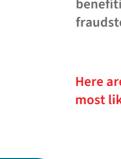


10 trends that will shape the fraud landscape in 2022



Many organizations face an upward battle when detecting and preventing fraud. Consumers continue to migrate to digital channels and while organizations are benefiting from this transition, it comes at a price. Where transactions occur, fraudsters follow, seeking out new vulnerabilities to exploit.

Here are our predictions for the top 10 trends to watch as they are most likely to impact fraud budgets and actions in the year ahead.

01 Digital transformation is unlikely to slow down

The effects of the pandemic have accelerated the digitization of customer interactions by several years. At the same time that businesses continue moving their services into the digital space, customers are also more comfortable and confident with consuming these services online.

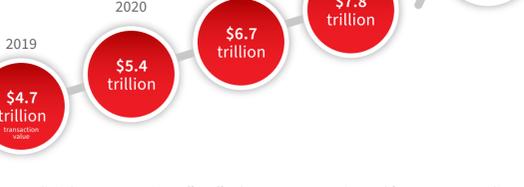
Although digital transformation was on an upswing prior to the pandemic, it took on new urgency once the pandemic hit. The pandemic fundamentally changed how people interact with businesses, making a range of inexperienced digital users available for fraudsters to target.

Globally, the average share of customer interactions that are digital grew by 22%¹.

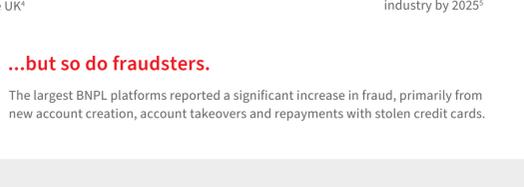


02 Increased automation

Automation is a double-edged sword. While it streamlines the customer journey by offering auto-fill and other conveniences, automation also makes it easier for fraudsters to launch attacks, prompting higher attack volumes. Automated methodologies can also do more harm more quickly.



Bot attacks across the customer journey are also on the rise:

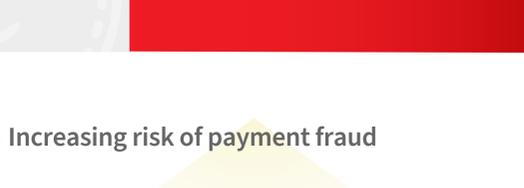


03 Adoption of new digital payments and methods

Digital payments sector: \$4.7 trillion in 2019, \$5.4 trillion in 2020, \$6.7 trillion in 2021, \$7.8 trillion in 2022, projected to reach \$10.7 trillion by 2025.

New digital payment options offer effortless account creation and fast access to credit, opening the door for abuse by fraudsters using stolen credentials.

Consumers love Buy Now Pay Later...



Number of consumers that have used BNPL in the UK⁴ | Growth in BNPL from 2020 to 2021 in the U.S.⁵ | Anticipated global gross merchandise volume of the BNPL industry by 2025⁶

...but so do fraudsters.

The largest BNPL platforms reported a significant increase in fraud, primarily from new account creation, account takeovers and repayments with stolen credit cards.

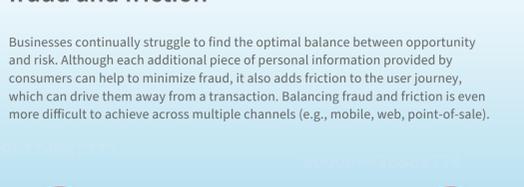
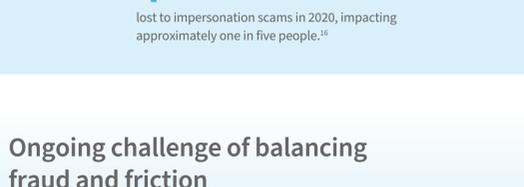
Cryptocurrencies present a growing challenge as well. The unregulated and novel way consumers can invest in cryptocurrencies opens up more opportunities for scams, ransom payments, money laundering and other illicit activities.

Hyperconnected networks contributed to a strong pattern of cross-organizational, cross-industry and even cross-regional fraud – an unfortunate but not unexpected outgrowth of digital transformation.



04 Increasing risk of payment fraud

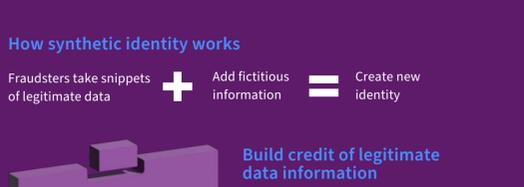
Consumers love the convenience of digital transactions. Globally, the digital payment market is projected to reach more than US \$236 billion by 2028, a CAGR of 19.4%.⁷ However, an increase in digital transaction activity also serves as a magnet for fraudsters, as data security awareness is not growing at the same speed as digital activities. Digital fraud attempts in financial services, for example, were up nearly 150%.⁸



While fraud losses occur across the customer journey, new account creation and the point of distribution appear to be most susceptible to fraud in the U.S.¹¹

05 The growing prevalence of scams

Account takeover (ATO) and social engineering scams – including authorized push payment (APP), romance, investment and impersonation fraud – are among the fastest growing financial crimes. In fact, 98%¹² of cyberattacks rely on social engineering. These scams represent an emerging global challenge due to the difficulty in detection.



06 Ongoing challenge of balancing fraud and friction

Businesses continually struggle to find the optimal balance between opportunity and risk. Although each additional piece of information provided by consumers can help to minimize fraud, it also adds friction to the user journey, which can drive them away from a transaction. Balancing fraud and friction is even more difficult to achieve across multiple channels (e.g., mobile, web, point-of-sale).



Incorrectly matching authentication methods with the risk of the transaction can lead to friction in the customer journey, causing a decrease in conversions. To continue to keep fraud low and to provide the right amount of friction, merchants and issuers are looking at alternative authentication solutions to maximize customer experience and minimize unneeded friction during the onboarding and checkout processes.

07 Rise of synthetic identities

The creation of new identities by combining elements of real and falsified information is one of the fastest growing online crimes in the U.S.¹⁷ Fueled by the rise in online banking and other digital financial services, synthetic identity fraud has become a multimillion-dollar challenge. It is also one of the hardest types of identity theft for businesses and financial institutions to detect because there is no real person to report the fraud.

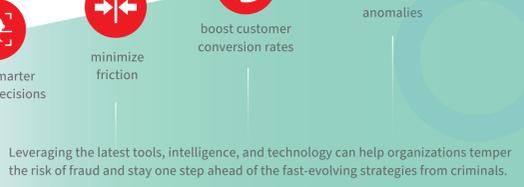
How synthetic identity works



- Build credit of legitimate data information
- Apply for credit cards
- Take out loans
- Open bank accounts
- Apply for government benefits

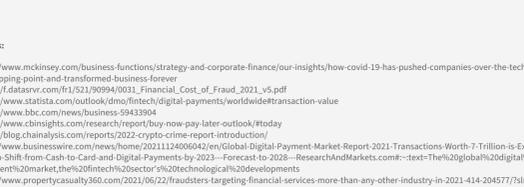
08 Escalating cost of fraud

The pandemic drove more consumers than ever to online and mobile channels. Fraudsters soon followed, leading to increased attack volumes and ultimately the cost of fraud, both of which remain significantly higher now than before the pandemic began.



In APAC, fraudulent transactions cost up to 3.87 times the value of the lost transaction, up from 3.40 in 2019.²⁰

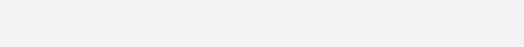
Fraudulent transactions in LATAM cost 3.68 times the value of the lost transaction in 2020, up from 3.46 in 2019.²¹



09 Growing need for multi-layered fraud assessment

Today's fraudsters deploy complex, multi-vector attacks and continually develop new strategies to bypass controls and exploit vulnerabilities. A multi-layered approach that includes physical identity, digital identity intelligence and behavioral biometrics is one of the best defenses for mitigating the risk of fraud.

Behavioral biometrics looks at how a user:



Behavioral Biometrics can be used to:

- Detect bots and aggregators
- Identify "good" customer profiles
- Reliably profile fraudsters
- Recognize unusual interactions
- Strengthen the trust of good customers

10 Heightened need for real-time risk assessment

The upward trend in online and mobile activity underscores the need for a global dynamic fraud solution that can verify identity and transaction attributes in near real time across the customer journey.

Leveraging the latest tools, intelligence, and technology can help organizations temper the risk of fraud and stay one step ahead of the fast-evolving strategies from criminals.

Discover how LexisNexis® Risk Solutions brings together fraud management, identity verification and risk insights by leveraging network intelligence, industry-trusted global coverage and intellectual property to enable your business to confidently differentiate between a trusted customer and threat, while maintaining a seamless customer experience.

<https://risk.lexisnexis.com/global/en/corporations-and-non-profits/fraud-and-identity-management>

Sources: ¹https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever; ²https://data.rvr.com/fr/521/30994/0031_Financial_Cost_of_Fraud_2021_v5.pdf; ³https://www.statista.com/outlook/dmo/finetech/digital-payments/worldwide#transaction-value; ⁴https://www.bbc.com/news/business-59433904; ⁵https://www.chinainights.com/research/report/buy-now-pay-later-outlook#10day; ⁶https://blog.chinainights.com/reports/2022-crypto-crime-report-introduction/; ⁷https://www.outstreet.com/wp-content/uploads/Outstreet-Fraud-Report-Q32021.pdf; ⁸https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices; ⁹https://purplesec.us/resources/cyber-security-statistics/; ¹⁰https://www.finextra.com/newsarticle/38884/app-fraud-losses-overtake-card-crime-in-h1-2021; ¹¹https://www.audience.org.uk/system/files/Fraud%20in%20the%20ACTS%202021-%20FINAL.pdf; ¹²https://www.scamwatch.gov.au/scam-statistics; ¹³https://www.ft.com/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf; ¹⁴https://www.fbi.gov/audio-repository/fhw-podcast-synthetic-ids-010220.mp3#view; ¹⁵https://data.rvr.com/fr/521/30994/0031_Financial_Cost_of_Fraud_2021_v5.pdf; ¹⁶https://risk.lexisnexis.com/about-us/press-room/press-release/2020106-annual-true-cost-of-fraud-study; ¹⁷https://www.businesswire.com/news-releases/2020106-annual-true-cost-of-fraud-study; ¹⁸https://risk.lexisnexis.com/global/en/insights-resources/research/app-true-cost-of-fraud-study#:~:text=Depending%20on%20the%20market%20CS20the%20other%20APAC%20markets%20is%203.40; ¹⁹https://www.pnwswire.com/news-releases/2020106-annual-true-cost-of-fraud-study-reveals-fraud-costs-3-75-times-the-lost-transaction-value-for-each-fraudulent-transaction-in-mexico-301403618.html#:~:text=Every%20fraudulent%20transaction%20now%20costs,digital%20transactions%20during%20the%20pandemic; ²⁰https://data.rvr.com/fr/521/30994/0031_Financial_Cost_of_Fraud_2021_v5.pdf

About LexisNexis Risk Solutions
LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

This document is for educational purposes only and does not warrant 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.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Copyright© 2022 LexisNexis Risk Solutions Group. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright© 2022 LexisNexis Risk Solutions Group. NXR515367-0222-EN-US

For more information, please visit risk.lexisnexis.com, and relx.com