Identity management... evolved

Foil fraud with a multi-layered, risk assessment identity management strategy.

Government programs, such as tax refunds and health and human services benefits, are under constant attack by a relentless and innovative population of fraudsters. In the wake of major ongoing security breaches, identities have become an easily accessible commodity allowing fraudsters to go online and purchase information ranging from basic name, Social Security number (SSN), address and date of birth (DOB) data, to complete social security cards, birth certificates and passports. Traditional, stand-alone identity management and verification tools are no longer capable of delivering efficient identity proofing while simultaneously fending off the onslaught of highly sophisticated fraud methods.

Identities for sale

- **Name, SSN, Address and DOB can be purchased online for as little as $5.00[1]**
- **Quality Social Security Cards, Birth Certificates and Passports are available for as little as $200[2]**

[1] Time Magazine [2] ReallyGoodFakes.net

Balancing government service delivery and risk management

As fraudsters become increasingly sophisticated, it is clear that identity management solutions need to incorporate a risk-based approach that looks beyond personal identity information when assessing fraud risks associated with identities interacting with agencies. Agencies must strike a careful balance between a critical need to employ stringent methods to prevent fraudsters from attacking their programs, and the need to ensure that recipients, citizens and/or beneficiaries receive the services they need in a timely and accurate manner. How are agencies balancing the acceptable level of risk with the impact to operations and their recipients?

The traditional approach

As the Internet matured, agencies began to offer online interactions with citizens, such as filing taxes and applying for benefits. These modernized systems provided better customer service and improved operational efficiencies, and were widely celebrated as “government online, not in-line.” However, fraudsters saw these new systems as an open invitation to commit mass fraud by interacting with systems that did not require them to step foot into an agency or present a physical ID. Often, agencies were left to investigate the fraud after the money or benefit had been released to the fraudster—creating a heavy burden on investigators and recovery agents. This reactive approach is called “Pay-and-Chase”—and it is neither efficient nor effective.

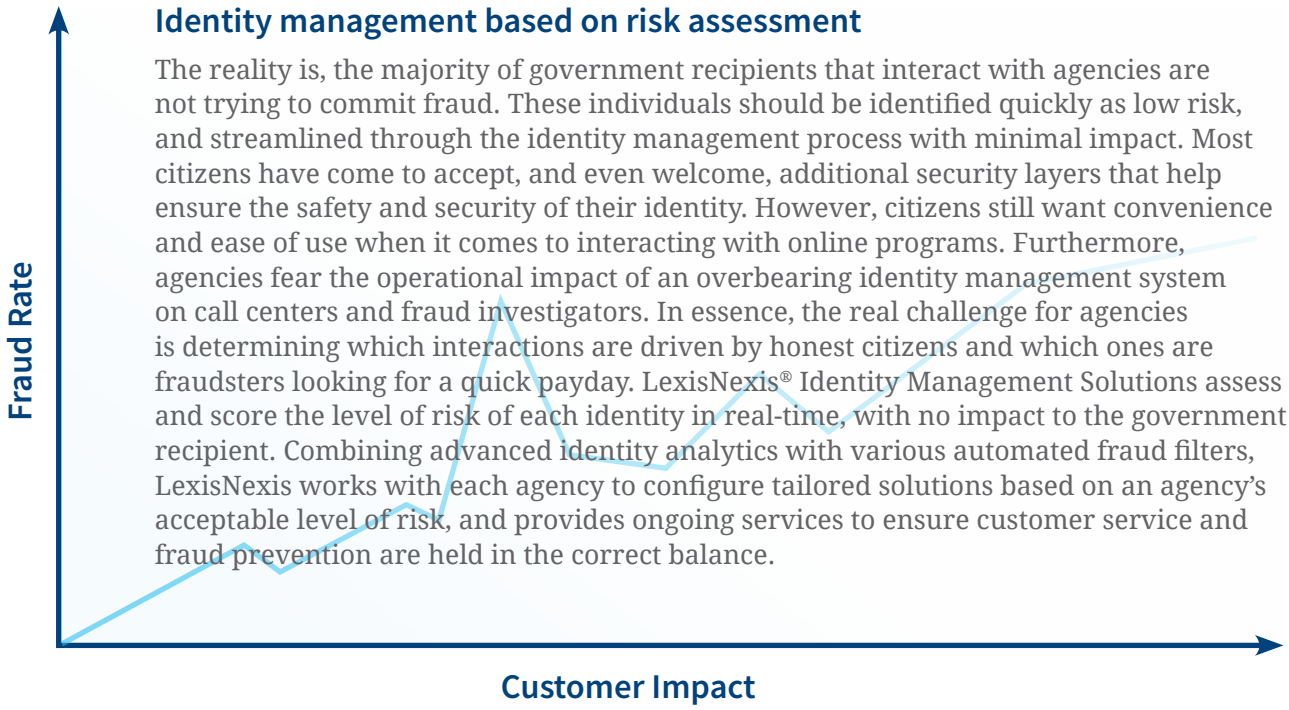
Over time, agencies began to implement Knowledge-Based Authentication (KBA). Industry leading KBA solutions work by first verifying that the Name, DOB and SSN are not fabricated, and match a known identity. Next, they ask a series of questions that only the true owner of the identity should be able to answer. For maximum effectiveness, KBA solutions should have access to vast amounts and combinations of public records data, financial information and even agency data. Solutions that reference only limited data sets are much less effective at preventing fraud and are unable to accurately authenticate a large percentage of users. Quality KBA solutions do provide a foundation for fraud detection and prevention and have been shown to mitigate the vast majority of common fraud attempts.

This layer of protection is the most commonly used for government organizations; however, more recently, highly skilled and highly motivated fraudsters armed with multiple pieces of identity data have proven to be capable of penetrating this layer. Fraudsters have evolved, and identity management solutions need to evolve with them—without making it more difficult for honest recipients or citizens to access important services.

A more advanced approach

As digital government accelerates, government recipients are demanding the ability to interact with agencies from multiple devices such as mobile phones and tablets. In fact, statistics show that today, a growing number of citizen interactions related to government services take place on mobile devices. As this trend continues to make government services more accessible to recipients, it will allow agencies to communicate with their citizens in new ways, and enable agencies to learn more about who is interacting with them.

40% of smartphone users with an income of less than $30,000 go online mostly using their cell phone.[3]

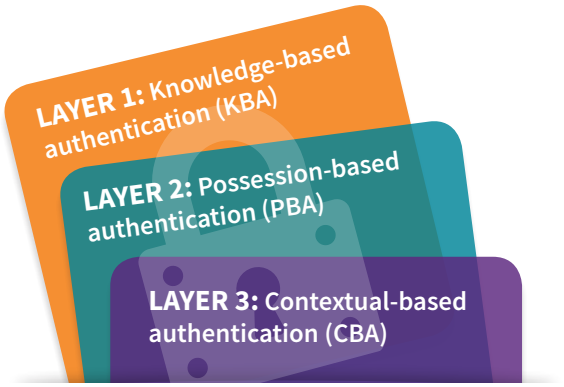


Identity management based on risk assessment

The reality is, the majority of government recipients that interact with agencies are not trying to commit fraud. These individuals should be identified quickly as low risk, and streamlined through the identity management process with minimal impact. Most citizens have come to accept, and even welcome, additional security layers that help ensure the safety and security of their identity. However, citizens still want convenience and ease of use when it comes to interacting with online programs. Furthermore, agencies fear the operational impact of an overbearing identity management system on call centers and fraud investigators. In essence, the real challenge for agencies is determining which interactions are driven by honest citizens and which ones are fraudsters looking for a quick payday. LexisNexis® Identity Management Solutions assess and score the level of risk of each identity in real-time, with no impact to the government recipient. Combining advanced identity analytics with various automated fraud filters, LexisNexis works with each agency to configure tailored solutions based on an agency's acceptable level of risk, and provides ongoing services to ensure customer service and fraud prevention are held in the correct balance.

Adopting a multi-layered defense strategy

More than just a trend, leveraging innovative identity data, analytics and insight driven technology to employ a multi-layered, risk-based fraud defense strategy is inevitably where the future of identity management is headed—and LexisNexis is blazing the trail. The layers of a multi-layered, risk assessment fraud defense strategy include:



Layer 1: Knowledge-based authentication (KBA)
Focus: Something known

The knowledge-based authentication (KBA) layer includes information that, theoretically, only the legitimate owner of the identification would know, for example:

- Email
- ID authentication quiz with personalized questions

Layer 2: Possession-based authentication (PBA)
Focus: Something owned

As the name suggests, possession-based authentication (PBA) requires the individual to have a particular item in the possession in order to pass this security layer. Here are a few examples of PBA methods available through LexisNexis identity management solutions:

- A One-Time Password is texted to a known smartphone, and then entered on the appropriate website
- A One-Time Password is emailed to a known email address and entered on the appropriate website
- A photo of the correct driver's license accompanied by a "selfie" photograph

Layer 3: Contextual-based authentication (CBA)
Focus: Something done

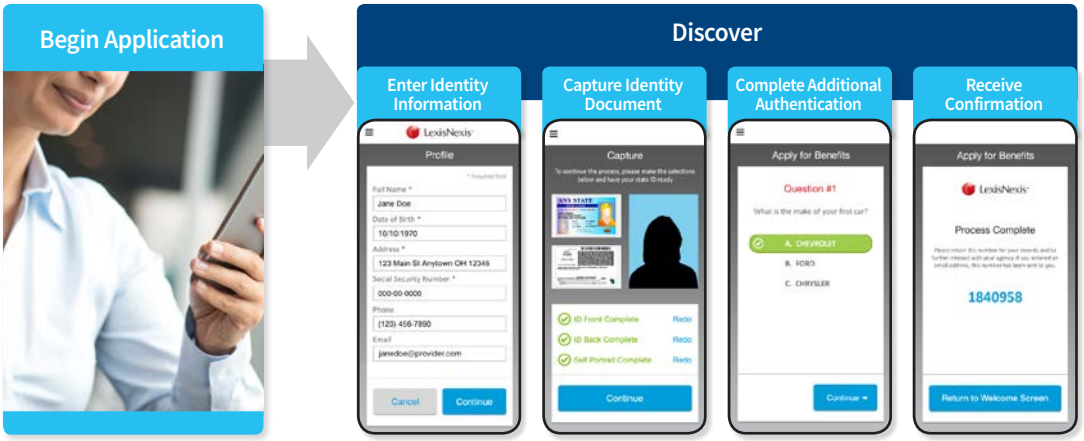
Contextual-based authentication (CBA) is an automated technology that takes advantage of the digital signals, trails and patterns triggered and established by device usage. Similar to credit card companies monitoring card usage patterns and flagging unusual spending, CBA analyzes multiple factors associated with the device being used during the ID validation process and flags anomalies that are indicative of fraud, for example:

- IP address recognition
- IP geolocation
- Device ID and attributes
- Device/IP traffic velocity

The risk score can be used to determine which authentication pathway (and how many fraud defense layers) each individual will be required to take. Low risk users may only be required to answer an easy knowledge-based authentication quiz, while high risk users (with multiple red flags) may be required to pass through multiple authentication layers, such as using one-time password or driver's license verification through a mobile application. LexisNexis understands the staffing, budget and policy of agencies can change, and works directly with agencies to configure a solution to minimize the impact on "good identities" and stop fraudsters before they impact systems.

In the world of mobile

More and more individuals are ditching the desktop in exchange for mobile and tablet devices. That is why LexisNexis has developed LexisNexis® Identity Snapshot—a multi-layered identity proofing solution that offers all of the flexibility and risk assessment features of our integrated Identity Management Solutions, including ID document capture and "selfie" image capture. Identity Snapshot is an easy way for agencies to leverage technology that citizens already use in order to be confident in the security of their online interactions with citizens.



The right tools can get the right money, benefits and services to the right people

With government recipients frustrated by the state of our nation's fiscal health, and increasing initiatives by the federal government to reduce improper payments, multi-layered identity proofing that incorporates an identity risk assessment is a strategic necessity for all agencies. With LexisNexis Identity Management Solutions, agencies can quickly validate and authenticate identities with confidence, stopping false identities from entering your system, reducing fraud and ultimately saving your agency resources and preserving revenue sources for those who truly deserve them.

For more information, call 866.579.7638 or visit lexisnexis.com/risk/government

LexisNexis® RISK SOLUTIONS | Government

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.

Our government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity and discovering and recovering revenue.

[3] WillowTree Apps, Mobile Trends in Low Income Communities, October 2012. http://willowtreeapps.com/wp-content/uploads/2012/10/mobile_lowincome_v2.pdf

Identity Management Solutions provided by LexisNexis is not provided by "consumer reporting agencies" as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and does not constitute a "consumer report" as that term is defined in the FCRA. Identity Management Solutions may not be used in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other eligibility purpose that would qualify it as a consumer report under the FCRA. Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified.