LexisNexis®
RISK SOLUTIONS

HOW SHARED GLOBAL INTELLIGENCE IS CHANGING FRAUD DETECTION AND PREVENTION

![LexisNexis Risk Solutions logo]

INTRODUCTION

Digital transactions and interactions are enjoying growth like never before. Due to the Covid-19 pandemic, even previously digital-shy businesses were compelled to rethink their digital presence and offer a range of mobile apps and online transaction options to meet changing consumer behavior. It was a matter of survival.

The result has been a digital transformation that has completely reset consumer expectations and preferences. The digital transformation has also spawned alternative payment methods such as digital wallets and buy now, pay later options, which enable businesses to appeal to the widest range of customers. This in turn further drives mobile and online transactions in an ongoing upward spiral.

With more and more of the population transacting digitally, there is a steady stream of personal information and other details feeding the datasphere, providing fertile ground for abuse by bad actors[1]. But fraud is a significant concern across all channels, devices, geographies, and business sectors.

Access to more accurate, more comprehensive data is critical to managing fraud risk. When combined with analytic technology, machine learning, and behavioral biometrics, the intelligence gained from this data can help companies more effectively identify high-risk activities across the customer journey – and do so without compromising the customer experience.

In this white paper from LexisNexis® Risk Solutions, we explore the changing digital landscape, its impact on fraud, and how a multi-layered approach is instrumental in delivering valuable insight into customer interactions for more informed risk decisions.

DATA AND THE DIGITAL WORLD

From established economies across Europe
and North America to small villages in emerging
markets, the digital world is booming.

This explosive rise in data is fueled by a digital transformation that shows no sign of slowing.

In 2021, internet penetration was pegged at more than 60% of the world's population[2] and by 2030, an estimated 90% of people six years of age and older will be active online.[3]

As people continue to embrace digital for all aspects of their daily lives, information collected at every touchpoint, from every transaction and each time a consumer completes an online form, will continue to feed the bottomless well of digital data.

Like DNA molecules which together provide a code that makes each human unique, these interactions add vital bits of information that help to build a consumer's digital identity and global footprint.

Data analytics from digital transactions, emails, digital behavior and mobile devices can shed light on a consumer's buying habits, allowing businesses to tailor offerings to specific needs. The data can also help businesses more reliably identify trusted customers to minimize the risk of fraud.

Although data can offer valuable insight to support risk decision-making, leveraging the embedded intelligence and working with vast stores of information is challenging on several fronts.

For data to be truly useful in fighting fraud, it needs to be:

Timely

Old or out-of-date data leaves the window open for opportunistic fraudsters to swoop in and place orders on an account that should have been closed or use an address that has changed. Data needs to be updated in real time or near real time to provide one of the strongest defenses against fraud.

Trustworthy

Data may be up to date, but if it isn't more accurate, more complete and from a reliable source, it may result in poor decisions regarding which transactions to trust and which to block.
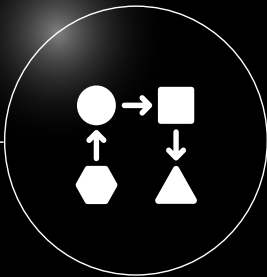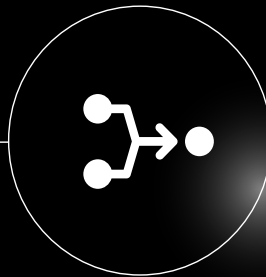
Comprehensive

Fraud and fraudsters are not constrained by boundaries, so data needs to be global and span a full range of business sectors, industries, devices, etc.
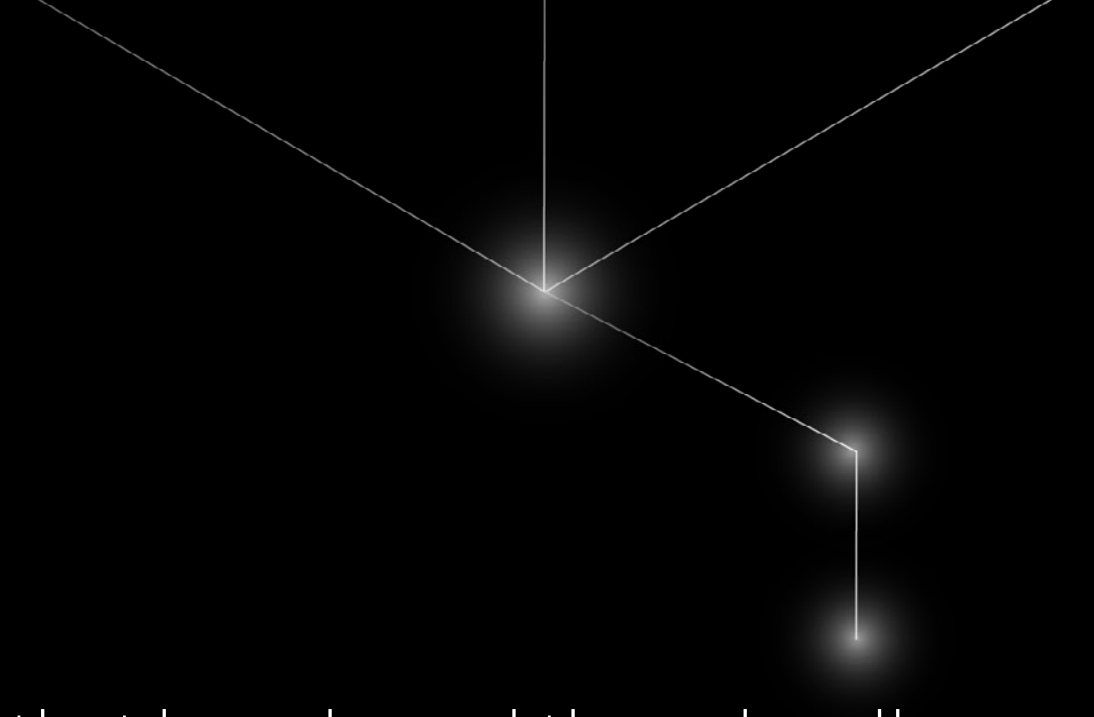
Accessible

Information should be easy to access so decisions can be made without delay to ensure a seamless customer experience.

Aggregated

It is time consuming to gather customer details from different sources and hope that each is providing more accurate, more complete and up-to-date information. Data that is available from a single, dependable database will offer greater efficiency.

Data that has cleared those hurdles must also be usable. In other words, it should provide organizations with the ability to extract actionable intelligence to support identity verification and fraud risk management.

Good data quality, enhanced analytics and automation are key for better decision making, successful customer acquisition and retention, improved customer relationships and ultimately business growth.

THE COST OF FRAUD

Data and fraud are profoundly linked. The ease with which digital data (email addresses, passwords, transaction details, etc.) can be compromised serves as a magnet for bad actors who are adept at identifying vulnerabilities that enable them to use this data to commit fraud. In addition, both data (or more specifically, poor data) and fraud can be costly.

LexisNexis®
RISK SOLUTIONS

2022 True Cost of Fraud Across the Globe

Each year organizations lose nearly $13 million[4] due to poor data quality. Fraud can be costly to businesses as well. In 2022, it is estimated that for every fraudulent transaction, the cost to business is over 3x the lost transaction value.[5]

NORTH AMERICA

3.74 times the lost transaction value

↑ 14% since 2019

U.S. financial services & lending = 4.00

EU MEMBER COUNTRIES

3.52 times the lost transaction value

↑ 12% - 35% since 2019

financial services & lending = 4.34

APAC

3.99 times the lost transaction value

↑ 10% - 16% since 2019

financial services & lending = 5.24

LATIN AMERICA

3.68 times the lost transaction value

↑ 6% since 2019

financial services & lending = 4.78

SOUTH AFRICA

3.51 times the lost transaction value

↑ 42% since 2019

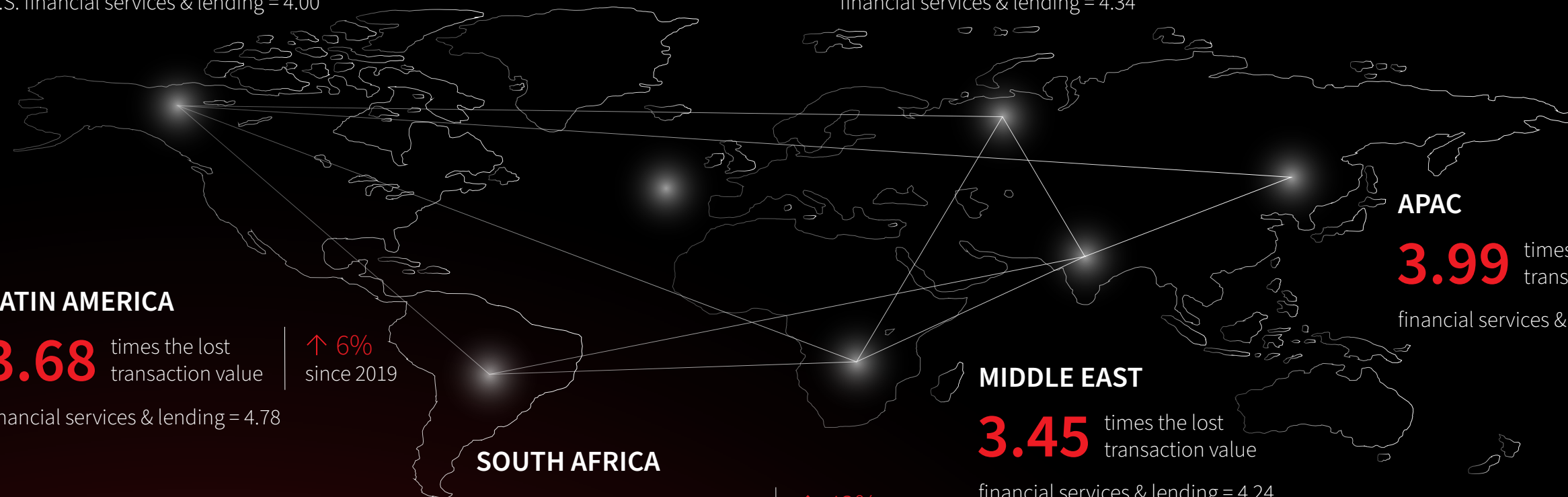financial services & lending = 4.23

MIDDLE EAST

3.45 times the lost transaction value

financial services & lending = 4.24

In addition to the financial cost of fraud, there is the potential for reputational damage, which can be more difficult to measure in absolute terms, yet deeper and longer lasting. A customer who has one bad experience – perhaps an issue with opening an account or where their personal data was compromised – may be loath to transact business with that company in the future. New businesses are most at risk as they have not had years to build a loyal following. Loyal customers may be willing to overlook one bad experience or even one breach of trust, but that 'generosity' is unlikely to extend to new customers doing business with an online company for the first time.

With consumers continuing to gravitate to digital markets there has been a corresponding rise in automated bot attacks, human-initiated attacks and other attack vectors that enable bad actors to gain access to valuable information. It is clear that identifying and preventing fraud is no easy feat. Fraudsters have proven themselves to be increasingly sophisticated and incredibly agile; honing their tactics to pivot quickly. When one avenue of deception is closed, they find new and creative ways to exploit weaknesses elsewhere.

Identity theft, including account takeover (ATO), new account application fraud, and synthetic identity fraud, are among the most common types of consumer fraud. In fact, identity theft is a major contributor to fraud losses across the customer journey.[1]

Adding to the complexity and insidious nature of fraud is its breadth – fraud occurs across industries, platforms, business types and geographies, often with networks of fraudsters using the same lists of stolen identities.

The challenge organizations face is finding more comprehensive information that will enable them to reliably distinguish trusted customers and interactions from potentially fraudulent ones.

Equally important, is how to do this across every interaction throughout the lifecycle of the relationship while providing the most seamless experience possible for customers.

In 2022:

Automated bot attacks:

+38%
GROWTH YoY[6]

Human-initiated attacks:

+23%
GROWTH YoY[6]
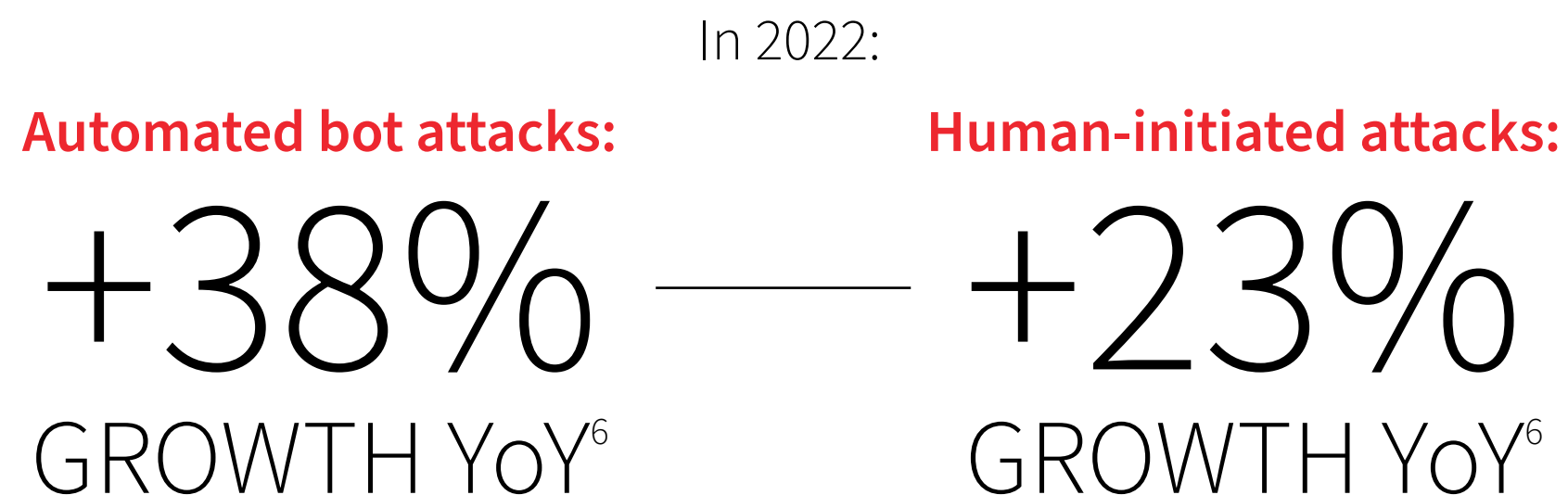
DOING BUSINESS IN THE GLOBAL DIGITAL ECOSYSTEM

The boom in mobile traffic and the overall growing trend towards digital has led to a corresponding shift in the ground rules. What might have once passed as an effective fraud mitigation strategy now leaves gaps.

It is no longer sufficient for an organization to rely on home-grown customer data for fraud risk management under the premise that they are 'just a local business.'

That approach can leave the business exposed to risk. In a global universe where boundaries have dissolved, customers may be worldwide, and fraud spans all industries. Fraud strategies often involve different industries, with fraudsters attacking each at their weak point - from data breaches to customer social engineering.

Fraudsters are not industry specific; they are industry agnostic. Fraud opportunities arise regardless of the customer's business model.
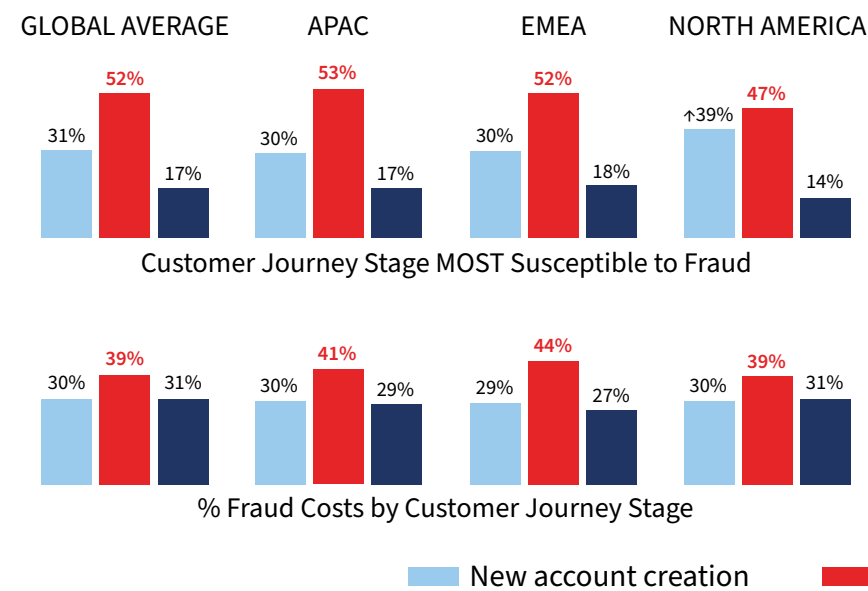
For an organization to truly know who they are doing business with requires a broad view based on visibility into multiple touchpoints and behaviors throughout the customer journey, including account login, new account opening, and purchase transaction. For an efficient risk assessment and identification of returning users, analyzing both physical and digital attributes are key. One or two isolated data points, such as a name and physical address, are not sufficient as they can easily be spoofed. However, if it is known that the digital identity has been at the same IP address with the same information through many previous trusted transactions, it increases the level of confidence that this person is who they say they are and can be trusted.
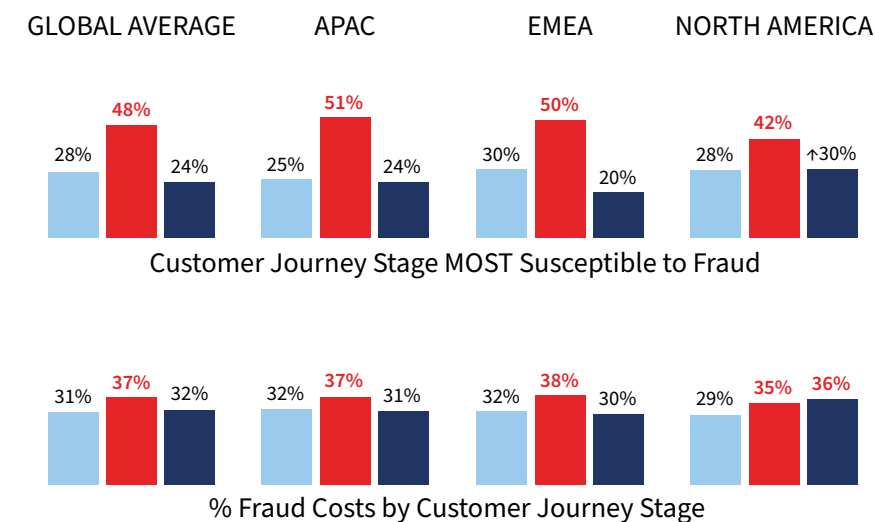
Nonetheless, verifying a customer's digital identity still poses challenges. This is particularly true at new account creation where a company has no past history and no transaction activity upon which to base a fraud decision. Still, the most susceptible stage to fraud in the customer journey is the financial transactions stage. A recent study from LexisNexis® Risk Solutions bears this out – it has shown that identity fraud at transactions or distribution of funds is a clear weak spot in fraud prevention.[1]

To mitigate the risk of fraud and ensure that each transaction with each customer is trustworthy, businesses have implemented checks (and rechecks) using the data that is available to them. When unnecessary, these well-meaning checks, or authentication "step-ups" can impact the customer journey, adding barriers to what should be a seamless experience. Every additional data element requested of a customer adds friction to the checkout process, which increases cart abandonment, decreases customer conversion rate, and undermines the chance to build a healthy relationship and trust between business and customer.

Retail and e-Commerce

GLOBAL AVERAGE   APAC   EMEA   NORTH AMERICA

Customer Journey Stage MOST Susceptible to Fraud

GLOBAL AVERAGE: 31%, 52%, 17%
APAC: 30%, 53%, 17%
EMEA: 30%, 52%, 18%
NORTH AMERICA: ↑39%, 47%, 14%

% Fraud Costs by Customer Journey Stage

GLOBAL AVERAGE: 30%, 39%, 31%
APAC: 30%, 41%, 29%
EMEA: 29%, 44%, 27%
NORTH AMERICA: 30%, 39%, 31%

Financial Institutions

GLOBAL AVERAGE   APAC   EMEA   NORTH AMERICA

Customer Journey Stage MOST Susceptible to Fraud

GLOBAL AVERAGE: 28%, 48%, 24%
APAC: 25%, 51%, 24%
EMEA: 30%, 50%, 20%
NORTH AMERICA: 28%, 42%, ↑30%

% Fraud Costs by Customer Journey Stage

GLOBAL AVERAGE: 31%, 37%, 32%
APAC: 32%, 37%, 31%
EMEA: 32%, 38%, 30%
NORTH AMERICA: 29%, 35%, 36%

■ New account creation   ■ Purchase transactions   ■ Account login

In shopping online,
a wait of longer than:

10 seconds
for a card to be processed

or

12 seconds
for a confirmation email

can make a consumer wary
of a site's authenticity.[7]

THE VALUE OF SHARED GLOBAL INTELLIGENCE

Another challenge in the fight against fraud is the fragmented nature of data. Gathering customer information with the breadth and depth needed often means relying on several third-party providers who may have information that is limited in scope or geographical reach.

Using incomplete data or data that needs to be aggregated from various sources can compromise identity verification and result in a poor or inaccurate fraud risk decision.

The ability to recognize trusted customers and prevent fraudulent transactions requires access to a deep well of dynamic threat intelligence fueled by data from globally contributed transactions across diverse industries.

Armed with insight from shared data, organizations can fill gaps in their risk review process, make smarter and more informed identity decisions, and boost their fraud defenses – without adding unnecessary friction to the customer experience.

The LexisNexis® Digital Identity Network® is a living, breathing
ecosystem of collective data from approximately

78
BILLION
**Global
transactions
+37%YOY[6]**

3
BILLION
**Digital
identities
+30% YOY[6]**

more
than 3
BILLION
**Email
addresses
+50% YOY[6]**

WITH 9 BILLION DEVICES[6]

Leveraging the shared intelligence from this vibrant network, organizations gain near real-time assessment
into potential fraud and can take preemptive action – entities or behavior flagged as high risk or fraudulent
by one organization can be blocked by other organizations before any transactions are processed.

The LexisNexis® Digital Identity Network® crowdsources insights across thousands of businesses globally, building one of the largest repositories of digital identity intelligence that grows more powerful with each transaction.

Travel Websites

Banks

Global Airlines

Global Credit Card Issuers

Ticketing Companies

Money Transfer Providers

Shared Economy

Largest Computer Manufacturers

Marketplace Lenders

Global Retailers/ eCommerce

The depth, breadth and global reach of intelligence in the LexisNexis® Digital Identity Network® is hard to match, and is what underpins its effectiveness in helping organizations to:
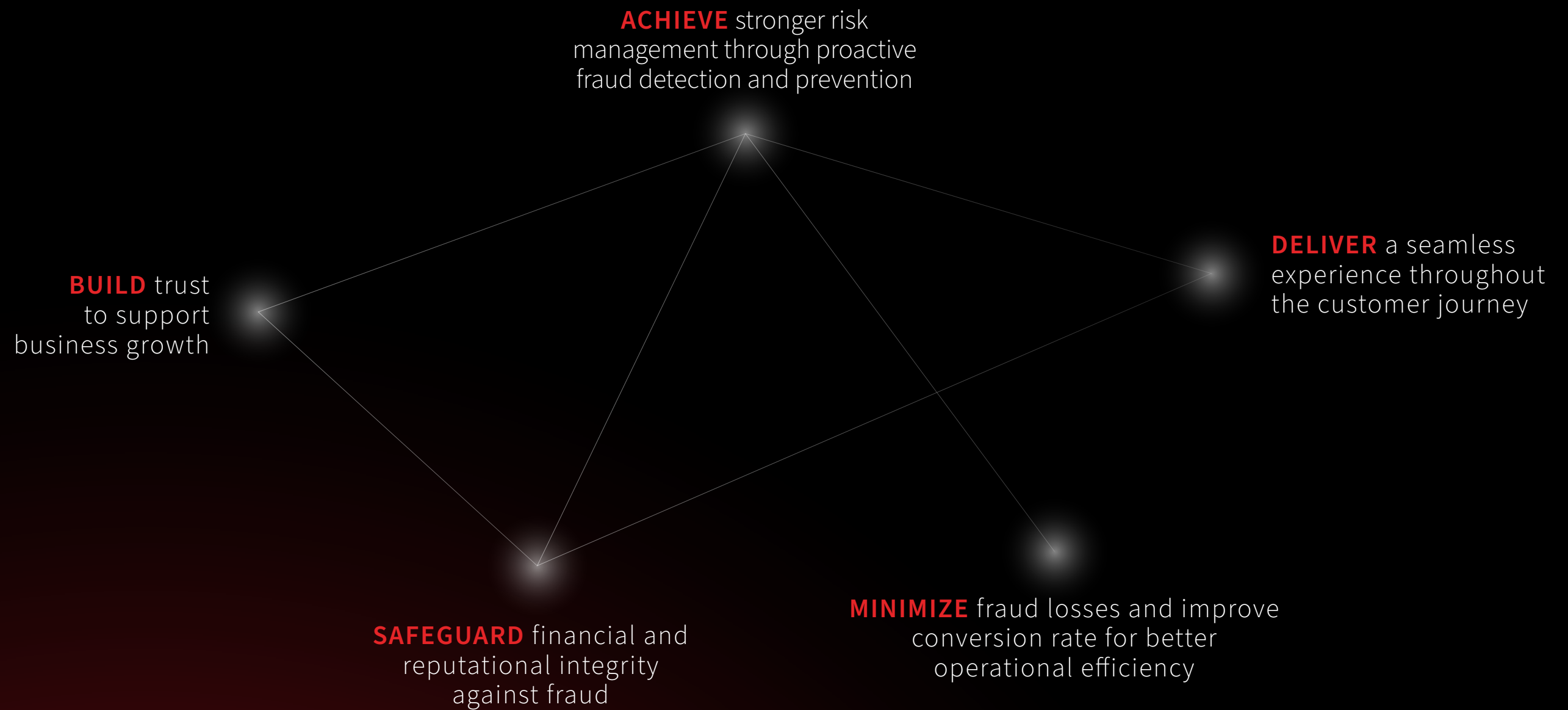
ACHIEVE stronger risk management through proactive fraud detection and prevention

DELIVER a seamless experience throughout the customer journey

BUILD trust to support business growth

SAFEGUARD financial and reputational integrity against fraud

MINIMIZE fraud losses and improve conversion rate for better operational efficiency

LexisNexis® Digital Identity Network® powers the fraud fighting capabilities of LexisNexis® ThreatMetrix®, LexID® Digital, LexisNexis® Behavioral Biometrics and the other digital identity intelligence and fraud prevention solutions from LexisNexis® Risk Solutions.

These solutions offer a multi-layered approach to fraud-risk management by connecting digital, physical, and behavioral attributes into a cohesive digital customer footprint for more informed and confident risk decisions.

![LexisNexis Risk Solutions logo]

CONCLUSION

The ongoing trend toward mobile and increasing digitalization across economies, regions, industries, and businesses provide a ripe stomping ground for bad actors to take advantage of vulnerabilities in fraud oversight. Their ingenuity never ceases to amaze and only adds to the complexity of keeping up with changing tactics and attack vectors. Fighting digital fraud has become too broad, too global, and too interconnected for businesses to 'go it alone.'

Successfully blunting this unrelenting challenge takes a village. By banding together and sharing collective intelligence that spans devices, industry sectors and touchpoints, businesses can more effectively recognize trusted interactions and prevent fraudulent ones while continuing to ensure a seamless experience for customers.

LexisNexis® Risk Solutions offers a robust suite of fraud management and identity solutions that combine physical and digital identities – including devices, behavioral biometrics and credit-seeking insights – providing companies with the tools needed to inform transaction decisions and prevent fraud.

CONTACT US TO LEARN MORE

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. Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

[1] https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study
[2] https://datareportal.com/reports/digital-2021-april-global-statshot
[3] https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030
[4] https://www.gartner.com/smarterwithgartner/how-to-improve-your-data-quality
[5] LexisNexis® Risk Solutions The True Cost of FraudTM - 2022 study
[6] LexisNexis® Risk Solutions Digital Identity Network® - 2022 data
[7] https://www.shopify.com/my/enterprise/faster-checkout-process