LexisNexis®
RISK SOLUTIONS

Get Actionable Insights into Data Trends for Better Decisioning

Special Investigations Unit (SIU) Delivers Deeper Level Understanding of Identity & Risk

By Ryan Blackwood, Senior Manager, Special Investigations Unit, LexisNexis® Risk Solutions

The **LexisNexis® Risk Solutions Special Investigations Unit (SIU)** offers next-level support in preventing fraud and identity theft. It has a full complement of advanced investigative tools and technology at its disposal, enabling it to cut across information silos and reduce system-wide vulnerabilities. In this interview with Ryan Blackwood, Special Investigations Unit, LexisNexis® Risk Solutions, we review how the SIU utilizes agency data to help uncover trends and patterns for better decision making.

What does the SIU do?

We provide agencies with actionable insights, utilizing all the tools, data and platforms available from LexisNexis Risk Solutions, as well as Open-Source Intelligence, to ensure that the platforms and solutions that our customers are using are effective and working as they are intended. We also provide insight into data trends and patterns that agencies may not know about due to limitations in manpower, technology, or data. This allows them to make better decisions about their population to ensure benefits and tax dollars are going to those that are entitled to them.

What types of expertise does the SIU team have?

Our team has over 150 years of combined analytical experience in the government and commercial space, specifically government intelligence and crime analysis. We are experts at finding patterns in data using a wide range of analytical tools and helping government agencies make better decisions.

What challenges are you seeing and how do they impact agencies?

The biggest challenge we are seeing with agencies is preventing and responding to an adversary that is using complex tools and methodologies to attack benefit systems. The pandemic allowed criminals and transnational criminal organizations to hone their skills and tradecraft. They are using sophisticated technologies such as generative Artificial Intelligence, deepfakes, and automated/scripted attacks with legitimate Personal Identifiable Information (PII) to appear as though they are real people. The technology is sophisticated but easy to use, and criminals are sharing their “methods” online in chat rooms and can quickly adapt. Simply looking for disposable emails, IP velocity, or verifying PII is not going to cut it anymore.

How does the team help agencies?

We assist in a variety of ways. First and foremost, we help them look for risk in their populations and identify those that are causing the most harm and are likely fraudulent. We provide the identities we’ve uncovered, along with our overarching analysis, back to the agency for them to act. When utilizing our front-end or back-end solutions, we also constantly monitor performance to identify anomalies and alert us when something seems off. We are also regularly proactively digging into the data to ensure that legitimate folks get in, and the bad ones are stopped on the front-end. When we identify risk, we provide it to the agency for them to investigate further. If the platform needs to be tweaked or optimized based on this research, we work with our technical teams to provide recommendations for improvement.

What type of analysis does the team do?

We mainly look for risk and likely fraud, and to do that we utilize a combination of analytical methods, from link analysis to geospatial analysis. We begin by reviewing an agency's population at a highlevel through layering our identity data on top of the agency data to identify patterns and known Tactics, Tradecraft, and Procedures (TTPs). We then explore new and evolving attack methods using our data and analytical tools. Next, we identify various networks and drill down into groups and individual identities to possibly find subjects of interest. Lastly, we review any attack to see what happened, how our platforms performed against it, and what signals our platforms provided. We then take those signals and incorporate them into any optimization processes.

What types of reports does SIU provide?

We provide various analytical reports depending on where in the sales process we are. At the beginning of an implementation, we conduct a population risk analysis which documents our analytical findings of the overarching risk, as well as significant patterns or unique aspects of the research. Our most basic report is the Fraud Analysis Report, which is a one-to-two-page document that explores a new pattern or tactic that we have seen in the data. We also can provide platform monitoring reports which provide a customer insight into how their platforms are performing over time. Lastly, we provide all of our customers with Fraud Alerts, which are new schemes or tactics we have observed that are impacting more than one customer. Fraud Alerts allow the SIU to share what we are seeing in the data with our customers across the government space.

What advice would you share with agencies?

You should consider a layered approach when protecting your government systems on the front-end. Also, work with your investigative teams, as too often the investigations groups are cut off from the folks that are implementing a front-end identity system. A front-end identity system is not a technology problem or issue, and in many instances is treated as such. It's an identity problem, and investigative teams like the SIU know what works and what doesn't work to prevent fraud and facilitate legitimate individuals. We are involved in every step of the process – from the implementation phase where we review configurations and workflows, to production a year out, we are always involved in analyzing data or consulting on best practices.

What have you seen approach-wise that has delivered good results?

Those agencies that are utilizing a layered, risk-based approach that can quickly respond to different types of attacks. We have also seen tremendous results when an agency that works closely with the SIU to respond to different challenges. Agencies that simply take our identity data and attempt to build their own machine or system tend to have a harder time understanding it all. They are experts in their data and tools – we are experts in our data and tools. When we have ongoing, open dialogue with our customers, that tends to have the best results.

How do agencies access SIU?

Agencies have many ways of getting a hold of us. They can contact us directly at SIU@lexisnexisrisk.com or work with their LexisNexis Risk Solutions contact – sales rep, project manager or SIU analyst. We pride ourselves on being open, accessible, and easy to work with. The SIU analyst is a part of this team because they love this work, and they love helping people.

LexisNexis® RISK SOLUTIONS

For more information, scan QR code.

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 o-ices 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.