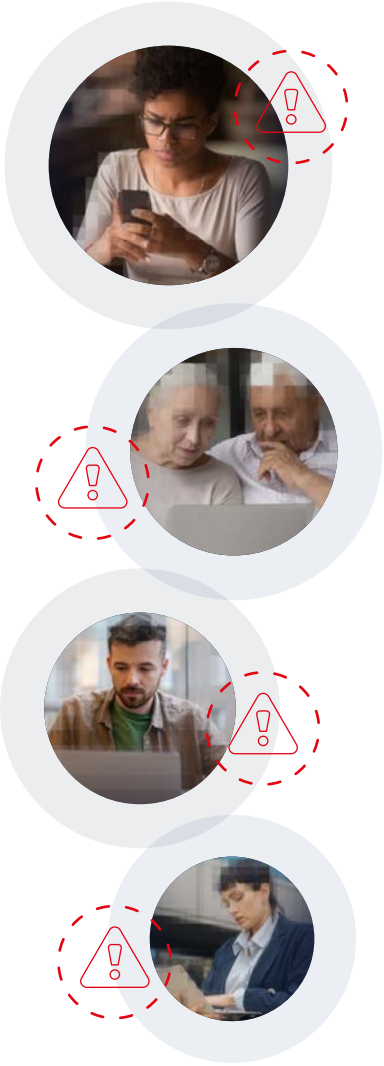
LexisNexis®
RISK SOLUTIONS

The Evolution of Scams

Learn how scams continue to grow in complexity and how to protect your customers from being swindled

A Global Crisis



Scams: Devastating Lives Worldwide

Whether it's a romance scam that leaves a lovelorn victim with a broken heart and an empty retirement account or a scam that results in an insignificant amount lost, stories of scams abound across the globe.

Scams are now an unfortunate and pervasive part of our everyday lives. In spite of awareness campaigns to educate consumers and technology-based interventions such as online alerts and multifactor authentication, last year scammers bilked consumers worldwide out of more than $1.026 trillion dollars. [1]

Scams have become so clever and scammers so adept at building trust that even the most tech-savvy individuals with their antennae perpetually set on high alert have fallen victim.

No one is immune. Scams impact all industry sectors, all businesses regardless of size, all consumers and all geographical locations.

A scam that starts with account takeover may unlock information that enables more complex social engineering attacks. Building a successful defense against scams and fraud begins with an understanding of the customer to detect nuances in behavior and interactions that signal potential fraud.

Anti-fraud solutions that unify multiple risk signals into an integrated view of a digital identity can help mitigate risk and protect both the organization and its customers from scams.

In this ebook, we'll discuss types of attacks and challenges, and provide actionable advice to prevent scams and protect your organization.

$40.62 Billion

Expected cost of fraud to financial institutions worldwide by 2027 [2]

78%

of people experienced at least one scam in the past 12 months [3]

When Did the Rabbit Hole Get So Deep?

The advent of the computer and exploding use of the internet provided a new universe ripe for exploitation. Phishing emails and social media posts afforded a simple and effective attack vector for tricking people into divulging sensitive information.

Bots introduced an unprecedented level of efficiency with their ability to send massive volumes of emails or test stolen credentials. Other technology that gave rise to mobile phones, texting and SMS messages, provided further access to an ever-widening pool of potential victims.

Today's scams have evolved in sophistication and complexity, making them difficult to detect. With artificial intelligence, the poorly worded emails with grammatical errors from a Nigerian prince asking for money are now perfectly crafted emails and text messages from a company CEO, package delivery service, authority figure or even a "friend" in need.

Rudimentary company logos have been replaced by perfect replicas. Even entire websites have been hijacked and duplicated, with all payments directed to the scammer.

61% of scams are perpetrated by phone *and* **58%** by text/SMS messages [4]

But it doesn’t stop there

Stolen data and information gleaned from social media posts provide a clear window into who victims are, what they buy, where they shop and even who their friends are. Scammers use these details to create highly personalized offers, even going so far as to invest in online ads customized to a target’s interests.

Scams perpetrated by phone are still popular around the world, but robocalls enable scammers to reach more potential victims more quickly. It used to be easier to spot phone scams when incoming calls displayed numbers from international locations, instantly raising red flags. Now, scammers spoof local numbers, deceiving people into a false sense of trust that the call is coming from a local business or their local bank branch.

Large, organized criminal networks run scam operations like a business. Scam centers manned by human trafficked victims have popped up in Southeast Asia and other regions, ensnaring both the innocent scammers and their unfortunate targets in the same evil web.

How Did We Get Here?

Technology might have opened new doors for bad actors to reach unsuspecting victims through phishing, vishing and smishing, but a confluence of other factors added fuel to the fire that got us where we are today.

These factors along with ever-changing technology will no doubt continue to feed the rise in fraud and scams for the foreseeable future.

Digitalization: a gateway for fraud

Globalization: scams have no boundaries

Real-time payments: narrowing the window to stop scams

Cryptocurrency: a new frontier for fraud

Generative AI: making scams even more convincing

Digitalization: a gateway for fraud

The digital transformation had been building steadily for over 50 years, gaining speed with the introduction of personal computing and the internet. But it was the Covid pandemic that propelled digitalization to new heights.

Covid sent the race to mobile and online into overdrive as businesses of all sizes and types rushed to modernize their digital presence to accommodate the surge in traffic. This year, the global digital payments market is now projected to reach US$11.53 trillion. [5]

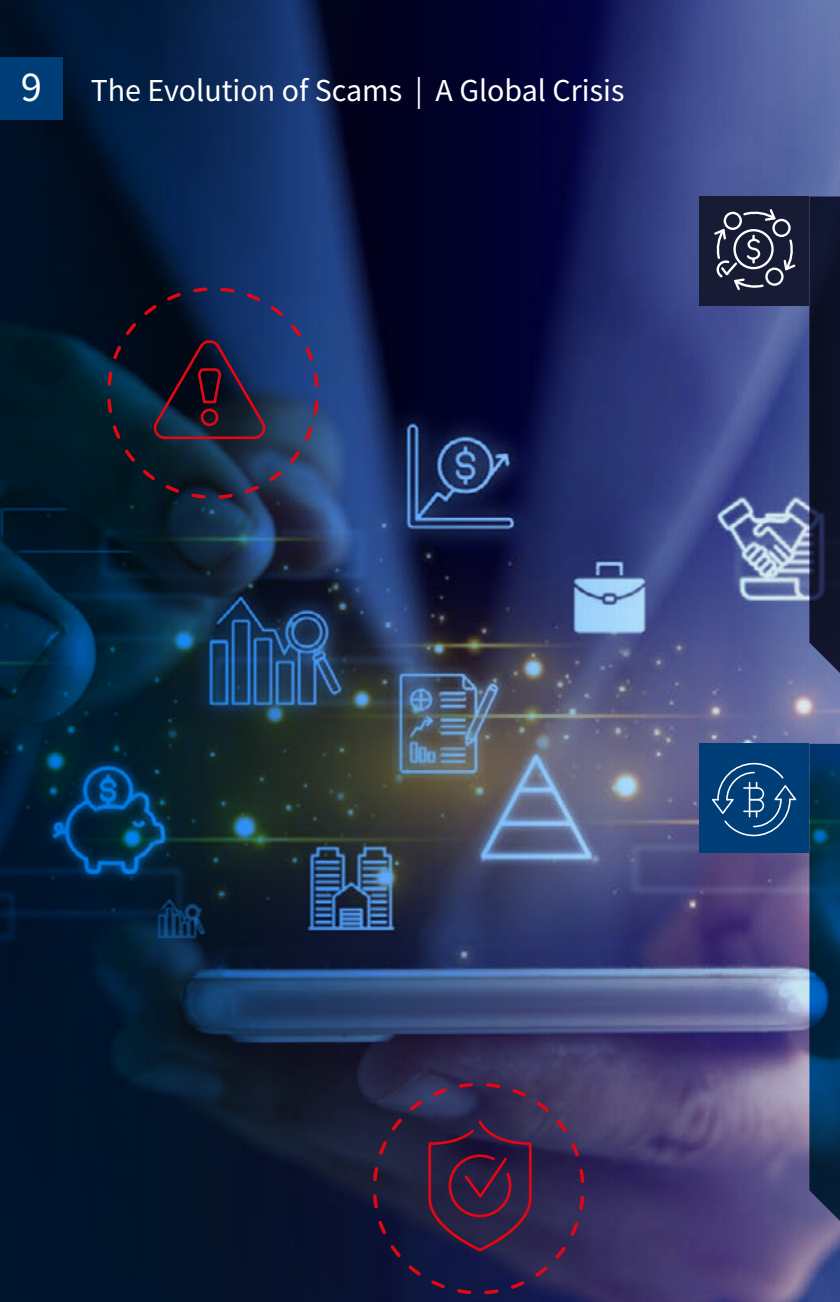
There is no going back. How businesses provide services, how merchants sell and how consumers shop and pay for purchases is forever changed. Unfortunately, the love affair with digital is shared by fraudsters. With more and more of our financial and everyday life transacted through mobile or online, the door for fraud keeps getting wider.

Globalization: scams have no boundaries

Technology has been a great equalizer, dissolving boundaries and opening markets so that anyone can purchase just about anything from anywhere in the world with a click of a button.

Globalization provides new markets and endless opportunities for small businesses, entrepreneurs and large corporations alike. But globalization is also a boon for fraudsters. Lax oversight in many countries has enabled the growth of large-scale scam operations – many using trafficked workers – and impacting thousands of victims all over the world. Complex scam networks operate with impunity across borders. Taking down these criminal enterprises requires cross-country collaboration.

Operation PANDORA is a perfect example of what can be accomplished with collaboration. What started as a German investigation drew in law enforcement cooperation from Albania, Lebanon and other countries as well as support from Europol. Working together, they raided a dozen call centers across Europe that were responsible for thousands of scam calls and arrested twenty-one perpetrators.



Real-time payments: narrowing the window to stop scams

The speed and efficiency that are the hallmarks of real-time payment systems provide huge benefits to scammers who can instantly receive payments from victims.

For consumers ensnared in authorized push payment (APP) fraud, instant and account-to-account transactions can be a source of pain. Once the money is gone, it's gone, and difficult to get back.

But regulations are changing. The UK's Payments Systems Regulator shared reimbursement model for APP fraud splits liability 50/50 between the sending and receiving organizations. By making both parties responsible for reimbursement, the intent is to encourage a strong anti-fraud posture that will reduce APP fraud going forward. The challenge is to keep payments safe for legitimate consumers but prevent criminals from taking advantage of instant payments.

Cryptocurrency: a new frontier for fraud

Cryptocurrency continues to gain traction among mainstream businesses and individuals. It eliminates the middleman so both global and domestic transactions are faster and less expensive than conventional payment methods.

Cryptocurrency also serves as a hedge against inflation, making it is especially popular in countries like Venezuela where inflation is rampant.

But there is a dark side to cryptocurrency as well. Because it is fast, cheap and offers anonymity, cryptocurrency is the preferred payment method for scammers. Transactions are difficult to trace and payments can't be reversed except by the party (in this case, the scammer) receiving the funds.

With the number of cryptocurrency users estimated to reach one billion worldwide by 2030, [6] protecting users from scammers will need to be a priority.

Generative AI: making scams even more convincing

Generative AI is a double-edged sword that brings us into unchartered waters. Although gen AI can automate processes, provide helpful chatbots for customer service, improve risk decisioning, minimize false positives and boost anomaly detection, it can also be misused by bad actors, taking scams to a new level.

Using actual images, videos and audio, gen AI enables fraudsters to develop synthetic identities and such realistic "deepfakes" that it is nearly impossible to discern truth from fiction. The ability to accurately reproduce someone's voice can be used to con grandma – or mom and dad – into sending money thinking their loved-one is in distress and needs help. Romance scams are more convincing when victims can see and chat with what appears to be a real person.

Combating the deepfakes of gen AI will be a formidable challenge. Using the power of gen AI 'for the good' is the only way to meet the challenge head on.

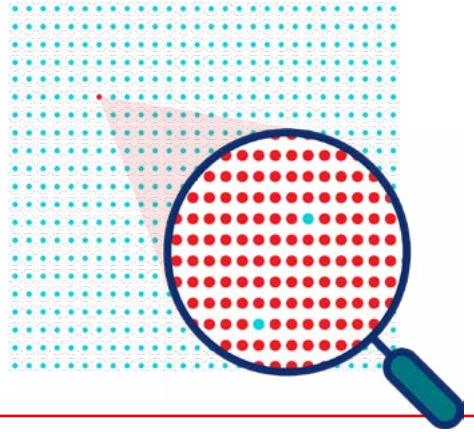
Though payments resulting from APP fraud respresented less than

0.1%

of overall faster payments volume in 2022, faster payments are used for

98%

of APP fraud payments [7]



UK's largest banks report up to

$454

lost to APP fraud by every $1.3 million sent in transactions [8]

83%

of financial institutions are considering using gen AI to fight fraud [9]

1 in 5

organizations has gen AI solutions in production [10]

Gen AI schemes contributed to a

60%

increase in global phishing attacks [11]

The Complexity of Modern Scams

From Nigerian Prince to Pig Butchering

When it comes to scams, there is no end to fraudsters' creativity. Relatively straightforward Nigerian prince scams still exist, but social engineering scams are the latest concern.

20% **of consumers** worldwide have been victims of payment fraud in the last 4 years. Nearly **27%** of that was APP fraud [12]

$75 billion

Amount lost worldwide to pig butchering within the same period [13]

Social engineering attacks prey on human emotion and human vulnerability. They exploit trust to elicit sensitive information that is used for identity theft or account takeover, or to perpetrate more involved romance, investment, impersonation or other scams.

In investment and romance scams, for example, the fraudster uses the trust and relationship they have built over weeks or months to trick victims into opening a bogus brokerage account or investing in a bogus business opportunity.

The ruse is supported by a realistic website with legitimate looking dashboards that show positive returns, and oftentimes even chatbots and help desk support – all of which are controlled by the fraudster. Once the fraudster is convinced they have taken all the victim's money and the victim is bled dry, they stop communicating and disappear. This type of APP fraud where the scammer "fattens up" the victim before going in "for the kill" is known as pig butchering.

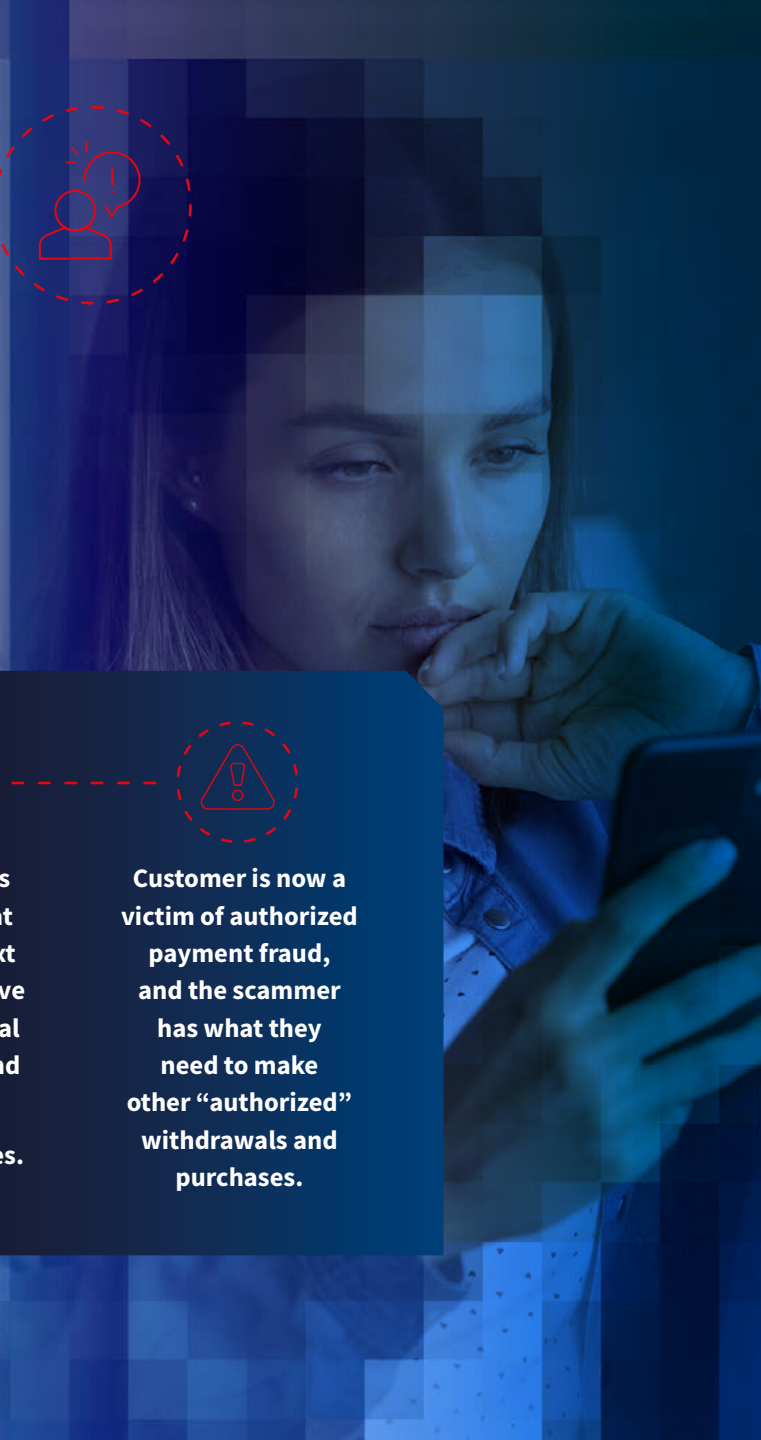
APP fraud is particularly difficult to identify and prevent because it is the genuine customer controlling the transaction themselves, not the fraudster. By the time the victim realizes they have been tricked into transferring money to a fraudster's account, the money is gone.

The expanding lexicon of scams

APP Fraud Hides in Plain Sight

For the consumer, APP fraud appears as just another interaction - by phone, email or other device - in the middle of the many digital transactions they might perform in a day.

The following graphic is a real-life illustration of how this complex scam often unfolds undetected - to damaging effect.



Customer answers a phone call.

Phone number was spoofed to appear to be from their local bank so customer trusts it.

Scammer impersonating a bank employee builds further trust by providing the customer's home address, last 4 digits of their debit card and account number.

Scammer advises the customer of a fraudulent transaction on their debit card.

Requests the PIN number to cancel the debit card.

Customer acts quickly and provides PIN number.

Bank sends them a one-time authorization code, which they provide to the scammer.

Scammer advises the customer that they will get a text message to approve an ATM withdrawal but to ignore it and just reply "yes".

Customer complies.

Customer is now a victim of authorized payment fraud, and the scammer has what they need to make other "authorized" withdrawals and purchases.

Business in the Crosshairs

Financial institutions and consumers are not the only victims of scams. Organizations of all sizes are also in the crosshairs of scammers; attacks between multiple industries are not uncommon.

Business email compromise (BEC) is a growing threat. Scammers use a hijacked email account to trick employees into initiating fraudulent wire transfers, paying fake invoices, divulging sensitive company information or changing banking details for future transactions. In 2023, BEC accounted for $2.7 billion in losses in the U.S. [14] and more than $50 billion globally since 2013. [15]

Scams undermine trust, which is a core component of a company's reputation. Once a reputation is damaged, it is harder to acquire new customers and retain existing customers.

Nearly **1/3** of financial fraud victims close the account with the institution where the fraud occurred [16]

Protect Customers From Bad Actors

It is hard to detect a scam with conventional fraud approaches, especially when it's the genuine user performing the transaction. Scams abuse consumer emotion and desire to trust.

However, with the right strategy and layers of intelligence, it's possible to turn the tide on scams and safeguard the people who depend on your services. Over these next few pages, we explain how.

Build a Defense for Every Stage of a Scam

There are several points of potential vulnerability that open the door to fraud. Identifying and stopping fraud early is crucial to prevent scammers from causing unfettered damage down the line.

A fraud that starts with stolen personal data could be used for account takeover or to apply for loans, change beneficiaries, open new accounts and carry out APP fraud and other scams.

Unlike direct attacks that exploit technical vulnerabilities, humans are the weakest link in social engineering scams. That's why the best way to prevent scams that prey on human nature is to understand customer behavior. Combining technology with behavioral intelligence helps organizations to proactively detect the nuanced signals that indicate potential fraud.

Four points of vulnerability

1 **Credential testing and information gathering**

2 **Calls and remote access tools**

3 **Authorized payment**

4 **Cash out**

1 Credential testing and information gathering

It all begins with data. Fraudsters perform credential testing of customer data such as usernames and passwords obtained from a data breach, phishing or social engineering to validate details for use.

Supplemental data captured from valid credentials (i.e., a mobile phone account) can be used to create synthetic IDs to open new accounts, for social engineering or to perpetrate other fraud such as SIM swaps to intercept the OTP.

Take action

Detect automated bot attacks performing credential testing

- **Authenticate the digital identity of the user**
- **Identify anomalous behavior in real time across all customer touchpoints**
- **Strengthen KYC with identity and document verification**

2 Calls and remote access tools

Armed with stolen data, the scammer may impersonate a bank employee or other trusted entity to convince the victim to send money, make an investment or take another action such as giving the scammer access to their computer.

Take action

Detect signs of coaching to identify the scam in real time

- **Leverage active call and remote access detection technology**
- **Use behavioral signals (i.e., keystroke patterns, mouse movements) to identify victim coaching**
- **Contextually confirm risk levels in the customer interaction**

3 Authorized payment

Convinced the scammer is legitimate, the victim authorizes payment to the scammer's account. Because it is the victim themselves doing the transaction, authorized payment fraud is more difficult to detect than account takeover or other fraud.

Take action

Identify behavioral nuances that indicate the victim is under duress

- **Use beneficiary intelligence to flag links with previous fraudulent activity**
- **Share mule information across organizations to proactively identify fraudulent activity**
- **Use push notifications to validate risky transactions by encouraging victims to stop and reconsider their intent**

4 Cash out

Mule accounts, which the fraudster establishes using synthetic or stolen identification, stand ready to accept payments or transfers from the scammed victim.

Mule accounts can be located in other countries or set up with different organizations' names. They offer a protective layer to obscure the fraudsters' bank account, making it difficult to follow the money.

Take action

Identify mule activity and two-party payments that link suspect accounts

- **Flag high-risk behavior on beneficiary accounts (i.e., unusual high-volume payments)**
- **Identify fraud networks and links of beneficiaries**
- **Perform cross-border transaction analysis and transaction risk assessment**

Putting the Pieces Together

An unusual typing pattern. Multiple high-volume transfers. New payment beneficiaries. These elements may appear innocuous on their own but when viewed together, another picture emerges – the activities are highly indicative of fraudulent activity.

LexisNexis® Risk Solutions brings together seemingly disparate digital, physical, behavioral, event and account signals into a single and holistic view of the customer for a stronger defense against scams and account takeovers. Our layered, multipronged approach to fraud risk management uses this robust identity intelligence to determine if an interaction is from a bad actor or a legitimate, trusted user.

For authorized fraud where the genuine user is initiating a transaction at the behest of the fraudster, LexisNexis® Risk Solutions enables organizations to detect and prevent the scam in real time by analyzing multiple data points to understand contextual risk.

By linking machine learning-powered technology, behavioral attributes, digital identity insight and global shared intelligence, LexisNexis® Risk Solutions offers an integrated solution to stop scammers in their tracks.

Unifying multiple contextual signals into an integrated view of a digital identity

Protecting People Around the World From Scams

We work with global industry leaders to push the boundaries of scam detection and prevention.

Unique combinations of crowd-sourced intelligence, responsible AI-powered analytics and innovative risk orchestration technology help our clients provide customers with greater security and peace of mind – all without unnecessary interruption.

Our clients achieve unprecedented results with our support, including:

$32.7m
in additional APP scams prevented on both browser and mobile app for a major banking client

$630k
worth of scams detected in ecommerce in just 20 days

A 260%
increase in the value of scams and account takeover fraud prevented within UK financial services

We help you fight back against scams with tailored solutions built with decades of award-winning expertise.

Winning the Fraud Arms Race

The tactics of scammers and modes available to reach their victims continue to evolve. Organizations need to be proactive and agile, using the latest technology and rich identity intelligence to battle changing fraud.

Unlike attacks that take advantage of weaknesses in networks or software, social engineering attacks are based on human vulnerability. Conventional fraud controls that rely on physical and digital attributes alone are insufficient to protect humans from being themselves and acting human. Anti-fraud solutions that layer AI-powered models, behavioral biometrics and robust identity intelligence with conventional fraud controls offer organizations a more flexible and effective posture to address complex fraud challenges.

New technologies such as AI will continue to transform fraud prevention. AI-supported solutions can analyze complex transactions at scale, detect synthetic identities and other fraud in real time and flag suspicious activity. AI's powerful capabilities to differentiate genuine from fraudulent behavior reduces false positives and improves the customer experience.

Yet, the most important element for identifying and preventing scams comes down to understanding the customer. Organizations that arm themselves with intelligence that spans digital and physical identities, associated attributes, events, behaviors and the parties' accounts and actions stand poised to win the arms race against fraud.

It’s time to live life secure and less interrupted.

Discover how we secure every customer interaction, enhance experience and boost business potential.

Visit risk.lexisnexis.com/fraudandidentity

LexisNexis® RISK SOLUTIONS

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.

Sources:

1 https://www.gasa.org/_files/ugd/B63e7d_92ac212a168843219668d5a28510ce16.pdf

2 https://www.paymentsdive.com/news/fraudlossesrealtimepayments-banks-aci-push-paymentscams/653219/

3 https://www.gasa.org/_files/ugd/B63e7d_92ac212a168843219668d5a28510ce16.pdf

4 https://www.gasa.org/_files/ugd/B63e7d_92ac212a168843219668d5a28510ce16.pdf

5 https://www.statista.com/outlook/fmo/digital-payments/worldwide

6 https://blockchain.news/news/metaverse-giants-collaborate-to-form-dao-metaverse-alliance

7 https://www.psr.org.uk/news-and-updates/latest-news/news/psr-publishes-first-app-scams-performance-report/

8 https://www.psr.org.uk/news-and-updates/latest-news/news/psr-publishes-first-app-scams-performance-report/

9 https://www.pymnts.com/news/artificial-intelligence/2024/new-data-genai-emerges-as-effective-weapon-in-banks-war-to-reduce-false-positives/

10 https://www.gartner.com/en/insights/generative-ai-for-business

11 https://ir.zscaler.com/news-releases/news-release-details/Zscaler-research-finds-60-increase-ai-driven-phishing-attacks

12 https://investor.aciworldwide.com/news-releases/news-release-details/app-scams-emerge-top-payments-fraud-threat-fraudsters-changing

13 https://time.com/6836703/pig-butchering-scam-victimlossmoney-Study-crypto

14 https://www.ic3.gov/Media/PDF/AnnualReport/2023

15 https://www.ic3.gov/Media/Y2023/PSA230609

16 https://investor.aciworldwide.com/news-releases/news-release-details/app-scams-emerge-top-payments-fraud-threat-fraudsters-changing