Positive ID: How the right identity strategy does a world of good for public healthcare and social services
In 2018, poverty in the U.S. fell to record lows.\(^1\)

Analysis of data from the U.S. Census Bureau and Columbia University\(^2\) attributes this to the effectiveness of our nation’s “safety net” programs. Programs that have slashed the poverty rate in America by nearly half since 1967. But recent events have shown how quickly things can change, and how important these programs can be.

This is how conversations about identity management should begin. Because this is the big picture. You are in the business of human well-being. The work you do positively impacts countless lives. What if you could do more of it?

The ability to positively verify beneficiary identities so you can efficiently deliver services is the critical first step.

Fast, accurate identity verification helps you

- Deliver faster, more efficient service
- Meet regulatory requirements
- Protect citizens from identity theft
- Ensure fiscal stewardship

\(^1\) Center on Budget and Policy Priorities, “Economic Security Programs Cut Poverty Nearly in Half Over Last 50 Years,” 2019
\(^2\) Ibid
IDENTITY INTELLIGENCE ISN’T JUST A SAFEGUARD. IT’S AN ENABLER.

According to the most recent U.S. Census data available, an estimated 1 in 5 U.S. residents are served by a means-tested government program. Currently the six main federal public assistance programs serve more than 175 million beneficiaries³ (including those in multiple programs).

These numbers are sure to continue rising substantially as the US weathers the ongoing health and economic impacts of COVID-19.

Even in normal times, various reports show that large numbers of people don’t apply for the benefits they’re entitled to. In recent years, almost half of the older Americans who qualified for the Supplemental Nutritional Assistance Program (SNAP) weren’t enrolled.⁴ One commonly cited reason has to do with the enrollment process.

A sample of comments from media reports brings certain issues to light:

- **Lack of Internet access**/difficulties using a computer
- **Limited transportation**/inability to get to in-person interviews
- **Long lines** at county offices
- **Notices mailed to residences**, addressed to applicants who are homeless or transient
- **Systematic problems** attempting to provide information to the agency by phone or fax
- **Mishandled or lost documentation** supplied to agency

⁴ Abdul Latif Jameel Poverty Action Lab/MIT, “Low-income Americans are missing out on the public benefits they’re eligible for. Simple interventions can help.” 2018
Unfortunately, the media is quick to highlight problems in public agencies without presenting the realities.

Many agencies are working with significant resource limitations, operating with legacy tools and manual processes that don’t live up to the expectations of a modern, digitally driven world.

Data breaches have compromised the identities of hundreds of millions of Americans, and criminals have honed their impersonation skills. This makes identity proofing and verification more complex and increases customer friction as more scrutiny is applied.

Applicants may be enrolling in duplicate benefits, unknowingly or on purpose — possibly under a different name. Tracing this history across agencies often delays the process.

Caseloads can quickly multiply. 2019 marked the fifth consecutive year that the U.S. suffered 10 or more billion-dollar climate-related disaster events. Job losses in the manufacturing and automotive sectors nearly doubled in the first nine months of 2019 compared to the same period in 2018. Sudden economic disruptions can bring an influx of demand for assistance, straining already-tight infrastructure.

The COVID-19 crisis crystallizes how quickly the demand for public services can escalate and strain resources. In just two months, the U.S. went from a 50-year unemployment low of 3.5% to a 14.7% surge in jobless Americans – the highest since the Great Depression. 33.5 million people applied for benefits over a 7-week period between March and May 2020.

---

1 National Oceanic and Atmospheric Administration, Billion-Dollar Weather and Climate Disasters Overview, 2019
2 24/7 Wall St, “Job Losses in 2019 Highest in 4 Years as Manufacturing and Auto Industries Falter,” 2019
3 The Center for Infectious Disease Research and Policy, “US job losses due to COVID-19 highest since Great Depression,” May 8, 2020
4 Associated Press, “33 Million Have Sought U.S. Unemployment Aid Since Virus Hit,” May 7, 2020
These dynamics challenge your ability to deliver aid in the way you wish you could.

Applicants and beneficiaries may be subject to difficult, time-consuming processes at a very stressful period in their lives. Caseworkers struggle with heavy workloads to review and approve. Investigators have their patience tested with excessive “false positives” and time spent chasing down leads.

*It’s time for a new approach to identity proofing and verification. One that:*
There’s a lot to consider. Let’s break it down.

Life has twists and turns — and so does life’s data

Data sets can be messy and difficult to harmonize. “Cynthia Baker” may also be known as “Cindy Baker,” “Cindy Lynn Baker” or by her maiden name, “Cynthia Lynn Hardy” depending on the database. The data you need comes from a variety of siloed locations, each with their own unique identifiers. This makes it hard to link data sets and spot connections between:

- Individual data elements
- Clusters of people, and
- Patterns of behavior.

It may not be obvious that Cynthia is newly married to Lawrence (a.k.a. “Larry”) Baker. And that her new husband is already enrolled in a housing voucher program which now covers her too. Likewise, a caseworker might not recognize that in addition to his new wife, Larry now has a 5-year old stepson in his household.
DATA BREACHES CREATE URGENCY FOR ENHANCED CONTROLS

The Federal Trade Commission’s Consumer Sentinel Network received nearly more than 650,000 reports of identity theft in 2019.\textsuperscript{9} And more recently, in the midst of the COVID-19 pandemic the U.S. Secret Service issued an alert of massive fraud perpetrated by a Nigerian crime ring against multiple state unemployment insurance programs. Between March - April 2020, Washington state found fraudulent claims totaling $1.6 Million.\textsuperscript{10}

Traditional knowledge-based authentication (KBA) that’s reliant on personally identifiable information (PII) has been a staple of account onboarding and security. However, as long as cybercrime exists, agencies need to augment this method with additional controls. The rise in synthetic identities makes this ever more urgent. Fraudsters use pieces of real identities alongside fake ones — or even multiple legitimate identity elements from different people, which makes them appear genuine enough to get past the gate.

These concerns prompted the U.S. Government Accountability Office to audit the identity proofing practices at six federal agencies that provide citizen benefits. Their findings, released in May 2019, reveal that agencies need more guidance on how to successfully implement alternative methods, particularly when serving large and diverse populations.\textsuperscript{11}

\textsuperscript{9} Federal Trade Commission, Consumer Sentinel Network Data Book 2019, published 2020
\textsuperscript{10} The Seattle Times, “Washington halts unemployment payments for 2 days after finding $1.6 million in fraudulent claims”, May 14, 2020
\textsuperscript{11} United States Government Accountability Office, Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes, 2019
WHAT’S THE “IDEAL” IN IDENTITY PROOFING AND CORROBORATION?

The 2018 Market Guide for Identity Proofing and Corroboration by Gartner urges leaders to strengthen legacy identity proofing tools and processes by investing in new technologies. Think broader than “fraud prevention” when building a business case: consider the potential revenue impacts of reduced false positives, lower consumer abandonment rates and improved customer experiences.

Seven characteristics of an airtight solution

1. **It’s designed as a continuous and contextual process** that begins at initial application.

2. **It’s built on two essential features:**
   - **Expansive, high quality data sets** that are recent (internal databases and limited free tools miss too much and can become quickly outdated).
   - **Powerful linking** that 1) can account for fuzzy matching or variations in the way data is represented, and 2) fills in missing gaps.

3. **It leverages both physical and digital identity elements.** Applicants and beneficiaries may be connecting with you in person or remotely, using a mix of channels and devices. You need to quickly trace activity across touchpoints and confidently connect it back to a singular identity. It’s also important to corroborate digital identities to help identify “out of the norm” behaviors and detect larger potential patterns of fraud.

Commonly used physical and digital identity elements include:

- PII
- Document-centric verification (driver’s license, passport, etc.)
- Biometrics (facial recognition, fingerprint)
- Email addresses
- Social profiles
- IP address
- Geolocation
- Device ID
- Digital user patterns (such as typing rhythm or swiping motion)
Data alone is not enough. This is about quickly making sense of data so you can keep the process moving in the right direction.

Solution short-list: Look for tools with the intelligence to make decisions based on multiple factors:

- Risk level of a domain
- Sudden spikes of activity and/or patterns of behavior that indicate increased risk
- Age of identity data
- Patterns of behavior or linkages between people that suggest escalated risk
- Inconsistencies in the identity data

It’s flexible and multilayered to address varying risk levels. For example, an interaction meant to route applicants to a particular office based on ZIP code would not require the rigorous security protocols of a direct deposit benefit payment. The National Institute of Standards and Technology issued new guidance in 2017 advocating a “mix and match” approach that enables agencies to select assurance levels based on their own risk assessment and user population.

- May involve a mix of passive, behind the scenes insight — i.e., based on known data points and the connections between them, behavioral attributes and/or device assessment — as well as step-up measures (i.e., knowledge-based/possession-based methods)
- Allows for “pseudonymity” when only part of an identity is required: for instance, asserting that an applicant is a certain age rather than querying the entire birthdate; this minimizes possession of sensitive information and protects privacy
- Enables you to swiftly move the “good” applicants through which improves user experience
- Improves resource management and cost containment by focusing manual interventions where truly needed
- Must account for variations in citizen demographics too — a digital native may have very different expectations/interaction styles than a senior citizen, for example

Ideally, you should leverage a contributory network so you can tap into insights beyond your own immediate agency/location.
It gives you visibility into larger patterns of activity such as dual participation scenarios or coordinated fraud schemes.

Should be capable of tracking dual participation both interstate and intrastate regardless of distance.

Eliminating dual participation in Medicaid alone can reduce national program costs by more than $106M annually

Needs to be sophisticated enough to stay ahead of fraudsters who continually update their tools and schemes. Data sharing across agencies and across state lines is essential:

Aids investigations  +  Helps establish risk thresholds and workflows in upfront verification activities

It's designed for public agencies:
Built to address the unique sensitivities of social services. Supported by knowledgeable experts who can help you decipher the data, create actionable plans and stay ahead of evolving technologies and risk patterns

Not just technical experts:
Professionals from law enforcement, national security intelligence, military intelligence and fraud should comprise the team
WE UNDERSTAND YOUR CHALLENGES. WE CAN HELP.

LexisNexis® Risk Solutions Identity Assessment & Assurance solutions offer the solution breadth and depth that makes identity proofing and authentication a true value driver. And a force for good across public healthcare and social services agencies.

More data on more U.S. residents than any single provider

- Immediate access to 10,000+ additional data sources and billions of relationships
- ThreatMetrix® for Government Digital Identity Network providing access to shared digital identity intelligence from over 6,000 entities (including commercial, financial and streaming services)
- Ability to locate about 98% of people who apply; compare this to credit file-based remote identity proofing sources like the Federal Hub that may be challenged to positively identify those with limited credit histories, certain immigrant populations and victims of identity theft

Solutions built specifically for the Government sector

- Designed for the way citizens and public agencies interact; provides for optimized user experience and agency workflow

A Special Investigations Unit that’s part of the package

- A team of cross-trained analysts with the skills, tools and expertise to help you make sense of big data, identity patterns of fraud and solve special challenges
- Helps your agency conduct research and assists with investigations
- Built into our solutions offering

Networked insights across agencies

- Government-specific contributory databases (technology supporting National Accuracy Clearinghouse, Risk Intelligence Network, Program Participation Analyzer) that provide inter-agency visibility into identity and risk patterns
- This collaborative exchange speeds agency services levels and adds muscle against large-scale, sophisticated fraud rings
- $116M in annual savings achieved in 5-state pilot alone; network continues to grow
OUR SOLUTIONS ARE PROVEN TO:

+ **Speed** the customer application process
+ **Reduce** transaction delays
+ **Optimize** workflow decisions for a more efficient operation

+ **Support** positive identification even in unbanked or underbanked communities
+ **Lower** abandonment rates
+ **Reduce** false positives and manual reviews
+ **Control** costs associated with improper payments

**Example:** We helped the State of Florida achieve $1.1B in SNAP cost avoidance over a 6-year period.²

Let’s do this.

Together we can solve a major pain point in public healthcare and social services at the federal and state levels, and benefit millions in the process. **Contact us to learn more:** 800.869.0751 or visit [https://risk.lexisnexis.com/government](https://risk.lexisnexis.com/government)

² Florida Department of Children and Families, Office of Public Benefits Integrity Annual Report 2017-2018, published 2019

---

**About LexisNexis Risk Solutions**

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit [www.risk.lexisnexis.com](http://www.risk.lexisnexis.com), and [www.relx.com](http://www.relx.com).

The LexisNexis Accurint services discussed above are 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 do not constitute “consumer reports,” as that term is defined in the FCRA. Accordingly, these LexisNexis Accurint services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used 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. LexisNexis, the Knowledge Burst logo, and LexID are registered trademarks of RELX Inc. Accurint and Relavint are registered trademarks of LexisNexis Risk Data Management Inc. © 2020 LexisNexis Risk Solutions. NXR14429-00-0520-EN-US