Pursue Portfolio Growth with More Confidence

Detect application fraud via highly predictive risk scores and data attributes.

The rush to digital transformation has caused organizations to offer online services without adequate defenses. Data breaches have increased the availability of personally identifiable information (PII) on the dark web. The result has been an average 29% increase in fraud costs in digital channels for U.S. lenders between 2021 and 2022.[1]

At the same time, organizations face increased compliance pressure from regulators. And customers expect frictionless experiences whenever they interact with your company. How can businesses meet these disparate demands?

Increase efficiency and revenue potential with Fraud Intelligence

The LexisNexis® Fraud Intelligence solutions suite can help you defend against new account acquisition fraud as you grow your portfolio. It provides clear, concise insights to inform your decision-making.

What distinguishes the Fraud Intelligence solutions suite is its extensive data sources and proprietary machine learning technology used for analyzing that data to deliver meaningful insights. One of the data sources that powers the Fraud Intelligence solutions suite comes from the LexisNexis® Inquiry Identity Network, an expansive data consortium network containing over 17 million reported frauds and over 24 billion consumer application events.[2]

Contributions from consortium members – including but not limited to banking, retail, FinTech and wireless carrier customers – add two billion transactions annually and over 10,000 new identity elements to the Identity Inquiry Network per day in real time.[3]

Another data source that powers the Fraud Intelligence solutions suite is one of the largest collection of public record and proprietary data sources in the industry, giving the Fraud Intelligence solutions suite the ability to provide organizations with a unique, more holistic and powerful view of 286 million identities in the U.S. and U.S. territories.[4] Those vast data assets, merged with leading-edge technology, enable businesses to discern identity fraud and implement sustainable, scalable mitigation strategies.

Detect third-party application fraud

LexisNexis® Fraud Intelligence Third-Party Scores provides a three-digit risk score that empowers smarter decisioning at the new account acquisition stage of the customer life cycle. With each score comes up to six warning codes describing the most influential risks driving the score, increasing efficiency in investigative queues.

Over 200 attributes indicate fraud risk, such as:

Digital anomalies
- Lack of Name and DOB elements and/or long strings of digits are indicative of randomly generated email accounts
- Large number of unique IP addresses associated with identity elements in a short period of time

Rapid exploitation
- High fraud occurrences perpetrated within the first 24 hours of the initial fraud event

PII tumbling
- Name and DOB associated with multiple SSNs and vice versa
- Name and DOB or SSNs tumbled with address or phone from other identities

Source record activity
- Short time on file and recency of last update
- Limited number of sources and types confirming identity

PII anomalies
- SSN is invalid by SSA standards, issued prior to date of birth or reported as deceased
- PII elements reported in past fraudulent applications
- Multiple suspicious identities associated with the consumer's address

– Application velocity of compromised identities is **6x higher** than legitimate identities.[5]

– **46%** of fraud associated with a compromised identity occurs within the first 24 hours of the compromise.[6]

In a recent test with a top-five card issuer, Third-Party Scores resulted in a $25 million fraud loss savings with a fraud detection rate of 59% at 3% risk depth, and a fraud detection rate of 88% at 1% risk depth.[7]

Uncover synthetic identities

Synthetic identity fraud drives significant fraud losses across the customer journey.[8] **LexisNexis® Fraud Intelligence Synthetic Scores** leverages over 170 indicators of fraud risk, such as:

Network emergence

- Lack of typical life events such as a driver's license or voter registration
- No known family members

Contact field crowding

- Phone numbers repurposed
- Mailing and/or email address repurposed

Recent bureau existence

- New addition to credit profile
- Lack of public record history

Synthetic Scores delivers a substantial improvement in fraud capture over existing solutions. A recent test, combining Synthetic Scores with Third-Party Scores, uncovered a $14.3 million fraud loss savings by detecting 60% of third-party fraud and 30% of synthetic fraud.[9]

Refine your fraud score with powerful data attributes

LexisNexis® Fraud Intelligence Attributes delivers 300 attributes, giving you a more granular and more comprehensive view of consumers. The attributes equip you with the flexibility and versatility to build solutions across identity fraud types for use in internal models, policy rules and manual reviews.

In recent tests, Fraud Intelligence Attributes showed a 15% lift over legacy attribute solutions.[10] The attributes improve predictive analytics, from new account opening to portfolio management, via four feature categories:

1. Application Element: Gain a historical and current overview of the input PII elements' source history on file. Learn whether those elements came from specific governmental and institutional sources, credit bureau, voter registration or other proprietary sources.

2. Application Stability: Corroborate PII via the number and types of sources that confirm the input PII elements reported together. Highlight patterns of incongruence by scrutinizing the number of unique PII elements associated with each other and with the identity.

3. Identity and Relationship: Discern the type of sources that report the identity, the emergence of that identity, whether the identity is deceased, the number of relatives and associates within that identity's network, and where and when those identities are first reported.

4. Consortium Network: Harness velocity and reported fraud associated with input PII elements supplied by members of the LexisNexis Inquiry Identity Network.

Help your organization grow its portfolio confidently via the LexisNexis® Fraud Intelligence solutions suite.

Contact us for more information. Call 408.200.5755 or visit
risk.lexisnexis.com/products/lexisnexis-fraud-intelligence

LexisNexis®
RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions includes seven brands that span multiple industries and sectors. We harness the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. 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 risk.lexisnexis.com and www.relx.com.

[1] *2022 LexisNexis® True Cost of Fraud™ Study: Financial Services and Lending Edition*

[2-3] LexisNexis® Inquiry Identity Network

[4] risk.lexisnexis.com/our-technology/lexid

[5] Based on internal analysis

[6] Based on internal analysis

[7] Source: a regional bank's card applications from 1/2018 – 6/2021

[8] *2022 LexisNexis® True Cost of Fraud™ Study: Financial Services and Lending Edition*

[9] Source: a top-five card issuer's applications from May 2021 to December 2021

[10] LexisNexis analysis using historical bankcard applications ranging from July 2018 through Dec 2019