by which a set of user data sources and observations can power fraud detection models in combination with detailed user identity proofing and authentication checks.

A risk-based fraud-detection system applies predictive analytics and allows institutions to make user relationship and transactional decisions in a timelier, measureable, consistent, and auditable manner. These decisions are not based on a handful of rules or siloed data, but on a holistic view of the identity. Additionally, agencies can make such decisions based on the predicted likelihood of identity theft or true name fraud.

A risk-based approach allows government to:

Reduce fraud exposure.

Government can use analytics and a more comprehensive view of an identity (good and bad actors) with consistent and auditable decisions over time. Agencies can ensure they are complying with regulations while overcoming the challenges of simple, rules-based programs.

Improve citizen and user experience.

By applying the right authentication and treatment at the right time, agencies can subject citizens to processes that are proportional to the risk associated with their identity profile and requested services. Lower-risk constituents are then less likely to be put through an arduous course of identity prompts. This saves time for both agency staff and the user, enhancing user experience for everyone.

Increase operational efficiencies.

With the right risk-based program, much of the decisions on whether an identity proves to be a fraud risk can be done without human intervention. This can be done using score-driven policies based on hundreds of attributes where agencies can use automated and standardized identity proofing and authentication processes for their applicants or account management cases. Agencies can worry less about compliance, use fewer human resources, and pay service providers for only what they require to establish confidence in an applicant or user. This automation offers cost savings which in turn allows agency staff to focus on more manual or arduous aspects of identity proofing and fraud detection where needed.

Solutions to Identity Proofing

Experian helps agencies achieve identity proofing compliance and optimal performance, fraud mitigation effectiveness and positive user experiences.

This is accomplished by leveraging a robust identity management platform called CrossCore® and a consultative team of experts to support clients in the creation and management of identity management strategies and workflows.

"Our services, used by hundreds of clients processing billions of transactions, rely on us to provide single points of integration and auditable processes," Breitenfeld said. "This is done with a breadth and depth of identity intelligence and decisioning that balances compliance, cost, reputation and risk."

Tools like Experian's CrossCore platform offers a myriad of identity checks and risk assessments in configurable combinations designed to balance compliance requirements with true identity risk segmentation. Additionally, the platform enables actionable intelligence across the user lifecycle.

The CrossCore platform can accommodate these capabilities via a single inquiry and response in real-time or batch. CrossCore can be designed to support limitless client or calling system strategies via three distinct functions:

- **Workflows** designed to deliver a range of checks and confidence levels depending upon a user process point across the lifecycle (ranging from onboarding access and authentication as well as passive risk monitoring). Each workflow is developed to ensure both risk-based and compliance-based treatments allow for the right set of services to meet predetermined policies.
- **Orchestration** layer that further specifies which services to call in what sequence or based on what preceding attributes may exist. Via connectivity to various services, CrossCore then validates requests, transforms and normalizes messages and enriches the transmitted data for use in customized decisioning strategies.
- **Decisioning** is then performed to ensure consistent and measurable outcomes based on attribute level information gleaned from one or more services invoked. Decisioning strategies can be developed to meet various use cases ranging from onboarding and identity proofing to authentication and population monitoring across the lifecycle.

State Tax Refund – Identity Proofing & Risk-Based Workflow Optimization

PROBLEM

A state agency was facing high levels of taxpayer refund fraud applications. On top of that, the agency's call center was overwhelmed with manual review volumes increasing as a result of legacy processes.

SOLUTION

Using Experian, the agency worked to deliver a process that segments high risk taxpayers requesting refunds using a custom identity risk model. This model is comprised of identity verification results, identity histories and link analysis, state agency data and other proprietary and unique attributes.

For those taxpayers identified as high risk, they're directed to additional set-up authentication methods employed via an online session along with the submission of an out-of-band control number.

RESULT

The average fraud detection and savings equates to approximately $1.50 for each refund request or return. The state agency experienced a substantial reduction in outbound letters to taxpayers and call center volumes.

Additionally, the agency has more effective risk segmentation overall, allowing for more efficient use of resources and limited friction processing legitimate taxpayer refund requests. The agency achieved a 2:1 false positive rate in segmentation.

Conclusion

The fraud threat environment is expanding rapidly, growing in volume and sophistication. For government, this means that modernizing identity proofing, fraud detection and identity management techniques is imperative. While government faces challenges unique to the public sector, there is hope.

Using predictive analytics and workflows based on high-quality identity intelligence, risk-based approaches can greatly improve fraud detection and identity proofing within government. At the same time, agencies can better maintain compliance with emerging standards in identity assurance level attainment.

With a comprehensive view of each user and automated processes for identity management across the user lifecycle, agencies can implement a future-proofed set of operational procedures that will evolve with the changing landscape.

About Experian

Experian is the world's leading global information services company. During life's big moments—from buying a home or a car, to sending a child to college, to growing a business by connecting with new customers—we empower consumers and our clients to manage their data with confidence. We help individuals to take financial control and access financial services, businesses to make smarter decisions and thrive, lenders to lend more responsibly, and organizations to prevent identity fraud and crime.

We have more than 16,000 people operating across 37 countries and every day we're investing in new technologies, talented people and innovation to help all our clients maximize every opportunity. We are listed on the London Stock Exchange (EXPN) and are a constituent of the FTSE 100 Index.

Learn more at experianplc.com or visit our global content hub at our global news blog for the latest news and insights from the Group at experian.com/blogs/news.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop