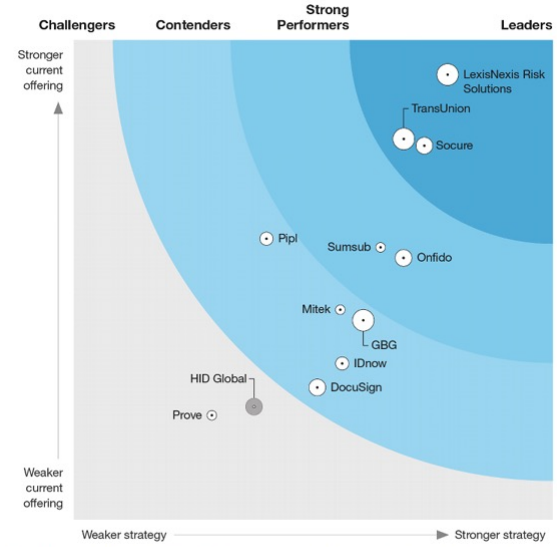
LexisNexis®
RISK SOLUTIONS

Implement Front-End Identity Verification to Reinforce Equitable Access While Stopping Online Fraud

The moment of greatest fraud risk to a potential applicant or current client is during eligibility determination. In recent years, LexisNexis® Risk Solutions ("LNRS") has seen government programs crippled by the overwhelming volume and "noise" of bot or machine-based application attacks using stolen or fabricated identity information. These attacks not only resulted in the outright theft of benefits, but swamped administrative systems to the point that legitimate applicants were either unable to call for assistance or forced to deal with the kind of delays that are not acceptable for a critical benefit program.

State benefit programs require the application of identity authentication techniques that are secure – ***but do not interfere with the swift delivery of needed benefits to legitimate applicants*** to protect program integrity from persistent, collusive attack. LNRS expects this attack vector to increase exponentially as the dark web is now reporting the use of bots to overwhelm the call centers.



LexisNexis Risk Solutions was recently announced **as a leader in the latest Forrester Wave report for Identity Verification Solutions**[2]

LNRS is ranked as a leader in The Forrester Wave™: Identity Verification Solutions, Q4 2022.[1]The report is evidence of LNRS market leadership in the identity authentication space without negatively affecting recipient experience.

The validity and benefits of the LNRS approach have been demonstrated in state and federal benefit programs nationwide. LNRS can streamline access for legitimate claimants, reduce administrative fees, and make it difficult for bad actors to the extent they abandon their attacks and stop bombarding these programs with illegitimate claims.

Our unique award-winning identity intelligence, combined with expertise in advanced analytics and services enable the LNRS solutions to outsmart fraud effectively and quickly without impacting participant experience.

LNRS is a recognized global industry leader in identity assurance, with over 45 years of experience acquiring assets and developing leading-edge solutions to protect the validity of identity use within critical government, financial, and legal contexts nationwide.

LNRS holds unique data assets that are of direct benefit to state-level program administrators related to an essential identity risk defense

Physical Data Attributes

LNRS provides header information from all three credit bureaus, augmented by over 10,000 additional sources, resulting in a comprehensive understanding of the population overall, and not just those individuals with deep credit histories. This data insight means that LNRS can recognize and securely authenticate the broadest possible range of potential applicants, without making them go through additional steps or processes. Our decades long history of gathering and making sense of identity records provides the ability

to recognize authentic and safe identities versus high-risk identities, by checking against elements such as name, SSN, date of birth, etc., alongside more sophisticated indicators of potential identity theft and misuse.

Digital Identity Resources

The LNRS extensive digital resources leverage a proprietary global network of intelligence comprised of individual connections with technology and online behavior. This layer of digital identity insight is critical when operating within current online and mobile channels. Often times the only indication that an application is high-risk is detection through digital means. Successful identity thieves can replicate individual information and answer questions related to their victims. What they cannot do is interact digitally in legitimate ways. LNRS digital resources can "pierce" the use of VPNs and proxy servers, to detect where on the globe an application is truly originating from. LNRS can detect the use of bots, or machine auto-fill of information in rapid fashion, using sophisticated behavioral biometric tools to highlight areas of concern. LNRS email risk detection capabilities are augmented each day with thousands of known compromised email addresses from a global consortium of e-commerce vendors. ***Perhaps the best part of the digital layer of risk defense is how thoroughly invisible it is to legitimate applicants.*** As long as applicants are not deploying elaborate VPN structures, or filling pages of application material in sub-second speed, the applications of those in need are processed without any disruption.

The LNRS deep data insight context recognizes the format in which individuals have appeared and should appear within public records. By connecting this data insight with the global resources of digital identity intelligence tools, LNRS provides a consolidated workflow that makes the process very easy for legitimate applicants, while remaining very hard to foil, even to those sophisticated fraudsters who have "successfully" stolen a physical identity.

This combination of resources means LNRS can deliver on strategic goals for state-level programs

An efficient process for legitimate applicants — that can automatically perform full identity assurance without forcing high volumes of applicants to undergo time-consuming additional steps required to overcome data shortcomings. Agencies can recognize masses of individuals and link them to known/secure device connections by leveraging the power and scope of LNRS data. In fact, LNRS data insight is sufficiently comprehensive that majority of applicants can be securely authenticated in a completely "frictionless" manner, with no additional activity on their part, expediting access to benefits.

An equitable process for all applicants — enables a seamless experience for applicants regardless of their socioeconomic status or credit standing, especially when compared to credit-data-driven solutions, which can force a disproportionate number of low-income individuals to undergo manual authentication techniques. LNRS recognizes that agency populations such as SNAP iare vulnerable and unique, and that traditional identity proofing tools are likely not appropriate for these individuals.

Our consolidated approach means that LNRS can provide security seamlessly for the majority of applicants, without resorting to problematic approaches such as facial recognition, or forcing them to take extra, time-consuming steps via help desks or in-person appointments to authenticate their applications.

This combination of capabilities has made LexisNexis Risk Solutions the vendor of choice for countless identity assurance projects across high-profile financial and government applications nationwide.

LexisNexis® RISK SOLUTIONS

For more information call 1-888-216-3544 or visit