LexisNexis®
RISK SOLUTIONS

ARTICLE

The Power of Digital Identity Assurance

By Amy Crawford, Director of Government Services Strategy, LexisNexis® Risk Solutions

Understanding identity is central to navigating the ever-evolving cybersecurity threat landscape and essential in ensuring government agencies have a secure, effective, positive interaction with those they serve. Delivering safe and equitable friction-appropriate service starts with a clear understanding of what comprises an identity — both the physical aspects and the digital. In this article, we will discuss the power — and importance — of digital identity assurance for the public sector.

ARTICLE

The power of digital identity assurance beyond identity verification

In the identity space, assurance can be defined as confidence — a certainty that the individual or business with whom your agency interacts is, in fact, who or what they proport to be. Identity assurance can also include your agency's confidence in its identity proofing or identity verification solutions. As we continue to move further away from the pandemic, government agencies continue to migrate more and more towards serving constituents at their point of need — online.

Assurance is required because people and businesses engage more often with online web portal sessions and less physically in person, creating added challenges and complexities. Traditional identity proofing and identity verification solutions only verify that the entity claiming to be "Amy" has Amy's information, leaving your agency vulnerable for taking the entity at its word. Some solutions can verify that, Amy — or rather this entity that claims to be Amy — has Amy's information and can answer questions about her. But it does not prove that this entity is in fact Amy. Because the identity landscape has changed, **we need to go a step further into identity assurance.**

It goes back to the adage, "trust but verify." The verification we complete through digital identity assurance exposes online risk and, by exposing risk, we can determine whether this entity can be trusted and is the purported individual. In today's world of identity, we must ask the following:

1. Is this entity Amy, or is it Amy's device being used by somebody else?

2. Has somebody compromised Amy's device?

3. Also, does this device originate from a geolocation or physical address consistent with the last time Amy came to our web portal?

ARTICLE

Risk aspects indicating account takeover threats or identity theft

When it comes to digital identity assurance, here at LexisNexis® Risk Solutions, we look for evidence of whether the device is trying to conceal its true source or location. Our solution evaluates whether that risk is consistent with an online entity using a stolen identity, because we consider Amy's device footprint as an integral facet of her complex identity.

Threat actors and criminals are constantly looking for an easy path to commit crime, and they will typically exploit the easy vulnerabilities. Online criminals with an individual's personally identifiable information (PII) will use it to try to convince an agency or organization that they are, in fact, the individual. Any device masquerading as someone else will typically hide where it truly is coming from, so fraudsters play tricks to conceal and cover up any details about their true source.

To combat this — LexisNexis Risk Solutions can review information such as **network timestamps** that reveal the device originates even on another continent, completely outside the scope of that agency's intended customers or citizens that should be coming in.

Additional identity assurance leverages **behavioral biometrics** to review the sensor data from the device. This exposes if the device is compromised, revealing ports that are typically used by remote access trojan (RAT) malware.

Additionally, we can expose if the device **is physically moving** while in use, or if the sensors instead indicate zero motion while the person/device appears to be actively online.

Our solution also provides insight into the digital history linked to each device including associated risk. Your agency can query to look for specific types of risk, such as velocities and the anomalies mentioned earlier.

The core of what we do is data science, intelligence, analytics, and technology. Our 10,000+ data sources, platform strength, and proprietary linking with 99.999% precision, work together to drive results.

LexisNexis® Risk Solutions can help your agency deploy multi-dimensional intelligence and risk frameworks proactively, so you can counter threats without impacting speed or constituent experience. This intelligence can free up resources, drive transparency, strengthen trust, and enable better outcomes.

ARTICLE

Identity verification may not be enough

Fraudsters do not stop, they evolve. Identity verification must also constantly evolve to keep up with new fraud trends and technologies. A multi-layered approach to identity verification is more critical than ever. When the overwhelming availability of stolen personal identifiable information (PII) is combined with easy-to-acquire and leverage deception technology, a single identity verification step is not going to keep any government program safe. These threat actors use automated scripts and BOTs to enter PII on millions of webforms on open web portals, improving the accuracy of PII, essentially cleansing the data.

When an identity verification solution does just that (and only that) — verify the correctness of the PII provided — it is ripe for exploitation.

This “blind trust” identity verification process is getting exploited at an increasing rate and is a leading source of agency fraud — both online and in call centers.

Prevention requires evaluating identity risk starting with the device, especially its history and decisioning. This needs to be completed before an agency can assume the person interacting with their web portal or call center is legitimate. LexisNexis® Risk Solutions can help accomplish this by understanding identity with precision.

ARTICLE

The evolving identity threat landscape is increasing in sophistication and constantly changing

The protections implemented by many government agencies have the potential to become a behemoth of stacked capabilities, less effective at stopping fraud because they have been designed to tackle issues that have occurred in the past. With our solution, you are completing checks at the front door that take the burden off the traditional paths that lead to exploit and vulnerability.

What about a data breach? No organization wants to go through that, especially government agencies. Statistically speaking, however, it will happen, and it may not be in the core agency itself. It could be a supplier or a third party with whom your agency works, such as, a merchant who conducts back-end credit card transactions. The merchant may have a data breach and threat actors targeted the agency due to their privileged connections. Now they have citizen data to use repeatedly around the country. This is yet another situation where our solution can help. Stolen breached identity data can be reused for account takeover or account creation. Our workflow solution exposes the risk presented by threat vectors and can help prevent future new account creations, or account takeovers.

Effective security enhances the end user experience

From a constituent user standpoint, once positive trust is determined, it leads to relaxed friction. Our solution minimizes noisy, high-risk traffic, and then pre-screens and determines trust with each device entering an agency's web portal workflow. When a known, trusted user returns to an agency's site after a prior positive experience, and as this user continues to exhibit trusted positive behavior, their friction reduces and the trusted user continues to enjoy a positive experience with your agency.

The end user perspective is one where risk workflows are transparent with no perceived latency. Data-driven decisioning revolutionizes risk strategies and is a significant step forward for equitable access. LexisNexis® Risk Solutions helps agencies deploy multi-dimensional intelligence and risk frameworks proactively, so you can counter threats without impacting speed or the constituent experience. This intelligence can free up resources, drive transparency, strengthen trust, and enable better outcomes.

This intelligence can free up resources, drive transparency, strengthen trust, and enable better outcomes.

ARTICLE

Building trust with constituents through a risk decisioning network

Risk is not always negative as our solutions also evaluate positive risk — or indications of trust. **Trust Tags** evaluate risk based on prior sessions, not only for any single agency, but for any global organization contributing to our LexisNexis® Digital Identity Network™. These prior sessions can include, for example, other agencies with which this same person has engaged, as found in our 6,000 plus customer ecosystem. From this, we have a good idea about the kind of trust they have exhibited in prior engagements and in these other locations and leverage that trust when that individual or business interacts with your own agency.

Trust Tags reduce friction when positive trust is determined. Your agency no longer has to push every user through verification. Trusted individuals can now experience risk-appropriate friction — a significant step forward in achieving user experience satisfaction. As a result, agencies end up with happier constituents.

ARTICLE

The power of digital identity linking

Our service is built on attributes, and attributes start at the device. Initially, we may collect as many as thirty-six device level attributes which are not based on personally identifiable information (PII). These attributes are very similar to what web portals collect, such as browser version, operating system, the brand of device hardware, etc.

Our service then places a **LexisNexis® ThreatMetrix® ExactID™ cookie** to identify the device and determine if it has been seen before. When the device returns to an agency's web portal, it's ExactID™ will recognize it again. The solution also associates the device to its **LexID® Digital identifier**, its unique digital identity. We can now review whether we can trust this device, and more importantly, does the device indicate any new risk? This incremental digital identity intelligence empowers additional precision, contextual history and reference.

Additionally, our solution exposes **velocity risk**, such as indicating that this is the 25th device seen by this LexID® Digital identifier. An agency's own policy can review this information to evaluate if this may be a negative risk to the organization. For most organizations, a user with over five devices begins to indicate negative risk. The higher the number of devices, the higher the risk. Velocity can also be caused by a BOT or some other automated process that's probing for information, or a weakness, and there is a significant amount of that activity happening on the public Internet.

The solution also reviews for **anomalies**, such as how many physical addresses have been associated with the same LexID® Digital identifier. This empowers agencies to make actionable decisions and gain indicators on whether this is a trusted device or if there is new risk. Many scams and online crime can often be exposed by revealing multiple identities linked to a single physical address. Other potential anomalies could include the same LexID® Digital identifier using numerous shipping addresses and policy rules that increase the negative risk weight (score).

ARTICLE

The value of digital identity assurance and the benefit in terms of orchestration or workforce optimization

Many of our customers leverage our services to integrate with other workflows and we can provide intelligence for existing agency workflows in multiple different use cases. For example, some states are not allowed to reject anyone applying for state benefits. Instead of rejecting a high-risk applicant, these states instead create a digital file of that online session, flagging it for additional scrutiny.

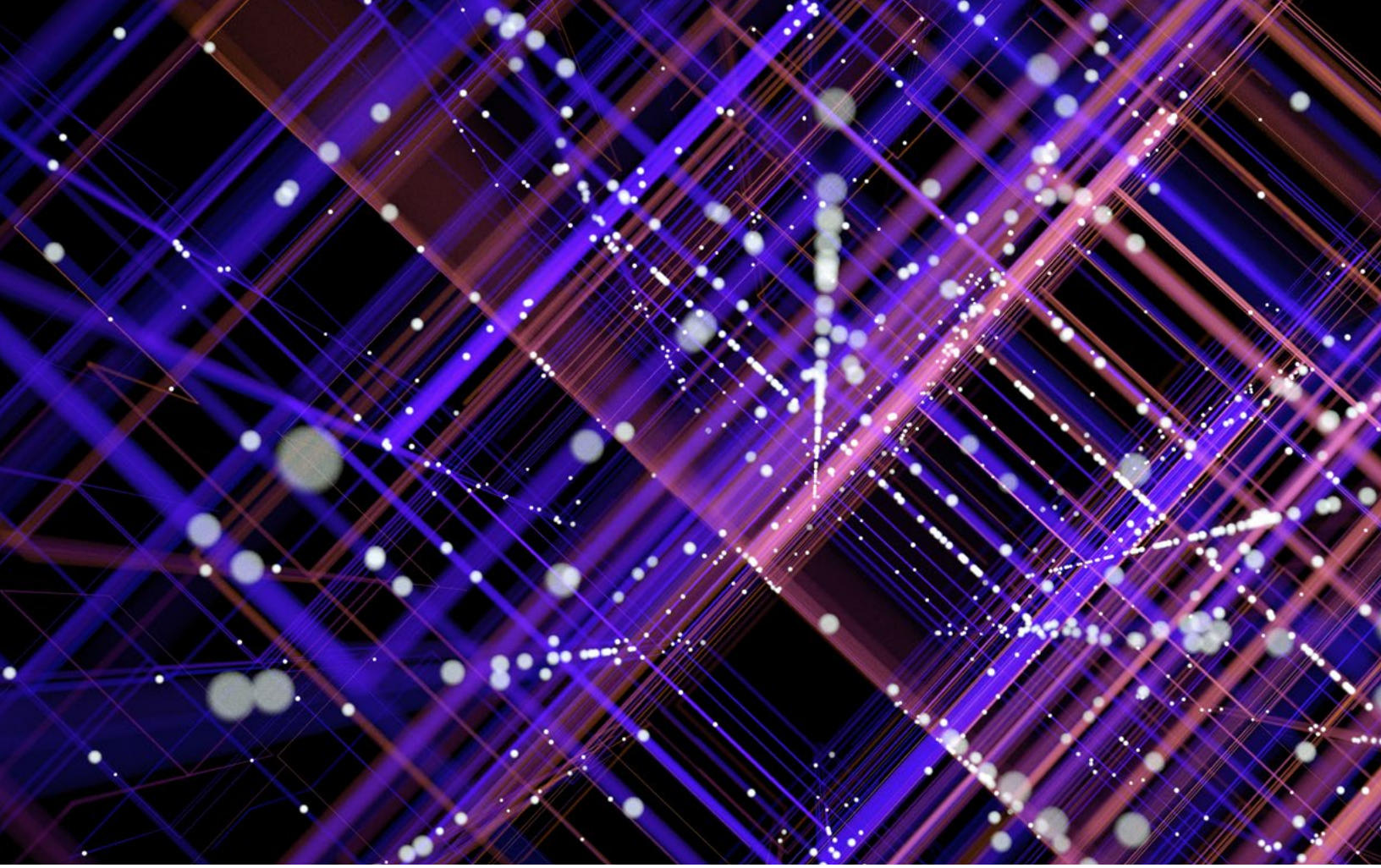
This benefit qualification can include any flagged fraud detected, or in other cases, we can determine that trust was high with measured risk being very positive during the session. From the information retrieved, your agency now has the ability to make a more informed decision.

Identity Made Simple. The LexisNexis® Risk Solutions Advantage

We collaborate with agencies to help them achieve their missions with ease. From empowering transformation, to delivering secure services to help drive efficiency, transparency, and oversight across channels and agencies. LexisNexis® Risk Solutions accomplishes this by understanding identity with precision.

The core of what we do is data science, intelligence, analytics, and technology. Our 10,000+ data sources, platform strength, and proprietary linking with 99.999% precision, work together to drive results. LexisNexis® Risk Solutions can help your agency deploy multi-dimensional intelligence and risk frameworks proactively, so you can counter threats without impacting speed and the constituent experience. This intelligence can free up resources, drive transparency, strengthen trust, and enable better outcomes.

In my role, it's my mission to leverage everything we understand about identities and risk, to help create secure and effective solutions for government agencies that inspire confidence and trust amongst those they serve.



LexisNexis® RISK SOLUTIONS

For more information:
Scan QR Code or Call 1-888-216-3544

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 (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.