LexisNexis®
RISK SOLUTIONS

Beyond One-Size-Fits-All:

Tackling the Full Spectrum of Identity Fraud

And Why One Approach Won't Stop Them All

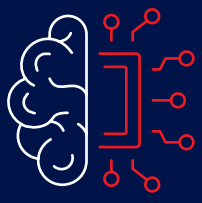
LexisNexis®
RISK SOLUTIONS

Contents

LexisNexis®
RISK SOLUTIONS

Introduction

Fraud today is far more complex than fabricating identities using fictitious personally identifiable information (PII) or stealing PII through data breaches and dark web marketplaces. These tactics represent just one facet of a rapidly evolving threat landscape. Fraudsters are increasingly leveraging a sophisticated arsenal of tools, including automation and artificial intelligence, to orchestrate multi-layered attacks. Deepfakes, synthetic identities and AI-driven impersonation techniques are becoming more prevalent, making detection and prevention significantly more challenging.



61% of financial institutions rank generative AI-driven fraud among their top three challenges in the digital customer journey[1]

First and third-party fraud account for a staggering 63% of challenges reported by organizations[2]

Fraud losses enabled by generative AI are expected to reach $40 billion by 2027[3]

At the same time, longstanding fraud tactics such as first-party fraud and conventional identity theft remain persistent threats, compounding the complexity of today's fraud landscape.

A typical fraud scheme often involves multiple coordinated components, requiring a layered defense strategy that can adapt to emerging threats. This includes not only reactive measures but also proactive capabilities that anticipate and neutralize fraud before it escalates. To stay ahead, organizations should continuously evolve their fraud detection frameworks by integrating adaptive modeling, behavioral analytics and long-term data insights to identify patterns and prove value over time.

While the fraud taxonomy encompasses myriad fraud types across the customer lifecycle, **this white paper zeroes in on one of the most pressing and complex areas: the emerging challenges of identity fraud during new application and onboarding stages.**

LexisNexis®
RISK SOLUTIONS

Understanding Types of Identity Fraud

Understanding the different types and patterns of fraud is the essential starting point for building an effective defense against fraudulent activity.

> Identity fraud is not a singular phenomenon; it spans a diverse landscape of behaviors, from impersonation and identity fabrication to misuse of one's own credentials.

By identifying how fraud manifests, organizations can tailor their detection strategies with greater precision.

Fraud typologies

Identity Misuse

Identity misuse, also known as first-party fraud, occurs when an individual uses their real identity but misrepresents PII to gain access to services. For example, a consumer applies for multiple accounts, makes a few initial payments to build trust then defaults on all. This "bust-out" strategy is often difficult to detect using traditional fraud models.

Indicators of Identity Misuse Include:

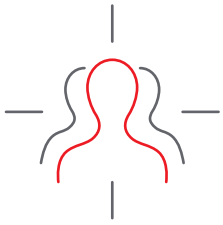
- **Consistent Identities with Some Variation:** Typically use real identities with minor inconsistencies across PII elements.
- **Velocity, Velocity, Velocity:** High application velocity or many inquiries spanning lending products. This behavior is often observed across industries and is a strong signal of likelihood to defraud.
- **High PII Tumbling:** Frequent reuse and recombination of identity elements across applications.
- **Established History:** Often have an established identity across trusted, credentialed sources. This makes them appear trustworthy at first glance, which is why behavioral analytics are critical.

Third-Party Fraud

Third-party fraud occurs when a fraudster uses someone else's identity, typically stolen or compromised, to commit fraud without the knowledge or consent of the actual person. Fraudsters purchase full identity kits (name, SSN, DOB, address) from dark web marketplaces and use them to open fraudulent accounts. Using stolen identity data, a fraudster applies for credit cards or loans. The victim is unaware until they see inquiries or defaults on their credit report.

Indicators of Third-Party Fraud Include:

- **Use of Unaltered Core PII:** Leverage authentic PII from public records or the dark web.
- **Blended Identity Construction:** Pair real identity elements with fraud-controlled contact info (e.g., burner phones or drop addresses).
- **Fraud Ring Association:** Appear in fraud rings with shared device or IP usage.
- **Contact Manipulation:** Change contact info to evade detection.



Synthetic Fraud

Synthetic identities use a combination of fictitious and real data (sometimes merging real elements from multiple people) to create a new identity. For example, a fraudster may use a valid Social Security number from one person, an address from another, and create a digitally-altered deepfake image of a third person's face; then they assemble these elements into a fake identity or form of identification.

They often lack the life-path signals of real individuals, such as legitimate ID documents or familial relationships, and appear isolated in identity networks, with no known associates. When deepfakes are used for fabricated IDs, they often contain subtle, imperceptible signs of manipulation and lack the biometric signals that distinguish a live human being from synthetic media.

Indicators of Synthetic Fraud Include:

- **Contact Field Crowding:** Reused phone numbers and email addresses across multiple synthetic identities.
- **Recent Bureau Existence:** Appear as "new to credit" profiles.
- **AI-Generated Deepfakes and Forged Documents:** Signs of ID tampering, photo manipulation and micro-expressions or inconsistencies that may indicate the absence of genuine human presence.

LexisNexis®
RISK SOLUTIONS

Risk Intelligence Across Physical and Digital Channels

Fraud detection hinges on understanding the full spectrum of identity components that individuals present during interactions. These identities span both physically and digitally and fall under four key categories:

1	2	3	4
WHO YOU ARE	WHAT YOU KNOW	WHAT YOU HAVE	HOW YOU BEHAVE

Who you are encompasses personally identifiable information (PII) such as dates of birth and full names, contact details like addresses, phone numbers and email addresses, biometrics like fingerprint, face, and voice and more. In the real world, official documentation is often used to prove this information, like driver's licenses, passports and birth certificates; online, digital representations of these kinds of identifiers (like mobile driver's licenses) and live selfies are used to verify these inherent traits that represent who you are. (See our whitepaper, The Rising Challenge of Verifying Identity.) As digital interactions become more common, however, these identity elements no longer provide enough assurance of your identity. Each of these data points can be easily stolen, corrupted, and/or fabricated by bad actors in impersonation or synthetic fraud schemes that resist efficient and accurate human verification.

A higher level of assurance requires additional layers of verification through **what you know** (e.g. passwords, PINs, security questions), **what you have** (e.g. a mobile device, hardware token, smart card or authenticator app) and **how you behave** (e.g. typing cadence, mouse movements and navigation patterns). These elements provide a dynamic and contextual view of user behavior, often revealing inconsistencies that static PII data alone cannot capture. Fraud detection depends not only on linking and verifying physical and digital identity elements, but also on how those elements behave over time. Patterns such as frequent changes to contact details, mismatched PII pairings or high application velocity on a single device can signal manipulation or synthetic identity use. A combined strategy that analyzes both the presence and behavioral patterns of many identity components is essential to uncovering today's sophisticated fraud.

LexisNexis®
RISK SOLUTIONS

Distinguishing Between the Types of Identity Fraud

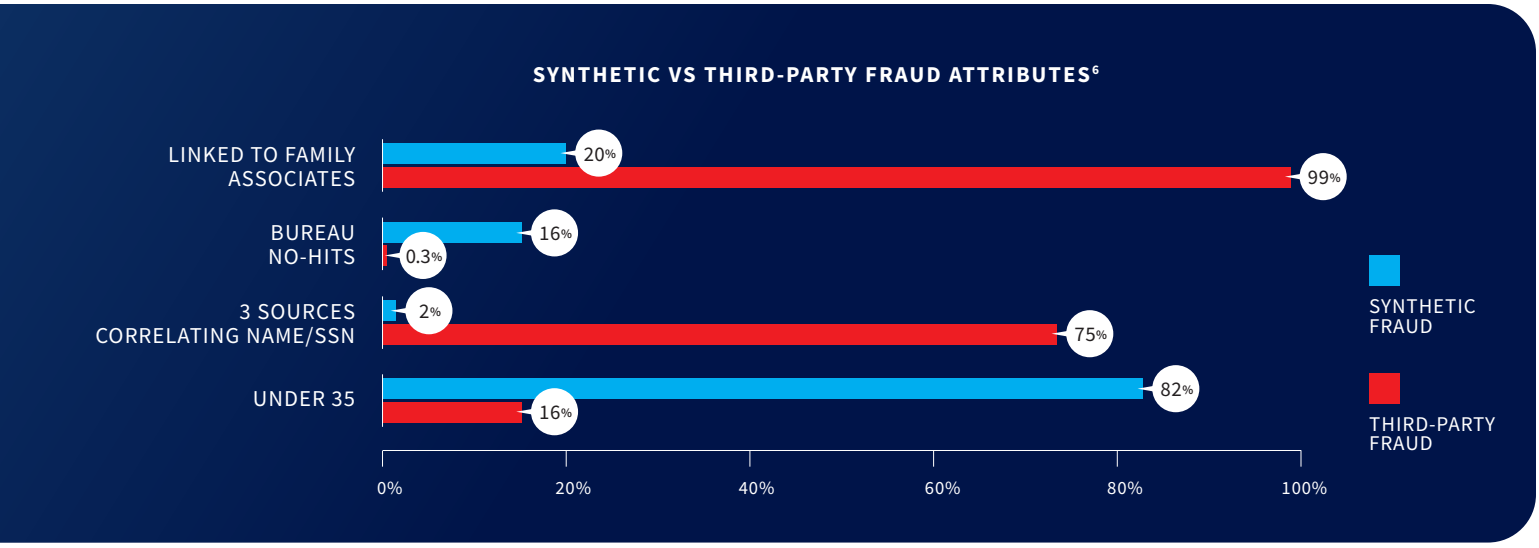
Understanding the different types and patterns of fraud is the essential starting point for building an effective defense against fraudulent activity. Identity fraud is not a singular phenomenon; it spans a diverse landscape of behaviors, from impersonation and identity fabrication to misuse of one's own credentials. By identifying how fraud manifests, organizations can tailor their detection strategies with greater precision.

Identity Misuse vs. Third-Party Fraud

First-party fraudsters tend to show higher application velocity over a longer period, often doubling the rate seen in good applicants. Their identity data is typically consistent, with low variation in core PII elements, and they may go undetected due to the legitimacy of their credentials. In contrast, third-party fraudsters display short bursts of intense activity, with 1.4× more variation in core PII and a higher likelihood of mismatched or inconsistent identity elements[4]. These differences are critical to the decoupling approach, which uses identity confidence, velocity, recency and PII tumbling to distinguish fraud types and apply targeted mitigation strategies.

Third-Party Fraud vs. Synthetic Fraud

Synthetic fraud typically involves fabricated identities that appear young (82% are under 35), lack strong data corroboration (only 2% have name/SSN matches across three sources) and are often absent from credit bureau records (15.7% have no bureau hits). They also show limited social connections, with only 20% linked to family or associates. In contrast, third-party fraud involves stolen identities that are well-established. Nearly all are linked to known associates (99.1%), have strong data matches (74.9%) and are present in credit records (only 0.3% are bureau no-hits).[5] These differences make synthetic fraud harder to detect using traditional fraud models.



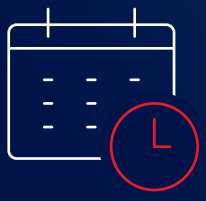
LexisNexis®
RISK SOLUTIONS

Decoupling Fraud Signals for More Clarity

Traditional fraud detection strategies leave many fraud events undetected, which limits companies' ability to mount a comprehensive defense. Decoupling is a strategic approach that addresses this challenge directly, classifying risk by analyzing behavioral and identity patterns across four key dimensions: Identity Confidence, Application Velocity, Application Recency and PII Tumbling. These dimensions help distinguish between fraud types by asking:

Do the identity elements reliably belong together?

How frequently is this identity applying for accounts across institutions?



How recently has this identity been active?

Are there identity elements being reused in suspicious patterns?

By decoupling these signals, organizations can enable more precise fraud profiling and differentiated treatment strategies, improving both detection and operational efficiency.

This layered framework enables organizations to move beyond binary identity verification and into dynamic fraud intelligence—**leveraging responsible AI, behavioral analytics and cross-channel signal correlation to expose fraud that would otherwise remain hidden.**

Proven Results in Practice

Case study

LexisNexis® Risk Solutions conducted a cross-industry study evaluating fraud scoring solutions optimized for specific fraud types across various lenders and sectors. The findings revealed that fraud in new credit applications is highly varied, with no single score performing best across all cases. This underscores the need to align strategies with unique fraud typologies affecting each portfolio to maximize detection and efficiency.

To evaluate the impact of targeted fraud strategies, we analyzed three application populations (each dominated by a distinct fraud type: synthetic, identity misuse or third-party). Using five purpose-built scoring solutions, we measured performance using Fraud Detection Rate at a 3% Depth of File (FDR3), a key metric for balancing fraud capture with operational efficiency. Each fraud type responded best to its corresponding optimized score. For instance, in one lender's portfolio, the third-party fraud score achieved an FDR3 of 42%, nearly double the average of other scores. **This highlights a critical insight: Fraud is not monolithic, and generic models risk missing significant exposure.**

These findings reinforce the value of a multi-score strategy tailored to the specific fraud vectors within each portfolio. Institutions that align detection tools with fraud typologies are better equipped to reduce losses and stay ahead of evolving threats.

PERFORMANCE ACROSS FRAUD TYPES[7]

Fraud Type	Third-Party Fraud	Synthetic	Identity Misuse
INDUSTRY	Retail	Credit Card	Credit Card
AVERAGE FDR3	21%	48%	15%
TOP FDR3	42%	59%	26%

The LexisNexis® Risk Solutions Approach

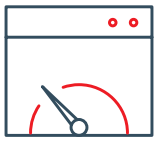
1. The Role of the Digital Profile

While identity-based profiling is essential for distinguishing between fraud types, it is equally critical to recognize that digital signals transcend fraud categories and offer a key contextual layer for detection. Fraudsters increasingly rely on digital tactics such as disposable emails, remote access tools and device spoofing to mask their identity and automate attacks.

Our client-contributed intelligence network, LexisNexis® Risk Intelligence Network, combines email and device intelligence to deliver robust, cross-industry visibility into evolving fraud patterns. This integrated approach is essential for staying ahead of increasingly sophisticated fraud threats.

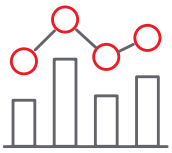
Network Intelligence: Strength in Collaboration

Multi-Element Linking: Connection of device IDs, email addresses and physical identity elements to expose synthetic identities and coordinated fraud rings.



Velocity Analysis: By analyzing velocity across multiple networks, we detect anomalies that signal fraud escalation before it peaks.

Contributory Networks: Our global, cross-industry collaborative intelligence gives organizations a dynamic, real-time view of risk by layering digital signals (e.g., device spoofing, email tumbling) with behavioral and PII-based profiling to amplify detection power and enable proactive defense.



Layered Intelligence: Digital behaviors in isolation are informative, but in combination they are transformative, helping institutions dramatically improve their ability to detect and prevent fraud.

The below case centers on a single LexisNexis® ThreatMetrix® digital identity that was linked to a broad and suspicious digital footprint, revealing a coordinated fraud ring[8]:

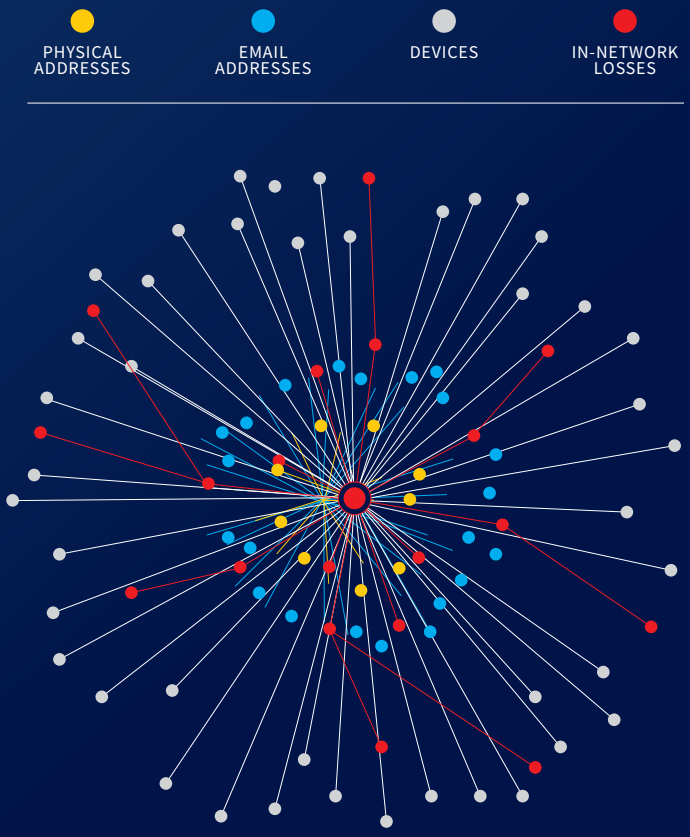
43 Devices: A high number of unique devices were associated with the same digital identity, suggesting device spoofing or shared fraud infrastructure.

22 Email Addresses: Numerous email variations were linked to the digital identity, indicating patterns commonly used by fraudsters to evade detection and bypass email-based checks.

9 Physical Addresses: The digital identity was tied to multiple physical locations, indicating synthetic identity use or address manipulation.

20 In-Network Losses: These were confirmed fraud events across the contributory network, all linked back to this single digital identity.

HOW DIGITAL LINKING HELPS IDENTIFY A FRAUD RING[9]



One Digital Identity

9
PHYSICAL ADDRESSES

22
EMAIL ADDRESSES

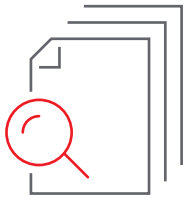
43
DEVICES

20
IN-NETWORK LOSSES

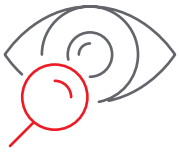
2. Document Authentication and Biometric Verification

To combat deepfake attacks at the point of new account origination, organizations should deploy advanced AI defenses capable of instantly and automatically distinguishing real applicants from synthetic imposters. Our market-leading document authentication and biometric verification solution goes beyond human detection—identifying forged documents, manipulated images, and biometric anomalies with precision, speed and scale that traditional methods simply can't match.

Optical Character Recognition: Using advanced OCR technology and natural language processing, our ID document authentication automatically extracts PII from virtually all government issued photo IDs across 220+ countries and territories and 140+ languages and typesets. This achieves accuracy of 98.5% for human-readable data and 99.98% for machine-readable text.



Document Fraud Analysis: Runs submitted IDs through hundreds of security checks to ensure the document is current, the photo is genuine and unaltered and no security element is damaged, modified or compromised.



Liveness Detection: Biometric verification ensures the applicant is a live human being and the session is happening in real time. Our technology flags virtually all deepfakes and other fraud vectors by analyzing micro muscle movements and other biometric signals. Additionally, it captures live video directly from the mobile device, preventing the use of uploaded images or prerecorded videos.

Face Matching: Verifies that the applicant using the device matches the photo on the presented ID, thwarting deepfakes and other fraud.

Together, these capabilities form a powerful first line of defense, enabling organizations to stop synthetic fraud at the source and onboard trusted customers with confidence.

Detection Guidance

Once you understand fraud, you can more effectively target it with optimal strategies.

Addressing the complexity of fraud requires a layered detection approach that blends signal intelligence, behavioral analytics and adaptive learning. Institutions should analyze both static and dynamic identity signals to uncover inconsistencies that may indicate fraudulent activity. These signals are not evaluated in isolation, but across time and channels, allowing systems to detect subtle deviations from expected user behavior.

AI models further enhance detection by identifying emerging fraud patterns, such as **synthetic identity creation or account takeovers**, through shifts in transaction velocity, login behavior or navigation paths. They also detect sophisticated forgeries including altered documents and deepfakes that humans can't spot. By correlating activity across digital and physical channels, organizations can expose coordinated fraud attempts that might otherwise go unnoticed.

Each interaction is assessed using a composite risk score that incorporates identity signals, behavioral cues and contextual data. These scores guide real-time decisions regarding whether to approve, challenge or block a transaction. Over time, detection systems evolve through feedback loops that integrate confirmed fraud cases and false positives, helping to ensure they remain responsive to new threats. While automation plays a central role, expert analysts remain essential for interpreting complex cases and refining model performance.

Conclusion

As fraud becomes increasingly lucrative and sophisticated, organizations should proactively fight bad AI from the very beginning of the customer lifecycle. Advanced detection techniques capable of identifying new tactics, spotting forged documents and recognizing deepfakes are essential to staying ahead of evolving threats.

While individual fraud solutions offer valuable insights, our research and client implementations consistently show that strategically combining multiple solutions yields significantly better outcomes. A multi-layered, multi-dimensional framework enhances detection by capturing a broader spectrum of fraud signals, reducing blind spots and improving operational efficiency without increasing review volume.

> Because fraud is dynamic, score combinations and thresholds should be regularly tested and recalibrated to reflect changing risk profiles. **The most effective strategies integrate data, technology, human expertise and adaptive processes, enabling organizations to respond swiftly and effectively across a wide range of fraud types.**

Discover how our comprehensive fraud detection solutions can help your organization stay ahead of emerging threats. Contact us to schedule a tailored demo.

FIND OUT MORE

LexisNexis®
RISK SOLUTIONS

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 LexisNexis Risk Solutions and RELX.

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

1 – LexisNexis® True Cost of Fraud™ Study

2 – LexisNexis® Risk Solutions Cybercrime Report

3 – “Generative AI is expected to magnify the risk of deepfakes and other fraud in banking,” Deloitte, May 29, 2024

4 – Sample of card issuer’s applications from LexisNexis® Inquiry Identity Network

5 – Sample of card issuer’s applications from LexisNexis® Inquiry Identity Network

6 – Sample of card issuer’s applications from LexisNexis® Inquiry Identity Network

7 – From internal LexisNexis® Risk Solutions data

8 – Applications from top regional bank

9 – Applications from top regional bank