7 tendances qui vont façonner le paysage en matière de fraude et d'identité en 2024

LexisNexis® RISK SOLUTIONS

Les professionnels en matière de fraude et d'identité devront jongler avec des défis croissants tels que l'impact d'une pression réglementaire accrue dans de nombreuses régions du monde, le problème persistant de la fraude à l'identité de synthèse, l'utilisation malveillante de l'intelligence artificielle et la nature de plus en plus interconnectée et transfrontalière des attaques frauduleuses.

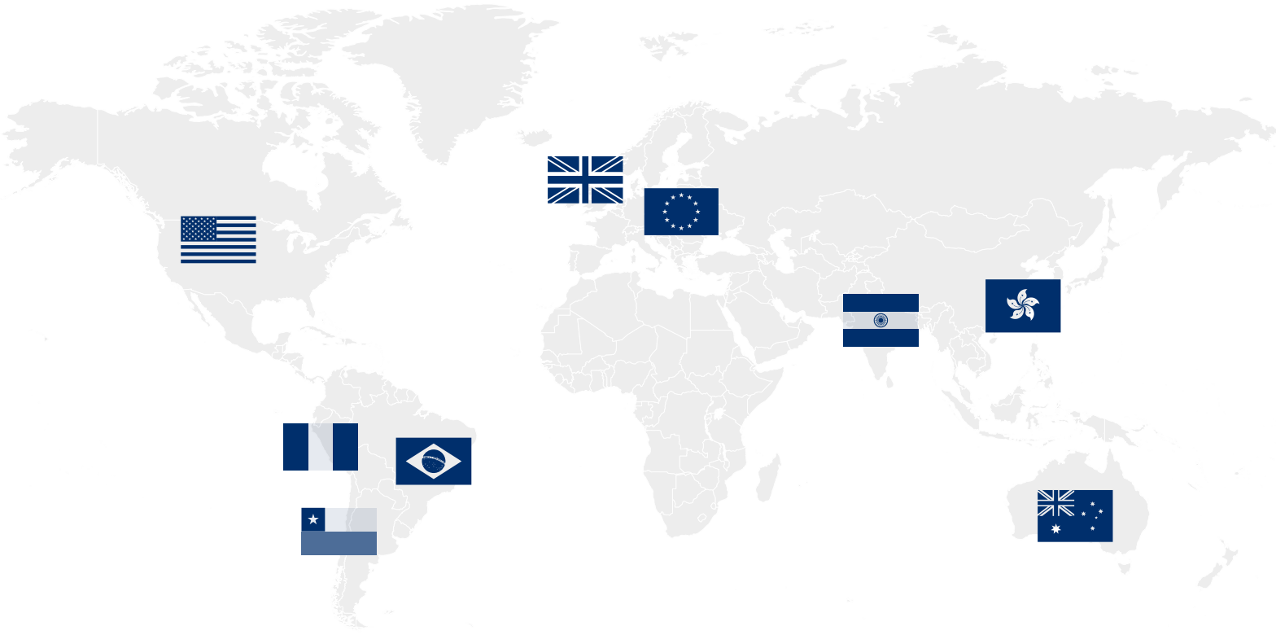
Il est primordial d'instaurer un climat de confiance et de maintenir une expérience positive pour le client.

Avec des opportunités telles que l'adoption accrue de la biométrie comportementale pour lutter contre les attaques frauduleuses à multiples facettes, le développement d'une vision à 360 degrés du client et le vaste potentiel d'une approche collaborative, les entreprises peuvent faire franchir à la prévention de la fraude de nouveaux sommets en 2024.

1

La pression réglementaire supplémentaire aura probablement un impact sur les coûts de gestion des risques

En 2024, les entreprises consacreront encore plus de ressources pour répondre aux changements réglementaires croissants.



ÉTATS-UNIS : incertitude persistante quant à la responsabilité en cas de pertes dues aux escroqueries

La loi sur les transferts électroniques de fonds pourrait être étendue aux escroqueries sur les transferts autorisés. Des établissements financiers visionnaires adoptent des mesures proactives pour détecter les escroqueries et réduire les risques.

82%

La plupart des responsables des services financiers américains chargés de la lutte contre la fraude et des stratégies de réduction des risques estiment que les consommateurs victimes d'escroqueries sur leurs comptes s'attendent à être remboursés par leurs banques.[1]

66%

Pourcentage de consommateurs américains qui déclarent qu'ils fermeraient probablement leur compte, si la banque ne leur remboursait pas les pertes dues à des escroqueries sur les transferts autorisés.[2]

Royaume-Uni : nouvelles exigences en matière de paiements push autorisés

Au Royaume-Uni, l'instance de régulation des systèmes de paiement a introduit un nouveau système de remboursement obligatoire en cas de fraudes aux paiements push autorisés (APP), qui ont coûté aux consommateurs l'année dernière environ 630 millions de dollars.[3]

Les nouvelles réglementations exigent que les banques et autres sociétés de paiement remboursent les victimes d'escroquerie dans un délai de quelques jours, le coût total étant partagé entre l'organisme expéditeur et l'organisme destinataire.

Bien que les paiements résultant de fraudes APP aient représenté moins de

0.1 %

des volumes globaux de paiements plus rapides en 2022, ces paiements sont utilisés pour

98 %

des paiements effectués dans le cadre de fraudes AAP.[4]

Les plus grandes banques britanniques citent des montants pouvant atteindre

439 dollars

de pertes dues aux fraudes APP pour chaque montant de 1,26 million transféré par transactions.[5]

Les paiements push autorisés sont également connus aux États-Unis sous le nom de « Authorized Transfer Scam » (escroqueries sur les transferts autorisés).

Europe : proposition d'une nouvelle directive sur les services de paiement et de monnaie électronique (DSP3)

La directive DSP3 fera évoluer les exigences pour donner la priorité aux intérêts, à la sécurité et à la confiance des consommateurs. Les propositions comprennent :

- l'extension des droits au remboursement des consommateurs victimes de fraude ;
- l'harmonisation des règles s'appliquant aux établissements de paiement et aux établissements de monnaie électronique ;
- l'amélioration de la protection des consommateurs et de la communication des droits financiers dont ils bénéficient.

Bien que la DSP2 soit efficace pour stimuler les paiements électroniques et réduire la fraude, le coût de sa mise en œuvre, estimé à

5,41 milliards de dollars,

et de l'augmentation des taux d'échec des transactions, estimé à

36,2 milliards de dollars,

a été considérable.[6]

Les établissements qui ne respectent pas les exigences de la directive DSP2 peuvent se voir infliger une amende pouvant atteindre

4 %

de leurs déclarations annuelles.

Amérique latine : nouvelles réglementations relatives aux jeux de hasard et d'argent

Le marché réglementé des jeux d'argent en ligne en Amérique latine devrait quadrupler et atteindre 6,75 milliards de dollars de recettes annuelles d'ici 2027, attirant à la fois des joueurs honnêtes et des joueurs malintentionnés.[8]

Au Brésil, une nouvelle loi sur les paris et les jeux d'argent en ligne a été votée en 2023, réglementant un marché informel qui génère plus de

30 milliards de dollars

chaque année.[9]

Le gouvernement chilien a récemment présenté un projet de loi visant à légaliser les jeux d'argent en ligne.

Il a été estimé qu'un marché légalisé pourrait générer des revenus de plus de

350 millions de dollars

par an.[10]

Au Pérou, des réglementations relatives aux paris sportifs et aux jeux en ligne ont été approuvées pour protéger les joueurs contre d'éventuelles fraudes et escroqueries.

Hong Kong : renforcement de la sécurité des services bancaires en ligne

L'autorité monétaire de Hong Kong a introduit des mesures supplémentaires pour renforcer la sécurité des services bancaires en ligne et lutter contre la fraude en ligne. Ces exigences sont obligatoires pour toutes les activités de banque en ligne et comprennent notamment :

- une authentification supplémentaire du client ;
- la révision des limites de transferts transfrontaliers ;
- des contrôles de la gestion des sessions pour empêcher les tentatives de connexion frauduleuses ;
- une plateforme pilote de partage d'informations entre banques, qui permet à ces dernières de partager des informations sur les risques et de prendre des mesures d'atténuation plus souples.

Inde : nouvelle orientation en matière de cybersécurité, de contrôle des risques et de gouvernance informatique

Les entités bancaires et non bancaires réglementées devront se conformer au nouvel ensemble de règles publiées par la Reserve Bank of India en 2023, notamment un cadre complet de gouvernance informatique pour atténuer les risques de cybercriminalité.

Des quelque 53 000 cas de cybercriminalité enregistrés en 2021,

60 %

étaient des fraudes.[11]

Australie : réglementation pour les prestataires de paiements numériques

Les nouvelles règles proposées par le gouvernement australien visent à réglementer les fournisseurs de portefeuilles numériques, en permettant à la Reserve Bank of Australia de contrôler ces transactions de la même manière que les réseaux de cartes de crédit.

Augmentation des transactions financières par portefeuille numérique en Australie[12]

29,2 millions
2018

2,4 milliards
2022

2

Explosion de l'utilisation des identités synthétiques

Les criminels profitent de la popularité croissante des services bancaires numériques et du commerce électronique pour ouvrir de nouveaux comptes frauduleux à l'aide d'identités synthétiques, qui associent informations réelles et inventées. La lutte contre la fraude à l'identité synthétique est un défi complexe qui constituera une priorité croissante en 2024.

48 % des détaillants et **53 %** des établissements fournissant des services financiers déclarent que l'augmentation des identités synthétiques est le principal facteur entravant la vérification des identités sur les canaux en ligne.[13]

Pourcentage d'entreprises qui signalent une augmentation de la fraude à l'identité synthétique, par région

52 %

des entreprises à l'échelle mondiale signalent une augmentation de la fraude à l'identité synthétique en 2023[14]

23 milliards de dollars US

Valeur attendue des pertes dues à la fraude à l'identité synthétique aux États-Unis d'ici 2030[15]

81 000 à 98 000 dollars US[16]

Il s'agit de la perte moyenne résultant d'une fraude à l'identité synthétique non détectée.

Pourcentage des responsables en matière de lutte contre la fraude et de risque qui considèrent l'augmentation des identités synthétiques comme la principale difficulté en matière de vérification des identités au cours.

55 % de l'ouverture du compte

55 % de la connexion

57 % des transferts / de la distribution de fonds[17]

3

L'utilisation accrue de l'intelligence artificielle par les criminels nécessitera de nouvelles stratégies de mitigation des risques

L'utilisation de l'intelligence artificielle (IA) avec des intentions malveillantes modifie le paysage de la fraude et du risque, en augmentant l'efficacité des efforts déployés par les escrocs et en générant de nouveaux défis pour établir et prouver l'identité d'une personne.

66 %

des professionnels de la cybersécurité ont détecté des attaques très élaborées dans leurs entreprises en 2022.[18]

90 %

du contenu en ligne sera généré de manière synthétique d'ici 2026 selon les estimations.[19]

38 %

des grandes entreprises de la région EMEA et des États-Unis ont été confrontées à des fraudes très élaborées en 2023, ce qui a entraîné des pertes allant jusqu'à 480 000 dollars.[20]

4

Utilisation accrue de la biométrie comportementale pour lutter contre les attaques frauduleuses à multiples facettes

La biométrie comportementale devient un outil essentiel pour les entreprises et les organisations afin de renforcer la confiance des consommateurs et de réduire les fraudes de plus en plus sophistiquées. Les entreprises visionnaires qui souhaitent améliorer leur stratégie de prévention de la fraude et se défendre contre les escroqueries sophistiquées adoptent la biométrie comportementale.

La biométrie comportementale peut être appliquée à tout stade du parcours de l'utilisateur et servir de défense contre certaines des formes les plus complexes d'escroquerie visant les consommateurs, telles que les escroqueries APP et par accès à distance, ainsi que d'autres formes perfectionnées de fraude.

48 % des responsables en matière de fraude ont classé les escroqueries visant des consommateurs parmi leurs principales préoccupations en 2022.[21]

612 millions de dollars

Pertes dues à des escroqueries par paiement push autorisé (APP) au Royaume-Uni en 2022.[23]

35 % des organisations auxquelles appartenaient les personnes interrogées dans les entreprises américaines de services financiers étaient équipées de solutions de biométrie comportementale en septembre 2023.[22]

À l'échelle mondiale,

1/3

des entreprises utilisent des solutions de biométrie comportementale tout au long du parcours client.[24]

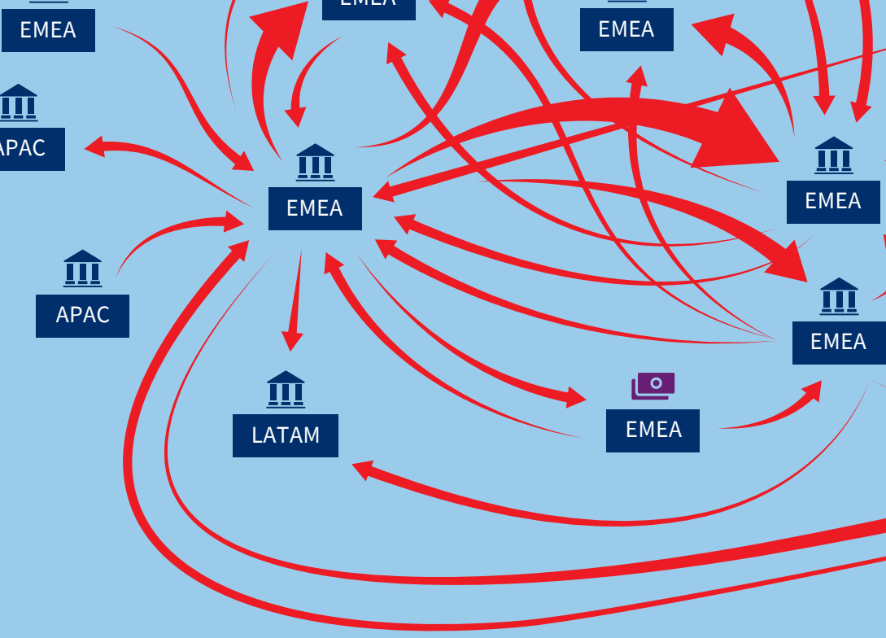
Facteurs clés pour l'adoption de solutions de biométrie comportementale[25]

- Accélération de la numérisation
- Fraude à l'ouverture d'un nouveau compte
- Fraude par prise de contrôle d'un compte
- Fraudes/escroqueries par paiement push autorisé (APP)
- Besoins en matière d'authentification forte du client (SCA)
- Connaissance de la clientèle et réglementations en matière de lutte contre le blanchiment d'argent
- Évolutions réglementaires en matière de responsabilité
- Amélioration de l'expérience des clients

5

Les fraudes sont de plus en plus coordonnées par-delà les frontières internationales

Les rapports sur les menaces suggèrent une augmentation significative des connexions transfrontalières et de la coordination entre les cybercriminels. Il faut s'attendre à ce que des groupes d'escrocs organisés lancent des attaques plus coordonnées en 2024.



Les revenus internationaux représentent 39 % du total des revenus, mais correspondent à 57 % de l'ensemble des fraudes pour les services financiers et les entreprises d'ecommerce à l'échelle mondiale.[26]

Les réseaux de mules reliés par des identités numériques opèrent dans différents pays et établissements financiers, effectuant des tentatives de paiement auprès d'une entreprise avant de passer à la suivante.[27]

Les traits plus épais indiquent un volume plus élevé d'identités numériques et de tentatives de paiements associées.

Pourcentage de plaintes pour fraudes transfrontalières déposées auprès de la Federal Trade Commission[28]

1 % 1992

11 % 2022

6

L'adoption d'une vision à 360 degrés du client devient impérative pour améliorer l'évaluation des risques

Une approche plus intégrée et plus efficace de la gestion de la fraude commence par la compréhension de la multitude de canaux et d'interactions que les clients utilisent pour entrer en contact avec les entreprises.

82 %

des consommateurs qui achètent en ligne avec leur carte de crédit utilisent également activement les services bancaires fournis par la banque émettrice de la carte de crédit, ce qui signifie que les informations relatives à l'identité numérique peuvent être partagées à travers les différents canaux pour renforcer la confiance et éviter des fraudes plus complexes.[29]

3/4

des personnes interrogées déclarent que la fraude a eu un impact négatif sur leur marque et sur l'expérience de leurs clients.[30]

133 %

Augmentation entre 2021 et 2022 du nombre de banques utilisant LexisNexis® Digital Identity Network® à la fois pour la banque numérique et les canaux sans présence de la carte 3D Secure.[31]

Plus de 60 %

Amélioration de l'évaluation des risques lors des paiements ultérieurs grâce à la collecte d'informations numériques contextuelles au moment de la connexion.[32]

7

Lutte collaborative contre la fraude

Les initiatives de partage d'informations, les renseignements collectifs, la coordination des opérations et les mécanismes de signalement unifiés sont les moyens par lesquels les entreprises de cybersécurité continueront à collaborer pour lutter contre les menaces croissantes de fraudes.

LexisNexis® Risk Solutions analyse chaque année environ 80 milliards de transactions dans le monde.

LexisNexis® Digital Identity Network® rassemble des informations provenant de milliers d'entreprises dans le monde entier, créant ainsi des archives de renseignements relatifs aux identités numériques qui s'enrichissent à chaque transaction.

Ce réseau de fraude ne montre que les connexions de plus de 10 identités numériques. Un trait plus épais indique un volume d'attaques plus élevé.

Ce visuel illustre les réseaux régionaux de fraude ciblant les banques et les opérateurs de réseaux mobiles.

Les attaques ciblant le secteur financier devenant de plus en plus complexes, les escrocs commencent souvent par obtenir de nouveaux contrats de téléphonie mobile ou par prendre le contrôle des comptes de clients existants pour les utiliser ultérieurement lors de tentatives de prise de contrôle de comptes bancaires ou de fraude à l'ouverture de nouveaux comptes.

Au moins

2,4 millions de dollars

de fraudes qui ont été stoppées

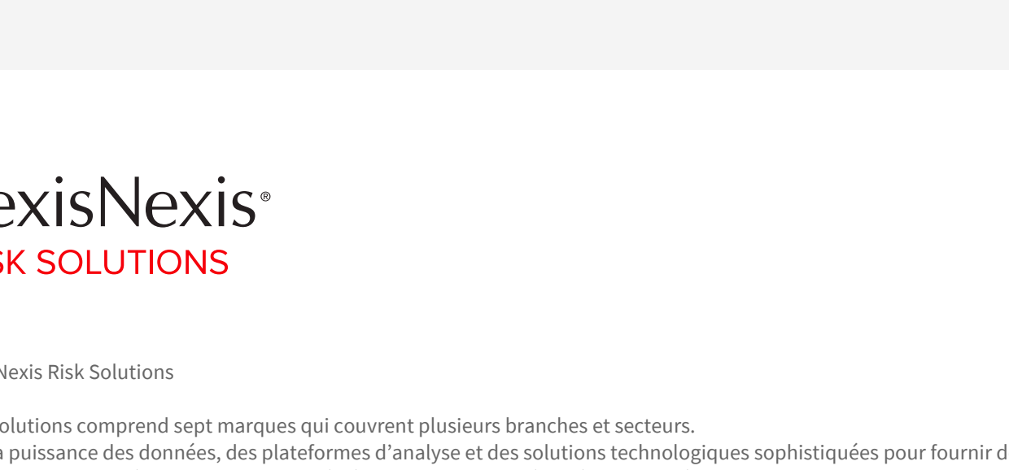
Au moins

10,3 millions de dollars

risquaient de tomber aux mains des escrocs sur l'ensemble du réseau[33]

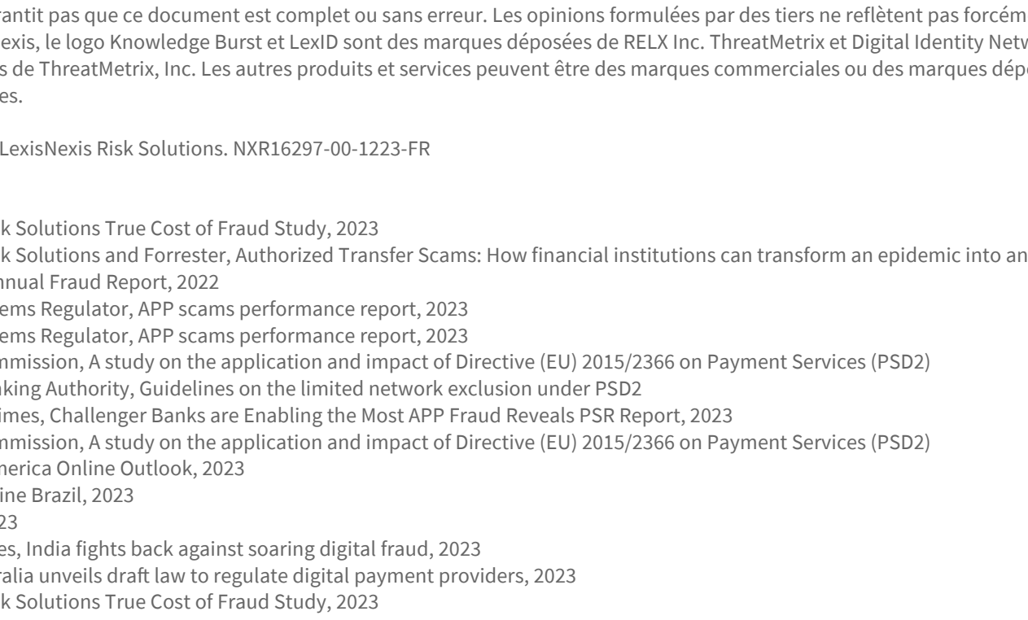
Le volume d'éléments de données clés de LexisNexis® Digital Identity Network® augmente rapidement

Taux de croissance en glissement annuel par élément de données[34]



LexisNexis® Digital Identity Network®

Pays et territoires figurant dans le Digital Identity Network®[35]



LexisNexis® RISK SOLUTIONS

À propos de LexisNexis Risk Solutions

LexisNexis® Risk Solutions comprend sept marques qui couvrent plusieurs branches et secteurs. Nous exploitons la puissance des données, des plateformes d'analyse et des solutions technologiques sophistiquées pour fournir des informations qui aident les entreprises et les entités gouvernementales à réduire les risques et à améliorer les décisions au profit des personnes dans le monde entier. Notre siège social est situé dans la région métropolitaine d'Atlanta, en Géorgie, et nous avons des bureaux dans le monde entier. Nous faisons partie de RELX (LSE : REL/NYSE : RELX), un fournisseur mondial d'outils d'analyse et d'aide à la décision basés sur les informations destinées aux professionnels et aux entreprises. Pour de plus amples informations, veuillez consulter LexisNexis Risk Solutions et RELX.

[1] LexisNexis Risk Solutions 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 Risk Solutions True Cost of Fraud Study, 2023
[14] LexisNexis Risk Solutions 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 Risk Solutions 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 Risk Solutions 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 Risk Solutions 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, 2022
[34] Data analysis from the LexisNexis® Digital Identity Network®
[35] Data analysis from the LexisNexis® Digital Identity Network®