7 trends that will shape the fraud and identity landscape in 2024

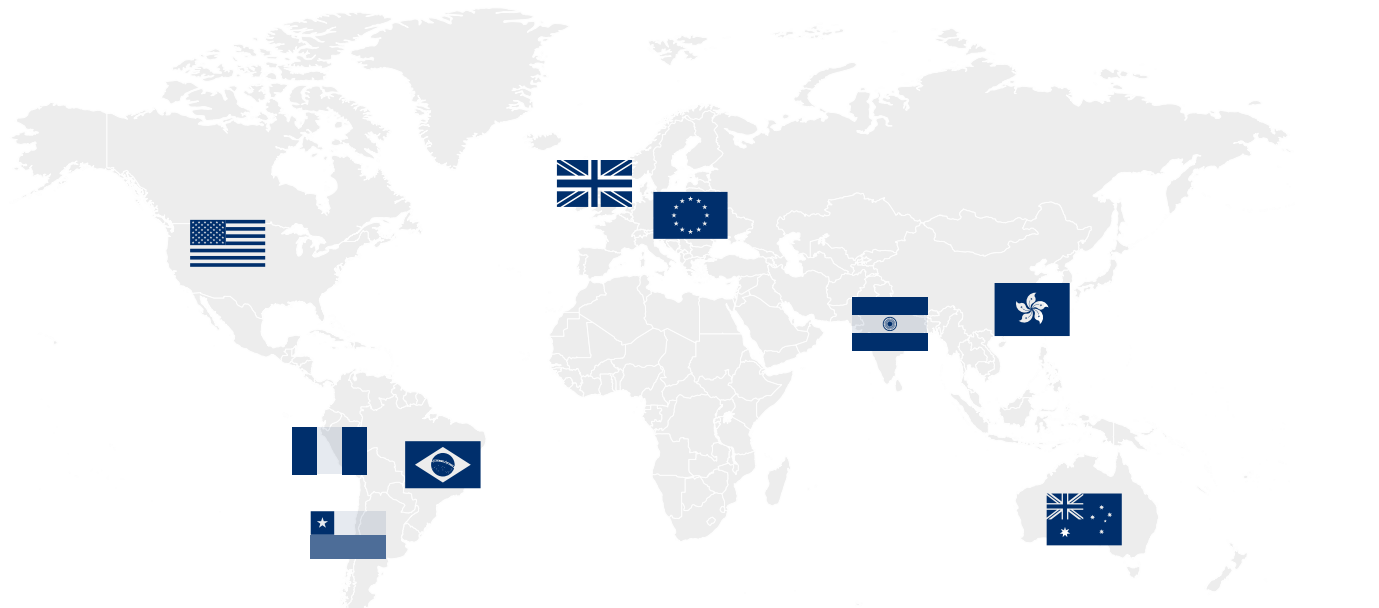
LexisNexis® RISK SOLUTIONS

Fraud and identity professionals will have to juggle mounting challenges such as the impact of added regulatory pressure in many parts of the world, the persistent issue of synthetic identity fraud, the malicious use of artificial intelligence and the increasing interconnected and cross-border nature of fraud attacks.

Building trust and maintaining a positive customer experience will be paramount. With opportunities such as the increased adoption of behavioral biometrics to tackle complex fraud, the remarkable value of developing a 360-degree customer view and the vast potential of a collaborative approach to fighting fraud, organizations can take fraud prevention to new heights in 2024.

1 Additional regulatory pressure will likely impact risk management costs

In 2024, organizations will dedicate even more resources to meet escalating regulatory changes.



US: Lingering uncertainty over liability for losses due to scams

The Electronic Fund Transfer Act could be expanded to include authorized transfer scams. Forward-thinking financial institutions are taking proactive measures to detect scams and mitigate risk.

82% Most U.S. financial services leaders with responsibility for fraud risk and mitigation strategies believe that consumers expect banks to reimburse them for successful scams involving their accounts.[1]

66% Of U.S. consumers say they would likely close their accounts with an institution that fails to reimburse them for losses due to authorized transfer scams.[2]

UK: New authorized push payment requirements

The Payment System Regulator in the UK introduced a new mandatory reimbursement system for APP fraud, which cost consumers an estimated $630m over the past year.[3]

The new rules require banks and other payment companies to refund victims who have been scammed within a few days, with the total cost shared between the sending and receiving organizations.

Though payments resulting from APP fraud represented less than **0.1%** of overall faster payments volumes in 2022, faster payments are used for **98%** of APP fraud payments.[4]

UK largest banks report up to **$348** lost to APP fraud by every $1 million sent in transactions.[5]

Authorized Push Payments are also known as 'Authorized Transfer Scam' in the U.S.

Europe: Proposal for a new payment services and electronic money services directive (PSD3)

The PSD3 legislation will evolve requirements for prioritizing consumers' interests, security and trust. The proposals include:

- Extending refund rights for fraud victims.
- Consolidating e-money institutions and payment institutions under a unified regulatory regime.
- Ensuring that consumers have better protection and understanding of their financial rights.

While effective in driving electronic payments and reducing fraud, PSD2 implementation costs – estimated at **$5.41billion** and increased transaction failure rates – estimated at **$36.2billion** have been substantial.[6]

Institutions that fail to meet the requirements of PSD2 can be fined up to **4%** of their annual returns

Latin America: New regulations on gaming and gambling

Latin America's regulated online gambling market is set to quadruple in size and reach $6.75billion in annual revenue by 2027, attracting both genuine and malicious players.[8]

In Brazil, a new law for betting and online gambling was approved in 2023, regulating an informal market that generates over **$30 billion** every year[9]

The Chilean Government recently introduced a Bill to effectively legalize online gambling. It is estimated that a legalized market could generate revenue of more than **$350m** a year.[10]

In Peru, regulations for sports betting and igaming have been approved, creating mechanisms to protect players from potential fraud or scams.

Hong Kong: Enhanced e-banking security

The Hong Kong Monetary Authority has introduced additional measures that increase online banking security and combat digital fraud. The requirements are mandatory for all e-banking activities and include:

- Additional customer authentication.
- Review of cross-border transfer limits.
- Session management controls that prevent fraudulent login attempts.
- A pilot bank-to-bank information sharing platform, which allows banks to share risk intelligence and take more agile mitigation measures.

India: A new direction on cybersecurity, risk controls and IT governance

Banking and non banking regulated entities will need to comply with the new set of rules issued by the Reserve Bank of India in 2023, including a comprehensive IT governance framework to mitigate cybercrime risks.

Of the almost 53,000 cybercrime cases registered in 2021, **60%** were fraud.[11]

Australia: Regulation for digital payment providers

New proposed rules by the Australian government aim to regulate digital wallet providers, enabling the Reserve Bank of Australia to monitor these transactions in the same way as credit card networks.

Increase in mobile wallet transactions in Australia[12]

29.2million 2018

2.4billion 2022

2 Explosion of use of synthetic identities

Criminals are exploiting the rise in popularity of digital banking and ecommerce to open new fraudulent accounts with synthetic identities, which combine real and fabricated information. Tackling synthetic fraud is a complex challenge that will be an escalating priority in 2024.

48% of retailers and **53%** of financial services institutions state that the rise of synthetic identities is the top contributing factor in making identity verification difficult in online channels[13]

Percentage of companies that report an increase in synthetic identity fraud by region

- **55%** in NA
- **50%** in EMEA
- **52%** in LATAM
- **50%** in APAC

52% of companies globally report an increase in synthetic identity fraud in 2023[14]

$23billion Expected value of losses due to synthetic identity fraud in the US by 2030[15]

$81,000 to $98,000[16] Is the average loss from an undetected synthetic identity fraud

Percentage of fraud and risk executives who rank the rise of synthetic identities as the main contributing challenge to identity verification during...

- **55%** Account opening
- **55%** Login
- **57%** Transfers / distribution of funds[17]

3 Increased use of artificial intelligence by criminals will require new risk mitigation tactics

The use of artificial intelligence (AI) with malicious intent is reshaping the fraud and risk landscape, increasing the efficacy of fraudsters' efforts and posing new challenges for establishing and proving someone's identity.

66% Of cybersecurity professionals detected deepfake attacks in their organizations in 2022[18]

90% Of online content is estimated to be synthetically generated by 2026[19]

38% Of large companies in EMEA and the US experienced deepfake fraud in 2023, resulting in losses of up to $480,000[20]

4 Increased use of behavioral intelligence to tackle complex fraud

Behavioral biometrics is becoming an essential tool for businesses and organizations to build trust with consumers and reduce increasingly sophisticated fraud. Forward-thinking businesses that want to elevate their fraud prevention strategy and defend against sophisticated scams are embracing behavioral biometrics.

Behavioral intelligence can be applied at any point in the user journey, acting as a defense against some of the most challenging varieties of scams aimed at consumers, such as APP scams and remote access scams, as well as other complex forms of fraud.

48% Of fraud executives ranked consumer scam attacks among their top concerns in 2022.[21]

$612 million Losses due to Authorised Push Payment (APP) scams in the UK in 2022.[23]

35% Of respondents' organizations in US financial services firms had implemented behavioral biometrics solutions by September 2023.[22]

Globally, **1/3** of organizations are using behavioral biometrics solutions across the customer journey.[24]

Key factors for adopting behavioral biometrics solutions[25]

- Accelerating digitalization
- New account opening fraud
- Account takeover fraud
- Authorized push payment (APP) fraud/scams
- Strong customer authentication (SCA) needs
- Know Your Customer and anti-money laundering regulations
- Regulatory changes in liability
- Improved customer experience

5 Fraud is increasingly coordinated across international borders

Threat intelligence reports suggest significant increases in cross-border connections and coordination among cybercriminals. Expect organized fraud groups to launch more coordinated attacks in 2024.

	Source of revenue	Source of fraud
International	39%	57%
Domestic	61%	43%

International revenue represents 39% of total revenue, but harbors 57% of overall fraud for financial services and ecommerce organizations globally.[26]

Mule networks linked by digital identities operate across regions and financial institutions, making payment attempts at one organization, then crossing over to others.[27]

Percentage of fraud complaints to the Federal Trade Commission that were cross-border[28]

1% 1992

11% 2022

6 Embracing a 360-degree customer view is becoming imperative to improve risk assessment

A more integrated and effective approach to fraud management begins with understanding the multitude of channels and interactions that customers use to engage with businesses.

82% Of consumers who shop online with their credit card are also active online banking users from the same bank that issued the credit card, meaning that digital identity intelligence can be shared across channels to drive trust and prevent more complex fraud.[29]

3/4 Of respondents report that fraud has negatively impacted their brand and their customers' experience.[30]

133% Increase in the number of banks using LexisNexis® Digital Identity Network® across both digital banking and 3D Secure CNP channels in 2022 vs. 2021.[31]

60%+ Improvement in risk assessment during subsequent payment events by gathering contextual digital intelligence at login.[32]

7 A collaborative approach to fighting fraud will be imperative to be ahead of rising threats

Information-sharing initiatives, collective intelligence, takedown coordination, and unified reporting mechanisms are how cybersecurity companies will continue to collaborate to combat rising fraud threats.

LexisNexis® Risk Solutions analyzes approximately 80 billion transactions worldwide every year. The LexisNexis® Digital Identity Network® platform crowdsources insights across thousands of businesses globally, building a leading repository of digital identity intelligence that grows more powerful with each transaction.

This visualization shows examples of regional fraud networks observed over a 3 month period targeting banks and mobile network operators seen in the Digital Identity Network®.

This fraud network only shows connections of more than 10 digital identities. A thicker line denotes a higher volume of attacks.

As attacks on the financial sector become more complex, fraudsters will often initiate their attacks by obtaining new mobile phone contracts or taking over the accounts of existing wireless customers for use later in bank account takeover attempts or new account fraud.

At least **$2.4million** in fraud value blocked

At least **$10.3million** was exposed to fraud by this specific network[33]

Key data elements in LexisNexis® Digital Identity Network® are growing quickly

Year-over-year growth rate by data element[34]

Data element	Growth
Phone Numbers	28%
Active Device IDs	10%
IP Addresses	20%
Email Addresses	19%
Scored Transactions	14%

LexisNexis® Digital Identity Network®

Countries and territories seen in Digital Identity Network®[35]

Period	Countries and territories
Every Second	90
Every Minute	193
Every Hour	230
Every Day	238
Every Month	245
All	249

Stay one step ahead of fraud.

LexisNexis® RISK SOLUTIONS

1 LexisNexis® True Cost of Fraud™ Study, 2023
2 LexisNexis® Risk Solutions and Forrester, Authorized Transfer Scams: How financial institutions can transform an epidemic into an opportunity, 2023
3 UK Finance Annual Fraud Report, 2022
4 Payment Systems Regulator, APP scams performance report, 2023
5 Payment Systems Regulator, APP scams performance report, 2023
6 European Commission, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)
European Banking Authority, Guidelines on the limited network exclusion under PSD2
The Fintech Times, Challenger Banks are Enabling the Most APP Fraud Reveals PSR Report, 2023
7 European Commission, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)
8 Vixio, Latin America Online Outlook, 2023
9 Games Magazine Brazil, 2023
10 SBC News, 2023
11 Financial Times, India fights back against soaring digital fraud, 2023
12 Reuters, Australia unveils draft law to regulate digital payment providers, 2023
13 LexisNexis® True Cost of Fraud™ Study, 2023
14 LexisNexis® True Cost of Fraud™ Study, 2023
15 Deloitte Center for Financial Services, Using biometrics to fight back against rising synthetic identity fraud, 2023
16 Deloitte Center for Financial Services, Using biometrics to fight back against rising synthetic identity fraud, 2023
17 LexisNexis® Risk Solutions True Cost of Fraud™ Study, 2023
18 World Economic Forum, How can we combat the worrying rise in the use of deepfakes in cybercrime?, 2023
19 World Economic Forum, How can we combat the worrying rise in the use of deepfakes in cybercrime?, 2023
20 World Economic Forum, How can we combat the worrying rise in the use of deepfakes in cybercrime?, 2023
21 Aite Novarica and LexisNexis® Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
22 Aite Novarica and LexisNexis® Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
23 UK Finance Annual Fraud Report, 2022
24 LexisNexis® True Cost of Fraud™ Study, 2023
25 Aite Novarica and LexisNexis® Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
26 LexisNexis® True Cost of Fraud™ Study, 2023
27 LexisNexis® Risk Solutions Cybercrime Report, 2022
28 Federal Trade Commission Press Release, FTC Reports Outline Efforts to Combat Cross-Border Fraud and Ransomware Attack, 2023
29 LexisNexis® Risk Solutions Cybercrime Report, 2022
30 LexisNexis® True Cost of Fraud™ Study, 2023
31 LexisNexis® Risk Solutions Cybercrime Report, 2022
32 LexisNexis® Risk Solutions Cybercrime Report, 2022
33 LexisNexis® Risk Solutions Cybercrime Report, 2021
34 Data analysis from LexisNexis® Digital Identity Network®
35 Data analysis from LexisNexis® Digital Identity Network®