LexisNexis® RISK SOLUTIONS

The Relentless Shift to Mobile:

Fraud Follows as Mobile Adoption Surges

1 The Age of Mobile: Globally, Mobile Usage Continues to Rise

67.1%
Of the world's population uses a mobile phone, as of 2022[1]

5.31 B
Unique mobile phone users globally at the start of 2022[1]

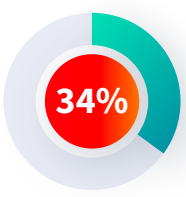
95 M
New mobile users globally in 2022, a 1.8% increase from 2021[1]

2 The Omnipresent Consumer: Adoption of Mobile Transactions is Widespread

77% of the global transaction volume in LexisNexis® Digital Identity Network® came from mobile devices in 2022, compared to 72% in 2021[2]

82% of global mobile transactions in LexisNexis® Digital Identity Network® were made via mobile app in 2022, compared to 76% in 2021[2]

3 The Mobile Battlefield: Attacks Targeting Mobile Channels Continue to Rise



The mobile attack rate went up by 34% globally (2022 vs 2021)[2]

ACCOUNT CREATION

The highest mobile attack rate in 2022 was seen at the point of account creation. 1 in 11 new account creations across digital channels, including mobile app and mobile browser, was seen as an attack[2]

LOGIN

Mobile app attack rate for logins increased by 104% (2022 vs 2021)[2]

PASSWORD

The highest increase in mobile attack rate was seen at the point of password reset, increasing from 1.7% in 2021 to 3.9% in 2022, a 134% increase. **On mobile apps, the password reset attack rate increased even more: 231%**[2]

LexisNexis® Risk Solutions Can Help Fight Against Mobile Fraud with Confidence and Provide a Positive User Experience for Consumers

Assess the anomalies associated with the growing number of attacks targeting the mobile channel, providing trusted customers with a positive experience on their chosen device. Our suite of fraud and identity solutions addresses risks at every touchpoint of the customer journey:

Account Creation	Login	Account Management and Payments	Device Integrity
Validate the identity of new customers, assessing whether the entity behind the application is a real user or a fraudster using a synthetic ID	**Recognize** legitimate customers on trusted devices in near real time and improve their digital experience	**Identify** if a customer's account has been taken over by a fraudster or if the customer is being coerced	**Identify** tenured devices and those which have no history at all
Identify the linkages between new customers and their associated credentials, devices, accounts, locations and hundreds of other risk attributes	**Highlight** contradictory or suspicious behavior at login, including password sharing and service abuse	**Determine** the legitimacy of the entity on the other end of a mobile transaction	**Understand** a device's current location along with its historical locations and movements
Help detect if stolen credentials or spoofed IDs are used to open a new account	**Identify** automated bot attacks attempting to log into accounts with compromised credentials	**Build** a sophisticated understanding of a customer's normal patterns of behavior on mobile channels	**Profile** all devices accessing the customer website or app
Identify if a bank account associated with a new account application has received confirmed fraudulent payments or shows concentrations of risky payments	**Manage** threats on the mobile channel in a contextually aware manner, aggregating information across physical, web and mobile touchpoints	**Apply** risk-appropriate friction in the payment process	**Evaluate** the overall security posture of a mobile device

For more information on our award-winning fraud and identity verification solutions, visit **risk.lexisnexis.com**

LexisNexis® RISK SOLUTIONS

1. datareportal.com/reports/digital-2022-global-overview-report
2. Data from LexisNexis® Digital Identity Network®