LexisNexis®
RISK SOLUTIONS

LEXISNEXIS® RISK SOLUTIONS

GLOBAL STATE OF FRAUD AND IDENTITY REPORT 2026

TABLE OF CONTENTS

LexisNexis® RISK SOLUTIONS

WELCOME TO THE

GLOBAL STATE OF FRAUD AND IDENTITY

Trust fuels confident decision making. But it's harder to come by in a complicated world.

Businesses today face an increasingly complex and dangerous risk environment. Real-time identity verification is necessary for any competitive business, but it's becoming harder and harder for thinly-stretched human teams to assess. At the same time, new payment systems are dramatically increasing the speed of global transactions, shortening the timeframe for risk teams to address issues.

Meanwhile, organized crime is thriving in the chaos. Global crime syndicates are sourcing security-breach details, talent, tools and other resources from the dark web. In their hands, powerful AI software enables incredibly realistic synthetic IDs, deepfake photos and videos. At the same time, individuals are increasingly engaging in first-party fraud, blurring the line between customers and fraudsters.

But there's good reason for hope.

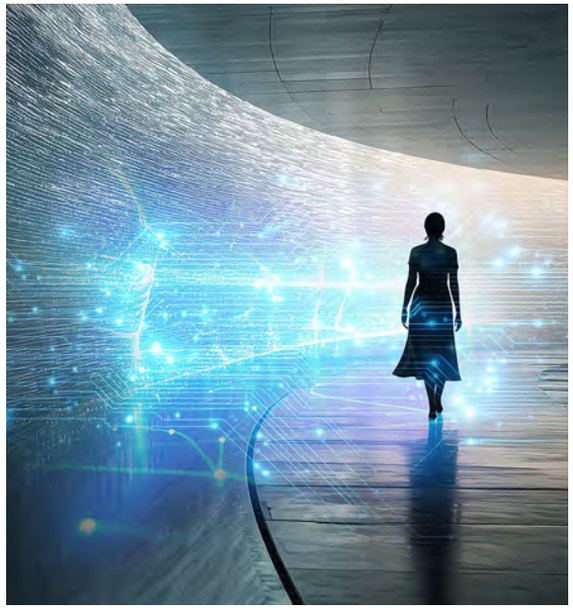
Companies around the world are beginning to collaborate and share risk data and insights. A better understanding of mule networks' vital role in money laundering is rising, and joint efforts are disrupting and disbanding them. While AI is helping criminals improve the quality of their fraudulent activities, it's also powering tools that help legitimate businesses quickly analyze a dizzying array of contextual evidence at scale.

Businesses run on trust. In a world of complex identity, trust requires gathering robust contextual data around every transaction, analyzing it with the best tools available and collaborating together with other organizations to thwart common threats. Only then can companies confidently accelerate action in something close to real-time and keep their businesses moving. This report dives deep into these challenges, and explores what organizations are doing today to meet the moment and thrive.

Kimberly Sutherland
Global Head of Fraud & Identity,
LexisNexis® Risk Solutions

Methodology

The LexisNexis® Risk Solutions Global State of Fraud and Identity Report discusses emerging trends in the following regions: APAC, EMEA, UKI, LATAM* and North America, including key pain points and opportunities related to fraud risk management. LexisNexis® Risk Solutions customers benefit from a global view of risks, leveraging solutions that are custom-tuned specifically for their businesses.



This report contains a mix of unpublished and published findings from our proprietary research and analysis, including:

- LexisNexis® True Cost of Fraud™ study, a global survey of 1,193 decisionmakers at financial institutions and retail and ecommerce merchants with responsibility in fraud management.
- LexisNexis® Risk Solutions Cybercrime Report, an exploration of over 104 billion transactions and 1.5 billion human-initiated attacks around the world, analyzed across the customer journey including new account creations, logins, payments and other non-core transactions such as password resets and transfers. Transactions are analyzed for legitimacy based on hundreds of attributes including digital identity, device identification, geolocation, previous history and behavioral analytics.

*For the purposes of this study, Mexico is included in the LATAM region.

FOR FURTHER READING

UNMASK DEEPFAKES AND FORGED DOCUMENTS WITH THE POWER OF AI

Our latest ebook, “Unmask Deepfakes and Forged Documents with the Power of AI,” reveals how to stop deepfakes in their tracks while providing digital experiences with risk- appropriate friction for your trusted consumers.

Start diminishing deepfakes’ power now

TACKLING THE FULL SPECTRUM OF IDENTITY FRAUD AND WHY ONE APPROACH WON'T STOP THEM ALL

Fraudsters are leveraging highly sophisticated tools to orchestrate multilayered attacks. As deepfakes, synthetic identities and AI-driven impersonation become more prevalent, detection and prevention are becoming significantly more challenging.

Coming soon: Your anti-fraud handbook

THE RISING CHALLENGE OF VERIFYING IDENTITY

The evolving concept of identity makes it harder to quickly and confidently verify at scale. In a world where no one IDV solution fits all, explore the value of a multi-dimensional modular approach.

See the full picture of modern identity

CHAPTER 1

Executive Summary: Trends in Global Fraud

INSIGHT:
First-party fraud has doubled in the last year, complicating risk management challenges.

First-party fraud has climbed rapidly, especially in EMEA and for ecommerce and financial services. It accounts for 36% of all fraud types now (after accounting for just 15% in the previous year[1]) and is an emerging source of risk for businesses, where it can be mistaken for third-party fraud or synthetic identity fraud.

Whatever form first-party fraud takes, including bonus abuse, chargeback abuse and unwitting mule activity, perpetrators can be driven by financial pressure and a perception of low risk. Steps taken to prevent these crimes can add friction for customers as well.

For more, see Chapter 2:
The Rise of First-Party Fraud: When Customers Become the Weak Link

INSIGHT:
The dark web has evolved into a comprehensive fraud-as-a-service marketplace for criminals.

The dark web has long provided criminals with an under-the-radar way to engage in all kinds of illicit activity. But as research commissioned by LexisNexis® Risk Solutions discovered, this collection of individual exchanges has effectively become a self-service collective marketplace for individual fraudsters and criminal networks alike.

Using cryptocurrency and other blockchain-based value stores, criminals can buy and sell ready-made synthetic IDs, mule accounts and a wealth of personally identifiable information (PII) data, often stolen in data breaches. They can also level up their game with advice, fraud tutorials, recruitment and even one-on-one mentorship. Conversations spotted on dark web forums can reveal criminals' pain points, like their reliance on new devices and their frustration with strong KYC techniques like biometrics and modern document authentication.

For more, see Chapter 3:
Fraud For Sale: Untangling the Dark Web

INSIGHT:
Money mules are enablers to fraud in the digital space, but their behavior is exposing them to risk teams.

Understanding is growing around the vital role mule networks play in laundering fraudulently obtained money and exiting funds quickly from the financial system. These networks are growing more complex, averaging around 15 mules per network[2], but risk management professionals have new tools to help them ramp up efforts to shut mule networks down and deprive criminals of their services.

Complicit, recruited and exploited mules shift money quickly and invisibly across geographies and channels including banks, cryptocurrency exchanges and gaming platforms. But cutting-edge fraud prevention solutions help financial institutions spot the telltale signs of mule activity, so they can stop illicit money from moving and disrupt these criminal organizations.

For more, see Chapter 4:
Insidious Mule Networks and the Global Fight Back

INSIGHT:
Leaning into modern identity complexity is enabling the rise of multi-dimensional identity intelligence.

Reliably verifying customers today means sorting ever larger and more intricate arrays of data representing aspects of each person's physical and digital selves including locations, devices, behavioral patterns and history. As a result, the concept of identity has itself become quite complex to assess, challenging companies who need to be able to verify customers quickly and reliably at scale.

Organized criminal networks are working overtime to exploit any security loopholes caused by this, for example by developing synthetic identities to try to bypass "thin file" emerging identity verification steps. Successfully thwarting them requires carefully assessing contextual data and applying cross-linking technology to create dynamic risk intelligence. Armed with the appropriate modular solution that fits their business model, each organization can then use this identity intelligence to make confident verification decisions with accuracy.

For more, see Chapter 5:
Embracing the New Complexity of Identity

INSIGHT:
Digital payments are bringing speed and convenience to consumers all over the world.

New payment methods are on the rise around the world, with digital wallets expected to account for 61% of ecommerce transactions by 2027 and neobanking poised to rise to $USD 2 trillion by 2030.[3] Buy-now-pay-later (BNPL) options and innovations like Canada's new Real-Time Rails system, India's Unified Payments Interface (UPI), Brazil's PIX and China's complete financial ecosystem 'super-apps' are bringing us ever closer to a world where everyone will enjoy instant access to money.

However, every new payment scheme adopted requires a learning curve for businesses, and this gap can sometimes be exploited by fast-thinking criminal organizations. It's critical for financial institutions to find risk management solutions that deliver a centralized view of customer activity to make informed decisions on which payments to approve or to challenge.

For more, see Chapter 6:
Keeping Pace with the Digital Payments Boom

INSIGHT:
The battle between "good" vs. "bad" AI is turning into an arms race.

It's estimated that 85% of identity fraud cases involve generative AI tools,[4] as fraudsters furiously improve fabricated IDs, deepfake selfie videos and other schemes to try to bypass verification and KYC steps. Legitimate businesses have no choice but to use their own AI-powered tools to stay ahead.

The fight isn't quite fair, because criminals don't have to use AI responsibly: Fairness, removal of bias and adherence to regulation are not on their agenda. Nevertheless, today's powerful risk management solutions are embedding AI to help improve performance and spot complex fraud patterns, cross-referencing and analyzing identity data at scale.

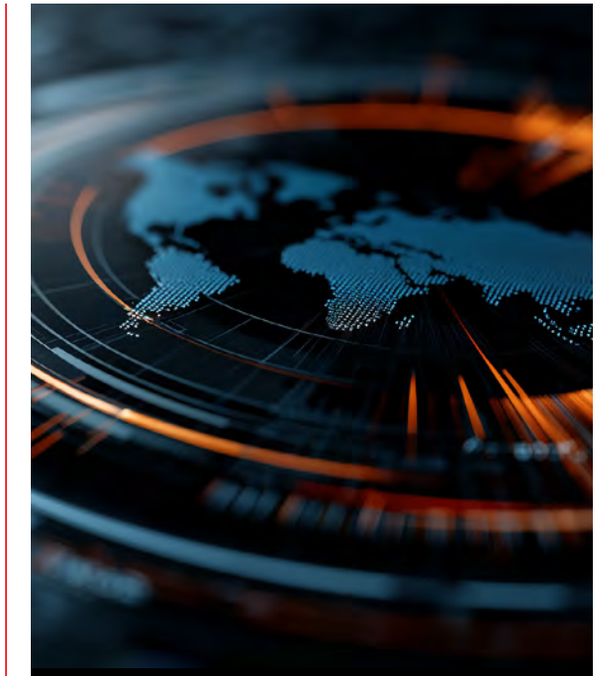
For more, see Chapter 7:
How AI Is Changing the Fraud and Identity Game

INSIGHT:
Data collaboration helps companies amplify their anti-fraud efforts.

The value of multiple companies sharing fraud data and insights (within the boundaries of regulation and privacy protection) in a well-organized way can't be overstated. Integrating crowd-sourced risk intelligence can improve fraud capture by over 40% relative to isolated approaches.[5] Each member's risk insights contribute to a regional and global inter-connected dataset that delivers value in real-time.

It's not just theoretical: Industry groups are joining forces to share real-time intelligence and fight their common enemies. The results are paying dividends.

For more, see Chapter 8:
Data Collaboration Goes Global



In North America, the top three identity verification challenges in online and mobile channels this year were the growth of emerging identities, the volume of malicious bot activity and the rise of synthetic identities.[6]

The Rise of First-Party Fraud: When Customers Become the Weak Link

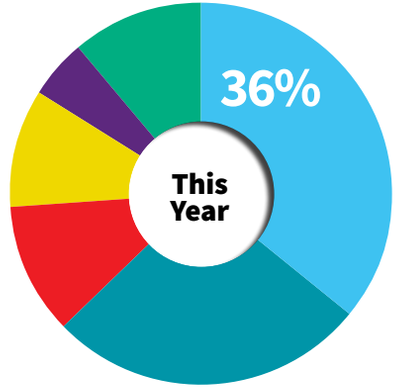
A Growing Threat from Within

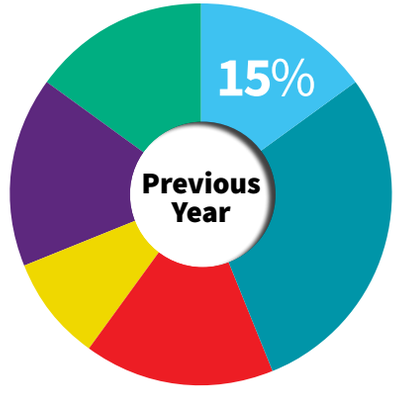
First-party fraud is escalating faster than most organizations anticipated, exposing weaknesses in conventional risk frameworks. As businesses have strengthened their defenses against external threats, a growing share of fraud now originates inside the customer base or at account origination.

Analysis from the LexisNexis® Digital Identity Network® shows that first-party fraud now represents 36% of all detected fraud events globally.[7] At more than one in every three frauds around the world, this more than doubles its portion of all fraud relative to last year's numbers. The impact is even more acute in EMEA, and in industries such as ecommerce and financial services, where customer verification relies heavily on trust-based relationships.

Losses attributed to first-party fraud are expected to reach $3.9 billion in 2025, and to climb to $4.8B by 2028.[8]

WHERE FIRST-PARTY FRAUD IS BEING FELT THE MOST[9]





APAC

FIRST-PARTY FRAUD

6%

▲ Last year **4%**

EMEA

FIRST-PARTY FRAUD

51%

▲ Last year **18%**

LATAM

FIRST-PARTY FRAUD

11%

▼ Last year **13%**

North America

FIRST-PARTY FRAUD

30%

▲ Last year **8%**

FIRST-PARTY FRAUD BY INDUSTRY

FINANCIAL SERVICES	ECOMMERCE	COMMUNICATIONS MOBILE & MEDIA	GAMING & GAMBLING
37%	**42%**	**9%**	**2%**
▲	▲	▼	▲
Last year **19%**	Last year **9%**	Last year **38%**	Last year **1%**

Understanding the Drivers: Why Good Customers Go Bad

Because first-party fraud often masquerades as third-party fraud or synthetic identity activity, many organizations underestimate its scale and risk. Outdated fraud detection tools struggle to accurately identify these types of fraud, forcing businesses into a reactive posture instead of a strategic one.

First-party fraud manifests in multiple forms, including:

Account "bust-outs." Customers use authentic identities to build trust, then default across multiple accounts.

Refund and chargeback abuse. Customers exploit lenient return policies or claim false non-receipt.

Promotion and bonus abuse. Individuals leverage fake data to extract unearned rewards.

Unwitting mule activity. Customers become conduits for laundering stolen funds.

First-party fraud isn't limited to banking. It occurs across a wide array of industries, accounting for more than a third of ecommerce fraud, for example.

15% of all retail returns were fraudulent last year, costing retailers an estimated $103 billion.[10]

Motivations vary:

Financial pressure. Job loss, inflation or debt convince perpetrators these deceptions are justified.

Perceived fairness. Some view these kinds of frauds as reclaiming what they're owed.

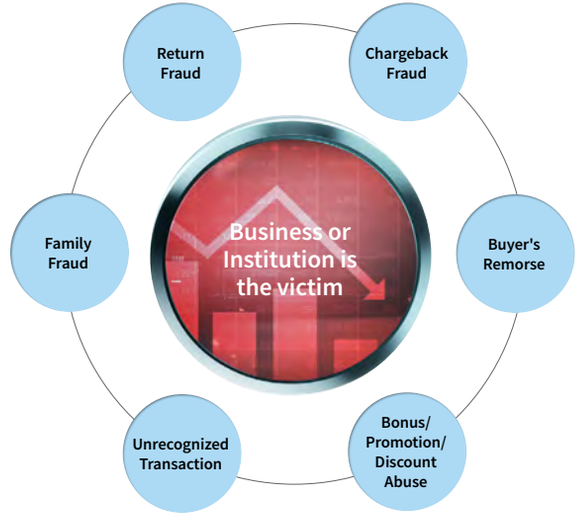
Low perceived risk. "Customer-first" policies and friction-less digital experiences make it easy to abuse trust.

This erosion of trust between consumers and institutions makes first-party fraud uniquely perilous. Every step taken to reduce risk adds friction for honest customers; every leniency invites abuse by less than scrupulous customers. Balancing empathy and enforcement is now a strategic imperative.

The challenge for institutions is getting the balance right: protecting customers without turning every transaction into a confrontation.

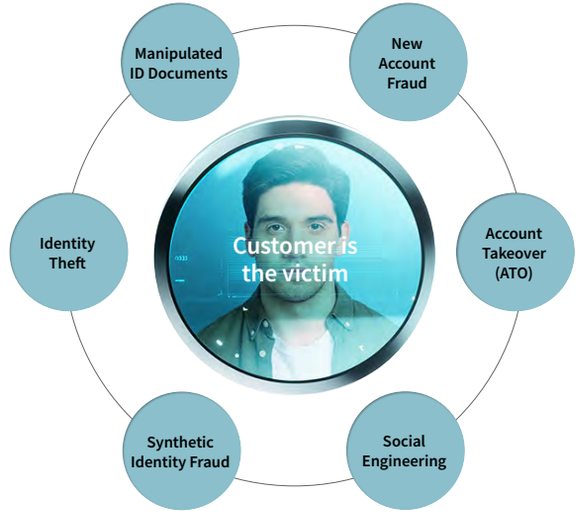
FIRST-PARTY FRAUD

An individual provides false information or misrepresents themselves



THIRD-PARTY FRAUD

An individual uses another person's identity or elements of it without their knowledge or consent



14% of financial services chargebacks are associated with first-party fraud.[11]

Why Traditional Defenses Fall Short When Detecting First-Party Fraud

Conventional identity verification first focuses on whether the identity is a real person, and then on whether they're who they claim to be. But first-party fraud demands a third dimension: What is the likelihood this person will commit fraud? Because the first-party fraudster is often a legitimate customer, businesses need a framework to spot indicators that can help them understand their motives in the present. This could include:

Established History

- **Many first-party fraudsters have at least some credit history, making them appear trustworthy at first glance**
- **Pattern fraud profile recognition (analyzing how identity elements behave or are subtly manipulated) is critical to detection**

Low PII Correlation with Subtle Variations

- **Real identity elements with slight changes in PII details, like a consistent address but slight variation in phone or email inputs**
- **Weak or inconsistent linkage between identity elements across trusted credential sources**

Elevated Velocity

- **Multiple applications coming from one IP address with slightly manipulated PII in a short period of time**
- **Frequent reuse and recombination of identity elements across multiple applications**

Adjusting policies to thwart first-party fraud is complex, says Maanas Godugunur, senior director of fraud & identity strategy at LexisNexis® Risk Solutions: "It's a delicate balance. Tighten refund policies too much and refund abuse can go down, but chargeback fraud may rise."

THE MANY FACES OF FIRST-PARTY FRAUD

First-party fraud manifests in forms that defy simple categorization. A customer might misrepresent personal information to access services, manipulate transaction timing or exploit return policies.

For example, a consumer might apply for multiple credit cards and loans, make a few initial payments to build trust, then default on all accounts. This "bust-out" strategy is often premeditated and difficult to detect in advance using traditional fraud models.

FRAUD TYPE	DEFINITION	RISK SIGNALS
Identity misuse	**A person knowingly misrepresents their identity or gives false information to obtain services**	**Minor PII variation, high velocity of applications, established identity across trusted, credentialed sources**
Bonus and promo abuse	**Gaining financial incentives at sign up/ checkout meant for other users**	**Email tumbling, minor PII variation, high familiarity with website**
Refund abuse	**Abusing refund policies to take unfair advantage of special offers**	**Return frequency, basket analysis, shipping address risk**
Mules	**Gaining financial incentives to move funds illegally**	**High velocity of outbound payments, linked mule accounts and devices in network**

Such patterns often appear trustworthy at first glance, which is why behavioral and contextual intelligence are now essential for accurate risk assessment. Organizations that struggle to discern first-party fraud face continued financial losses and risk implementing reactionary processes that degrade the application experience for legitimate consumers.

Seeing Customers in Context: A New Lens on Fraud Prevention

As first-party fraud grows more sophisticated, organizations are rethinking how they assess risk. The challenge lies in understanding potential identity manipulation and the person's likelihood to commit fraud.

To do that, businesses need a more nuanced, contextual view of each customer. That means analyzing not just who someone is, but how they behave over time, across platforms and in relation to others. This requires:

- **Holistic identity intelligence**
- **Behavioral tracking across devices and geographies**
- **Continuous recalibration of models based on velocity, device reputation and transaction history**
- **Recognition of cross-industry activity patterns**
- **Layered analysis combining behavioral intelligence, device intelligence and shared fraud signals**
- **Alternative data to better assess risk of payment default**

This shift toward behavioral and contextual analysis is already reshaping how fraud is detected. Instead of relying on static rules, organizations are adopting adaptive models that evolve with fraud tactics, capturing a broader spectrum of signals while minimizing false positives.

VIRAL FRAUD AND THE POWER OF COORDINATION

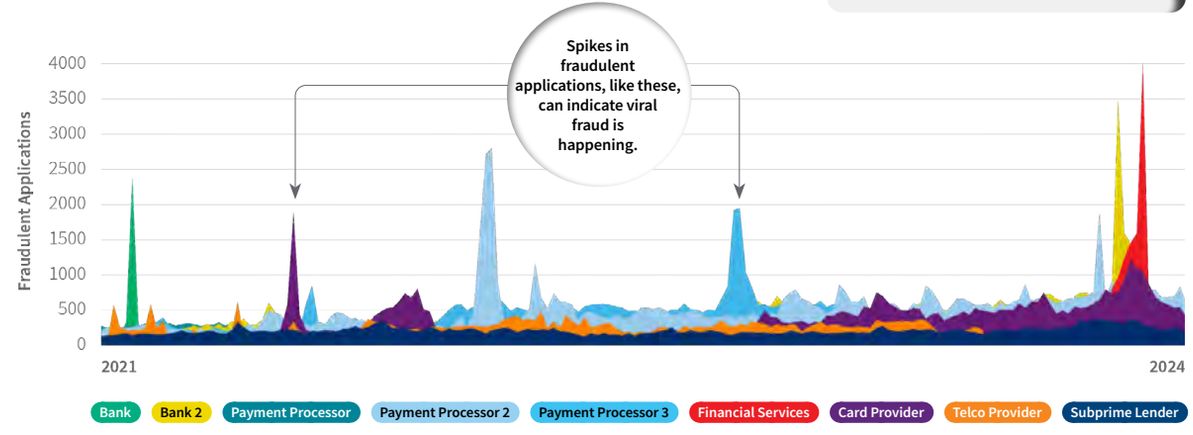
First-party fraud is no longer an exclusively individual pursuit. Increasingly, groups of consumers collaborate through online communities and social platforms to exploit the same vulnerabilities simultaneously, in what's known as viral fraud.

In these events, entire fraud cohorts coordinate on social media, executing synchronized attacks that mimic normal transaction surges until losses reveal what's behind them. These "viral fraud" waves can overwhelm defenses in hours.

By leveraging global network intelligence, LexisNexis® Risk Solutions identifies shared digital traits across hundreds of identities and across industries, isolating these coordinated fraud cohorts before the damage spreads.[12]

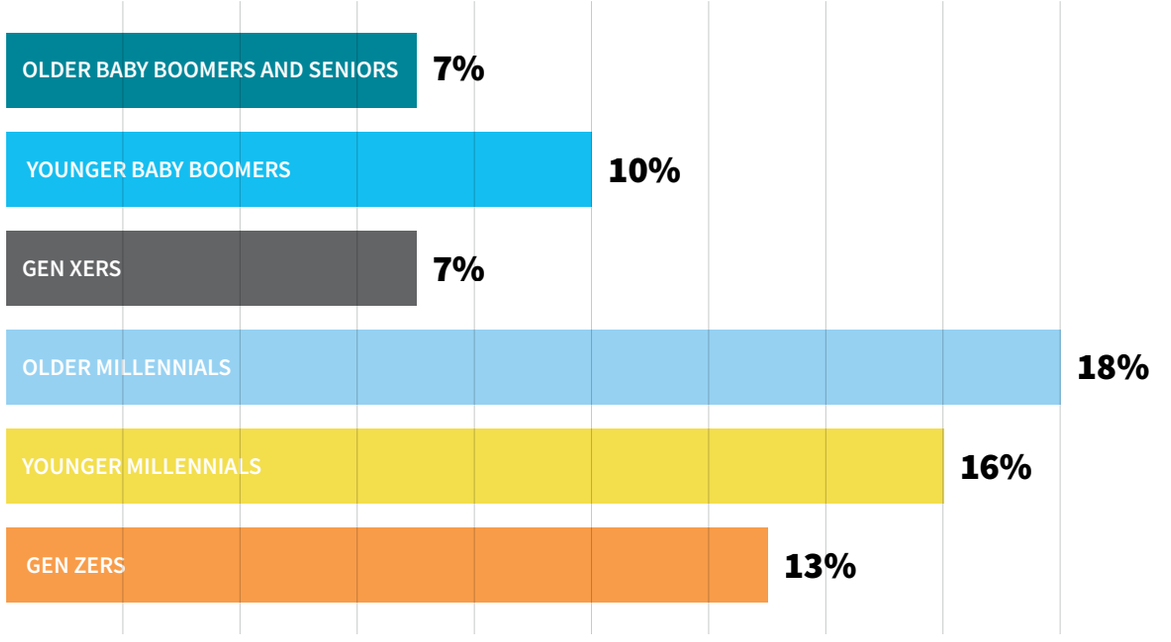
Shared characteristics

- **2x** more inquiries
- **3x** more likely to have a previously tagged fraud
- **7.4x** more likely to have a felony record
- **12** years younger



FIRST-PARTY FRAUD BY GENERATION

First-party fraud is a behavior that spans all generations: from older millennials (18% admitting participation) to Gen X and even seniors.[13]



"First-party fraud is tied to economics and an increased cost of living. When you have money problems, you're more likely to respond to a mule-recruitment advert or take a loan without any intention to repay."

Mike Nathan, vice president of international professional services, LexisNexis® Risk Solutions

RETURN FRAUD CAN BE INITIATED ACROSS MULTIPLE CHANNELS

ENHANCING FRAUD DETECTION WITH THE LEXISNEXIS® RISK INTELLIGENCE NETWORK

Adding cross-industry insights helped a financial institution add real-time velocity data and inquiries across the network, surfacing hidden connections to synthetic identities, first-party fraud and PII misuse.[14]

The financial institution faced three major challenges:

- **Limited fraud visibility.** Lack of cross-institutional insights hindered detection of known bad actors.
- **Increased losses and friction.** Gaps in data and weak risk signals led to higher fraud and poor customer service.
- **No consortium intelligence.** They were unable to link high-risk applications or reused PII across fraud events.

Enabling network intelligence inquiries provided:

- **Hidden fraud links.** Real-time cross-industry insights revealed synthetic IDs and identity misuse hiding in their portfolio.
- **Enhanced business rules.** Key warning indicators were integrated into fraud decisions.
- **Broadened fraud detection.** 50k applications were tied to known fraud in 15 months.

THE RESULTS:

63% uplift in model performance

$1.6M estimated fraud savings

Mapping Identity Misuse Through Smart Analysis of Multi-Dimensional Signals

Understanding identity misuse at scale requires more than just better data: It demands smarter interpretation. Legitimate users tend to show more stable identity patterns: consistent email addresses, devices, payment methods and velocity signals. In contrast, serial fraudsters often exhibit volatility, including frequent IP changes, device turnover and subtle manipulation of personal information.

To separate signal from noise, organizations are turning to multi-dimensional frameworks that analyze:

- **Application Element Insights: Tracing the origin and credibility of personal data over time**
- **Application Stability: Identifying inconsistencies in how identity elements are used together**
- **Identity and Relationship Mapping: Understanding how identities connect, evolve and reappear**
- **Consortium Network Intelligence: Detecting velocity and fraud patterns across industries**

These layers of analysis help distinguish between honest mistakes (like a typo in a birthdate) and deliberate misrepresentation. When combined with real-time behavioral data, they allow for more precise risk assessments and smarter interventions.

The Road Ahead: Scaling Misuse Intelligence

Looking forward, the fraud landscape is poised to become even more complex. Economic pressures, the rise of generative AI and the normalization of opportunistic digital behavior are accelerating the pace and scale of deception. In the next three years, organizations can expect:

- **A rise in hybrid fraud, blending real and synthetic identity elements**
- **Increased coordination among fraudsters across borders and platforms**
- **Growing regulatory scrutiny over how fraud, credit risk and consumer behavior are classified**

To stay ahead, businesses must treat intent analytics as a core capability, not a niche function. That means investing in shared intelligence, cross-industry collaboration and adaptive systems that can evolve with each new threat.

Ultimately, this isn't just about stopping fraud. It's about preserving digital trust in an era where the line between customer and fraudster is increasingly blurred. The organizations that can interpret misuse with clarity and speed will be the ones that define the next generation of secure, intelligent digital interactions.

CHAPTER 3

Fraud For Sale:
Untangling the Dark Web

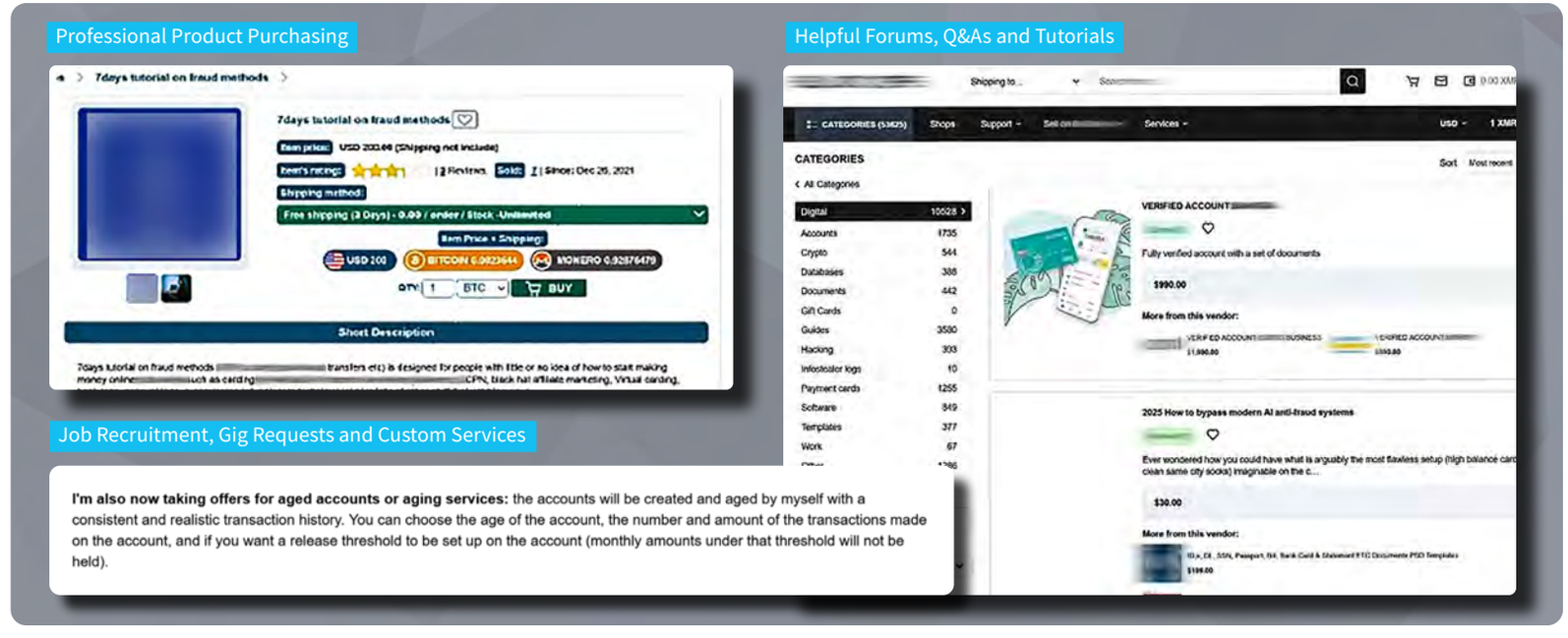
The Dark Web Has Become a Shockingly Comprehensive Fraud Resource

For more than a decade, the dark web has sheltered fraudsters, presenting an array of fraud-as-a-service offerings with convenience. It's given every data breach a long tail, and turned customers' personally identifiable information into a commodity that can be sold and resold endlessly.

Though it's estimated at less than a hundredth of a percent of the World Wide Web's size (by total addresses), the dark web has an outsized hold on the popular imagination. Invisible to traditional web search, these sites can only be accessed through special software that carefully preserves users' anonymity.[15]

The dark web has long been a safe haven for criminals to engage in a wide variety of secret, illicit activities. It's become an incredibly rich resource for fraudsters and helps generate billions in illegal proceeds annually.[16]

LexisNexis® Risk Solutions commissioned a study this year to explore the dark web and better understand this phenomenon.



An estimated four million individual users access the dark web every day through just one of many popular browsers, up from two million users in 2021.[17]

Meet Fraud-As-a-Service: An Anonymous, One-Stop-Shop Criminal Superstore

On today's dark web, fraudsters can shop confidently and anonymously. They can buy products, like lists of consumer credit card numbers, plug-and-play synthetic identities, mule accounts and private medical data. And they can tap into a rich pool of business insights like consulting forum threads before targeting particular institutions, or can read whitepapers on bypassing fraud controls. They can download self-help how-to tutorials or sign up for dedicated seven-day mentorship programs.

Many dark web sites require an administrator's invitation. But once inside, fraudsters typically find an oddly familiar customer-centric world of product descriptions and shipping methods, ratings and reviews, selling histories and complaints investigations. Our study revealed that many marketplace administrators are eager to present a legitimate, professional space with zero tolerance for fraudulent behaviour, to reassure suspicious fraudsters that they won't themselves be scammed.

At least 31 major dark web marketplaces have been identified since 2011, with many being closed due to exit scams or the efforts of law enforcement.

Individual marketplaces disappear with some regularity. Sometimes this is due to high-profile takedowns by coordinated law enforcement efforts (like one known market which had been enjoying 12 million USD in monthly turnover before its 2023 demise). Sometimes the owner of a marketplace will take it down unexpectedly, seizing customers' cash and/or inventory, in a phenomenon known as an exit scam. This institutional instability is understood to be part of the cost of doing business here.

The Number of Offerings, By Content Type, At One Typical Dark Web Store

▼ FRAUD	(5504)
Accounts & Bank Drops	(2160)
CVV & Cards	(542)
Dumps	(816)
Personal Information & Scans	(1085)
Other	(901)

▼ Guides & Tutorials	(4850)
Narcotics	(125)
Fraud	(2931)
Hacking	(597)
Security & Anonymity	(157)
Social Engineering	(260)
Other	(780)

A Professional Supply Chain for Organized Crime

Email accounts and bank accounts, purchased individually or in bulk, are the basic tools of fraud and are often sold at commodity pricing levels. These can vary in quality, from low-detail lists on up to "fullz" (slang for 'full contacts' that might contain names, addresses, contact details and even usernames and passwords.) Fraudsters have also learned to package their knowledge into more advanced offerings, often for higher rates, as seen in the pricing examples on this page.

FOR SALE: BASIC FRAUD DATA[18]

$3 - $5 each

Aged email accounts

These higher-value emails can more easily bypass fraud controls, sometimes with the help of included browser fingerprints designed to work in conjunction with cookies and proxies.

Pricing varies

Traditional bank accounts

These account numbers might be stand-alone, which are useful to synthetic identity creators, or might be connected to other PII.

$300-$900

Digital-first bank accounts

Access to challenger, cryptocurrency and neo-investment accounts may appeal to savvier customers or may provide better opportunities to see into account balances.

$120 for 400k-500k points

Reward point accounts

Converting rewards points into tickets, vouchers or cash involves more steps, but scamming airlines, hotel operators and cruise lines can be easier than defrauding financial institutions.

> You can buy an account from a challenger bank known for particularly strong mobile phone fraud controls, preinstalled on a physical phone, for roughly$900 including shipping.
>
> **From LexisNexis® Risk Solutions dark web research**

FOR SALE: ADVANCED OFFERINGS

$200 each

Bundled services and tutorials

These all-in-one fraud kits target those new to the fraud game, with packages that buttress product offerings with whitepapers, tutorials and guides and even 1:1 mentorship.

Pricing varies

Plug-and-play fraud kits

These pre-configured virtual machines come installed with secure undetectable web browsers designed specifically to evade fraud detection systems.

$500-$800

KYC as a service packages

These help purchasers circumvent advanced onboarding checks by verifying accounts that have not yet passed the KYC stage. They can also enable reactivation of KYC-ready accounts that have been blocked.

$1000-$2000 each

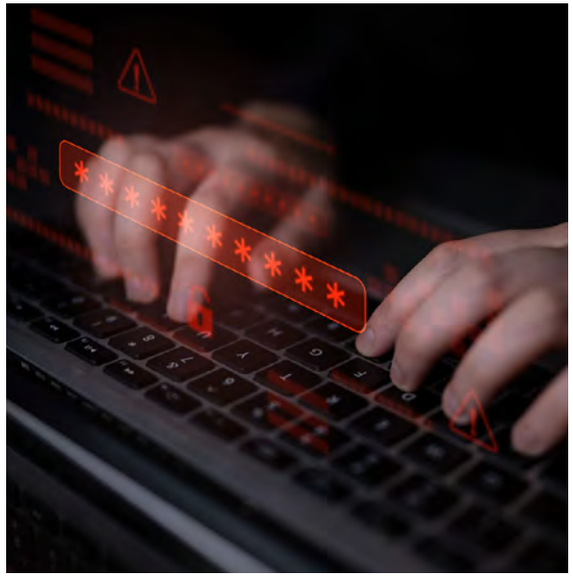
High-value business accounts

These are a rarer commodity, but can be helpful for lending a professional sheen to the business of laundering the proceeds of smaller scams.

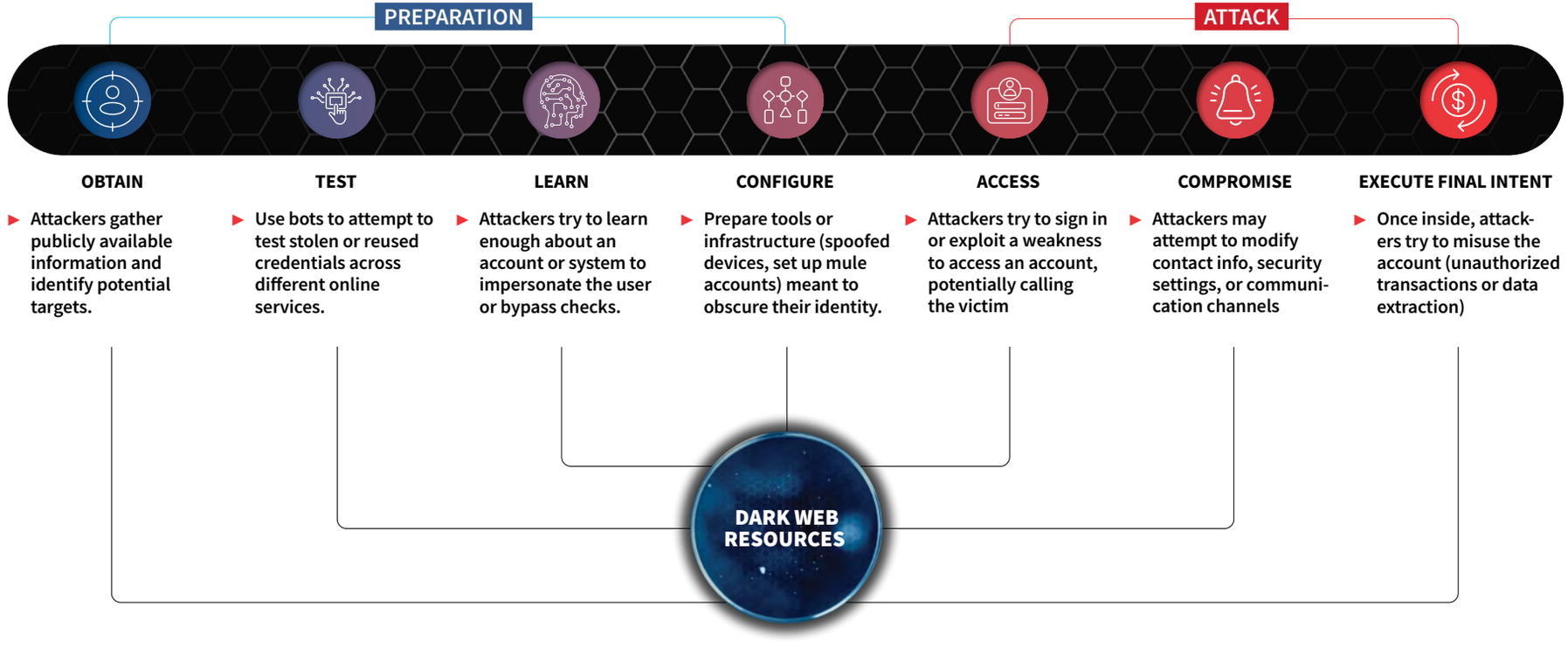
> "You have to choose non refundable rooms because [that] will block any chargeback request from the cardholder… Pretend to be looking for a room…"
>
> **From a reward points account tutorial on the dark web**

Fraud In Practice: How Dark Web Resources Can Support All Aspects of an Account Takeover

Last year, account takeover accounted for more than one in every four fraudulent attacks.[19] Part of why fraudsters have grown so adept at this particular sort of attack is thanks to the step-by-step support they can count on from the dark web.



THE STAGES OF AN ACCOUNT TAKEOVER ATTACK FROM A FRAUDSTER'S LENS



How the Dark Web is Evolving, And What's Being Done About It

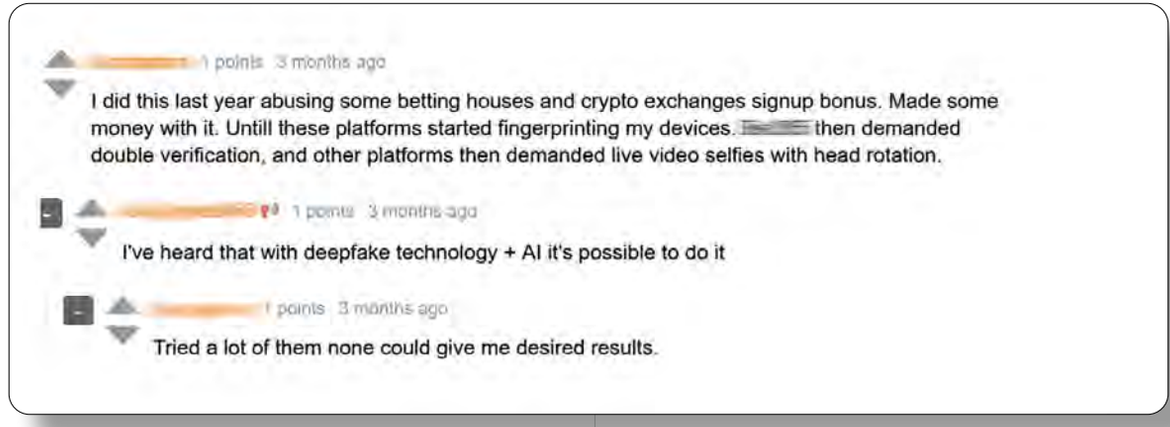
The dark web has been around for many years now, and it's evolved over time to try to stay ahead of changing consumer preferences and to avoid the efforts of law enforcement to rein it in. But the tide of the battle is turning at last. Here are some of the major shifts our research reveals.

The currency of choice for the dark web is in flux. Cryptocurrency has long been the dark web's de facto currency, and newer blockchain-based solutions are giving fraudsters options that are deemed more private and less trackable.

Smaller, more focused marketplaces are becoming the norm. Several high-profile marketplace closings have led dark web sellers to gravitate to more specialized markets that may more easily evade the focus of global law enforcement.

Fraudsters face imposing new obstacles. Fraudsters are vocalizing their frustration in dark web forums about which anti-fraud efforts are pain points for them. These include real-time liveness KYC checks, phone and email risk analysis, account activity checks, device fingerprinting and IP analysis.

Modern identity verification is a problem. Demand is outpacing supply for "verification mules" and deepfakes that can pass advanced KYC checks. Some leverage Generative Adversarial Networks to create video-swapping solutions that try to bypass live verification, but it's proving quite challenging.



Automating workflows for efficiency. Fraud involves time-consuming, repetitive tasks that agentic AI can now perform, saving fraudsters time and making it easier for new criminals to join the party.

Fraudsters are scamming each other. Sometimes defrauding other criminals can be an attractive option, and dark web admins are kept busy cracking down on shady offerings that are often used to scam other scammers, like cloned credit cards.

Fear of "exit scams" is growing. The risk of investigators shuttering a marketplace hovers over every dark web transaction. Sometimes, fraudsters will close a shop without warning, offering no explanation and no refunds.

The pool of mule candidates is shrinking. Fraudsters may need more mules than ever, but the candidate pool is starting to shrink as recruits grow wary of the growing risks of arrest and long-term credit trouble mule behavior can bring, resulting in chronic mule-network shortages.

Customer satisfaction and positive vendor ratings matter. Many dark web forums have similar reputation systems to "surface web" forums, often with strict moderation and the ability for users to upvote or downvote other users on the basis of good and bad experiences.

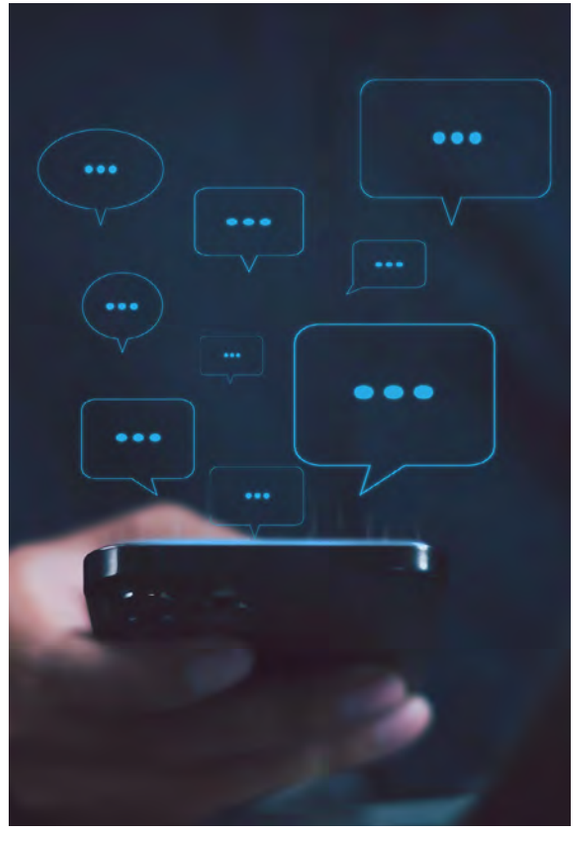
Admins are increasingly prioritizing security, to keep the threat of getting scammed from deterring potential customers. Standard practices now include PGP (Pretty Good Privacy) encryption, multi-factor authentication and a reliance on dark web escrow services.

Social Media Platforms Are Now Bringing Fraud-as-a-Service to Criminals' Fingertips

The Dark Web remains the primary hub of online criminality, but social media messaging platforms are starting to get a foot in the door. These mobile-first solutions present app-level convenience, presenting an easier arena for criminal customers to operate in and, evidence suggests, attracting a younger audience. Advantages include:

- **More favorable ecommerce functionality, e.g. peer-to-peer transactions without paying a dark web administrator's cut**
- **Search-engine style functionality (though only inside secret groups) that make fraud solutions more accessible**
- **Faster connection speeds, comparable to what the "surface web" enjoys but the dark web often lacks**

Dark-web style interactions are proliferating across social media messaging platforms at a dizzying rate: Recently, one social platform reportedly used AI to help it remove more than 15 million illicit sites in just one industrial-scale shuttering.[20]



FIVE KEY WAYS COMPANIES CAN OFFSET ANY ADVANTAGES THE DARK WEB GIVES FRAUDSTERS

- **Thwart fraudsters with deepfake detection and robust KYC checks.** Real-time biometrics, document authentication and behavioral solutions are difficult and expensive for fraudsters to defeat, and incorporating them into an organization's fraud controls can be a powerful deterrent.

- **Exploit fraudsters' reliance on unused identities and devices.** So-called virgin phone numbers, unused email addresses and devices with no prior digital footprint are a powerful weapon in a fraudster's arsenal. Fraud analytics and device fingerprinting can flag these for extra scrutiny in real-time.

- **Increase visibility around insider threats.** Criminals often have confederates inside organizations who can help them bypass security measures. Robust vetting and ongoing observation can help prevent disloyal employees from enabling fraud.

- **Monitor the threat landscape constantly for change.** Organized crime is well-funded and innovative, and gains advantages when they work together. But legitimate businesses can work together too, staying ahead of emerging threats by joining forces with global partners who can increase their visibility into fraud trends unfolding on the global stage.

- **Protect customer accounts from takeover.** Businesses can do more to secure confidential information from illegal access and frustrate fraudsters with global device-based analytics, advanced user profiling and risk-based authentication.

CHAPTER 4

Insidious Mule Networks and the Global Fight Back

Mule Networks May Finally Be On The Run

Organized mule networks have been outpacing fraud teams for years, and it's been costing financial institutions billions.

By helping criminals move stolen funds faster than banks can detect and stop them, mule networks have become a critical enabler of modern financial crime. In the UK alone, mules are estimated to launder over £10 billion annually. Last year, banks in the region working together flagged 377,000 mule payments in just eight months. These payments represented over £100 million in stolen funds: a 65% year-over-year surge.[21]

The average mule network consists of 15 mules moving money among 3.4 banks, though some are considerably larger, containing hundreds of mules.[22]

THE THREE FACES OF A MULE

Complicit mules:
Willing participants who open or use accounts to launder funds.

Recruited mules:
Persuaded, paid or forced to use their legitimate accounts.

Exploited mules:
Unwitting participants who don't realize their accounts are being misused.

THE ANATOMY OF A MULE NETWORK

Mule networks thrive on complexity. They move money across borders, use cryptocurrency and gambling accounts and exploit legitimate businesses with high cashflow, like construction firms, to mask illicit transactions.

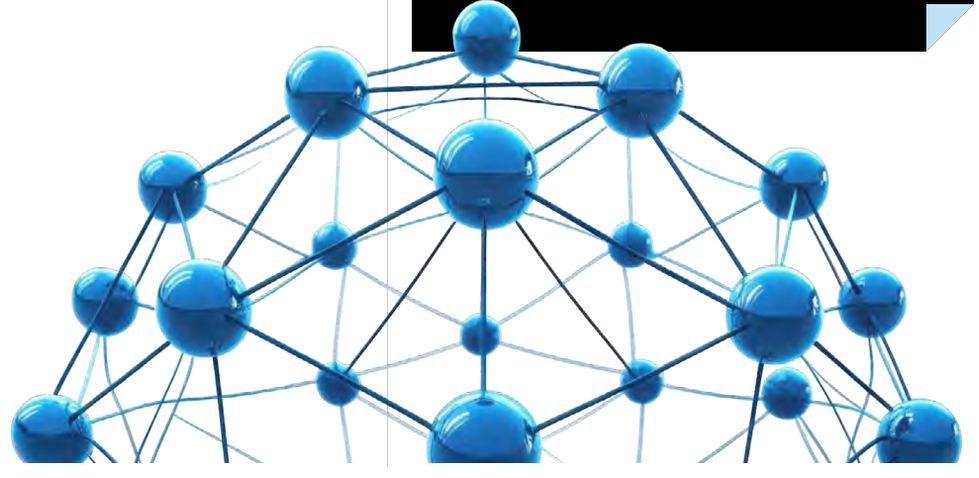
An average mule network consists of 15 mules and moves money among 3.4 banks. But some are far larger: One uncovered network involved 543 mules and moved more than £130 million.[23]

Mules often lend temporary legitimacy to transactions, making stolen funds harder to detect. Their accounts, often belonging to students, small business owners looking for extra income or foreign nationals returning to their home countries, act as camouflage. Some mules are complicit, others coerced and many are unaware their accounts are being used for crime.

Mule recruitment crosses demographic groups, but youth is a factor: 35% of Generation Z say they would consider moving money for a stranger in exchange for a fee; 14% say they are "very likely" to do so.[24]

Authorities are taking notice and placing greater responsibility on financial institutions to find new ways to clean up their ecosystems.

In a recent survey, 30% of 18-24 year olds said that they or someone they know has been approached to make a fraudulent transfer, and 27% said that they'd be open to make such a transfer in exchange for a financial cut.[25]



A Global Threat with Local Signatures

Mule operators have evolved from basic IP-masking to sophisticated multi-layer fraud schemes. These include GPS spoofing, roaming SIM cards and satellite internet terminals that can bypass location checks in regional banking systems.[26]

Europe: Transnational mule rings often launder proceeds from phishing and online scams. Europol supported a large-scale operation led by Italian and Portuguese authorities against two networks of money-mule recruiters working for a criminal group that had profited over $10M from cryptocurrency scams. Law enforcement from Austria, France, Germany, Romania, Spain and Switzerland were also involved in the investigation, as well as Eurojust.[27]

United States: Many money mules begin as victims of lottery or romance scams and are unknowingly lured by fraudsters into transmitting fraud proceeds based on lies. Other mules are recruited into what they think are legitimate work-at-home jobs. In its 2024 Money Mule Initiative, the U.S. Department of Justice took action to stop over 3,000 of them.[28]

Asia-Pacific: In regions like Hong Kong and Singapore, mule networks increasingly exploit crypto exchanges and gaming platforms to move funds. A recent crackdown in Hong Kong dismantled a ring that laundered HK$118 million through crypto-currency and more than 500 mule accounts.[29]

Regional variations like these reinforce the need for globally coordinated intelligence sharing that can inform local detection strategies. What works in one market may not work in another. But together, these insights form a more complete picture of a firm's options for fighting back.

MULE-FOCUSED REGULATION FUELS A GLOBAL RESPONSE

Governments and regulators are increasingly stepping in with new protocols aimed at disrupting mule operations and preventing scams:

Australia: AUSTRAC has issued fines and placed conditions on crypto ATM operators, including limits on cash deposits and withdrawals and further regulatory requirements. Earlier in the year a taskforce had identified trends confirming that crypto ATMs were being used for illicit transactions.[30]

United Kingdom: United Kingdom: Since October 2024, the Payment Systems Regulator (PSR) requires banks to reimburse scam victims, splitting liability 50/50 between sending and receiving payment service providers. In 2025, it was announced the PSR's responsibilities would fold into the Financial Conduct Authority to streamline oversight.[31]

Hong Kong: The Anti-Scam Consumer Protection Charter focuses on reporting, information sharing and public education, though it stops short of shifting liability.[32]

These regulatory shifts, combined with a growing awareness of mule networks' role in laundering and a heightened duty of care for customers, are prompting financial institutions to rethink their anti-fraud strategies and invest in real-time analytics.

Given that initial scam payments are increasingly found within a bank's own book, it's no surprise that institutions are investing heavily in targeted anti-mule measures.

GONE IN 30 MINUTES[33]

When money starts moving through a mule network, it moves fast.

This snapshot of a network retro analysis shows how stolen funds from two separate real world scam victims (the green bank accounts on the left) were washed in just 30 minutes, funneled through other banks and, ultimately, gaming and retail websites.

Telltale Signs of Mule Activity

For an authorized push payment scam to succeed, a financial beneficiary account has to be ready to receive the victim's funds and quickly disburse them.

The money mule who controls this account monitors the account obsessively, rapidly disbursing each deposit the minute it comes in. In this way the money spreads to additional mule accounts, often in parallel, dividing and recombining in unpredictable ways, making it incredibly difficult for banks or law enforcement to follow the flow of money until it's too late.

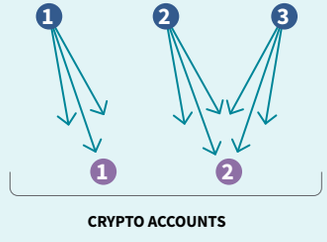
But by monitoring payment behavior, banks are learning new ways to spot mule activity and disrupt these accounts long before their customers are victimized.

A deep dive into some recent authentic, anonymized account activity demonstrates how deep contextual intelligence can help banks quickly spot and thwart mule activity.[34]

A mule appears.

This "customer" sets up 3 bank accounts in a single month.

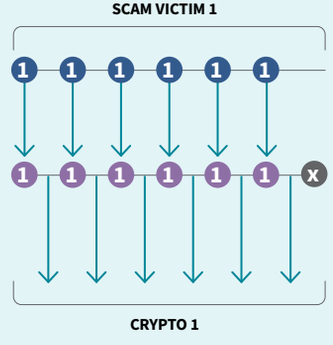
Deposits thousands of USD to 2 crypto exchanges in months 2 and 3.



The scams are well underway.

Here today. Gone tomorrow.

A scam victim at Bank 1 makes multiple credit card payments to one of the mule's crypto exchanges.

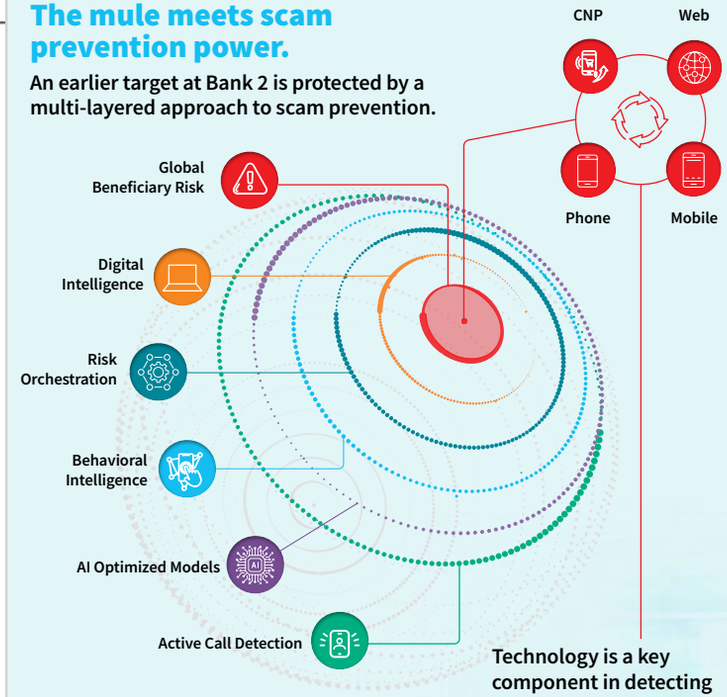


The funds are withdrawn immediately, and the crypto wallet isn't used again.

The victim's money is gone.

The mule meets scam prevention power.

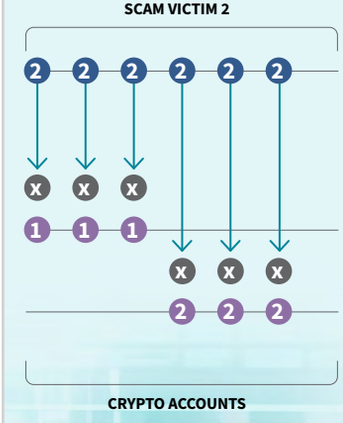
An earlier target at Bank 2 is protected by a multi-layered approach to scam prevention.



Technology is a key component in detecting scams, but organizational collaboration is essential.

This time the mule is thwarted.

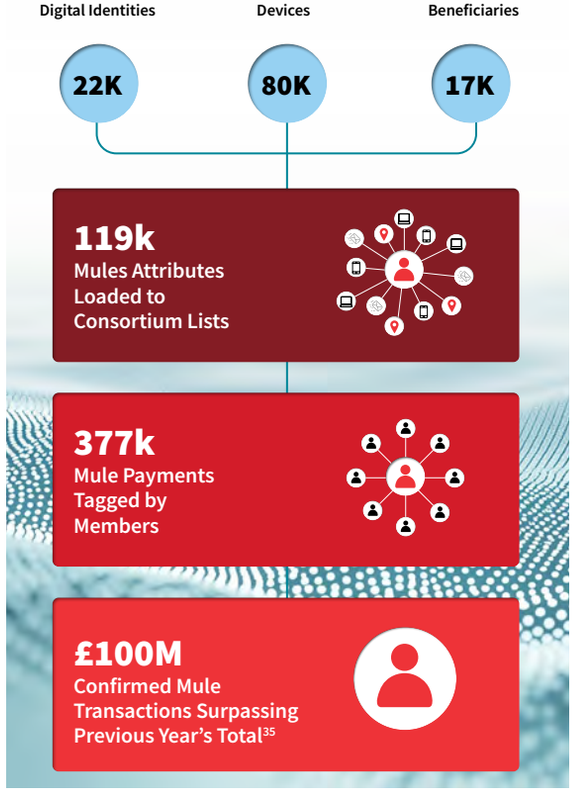
Convincing the intended victim to try smaller transaction values and switch crypto exchanges didn't help the scammer beat the bank's defenses.



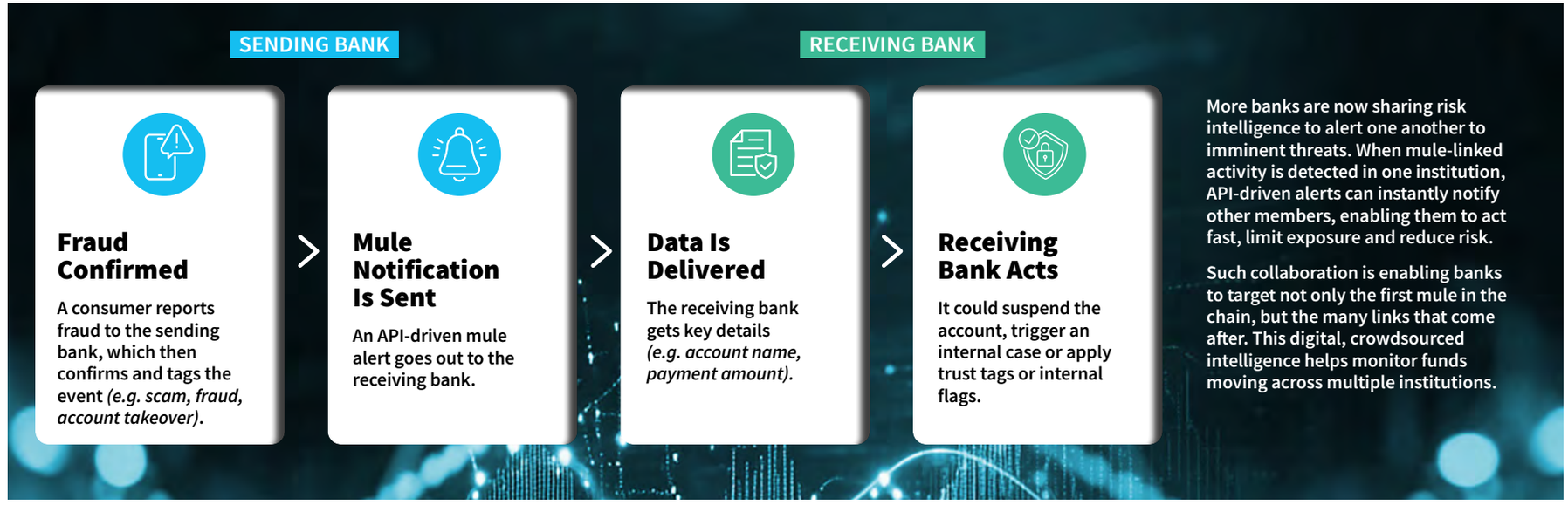
The customer from Bank 1 could have been protected with a similar approach.

Collaboration in Action: Stop the Flow, Stop the Fraud

Through collaborative efforts, UK banks have successfully identified thousands of mule payments, enabling the creation of a robust set of attributes for proactive prevention of future mule activity.



For financial institutions participating in the LexisNexis® Risk Intelligence Consortium and taking advantage of the Early Mule Warning capability, shared bank-to-bank intelligence is helping them detect mule activity before any money moves.



"Just a few years ago, mule hunting in financial services was still in its infancy with only the largest organizations being able to allocate time and resources to it, and even then, it was a low priority. Today, many customers' fraud operations include a global anti-mule team of over a hundred specialists using advanced tech to evaluate inbound payments."

Rob Woods, senior director of fraud & identity, LexisNexis® Risk Solutions

THE FIGHT BACK IS UNDERWAY: INSIDE ONE BANK'S BATTLE AGAINST FIRST-GENERATION MULES

THE RESULTS WERE STRIKING:[36]

50% uplift in mule account detection
£750,000 returned to victims
140 mule accounts uncovered in a single sweep

This case study highlights how real-time intelligence and global data sharing can help banks not only protect customers, but dismantle the networks supporting the crime.

THE ANTI-MULE PLAYBOOK

As banks grow their ability to analyze behavior and share insights, mule detection improves and these insidious networks become more expensive and riskier to operate. Some mules may only be deployed once before their accounts are flagged or shut down, forcing criminals into a costly cycle of constant recruitment.

Here's how leading institutions are fighting back:

▶ **Benchmarking against global intelligence.** Comparing activity against anonymized global data helps distinguish legitimate behavior from mule-linked anomalies, as does leveraging global transaction data that improves a bank's ability to 'follow the money'.

▶ **Collaborating across institutions.** Real-time alerts allow banks to intercept mule activity before funds are fully laundered, reducing losses and improving recovery rates.

▶ **Following the mule with digital assessment beyond banking.** Across industries like ecommerce, gaming and telecommunications, banks can make it harder for networks to recruit, communicate, transact and clean their profits, sharing multi-layered beneficiary insights like device data and PII re-usage.

▶ **Scrutinizing inbound payments.** Monitoring incoming funds, not just outbound transfers, helps identify mule accounts earlier in their lifecycle. As regulations for shared liability like the UK model take hold, this will shift from strategic tactic to compliance necessity.

▶ **Analyzing the full customer journey.** New accounts with a high velocity of activity, multiple existing accounts being accessed by the same device and increased payment volumes in short periods are all examples of different signals banks can leverage at different stages of the customer journey.

▶ **Taking down mule networks with actionable analytics.** Sharing data and analysis after detection with like-minded institutions can better prepare communal defenses to break the chain and stop the flow of illegal funds.

Disrupting mule networks is more important than ever.

Mule networks won't vanish overnight. But with smarter tools, stronger collaboration and sharper regulation, financial institutions are finally gaining the upper hand.

CHAPTER 5

Embracing the New Complexity of Identity

The Rising Challenge of Verifying Identity

A generation ago, your name and an identity card or document were enough to identify you in most situations. Today, your digital identity is arguably just as important as your physical identity, and the "real" you is a dynamic combination of hundreds of factors: your email addresses and phone numbers, your location and device, your unique unconscious behavioral patterns, your digital footprint, your relationships to others and much more.

All of these data points contribute to establishing whether we can be trusted on and offline. But for companies trying to reliably authenticate end users at scale, building a unified persona from these scattered clues and evaluating it quickly enough to keep business moving is a formidable challenge.

Synthetic fraud is expected to generate $USD 23 billion in losses by 2030.[37]

DECIPHERING THE NOISE

It's critical to have breadth and depth of data, but a sea of disjointed identity signals can be too scattered for human teams to process in real-time. AI-powered tools and analysis can help decipher and resolve them.

Fast, reliable identity verification is the challenge of our times. To be competitive, companies need to meet customers' expectations of low friction, while keeping accounts safe from fraudsters and staying compliant with regulations. Overwhelmed fraud and onboarding teams need new solutions to parse modern identity complexity, so they can filter out bad actors quickly and with minimal friction.

But every initiative that reduces friction for customers has the potential to make life easier for criminals, too. Armed with powerful tools and easy-to-access dark web resources, they can create fake and synthetic identities, clone identity documents and create very believable deepfake images and videos to try and bypass fraud prevention workflows.

And that means companies can no longer rely on a single point-solution for anti-fraud measures. There is no "magic bullet."

IDENTITY COMPLEXITY TAKES EXISTING VERIFICATION CHALLENGES TO THE NEXT LEVEL.

CHALLENGE: Efficiently onboarding emerging identities.

Digitally fluent young people and new-to-country immigrants can be attractive prospects for rapidly expanding companies, but may lack traditional data like credit histories. Onboarding these "thin-file" identities can require companies to find alternative data sources that can fill in the gaps. Meanwhile, fraudsters can deploy synthetic identities that mirror these "acceptable" thin-file profiles and can simultaneously target these vulnerable populations to leverage their legitimate bank accounts as money mules.

CHALLENGE: Safely reducing customer friction at onboarding.

Having to plug in long ID numbers is a tedious task for busy customers. The U.S. Financial Crimes Enforcement Network (FINCEN) approved a new policy this year allowing banks to collect a customer's tax ID number (TIN) from a third-party rather than directly from the customer; another proposal would let a user supply just four digits of their social security number, with a third-party providing the rest.[38] It's designed to streamline the process for customers, but this could open a new attack vector for fraud. This approach should be grounded in a more comprehensive understanding of the transaction's overall risk, incorporating digital risk assessment as a critical component.

CHALLENGE: Verifying age while preserving privacy.

Online sites with sensitive material or age-restricted goods can struggle to block out people who should not be accessing them without capturing their private information and putting them at risk. In 2025, the European Union released a blueprint for an effective age-verification system that preserves privacy and that will interface with the coming EU Digital Wallet.[39] Australia's Online Safety Act, similarly, was amended to require social platforms to actively restrict specific user groups from setting up accounts, rather than merely requiring them to self-gate.[40]

CASE STUDY: VERIFYING SKILLED MIGRANTS IN APAC

An organization in APAC transformed its identity verification of skilled migrants[41] with LexisNexis® IDVerse®.

CHALLENGE:

This organization wanted to modernize its digital identity verification process without falling out of compliance with domestic regulators. Time-consuming manual ID checks created internal bottlenecks, resulting in a poor user experience, unnecessary administrative overhead and a turnaround time of up to three months.

When the Migrant Skills Assessment project went live, verification requirements initially mandated two documents: a primary passport plus a secondary ID card or driver's license. While passports generally performed strongly, the secondary document requirement frequently caused OCR and document-quality issues (particularly when applicants supplied paper-based or laminated IDs), increasing flagged verifications and slowing throughput.

After implementing IDVerse® into its identity verification stack, the company was able to confidently move to passport-only checks, speeding verification, driving improved conversion and reducing the administrative burden of manual checks. In parallel, the verification flow was strengthened to prevent applicants from altering key fields such as expiry dates, which had previously been exploited for fraudulent purposes.

As a result, verification turnaround time fell from up to three months to approximately two days, while the organization maintained compliance.

RESULTS:

98%

The ratio of initiated-to-completed verifications rose from 85% due to greater efficiency and reduced drop-off.

6-9%

Improved verification accuracy reduced the ratio of flagged verifications from 28% to single digits, reducing costs.

75%

Expired rates fell by three quarters, from 32% to 8%, within six months, reducing delays and improving throughput for applicants.

Businesses Are Leaning Into Powerful New Solutions That Fully Embrace Identity Complexity

For every transaction attempt, a company needs to understand the identity, its history and its intent, and deliver a single go-or-no-go risk decision. But the risk signals around every transaction today are numerous, disconnected and hard to interpret, calling for a layered approach.

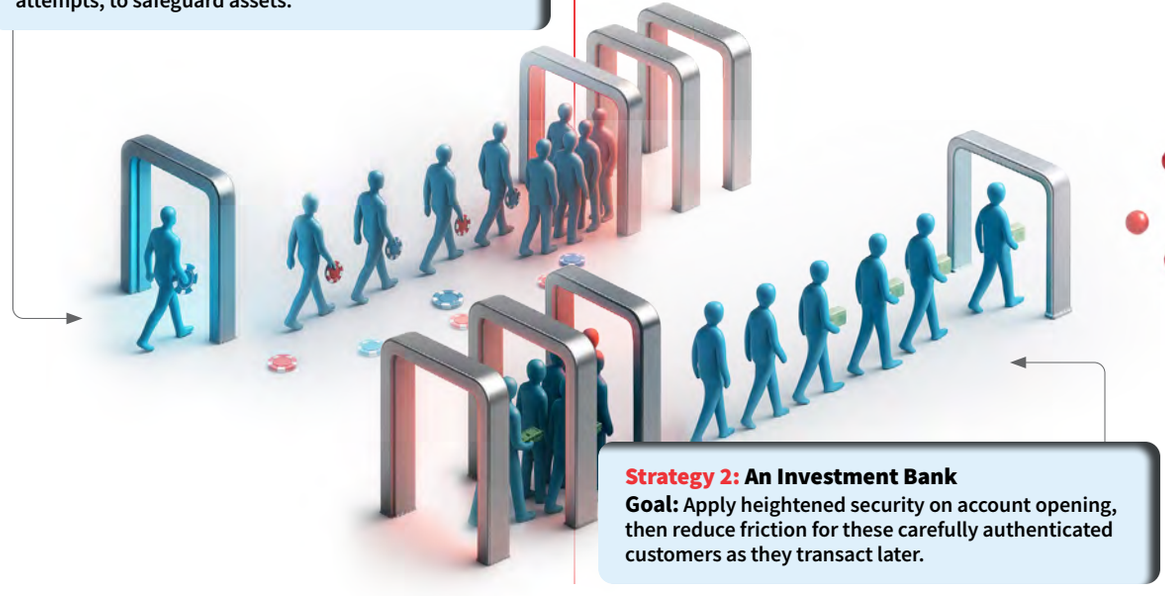
- **Gather a comprehensive pool of identity data, from multiple sources, around every transaction**
- **Cross-reference using advanced linking technology, and process into insights with AI-powered analytical solutions**
- **Benchmark these insights against known identities, behaviors and fraud vectors around the world**
- **Simplify all of this into dynamic risk insights that enable automating confident decisions at scale**

Comprehensive identity verification solutions are built on foundational technologies such as LexID® and LexID® Digital from LexisNexis® Risk Solutions. The backbone of our identity intelligence capabilities, these technologies enable the creation of persistent, tokenized identifiers that unify multiple data points to provide a clear, connected view of an identity. This powerful linkage supports robust risk assessments and empowers verification systems to deliver deeply informed, confident decisions around which customers to trust in which scenarios.

DIFFERENT IDV GOALS CALL FOR DIFFERENT SOLUTION STACKS

Strategy 1: A Gaming Company
Goal: Keep account opening friction low, to stimulate growth, but increase security on withdrawal attempts, to safeguard assets.

There's no one-size-fits-all solution for identity verification, because every company has its own unique customers and growth goals, regulatory and fiscal requirements, tolerances for risk and for customer friction and more. These unique aspects may change as the company grows and evolves.



Strategy 2: An Investment Bank
Goal: Apply heightened security on account opening, then reduce friction for these carefully authenticated customers as they transact later.

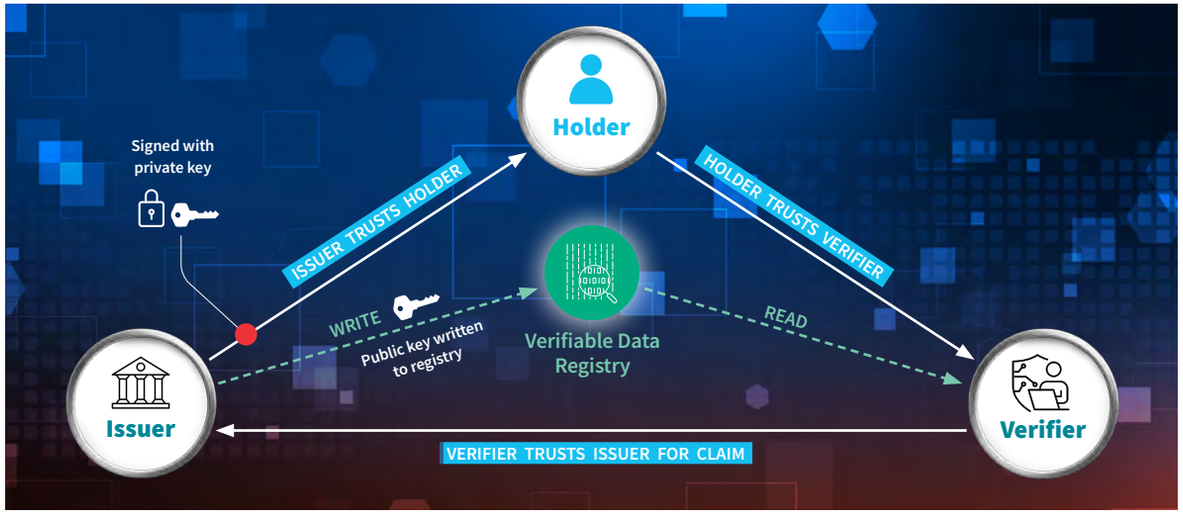
To be able to assemble the perfect solution stack for their unique needs right now, companies need flexible, modular solutions, integrated together seamlessly. These solutions need to be adjustable, to continue supporting their particular IDV strategy even as that strategy, and the company's needs, evolve over time.

Modular Solutions
With the right strategy, a company can build the specific identity verification and identity fraud protection solution they need to support a given set of goals.

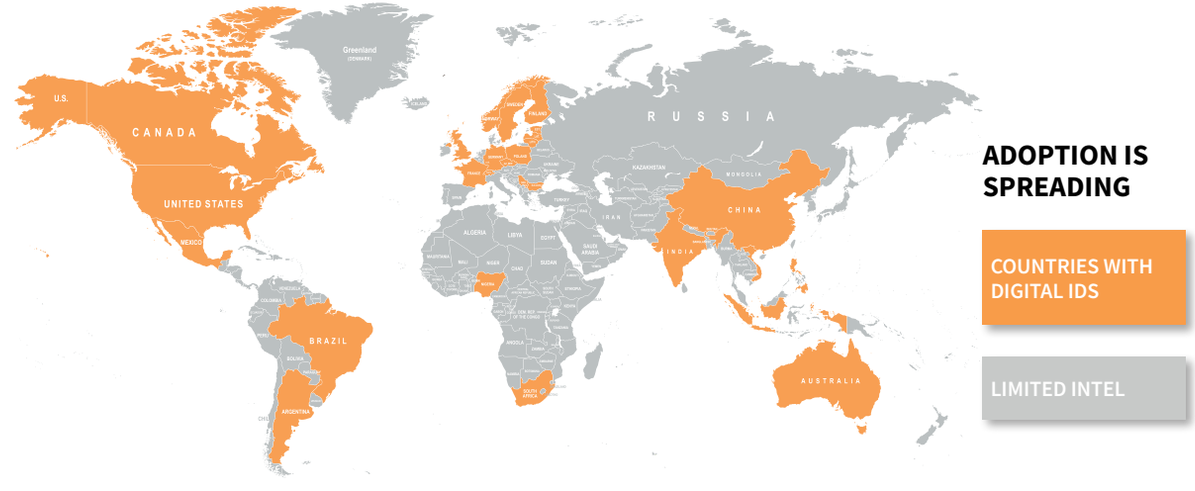
Government Digital Credential Issuance Is On the Rise Worldwide

Digital credentials are created when physical documents like passports, driver licenses and diplomas are converted into a digital format that's cryptographically protected with a public/private key pair. This "zero-knowledge proof" system allows consumers to securely reveal part, but not all, of the information they hold. This lets customers take more control over their own data, typically from their smartphone, so they can choose to reveal only the minimum information necessary to gain the permission they need for a particular operation. More than 160 countries have developed or are implementing the technology around the world, and five billion digital IDs have already been issued globally.[42]

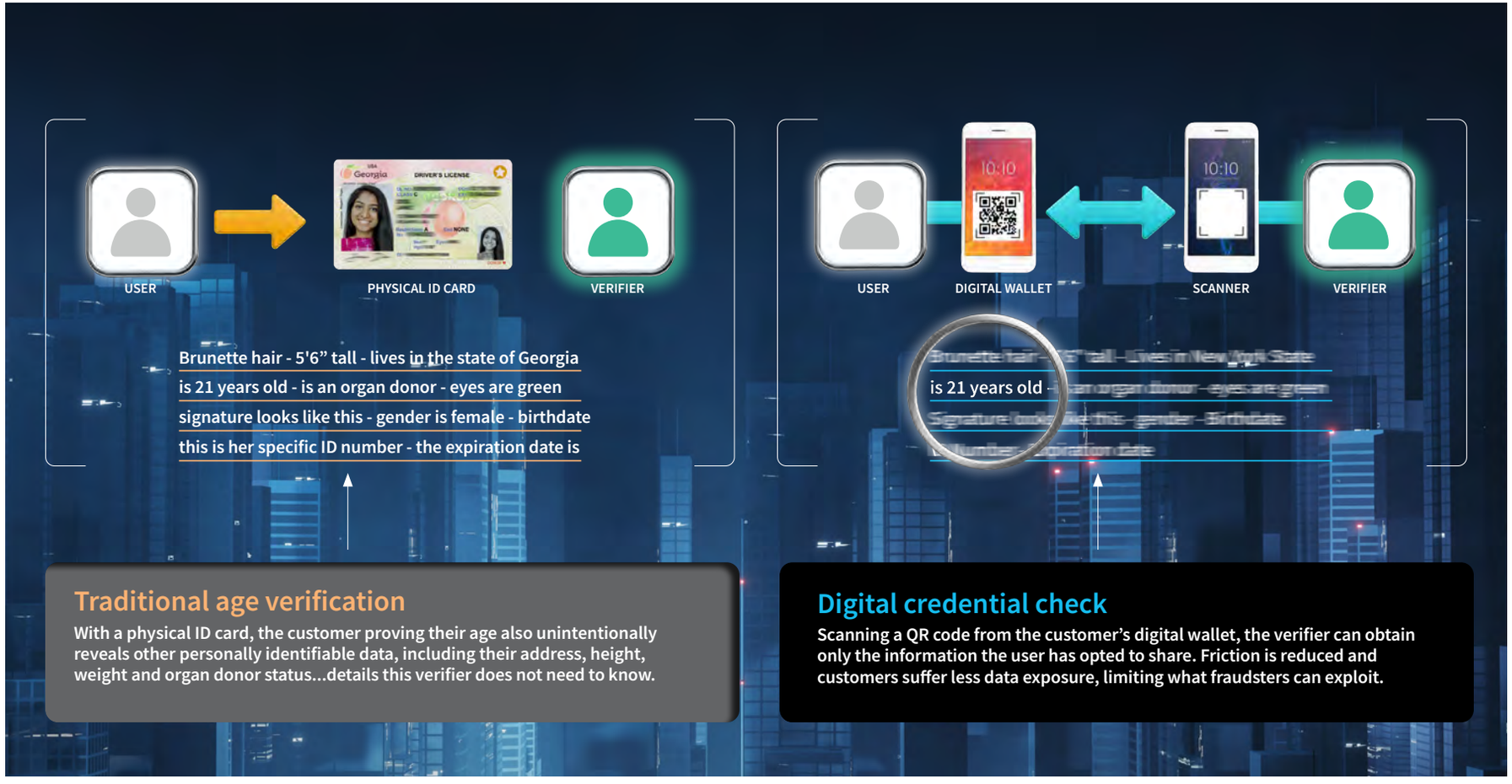
Digital ID systems are coming online around the world, many with custom formats and protocols, but we are seeing a slow convergence towards ISO 18013-5/-7 formats as an emerging global standard.



In Europe, the European Digital Identity Wallet (EUDI Wallet), established under Regulation (EU) 2024/1183 (eIDAS 2.0), is required to be made available by EU Member States to citizens and residents within 24 months of the implementing acts' entry into force, expected by late 2026.[43] In the U.S., mobile driver licenses are now accepted at more than 250 TSA checkpoints: Compatible with easily obtained wallet apps, these mDLs been embraced by 20 American states plus Puerto Rico, covering well over 50% of the U.S. population, with more adoption on the horizon.[44] As digital credential issuance continues to advance, we expect the next stage to focus on digital ID and mDL acceptance across use cases beyond travel including bank account opening, age verification, authentication, and more.



Digital Credentialing in Action



IDENTITY COMPLEXITY IS A CHALLENGE, BUT IT'S AN OPPORTUNITY AS WELL

The sheer quantity of data surrounding digital interactions and transactions today can seem daunting, especially for companies trying to emerge from legacy IDV solutions.

But there's a silver lining: Today's powerful solutions can effectively cross-reference and analyze each identity's diverse, comprehensive and unique set of online and offline datapoints in near real-time to form a firmer foundation for strong identity verification. And this foundation is increasingly important as fraudsters look to exploit any vulnerabilities in the evolving digital credentialing ecosystem.

Effective identity verification today, and for the foreseeable future, requires finding solutions that fully embrace this complexity. These need to be purpose-built to be able to efficiently sort high quantities of identity data into layered solutions that drive faster, smarter risk decisions.

Keeping Pace with the Digital Payments Boom

Digital Payments Are Growing Exponentially. Fraud Professionals Need to Connect the Dots To Keep Up

Innovative payment systems have spread around the globe, speeding up transactions and transforming consumer expectations.

The change is happening with breathtaking speed.

- **The all-digital neobanking market, just $96 billion in 2023, is poised to climb to $2 trillion by 2030.[45]**
- **The use of digital wallets is expected to rise from 49% in 2021 to 61% in 2027.[46]**
- **Buy Now, Pay Later (BNPL) payments grew from $316 billion in 2023 to $452 billion this year.[47]**

Competitive companies need to be open to evolving consumer preferences. But every new payment method and every shortening of transaction times brings more risk.

The digital yuan has topped $7.3 trillion in volume over more than 29 cities in China, and most digital transactions are via digital wallets.[48]

REGION: LATAM

In Latin America, a payments revolution has brought more than 60 million new consumers into the financial system through digital wallets and instant transfers.

Brazil: The PIX system, established in 2020 and the poster child for digital payments innovation, now claims 605 million accounts and processes more than R$6Bn in transactions every month.[49]

Colombia: The payment system Bre-B, promising to save time and transaction costs, launched in 2025 here to great fanfare: More than 30 million people had already pre-registered to use the system.[50]

Mexico: CoDi has more than 18 million validated accounts.[51] Notably, PIX, Bre-B and CoDi are setting standards that could allow the three nations, and others, to eventually interoperate.

REGION: APAC

Payments innovation and biometrics are embedded in all facets of daily life here, linking payments to identity using users' devices, faces and voices.

China: A first-mover advantage in mobile payments evolved into a financial ecosystem where credit, savings, insurance and investments are all embedded within "super-apps."[52]

India: Unified Payments Interface built trust quickly: 300+ connected banks now process over 10 billion transactions per month.[53]

Japan: Biometric authentication and contactless payments let consumers use a palm or face for transit, in cities from Tokyo to Osaka.[54]

Singapore: The world's first cross-country payments corridor connects their instant payment system to Thailand, India and Malaysia.[55]

REGION: EUROPE

In Europe, where non-cash payments reached a total value of €113.5 trillion in 2024,[56] the Single Euro Payments Area (SEPA) allows 41 member countries, including a few outside the European Union, to make cashless euro payments to anywhere in the EU.[57] The European Central Bank's work on the Digital Euro, a proposed digital currency for the continent that could be online as early as 2029,[58] might add programmability to this network.[59]

The UK: The Faster Payment System, no longer regarded as 'emerging' since it launched back in 2008, now allows instant transfers of up to £1 million within the UK. In 2024 the system processed 5.09 billion transactions with a value of £4.2 trillion.[60]

REGION: NORTH AMERICA

The U.S. Federal Reserve launched FedNow in 2023 to enable banks and credit unions to offer instant payments to their customers.[61] It competes with RTP, an older (2017) and larger private real-time payment network owned by large commercial banks including J.P. Morgan. Many banks have adopted a multi-rail strategy for payments, with 58% using both systems.[62]

Canada: With 60% of Canadians saying they'd like to send and receive payments in real time, there's a lot of excitement around the planned 2026 launch of Real Time Rail, an emerging A2A payment that will give Canadians both real-time exchange and real-time clearing and settlement in a single system.[63]

Faster Payments Raise New Challenges

Faster payments:

- **In the UK,** the irreversible nature of the Faster Payment System's instant payment transactions contributed to a concerning uptick of authorized push payment scams.[64]
- **Brazil's** PIX is one of the most successful financial inclusion stories in modern history, with 150 million active users logging 40 billion transactions a year. But as it has linked up with other payment systems in the LATAM region it's also attracted a rash of impersonation scams to set up kidnappings for money.[65]
- **In India,** the convenience of UPI's introduction was undercut by a reported $1.7 billion in UPI fraud in 2023, most of it backed by social engineering schemes.[66]

Crypto:

- Fraud continues to be a major hazard. In the U.S. alone, consumers lost around $9.3 billion to crypto fraud in 2024.[67]
- Assessing these risks has required merchants to invest in new tools for on-chain and off-chain analysis, and to absorb evolving compliance issues.

BNPL:

- BNPL usage is rising fast. Over the last five years, the percentage of customers who've applied for BPNL at least once rose from 13% to 40% in the U.S., from 4% to 49% in the UK and from 3% to 21% in Canada.[68]

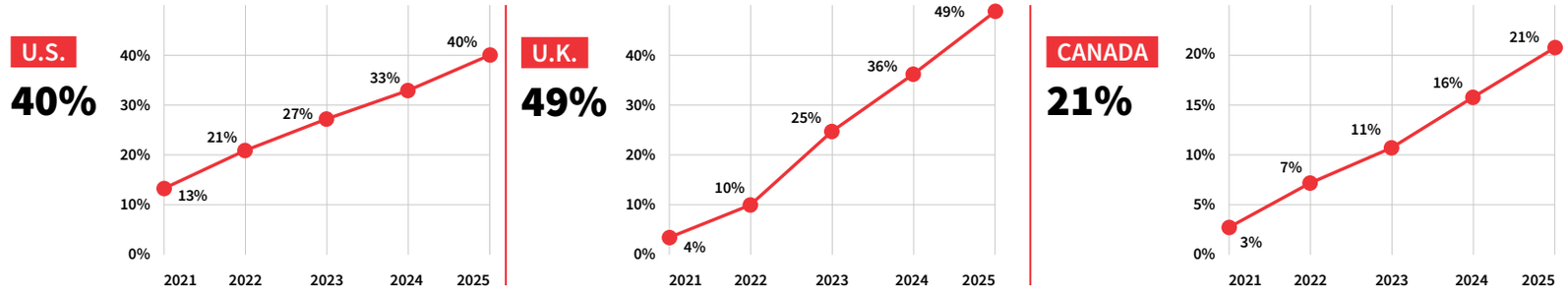
Card-Not-Present:[69]

- Card transactions and digital wallets make up the largest share of payments in APAC and together comprise nearly half of all APAC's fraud losses in 2025 (45%).
- In EMEA, card and wallets channels also make up 45% of total fraud losses.
- In LATAM, card transactions (24%) and digital wallets (22%) together account for 46% of total fraud losses.
- In North America, card transactions (28%) and digital wallets (13%) make up 41% of losses.

Criminal networks capitalize on new payment methods at lightning speed. Payment systems need to advance fraud-detection frameworks and present a united front against fraud to keep pace.

For financial institutions with consumers transacting across multiple channels, that means joining up the dots internally as well as tapping into global risk intelligence across the world's growing number of accepted payment methods.

PERCENTAGE OF ADULTS, BY COUNTRY, WHO HAVE USED BNPL[70]

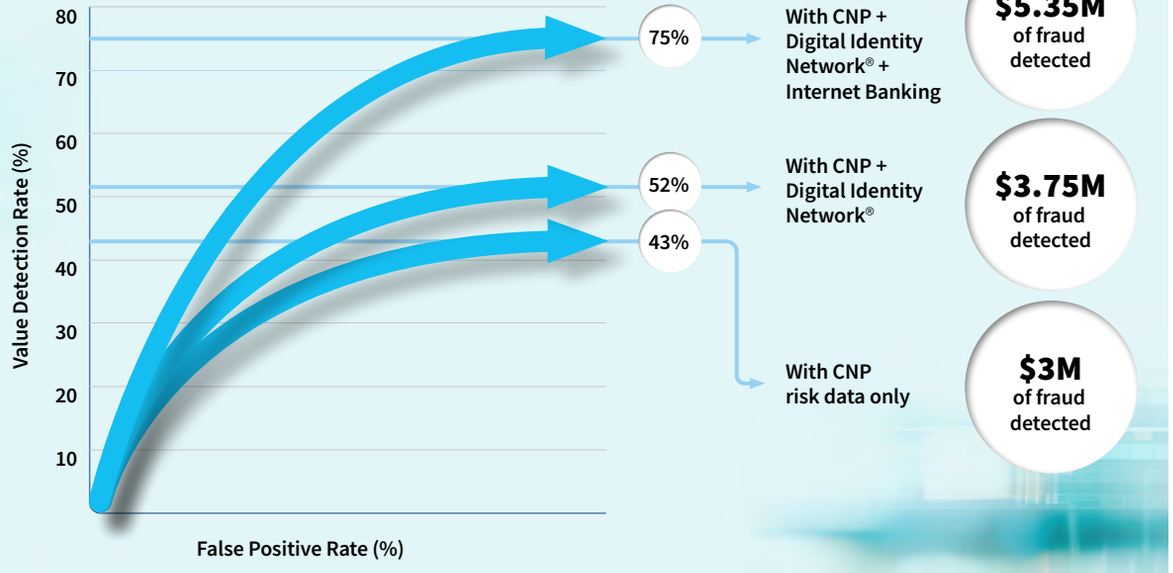


The Power of a United View of Digital Payments Risk

A major international bank has taken the initiative on considering global payments intelligence, and is seeing astonishing results.

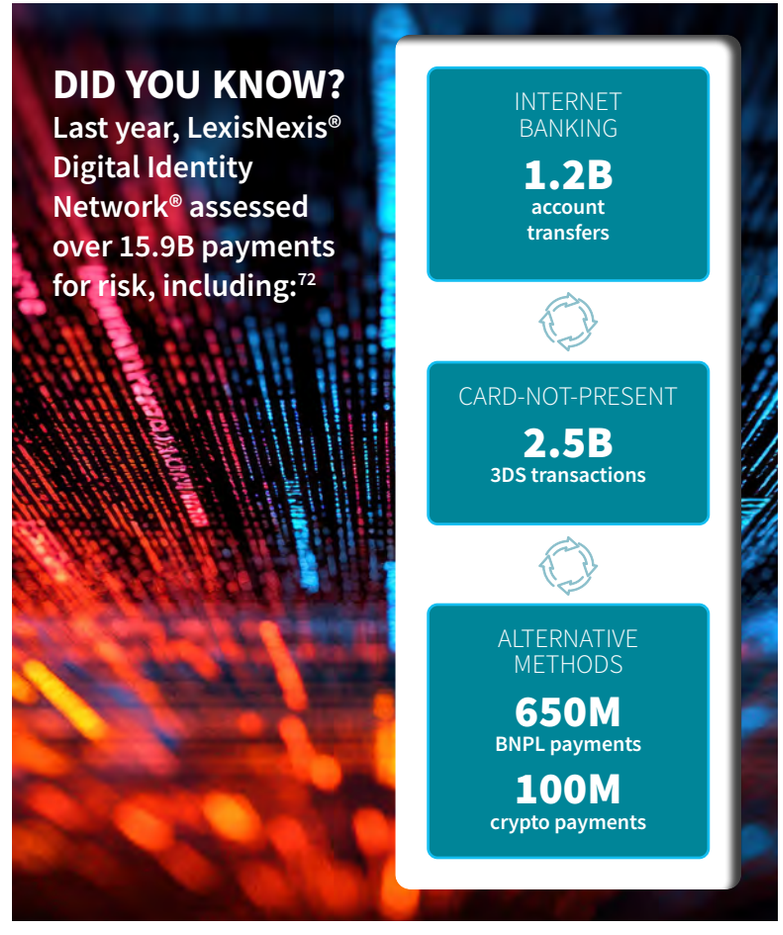
The following graphic shows the uplift in total value of fraud detected when combining these intel sources:
1) risk insight from the card-not-present channel,
2) global transaction-based intelligence spanning numerous payment technologies and non-payment interactions, and
3) insight from their own internet banking channel.

Keeping false positives at 1.0%, a major banking client achieved fraud value detection rates, over one month, of:



Advanced linking technology plays an important role here in constructing one centralized view of customer activity. It's crucial for financial institutions where digital payment channels and risk teams operate independently.

Risk signals such as merchant risk and suspicious consumer behavior on the CNP channel, can be combined with risk signals including victim coaching, account takeover and payee risk on internet banking. This particular example represented a $28.2M increase in total value of fraud detected per annum.[71]



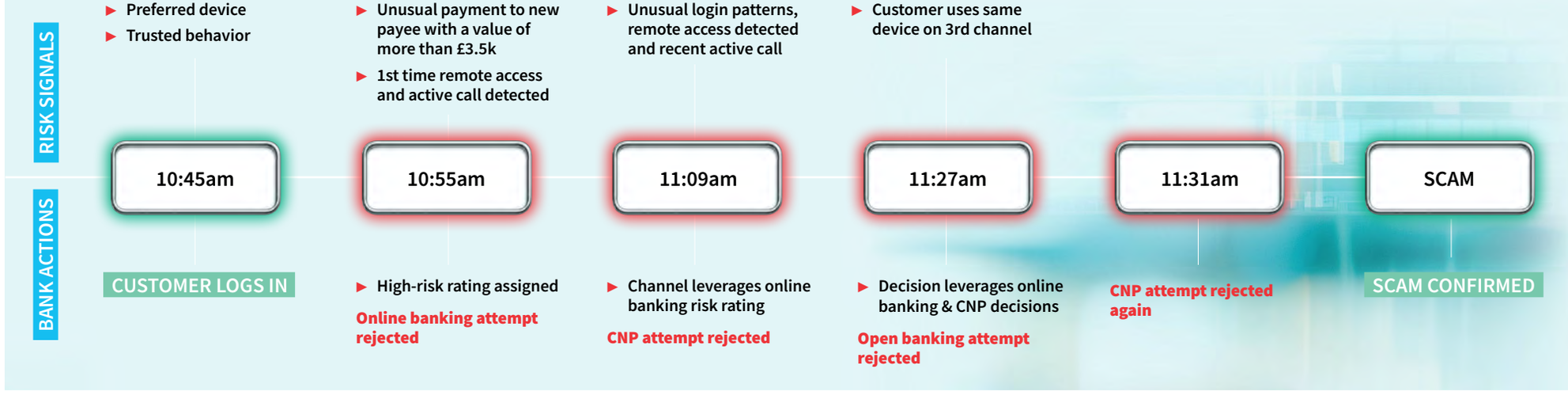
Preventing Scams With a Holistic View of the Customer

In another example of the power of sharing risk signals across channels, a leading UK-based bank blocked £500k of social engineering scams in just twenty days by leveraging risk signals across three digital payments channels.[73]

The following illustration shows how one scam victim attempted to exit funds across the online banking, card-not-present and open banking channels in less than an hour, and how the organization stopped the scam in action.

THE POWER OF SHARING RISK SIGNALS ACROSS CHANNELS

A leading UK-based bank blocked £500k of social engineering scams in just twenty days by leveraging risk signals across three digital payments channels.[74]



As global commerce continues to favor low-friction, high-speed transactions and scammers evolve their tactics to take advantage, securing transactions can't be the only line of defense anymore. Banks and ecommerce companies must build more complete pictures of customer activity and look beyond singular interactions.

This means orchestrating billions of data points gathered from device intelligence, behavioral intelligence, digital identity graphs, geolocation signals and machine learning models, then sharing these deeply informed insights, and the data behind them, with collaborating institutions.

Finally, this invisible intelligence infrastructure then needs to be integrated across all supported payment types to support continuous, frictionless real-time merchant-customer relationships. Think of it as a sort of "Trust Layer" for the digital economy.

CHAPTER 7

How AI Is Changing the Fraud and Identity Game

There's a Rapidly Developing Arms Race Between "Good" AI and "Bad" AI"

The hype that surrounds us says AI is going to transform everything. But will that transformation deliver benefit or harm? On the one hand, the World Economic Forum predicts that AI will unlock untold wealth.[75] On the other, some policymakers and industry leaders have compared the dangers of AI to those posed by pandemics and other catastrophic risks.[76]

In the world of fraud and identity, the arms race between these two extremes is already well underway. Criminals are leveraging generative AI to create high-grade fake IDs and selfie videos and to create synthetic identities at the speed of light, for more effective scams or to bypass verification checks, and they're racking up some wins.

- **More than a third of fraudulent attacks in the past year involved generative AI, a sharp increase from 20% the year before.[77]**
- **85% of identity fraud cases involve generative AI tools.[78]**
- **A recent study revealed that people correctly spot deepfakes just 20% of the time.[79]**
- **In 2021, virtually no forged documents were generated by AI. In 2024, AI-generated forgeries were involved in 57% of attacks.[80]**
- **Recently, a fraudster scammed $20 million from Brazilian financial institutions using multiple deepfake accounts.[81]**

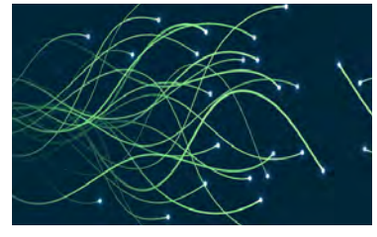
Criminals have been using generative AI to step up their tactical game, improving the quality and expanding the frequency of deepfake IDs and selfie videos, while also crafting highly convincing phishing emails, automating social engineering attacks and even generating mass synthetic identities. But for most, that's as far as it's gone. New AI capabilities haven't (yet) translated into a broader uplift in overall fraud attacks, according to experts.

"Losses aren't up from AI at the moment," notes Mike Nathan, vice president of international professional services, LexisNexis® Risk Solutions. "Fraud follows the money, and until we see consumer habits change fundamentally, like the rise of agentic shopping, expect AI to have only incremental effects as fraudsters explore these new tools."

AI is a powerful weapon in the hands of fraudsters, and a growing threat that risk professionals need to monitor closely. But it remains a mostly sleeping giant that may yet change the game.

BAD BOTS ARE "BOTS," GOOD BOTS ARE "AGENTS"

As agentic AI goes mainstream, proving that a suspect identity isn't human won't be enough to disqualify it. Instead, companies will need to invest further in understanding intent.



GOOD BOT:

- **Has authorized access to your accounts**
- **Acts on your behalf with your permission**
- **Follows rules and regulations**
- **Is transparent about its actions**
- **Is constrained by ethics and policies**

Examples: Booking flights, managing finances, gathering information you requested

BAD BOT:

- **Works to establish unauthorized access to your accounts**
- **Acts against victims without permission**
- **Ignores all rules and regulations**
- **Operates in secret**
- **Has no ethical or operational constraints**

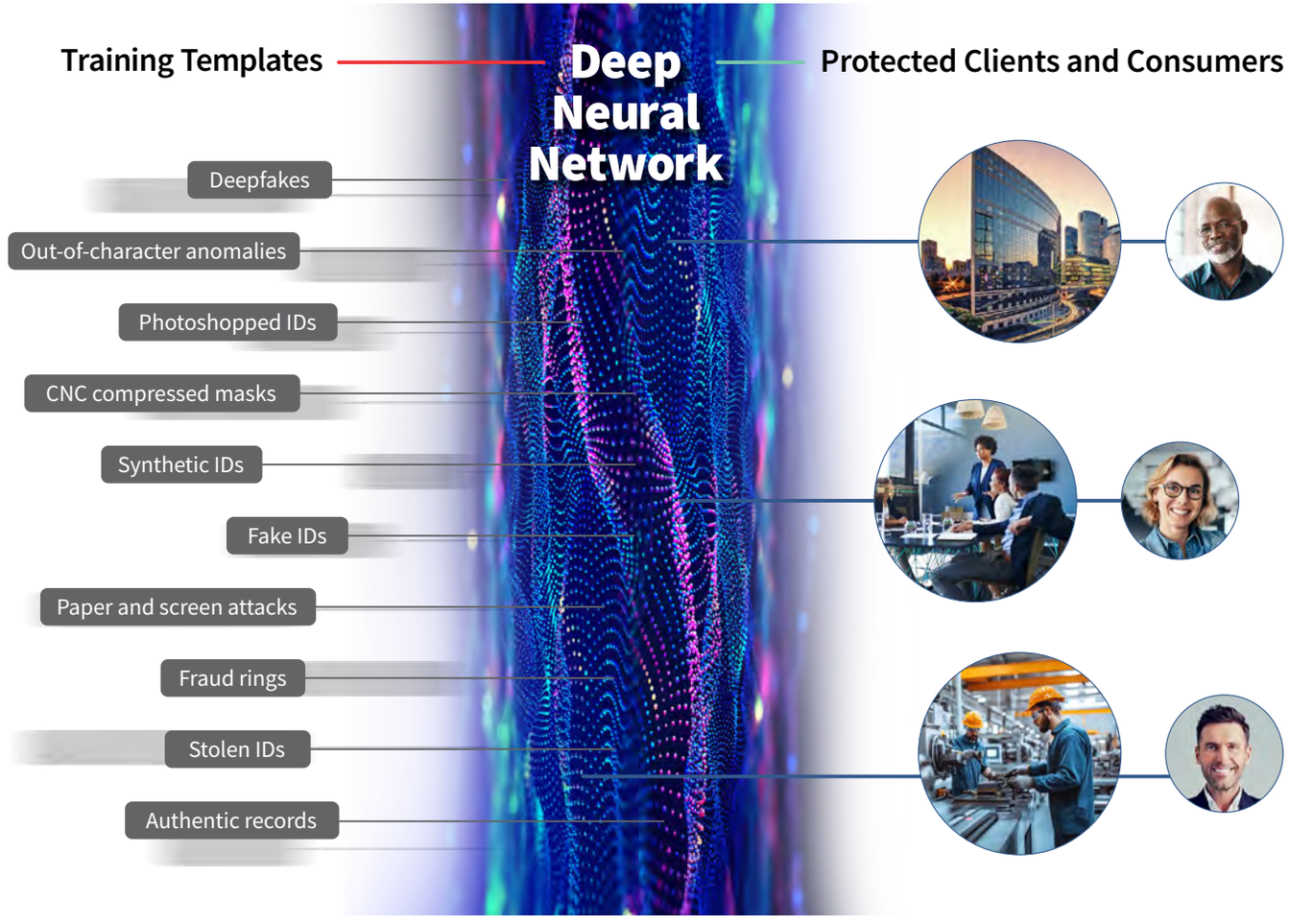
Examples: Identity theft, credential testing, data manipulation

Meanwhile, genuine businesses are leveraging AI to supercharge IDV and fraud detection solutions.

Artificial intelligence is being eagerly put to good use, too. Some identity verification and fraud detection solutions already use AI regularly to improve accuracy and speed. In the realm of fraud detection, LexisNexis® ThreatMetrix® and LexisNexis® Fraud Intelligence have been using AI to deliver more precise risk decisions to customers for decades, and these systems are only getting smarter, evolving every day to stay ahead of increasingly sophisticated threats. Our newest solution, LexisNexis® Emailage® Adaptive, is powered by a fully AI model-based architecture that self-learns to more accurately predict risk based on fraud feedback from an organization's unique environment. Meanwhile, in identity verification, groundbreaking technologies like LexisNexis® IDVerse® are deploying deep, self-learning neural networks that can process powerful algorithms that detect inconsistencies, anomalies, and artifacts of AI-generated fraud too subtle, or in too high volumes, for humans to spot.

The neural network at the core of IDVerse® delivers a major leap forward in both document and biometric liveness authentication. Unlike traditional template-based systems, it uses deep learning to "see" and interpret identity documents holistically, assessing up to 300 elements of patterns, fonts, holograms and security features across a large number of government issued photo IDs worldwide.

HOW DEEP NEURAL NETWORKS IN IDVERSE SPOT SUBTLE FRAUD[82]



This neural architecture learns from new data continuously, enabling the system to adapt to developing fraud techniques including deepfakes, injection and presentation attacks.

Its document-wide and context-aware reasoning allows it to validate whether or not an ID is real, present and unaltered.

The neural network crosschecks the machine-readable zone (MRZ), barcode and front-back alignment for data integrity.

The result is 99.7% language coverage with 99.98% machine-read accuracy across 140+ languages and typesets.

By mirroring human perception at machine speed, the neural networks of IDVerse provide an ever-evolving layer of defence that ensures every verification event is faster, more inclusive and more trustworthy.

CASE STUDY: CHANGING THE FRAUD AND IDENTITY GAME WITH AI

CHALLENGE:

A leading global ecommerce organization needed to improve fraud capture precision for payments across multiple regional markets. Its manual, rule-based fraud controls required frequent updates to keep up with evolving threats.

AI RISK SIGNALS AND INSIGHTS

Thousands of risk signals were analyzed in real time, including:

- **Device, geography and behavioral pattern changes**
- **Suspicious transaction and account activity across multiple markets**

Additionally, feedback loops make the models smarter with each interaction.

HOW WE HELP:

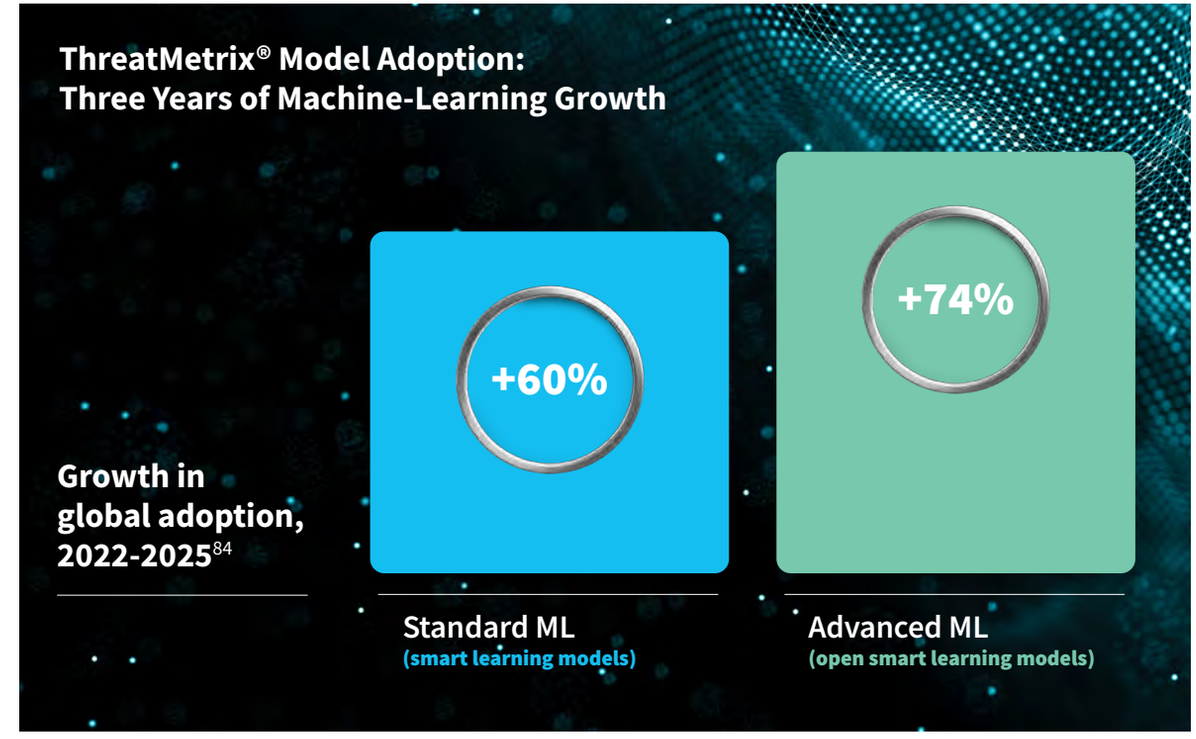
The organization replaced static rules with Emailage® Adaptive, an AI-driven, self-calibrating fraud prevention solution that:

- **Continuously learns from real-time transaction and fraud feedback data**
- **Builds customer-specific models that adjust automatically to new behaviors and risk signals**
- **Reduces manual intervention and streamlines decision-making through API integration with the LexisNexis® Dynamic Decision Platform**

RESULTS:

- **2x More Fraud Detected in High-Risk Bands.** The organization captured twice as much fraud in the highest risk bands, proactively blocking fraudulent transactions without impacting operational speed or accuracy.
- **83% Fewer Transactions in Low-Risk Bands Sent for Manual Review.** By allowing more legitimate customers to transact without unnecessary delay, the model reduced friction and improved revenue flow.
- **1.7x More Auto-Rejected Orders in High-Risk Bands.** Automated decisioning reduced manual intervention and improved operational efficiency by eliminating the need for ongoing rule calibration.

Responsible AI enables fraud teams to act faster and smarter, blocking more fraud, reducing friction for legitimate customers and unlocking lost revenue.[83]



"For any clever new anti-fraud idea we have in real-time, it could take additional time to implement because of regulations, company policies and other well-meaning checks and balances. Meanwhile, a fraudster wakes up in the morning with a new evil plan, and 10 minutes later they're testing it."

Dr. Jeffrey Feinstein, vice president of global advanced analytics strategy, LexisNexis® Risk Solutions

Is The AI Battle Fair? Testing the Advantage of Scale

Good and bad actors are both taking advantage of AI's transformative power. It's an arms race, but the threat lies in the fact that the two sides are playing by different rules. Legitimate organizations strive to use new technologies responsibly and to obey industry and governmental regulations. Fraudsters and scammers face no such constraints and their unfettered use of AI tools conveys an advantage.

But legitimate businesses have an advantage as well: They can scale the challenge. In the case study of a large bank referenced earlier, where our customer prevented £500k of social engineering scams in twenty days,[85] the result was achieved by combining global, crowd-sourced entity intelligence from the LexisNexis® Digital Identity Network® with a range of other fraud signals and device intelligence that built a more complete picture of each customer.

One example, active call detection, determines whether a customer is on a live call on their mobile device at the same time that a transaction is taking place (a common factor linked to APP scams).

Another, remote desktop functionality, can detect if a customer's device is being controlled by remote access software. In isolation this could simply mean that the individual is having their computer fixed by an engineer remotely, but combined with a situation where they are making an ecommerce purchase (combined with other risk factors) could strongly indicate social engineering is taking place.

The team at LexisNexis® Risk Solutions, to bring these disparate insights together into actionable insights, built an advanced machine learning model capable of analyzing the data quickly so as to not interrupt the customer journey. The models draw on past instances of confirmed fraudulent behaviour to produce an output in near real-time that can confidently predict when a scam is underway.

Fraud schemes can grow more complex in response to companies shoring up their defenses, and the power of AI is helping scammers pull off some well-executed deepfakes. But if a successful fraud means the criminals also have to spoof device, location, behavioral clues and dozens or hundreds of other contextual clues being checked by a superior anti-fraud solution, this makes each fraud harder, riskier and less profitable.

The Spread of Agentic AI is Adding Next-Level Complication

Agentic AI promises a new world of consumer convenience: Where a digital assistant can only show you flights to Sydney, a digital agent can actually book and buy the tickets. But to execute tasks like these, agents will need to be empowered with customers' authentication credentials and access to their bank accounts or credit cards, presenting new privacy, security and regulatory challenges.

Fully 88% of senior executives plan to increase AI-related budgets in the next 12 months because of agentic AI specifically.[86] As these nonhuman, but benign bots enter the global transaction stream, it's likely to be a bumpy ride.

One challenge is repeatability: When an AI agent gives different responses in separate instances to the same user, how should that be handled? Other challenges include uptake (will people really let bots control their financial accounts?) and legal and regulatory issues. One report estimates we'll trust future AI agents to make 15% of day-to-day work decisions by 2028. But for today, agentic ability is limited to specific areas and levels of difficulty. (In a test, the top-performing AI agent could only autonomously perform about 30% of its software development tasks to completion.)[87]

For legitimate organizations, responsible, carefully-deployed agentic AI could help automate complex business tasks like sourcing backup for identity proofs in real-time. But the powerful technology could also play a critical role in helping fraudsters scale their attacks, and could complicate anti-fraud algorithms. Passing a digital test to prove you're human will have less anti-fraud value in a world where non-human identities are performing authorized digital errands for legitimate users.

Imagine, for example, a shopping bot you could deploy on an online marketplace to buy the shoes you want if the price drops below a certain point. How does the marketplace know whether this is a legitimate request, or just a bot created to steal shoes? And if the marketplace allows an exclusion for this sort of bot, then fraudsters will quickly find ways to simulate that interaction and take advantage.

HOW "GOOD AI" AND "BAD AI" ENGAGE AND ADAPT

As each side fights for advantage, artificial intelligence is driving a kind of co-evolution.

Step 1: Easy identity spoofing	Step 2: Knowledge-based exploits	Step 3: Synthetic identity building	Step 4: Agentic AI shopping/bots	Step 5: Scale challenge
BAD AI can create a new email address, using stolen data, as a place to initiate new fraud from.	**BAD AI** can efficiently mine social media or the dark web for knowledge-based answers.	**BAD AI** can be used to log into a credit bureau and assemble a synthetic profile.	**BAD AI** can deploy an AI 'agent' to fraudulently transact or shop at scale.	**BAD AI** can test new fraud ideas instantly, without waiting for approval.
GOOD AI can defeat this by performing basic checks like email risk signals and device fingerprinting.	**GOOD AI** can perform layered data checks and behavioral intelligence for more definitive ID verification.	**GOOD AI** can provide cross-source verification (credit + digital + behavioral + email).	**GOOD AI** can employ behavioral intelligence to reliably identify malicious non-human actors.	**GOOD AI** can perform regulatory checks even against fast moving attackers.

Responsible AI Remains a Critical Discipline

AI is developing at breakneck speed, and the risks to business are top of mind right now. A recent report surveyed how the largest public companies in the U.S. described AI risks in public filings between 2023 and 2025. Leaders from firms adopting the technology said they faced "regulatory scrutiny over data and fairness, operational risks from automation and reputational exposure in consumer markets." They expected to be challenged to come up with greater controls and vendor oversight as the technology developed.

As AI usage and adoption expands, it's introducing new risks. In the same survey, respondents from nearly three out of four S&P 500 companies (72%) disclosed at least one material AI risk in 2025. Two years earlier, in 2023, just 12% of respondents noted material AI risks, a sizeable jump.[88]

Agentic AI could be responsibly leveraged by legitimate organizations to operate on proprietary datasets. An organization could use AI to summarize reports on a group of individuals, successfully reducing the work for human teams without exposing the company's data to the internet at large.

AI has enormous potential to cause harm, even in the hands of legitimate organizations, and LexisNexis® Risk Solutions have made a long-term commitment to responsible AI, consisting of five pillars:

Consider the real-world impact of our solutions

Take action to avoid creating or reinforcing unfair bias

Explain how our solutions work

Create accountability through human oversight

Respect privacy and champion robust data governance

As AI tools continue to progress at breakneck speeds, it's becoming imperative that we all take proactive, collaborative steps to protect governments, businesses and ordinary people by making sure that we engage only in responsible AI development that balances progress with safety. These guardrails represent reasonable caution that can be enforced by smart regulations, transparent reporting, traceability and accountability for decisions.

Data Collaboration Goes Global

Collaboration Among Companies Is Transforming Their Ability To Detect Risk With Agility

Many organizations are beginning to boldly share data and insights with one another in the face of rising risk.

Criminals have long profited from collaboration on a local, regional, and global scale, through tactics like:

- **Building highly professional crime organizations, like scam centers that operate openly**
- **Trafficking data leaks and expertise openly on the dark web**
- **Moving stolen funds through vast international mule networks until they're functionally untraceable**

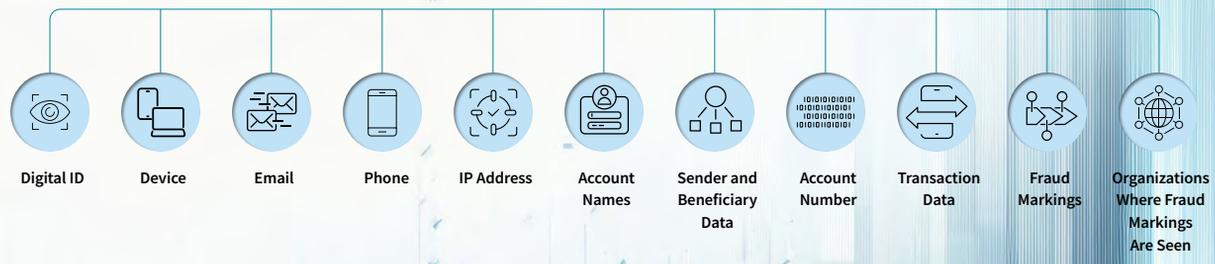
But genuine organizations can gain advantages from working together too. Around the world, organizations are rallying to find ways to safely collaborate within the boundaries of business and regulation. Sharing trusted data with a trusted network of partners gives organizations instant, accurate visibility into the identity of the people they transact with in digital channels. Through collaboration, similarly targeted businesses can turn scale into a powerful advantage and create a unified front against global fraud. For example, sharing fraud insights can help businesses thwart coordinated efforts by criminals to test stolen identity credentials in one industry for weaponization in another.

The way forward is clear. Businesses that bridge gaps and share risk intelligence are most likely to detect risk earlier, respond faster and keep customers safer. Together, we see more, we know more and we can act faster. By securely sharing insights with trusted, industry-leading partners through a shared agreement, organizations can work together to detect shared threats sooner, respond faster and build more resilient defenses around the world.

STEP ONE:

Consortium members each contribute data.

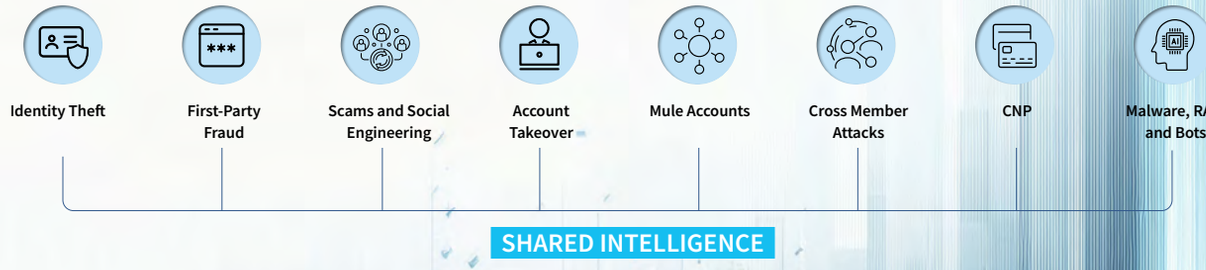
Examples of contributory data shared amongst consortium members can include:



STEP TWO:

This helps identify and prevent a variety of frauds.

Through real-time data sharing and advanced detection capabilities, a wide range of fraud types can be identified and prevented.



STEP THREE:

Leveraging local insights informs a comprehensive global database.

These critical local insights join consortium intelligence, which in turn informs global intelligence that strengthens fraud protection for all collaborators.

THE INGREDIENTS FOR SUCCESSFUL COLLABORATION

A wide variety of data around each interaction, including device fingerprinting, IP addresses, behavioral intelligence, histories and connections all play a role. These multi-faceted risk indicators create a level of detail fine enough to help distinguish between legitimate customers and clever impersonators.

A standardized approach. Recognizing patterns for different types of fraud may vary by each organization's risk appetite and policies. A more consistent strategy allows each member to collectively detect the same types of fraud and attack them with the right tools.

Real-time insight sharing. This enables immediate action. When risky attributes detected at one institution reappear elsewhere, members should be alerted instantly to close gaps and stop fraud before it spreads.

Non-negotiable trust and autonomy. Each member should control how and when data is shared, with agreement by the other members. Clear rules on responsibilities, privacy, compliance and legal protections will help ensure collaboration strengthens defenses without compromising their legitimate competitive interests.

Seamless integration and ease of use. Solutions built for simplicity and interoperability can ensure data flows easily between systems and integrates smoothly into current processes via one consolidated platform.

Ongoing collaboration. Companies must work hand in hand to share local threats and industry challenges to spark innovation and establish strong, forward-thinking solutions that truly reflect the risk assessment needs of the region and industry.

Strength in Numbers: Consortiums are Forming Across Industries and Regions Worldwide

Consortiums, industry collaborations and similar fraud-insight sharing arrangements are springing up all over the world. Some are large organizations spanning multiple nations, like Europol's Global Coalition to Fight Financial Crime. Others have a tighter industry focus, like the Tech Against Scams Coalition of prominent cryptocurrency companies.[90] Still others combine public and government initiatives with private entities into interesting partnerships.

New fraud-prevention regulations in Latin America, like Brazil's Resolução BCB 501 / 498 for PSTIs, Mexico's CoDi framework and Colombia's Bre-B instant-payment initiative, show how regulators are increasing pressure on banks to strengthen onboarding and synthetic-fraud controls.[91]

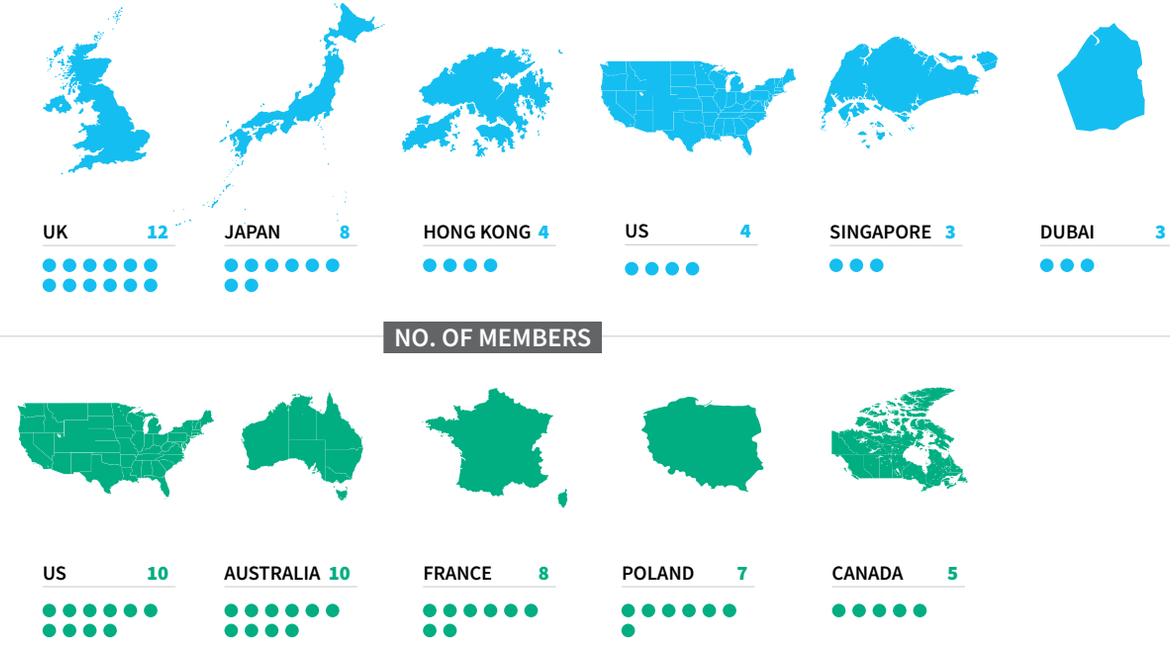
The region's financial inclusion and in-stant-payment adoption (e.g., PIX in Brazil, with more than 170 million users) have boosted onboarding volumes, creating both opportunity and exposure.[92]

However, LATAM still faces high rates of first-party ("contas laranja") and mule account fraud, often intertwined with social-engineering scams. Many local institutions lack mature consortium data-sharing and real-time behavioral models.

LexisNexis® Risk Intelligence Network is a global solution that provides regional data coverage for our LATAM customers.

REGIONAL COLLABORATION CAN TAKE MANY FORMS

As seen in the examples below from the LexisNexis® Risk Intelligence Consortium,[93] members are choosing to work together more closely and share risk intelligence, either in formal consortiums (top row) or through discussion and sharing of best fraud-fighting practices without a direct consortium agreement (bottom row).



UK Banking: The Frontrunners, With Proven Collaboration Success

One of the first dedicated digital consortiums, the LexisNexis Risk Intelligence Consortium - UK Banking unites more than ten trusted UK financial institutions, who have been working together to share risk intelligence and enhance consumer protection for more than seven years.

From the outset, members recognized the value of data sharing and supported a consortium led by LexisNexis® Risk Solutions, a trusted third-party facilitator operating under agreed-upon rules and clear definitions of what constitutes fraud or a risky device. This foundation paved the way for measurable success, demonstrating how collaboration can significantly reduce fraud and strengthen an industry's defenses through strength in numbers.

HOW INTELLIGENCE SHARING HELPS ONE JAPANESE COMPANY

A Tokyo-founded company manufactures products and also provides digital services, including providing access control server (ACS) services to issuing banks in Japan. Leveraging LexisNexis® ThreatMetrix®, this company helps banks share transaction data like user devices, current and historic behavior and other details across 3DS secure journeys, to help reduce credit card fraud for Japanese merchants. The arrangement allows the company to fine-tune its rules, flagging high-risk transactions in real-time as customers proceed through the site, and the company saves several million yen every month by blocking scams.[95]

"[The] consortium has been a game-changer for us. We are able to share what we are seeing with peers in our network, allowing us to collaborate and identify common fraud attributes and emerging attack vectors."

THE WORLD'S FIRST TELECOM FRAUD CONSORTIUM

CHALLENGE:

Telco providers are high-value targets for networked fraud attacks. Fraudsters blocked by one operator often simply pivot to the next and try again. Tactics include phishing, manipulated documentation, deepfakes and synthetic identities.

Switzerland's largest telecom operators, working hand in hand with LexisNexis® Risk Solutions, created the Swiss Telco Consortium, a responsible data-sharing framework designed to facilitate an exchange of real-time fraud intelligence.

Risk signals that the Swiss Telco Consortium's member organizations watched for and reported back to the consortium included:

- People who had been involved in fraud before (identified through digital identity and behavioral intelligence)
- Identities displaying the attributes of synthetic identities
- Devices, email addresses, IPs and phone numbers believed to be risky

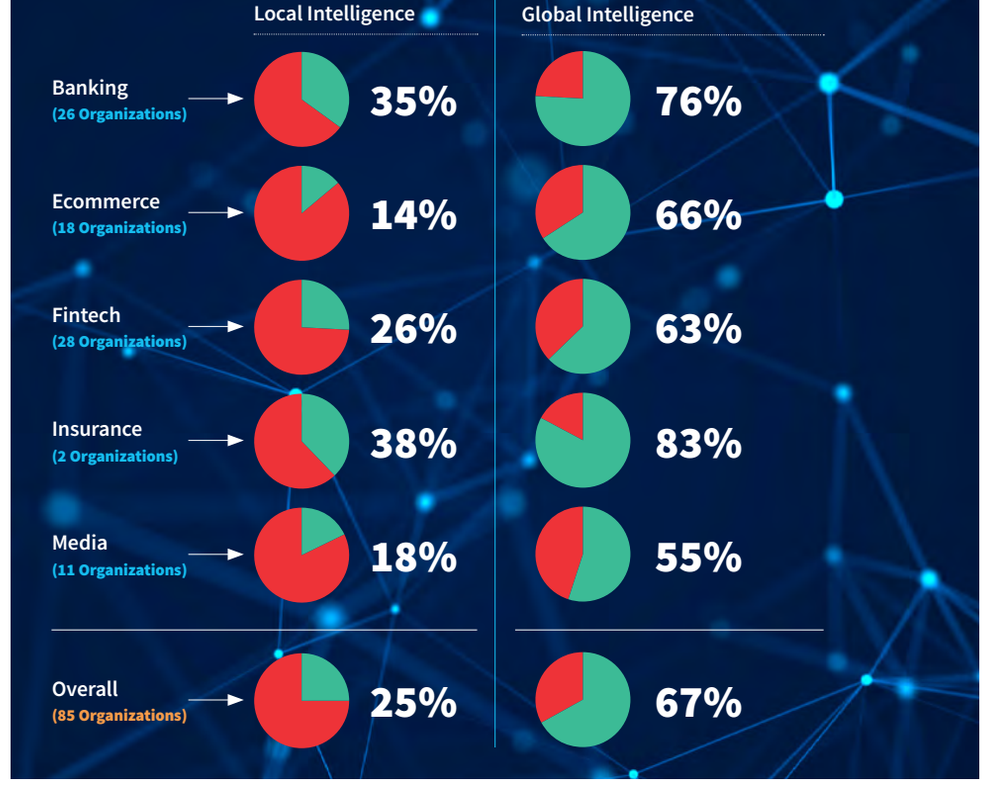
RESULTS:

The Consortium's members now successfully share real-time intelligence to fight their common fraud threats, in a great example of agile, effective and efficient cross-industry collaboration. The system responds to high-risk signals before a fraud attempt hits, maintaining a responsive defense that helps keep member organizations safe from opportunistic fraudsters. Results to date include:[96]

- **4,000+** high-risk data attributes identified
- **150%** increase in fraudulent transaction detection
- **Almost 100%** confidence rating achieved in consortium fraud alerts

Digital Identity Recognition is Dramatically Enhanced By Global Intelligence

At digital new account openings across industries, digital identity recognition rate improves from 25% to 67% when companies join forces through the Digital Identity Network. This data collaboration doubles the recognition rate for banking, insurance and fintech, triples it for media and quadruples it for ecommerce.[97]



THE FUTURE OF FRAUD COLLABORATION: CROSS-INDUSTRY & PRIVATE-PUBLIC PARTNERSHIPS

Banks and telecommunication providers collaborating with like-minded companies inside their own industry is just the beginning. Innovative companies are stepping across industry lines to join forces with law enforcement, government and public-private initiatives to expand the boundaries of how industry intelligence can be enhanced when combined with other types of institutions. Examples:

- **The Hong Kong Monetary Authority strengthens a number of anti-fraud data sharing initiatives like the Fraud and Money Laundering Intelligence Taskforce (FMLIT), which enables local banks and the police department to share resources and work together to solve financial fraud.[98]**

- **LexisNexis® Risk Solutions is working alongside consortium members and third-party organizations to share digital identity data linked to confirmed money mule accounts. This collaboration aims to exchange mule network intelligence across organizations, provide key data to law enforcement for investigations and partner with social media platforms to help identify mule herders posting recruitment content.[99]**

Collaborating across industries brings a new set of tactics and weapons to meet the ever-evolving challenge of fraud, and these and other innovative cross-industry partnerships hold the promise of keeping fraudsters on the run for years to come.

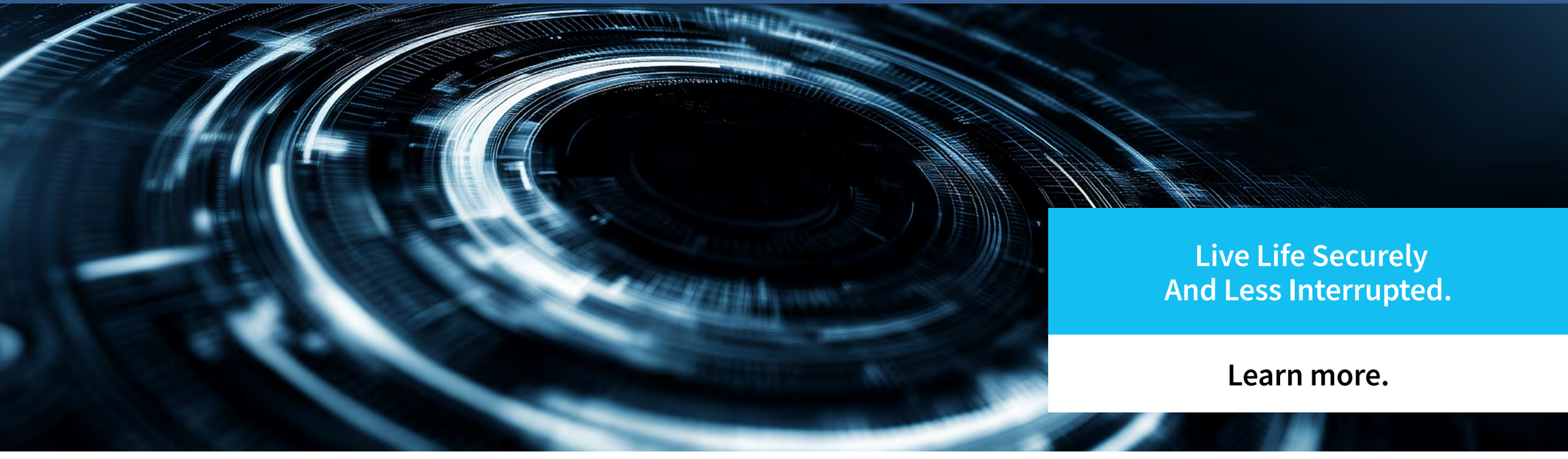
Conclusion: Trust Is On The Move

The landscape is changing fast, raising a new set of leading questions.

- Will digital IDs and ever faster payments bring about a new age of accessibility?
- Can agentic AI help fraudsters scale their attacks, or will “good AI” win out?
- What effect will new regulations have on helping us thwart criminal operations?

Criminal enterprises run vast networks of mules, have a robust supply chain and are expanding their use of AI. As financial services, retailers and other businesses have tightened controls to thwart third-party fraud, first-party fraud has taken the lead. Identity grows ever more complex to assess, and it can seem sometimes like trust itself is on the run.

But legitimate businesses aren’t standing still. They’re leaning fully into identity’s new complexity, enabling faster and more democratic payment systems, even while firming up their identity verification processes to deny fraudsters easy wins. They’re collaborating on data and insights and using AI fearlessly but responsibly to harden their defenses. And they’re leveraging ever more powerful solutions to build a safer, brighter future for all.



LexisNexis®
RISK SOLUTIONS

Recognized Around the World for Award-Winning Technology

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries 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 www.risk.lexisnexis.com and www.relx.com.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis® Risk Solutions products identified. LexisNexis Risk Solutions does not warrant this document is complete or error-free. If written by a third-party, the opinions may not represent the opinions of LexisNexis Risk Solutions. The opinions expressed within the case studies referenced above represent customer opinions. LexisNexis Risk Solutions believes the case study experiences generally represent the experiences found with other similar customer situations. However, each customer will have its own subjective goals and requirements and will subscribe to different combinations of LexisNexis Risk Solutions services to suit those specific goals and requirements. These case studies may not be deemed to create any warranty or representation that any other customer's experience will be the same as the experience identified herein.

SOURCES

1. LexisNexis® Risk Solutions Cybercrime Report, 2025
2. LexisNexis® Risk Solutions Cybercrime Report, 2025
3. From LexisNexis® Risk Solutions internal data
4. "Unmask Deepfakes and Forged Documents with the Power of AI," LexisNexis® Risk Solutions, 2025
5. "The Success Multiplier: How Collaborative Data Makes or Breaks Trust and Drives Sustainable Growth," LexisNexis® Risk Solutions
6. LexisNexis® True Cost of Fraud™ Study 2025 North America
7. LexisNexis® Risk Solutions Cybercrime Report, 2025
8. "When Customers Become Fraudsters: The Hidden Cost of First-Party Fraud," Datos Insights
9. LexisNexis® Risk Solutions Cybercrime Report, 2025
10. "2024 Consumer Returns in the Retail Industry Report," Appriss Retail
11. "When Customers Become Fraudsters: The Hidden Cost of First-Party Fraud," Datos Insights
12. "Viral Fraud: Risks, Signals, and Solutions," LexisNexis® Risk Solutions
13. "When Customers Become Fraudsters: The Hidden Cost of First-Party Fraud," Datos Insights
14. From LexisNexis® Risk Solutions internal data
15. Definitional elements from Brittanica.com/technology/dark-web
16. EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025
17. LexisNexis® Risk Solutions Fraud on the Dark Web research
18. LexisNexis® Risk Solutions Fraud on the Dark Web research
19. LexisNexis® Risk Solutions Cybercrime Report, 2025
20. "AI helps Telegram remove 15 million suspect groups and channels in 2024," TechCrunch
21. LexisNexis Risk® Solutions Cybercrime Report, 2025
22. LexisNexis Risk® Solutions Cybercrime Report, 2025
23. LexisNexis Risk® Solutions Cybercrime Report, 2025
24. "When Customers Become Fraudsters: The Hidden Cost of First-Party Fraud," Datos Insights
25. "Almost One-Third of Young Adults Approached to Become Money Mules," The Irish Times
26. "Mule Operators in META Adopt Advanced Fraud Schemes," Infosecurity Magazine
27. From LexisNexis® Risk Solutions internal data
28. "U.S. Law Enforcement Takes Action Against More Than 3,000 Money Mules in Initiative to Disrupt Transnational Fraud Schemes," United States Department of Justice website
29. "Hong Kong Police Crush HK$118M Crypto Laundering Ring, 500 Mule Accounts," FinTech News
30. "AUSTRAC Cracks Down on Cryptolink for Late Reporting," Australian Government's AUSTRAC Online site
31. "Regulator Axed as Red Tape is Slashed to Boost Growth," Gov.UK website
32. "HKAB and HKMA Join Hands to Launch the Anti-Scam Consumer Protection Charter," Hong Kong Association of Banks press release
33. From LexisNexis® Risk Solutions internal data
34. LexisNexis® Risk Solutions Cybercrime Report, 2025
35. LexisNexis® Risk Solutions Cybercrime Report, 2025
36. LexisNexis® Risk Solutions Cybercrime Report, 2025
37. "Using Biometrics to Fight Back Against Rising Synthetic Identity Fraud," Deloitte Insights
38. "FINCEN Permits Banks To Use Alternative Collection Method For Obtaining TIN Information," FINCEN.gov
39. "Online Age Verification: Global Regulations and What's Next," LexisNexis® Risk Solutions
40. "Online Age Verification: Global Regulations and What's Next," LexisNexis® Risk Solutions
41. From LexisNexis® Risk Solutions internal data
42. "The Proliferation of Digital Credentials," Risk Ready Fall 2025 Summit, New York
43. "Digital Identity for All Europeans: A Personal Digital Wallet for EU Citizens, Businesses, and Residents," European Commission website
44. "Real ID Mobile Driver's Licenses (mDLs)" FAQ page, TSA.gov
45. "5 Payments Trends to Watch in 2025," LexisNexis® Risk Solutions
46. "5 Payments Trends to Watch in 2025," LexisNexis® Risk Solutions
47. "5 Payments Trends to Watch in 2025," LexisNexis® Risk Solutions
48. "China Payments & Ecommerce Market Report 2025 - WeChat Pay and Alipay Extend Their Reach Across 20+ Countries," GlobeNewswire, June 24, 2025
49. "PIX Statistics," Banco Central Do Brasil
50. "Bre-B is Live in Colombia, and EBANX Merchants are Enabled From Today," LinkedIn announcement from EBanx CEO João Del Valle
51. "Real-Time Digital Payments: The CoDi Case In Mexico," Mexico Business News
52. "Embedded Finance and the Rise of the Super-App," FTT Embedded Finance blog
53. "India's Digital Payments Revolution is Inspiring, Both for Developing Nations and Cyberscammers," Tech Monitor
54. "Facial Recognition and the Two Expos in Osaka," LSE International History
55. "Cross-Border Payment Linkages," Monetary Authority of Singapore website
56. "Payments Statistics: First Half of 2024," European Central Bank website
57. European Central Bank website, Single Euro Payments Area (SEPA) page
58. European Central Bank website, Digital Euro page
59. European Central Bank website, Single Euro Payments Area (SEPA) page
60. "Faster Payment System," wearepay.uk website
61. FedNow FAQs page, U.S. Federal Reserve website
62. "58% of U.S. Banks Use Both RTP and FedNow for Instant Payments," PYMNTS, June 27, 2025
63. "Canada's Real-Time Rail: Collaborating For the Benefit of the Payment Ecosystem," Payments Canada

SOURCES

64. "Fraud Concerns May Be Slowing Real-Time Payments Adoption in the UK," Payments Journal, Mar. 28, 2025
65. "Brazil's Kidnappers Turn to Flash Kidnapping As They Take Advantage of New Tech," Financial Times
66. "Combating Payments Fraud in India's Digital Payments Landscape," PwC, April 2025
67. FBI Internet Crime Report, 2024
68. From LexisNexis® Risk Solutions internal data
69. From LexisNexis® Risk Solutions internal data
70. From LexisNexis® Risk Solutions internal data
71. From LexisNexis® Risk Solutions internal data
72. From LexisNexis® Risk Solutions internal data
73. From LexisNexis® Risk Solutions internal data
74. From LexisNexis® Risk Solutions internal data
75. "How AI Can Unlock New Possibilities for Global Productivity and Sustainability," WEF, January 3, 2025
76. "How Afraid of the A.I. Apocalypse Should We Be?" The New York Times, October 15, 2025
77. "Unmask Deepfakes and Forged Documents with the Power of AI," LexisNexis® Risk Solutions, 2025
78. "Unmask Deepfakes and Forged Documents with the Power of AI," LexisNexis® Risk Solutions, 2025
79. "Unmask Deepfakes and Forged Documents with the Power of AI," LexisNexis® Risk Solutions, 2025
80. "Unmask Deepfakes and Forged Documents with the Power of AI," LexisNexis® Risk Solutions, 2025
81. LinkedIn post by Isabel Davila, delegate of the Civil Police of the Federal District, 2024
82. "Unmask Deepfakes and Forged Documents with the Power of AI," LexisNexis® Risk Solutions, 2025
83. From LexisNexis® Risk Solutions internal data
84. From LexisNexis® Risk Solutions internal data
85. From LexisNexis® Risk Solutions internal data
86. PwC's AI Agent Survey, PricewaterhouseCoopers, May, 2025
87. "Science & Tech Spotlight: AI Agents," U.S. Government Accountability Office, September 10, 2025
88. "AI Risk Disclosures in the S&P 500: Reputation, Cybersecurity, and Regulation," Harvard Law School Forum On Corporate Governance, October 15, 2025
89. "The Success Multiplier: How Collaborative Data Makes or Breaks Trust and Drives Sustainable Growth," LexisNexis® Risk Solutions
90. "Announcing the Tech Against Scams Coalition," Coinbase.com
91. From LexisNexis® Risk Solutions internal data
92. "Pix: the Latest Updates on Brazil's Leading Instant Payments Scheme," European Payments Council
93. LexisNexis® Risk Solutions Cybercrime Report, 2025
94. LexisNexis® Risk Intelligence Consortium - UK Banking from Jan – Sep 2025
95. "LexisNexis® ThreatMetrix® Helps Dai Nippon Printing Secure Card-Not-Present Payments, Reducing Fraud Losses in the 3-D Secure (3DS) Transaction Authentication Workflow," LexisNexis® Risk Solutions, 2025
96. From LexisNexis® Risk Solutions internal data
97. From LexisNexis® Risk Solutions internal data
98. "How Banks Can Contribute More to the Fight Against Fraud and Money Laundering," Hong Kong Monetary Authority
99. "Not All Mules Are Born Equal," LexisNexis® Risk Solutions