



# Les tendances majeures qui façonnent le paysage de la fraude et de l'identité

**Les transactions en ligne ont dominé le marché mondial. Entraînées par la pandémie, elles sont devenues un mode de consommation courant.**



Les défis liés aux transactions en ligne, activement ciblées par des réseaux de fraude, et avec des consommateurs désormais habitués au numérique, ne cessent d'évoluer. Les voies par lesquelles un fraudeur tente de s'interposer lors d'une transaction sont infinies. Ces réseaux de fraude professionnels s'organisent pour monétiser toute une série de fraudes à l'identité.

**Voici nos prévisions concernant les 7 principales tendances à observer dans le domaine de la fraude et de l'identité qui sont les plus susceptibles d'impacter votre entreprise.**

**1**

## LA MONTÉE EN PUISSANCE DE L'ÉCONOMIE NUMÉRIQUE CRÉE DE NOUVELLES OPPORTUNITÉS DE FRAUDE

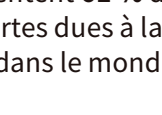
Les données du réseau d'identité numérique Digital Identity Network® de LexisNexis® montrent une augmentation du volume mondial de transactions numériques.

DE JANVIER  
À JUIN 2022¹

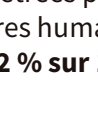
+37 %  
sur  
1 an

39,4  
milliards  
de trans-  
actions

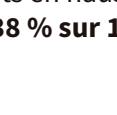
L'augmentation des transactions numériques s'accompagne d'une hausse des attaques frauduleuses presque équivalente.



Les canaux numériques  
représentent **61 %** de toutes  
les pertes dues à la fraude  
dans le monde²



Taux d'attaques  
perpétrées par des  
êtres humains  
**+32 % sur 1 an**



Des attaques de  
bots en hausse de  
**38 % sur 1 an³**

Alors que les interactions numériques deviennent la norme et que la connectivité s'accroît dans le monde, les entreprises doivent se préparer à des tentatives de fraude toujours plus complexes.

**2**

## LES MARCHÉS MONDIAUX COMPLEXES ET LES POSSIBLES MENACES INTERCONNECTÉES NÉCESSITENT UNE RÉPONSE COLLECTIVE

**Les fraudeurs agissent dans des environnements complexes, chaque élément de données utilisé étant lié au prochain élément de données à une échelle mondiale.**



Par conséquent, les entreprises et les secteurs d'activité ont besoin d'une plus grande collaboration au niveau mondial pour lutter contre les réseaux de fraude mais aussi pour comprendre qui sont les consommateurs dignes de confiance. La reconnaissance de ces derniers permet aux entreprises de créer de nouveaux canaux de revenus et d'augmenter les ventes auprès d'une base de consommateurs fidèles.

**3**

## DES SCHÉMAS COMPLEXES D'INGÉNIERIE SOCIALE CIBLÉS, RÉPARTIS SUR PLUSIEURS ZONES GÉOGRAPHIQUES ET SECTEURS D'ACTIVITÉ

**Les attaques d'ingénierie sociale font partie des menaces de cybersécurité qui se développent le plus vite, tant sur les marchés développés que sur les marchés émergents. De plus, elles continuent de poser des difficultés aux entreprises, car elles constituent l'un des types de fraude les plus complexes à détecter.**

**Il existe de multiples raisons pour lesquelles les criminels ciblent les consommateurs finaux pour commettre des délits :**



La numérisation et disponibilité rapides  
des données à l'échelle mondiale



La croissance de l'open banking, des  
transferts plus rapides et des paiements  
instantanés



Une augmentation de l'automatisation et  
des interactions à distance



L'amélioration des contrôles de  
prévention de la fraude met en évidence  
le point le plus vulnérable de la chaîne :  
le consommateur

**4**

## LA MIGRATION VERS LES TRANSACTIONS MOBILES ET LES NOUVEAUX MODES DE PAIEMENTS NUMÉRIQUES RENDENT LA RECONNAISSANCE DE LA CONFIANCE ET LA GESTION DES RISQUES DIFFICILES



Le volume des transactions mobiles dans le réseau d'identités numériques Digital Identity Network® a atteint **76 % de l'ensemble des transactions au premier semestre 2022.**⁴



Les **méthodes alternatives de paiement, notamment les portefeuilles électroniques et les crypto-monnaies, représentent 24 % du volume des transactions dans le monde**, une répartition qui est similaire à celle des méthodes de paiement traditionnelles comme les cartes de crédit et de débit. 29 % des pertes dues à la fraude sont attribuées à ces méthodes de paiement.⁵

**5**

## IL EST IMPÉRATIF DE TROUVER LE BON ÉQUILIBRE ENTRE RISQUE ET FRICTION, CAR LES ENTREPRISES CHERCHENT À PROTÉGER LES CONSOMMATEURS SANS PERTURBER LEUR EXPÉRIENCE

Les dernières solutions d'identité et d'authentification adoptent une vision globale de l'identité et du risque, en combinant la vérification de l'identité physique à des données d'identité numérique basées sur l'appareil utilisé, l'emplacement géographique et le comportement du consommateur.



Grâce à l'identité numérique et aux renseignements fournis par les appareils, même les transactions à haut risque peuvent être effectuées sans étape gênante.



La biométrie comportementale évalue la manière dont un consommateur interagit avec l'appareil, ce qui permet de reconnaître les utilisateurs de confiance et d'identifier avec précision les transactions suspectes.

**6**

## L'AUGMENTATION DE LA CONNECTIVITÉ MONDIALE AMÈNE LES RÉSEAUX DE FRAUDE À ACCROÎTRE LA COMPLEXITÉ DES SCHÉMAS DE FRAUDE

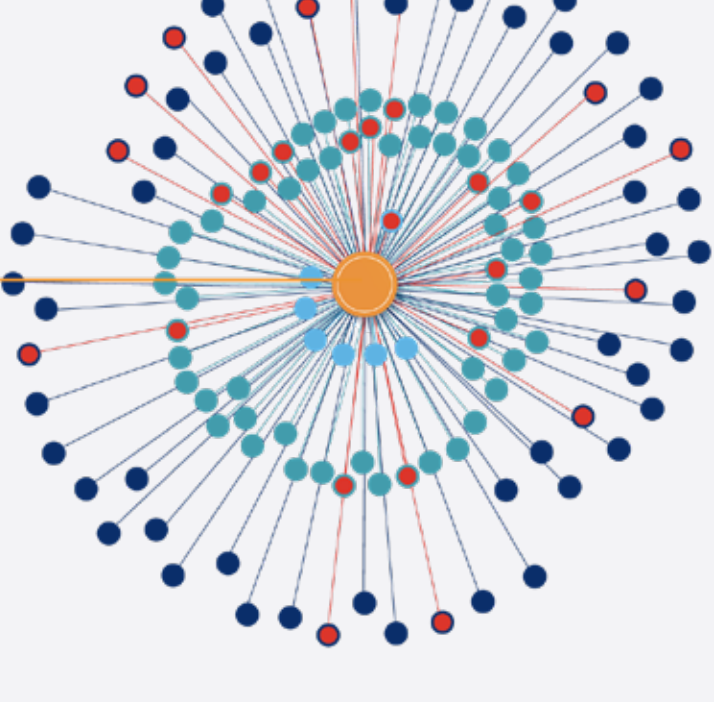
**Les identités synthétiques et volées deviennent plus difficiles à découvrir lorsque les entreprises ne disposent pas du contexte et des informations qui permettent de relier les consommateurs sur l'ensemble des dimensions de l'identité numérique, physique et comportementale à l'échelle mondiale. Les différentes dimensions d'une identité doivent être analysées afin de détecter et d'exposer les schémas de fraude complexes.**

UN RÉSEAU DE FRAUDE EXPLOITANT 63 NUMÉROS DE TÉLÉPHONE ET LOCALISATIONS ÉTAIT LIÉ À UN SEUL E-MAIL⁶

UNE ADRESSE E-MAIL

- 7 adresses IP
- 63 numéros de téléphone
- 63 localisations (63 identités volées)
- 12 pertes à l'intérieur du réseau

Adresses IP    Numéro de téléphone    Adresse    Pertes connues liées à la fraude

**7**

## LES IDENTITÉS MULTIDIMENSIONNELLES DES CONSOMMATEURS EXIGENT UNE RÉPONSE PLUS DYNAMIQUE À CHAQUE ÉTAPE DU PARCOURS⁷



**1 compte créé sur 12** représente une tentative de fraude

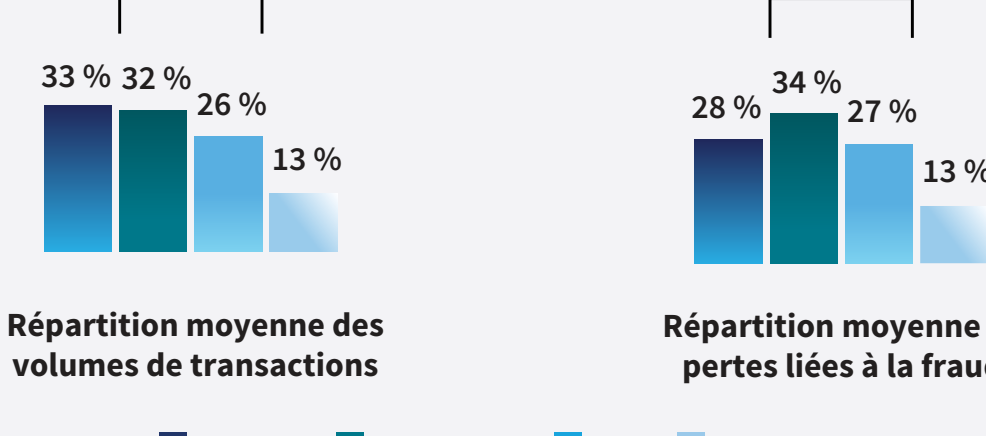


**1 réinitialisation de mot de passe sur 20** est une attaque

**Les approches statiques de la fraude ne permettent pas d'opérer avec succès et en toute sécurité dans le monde interconnecté d'aujourd'hui.**

**Les parcours des consommateurs ne sont plus simplement linéaires et se déroulent souvent sur plusieurs canaux numériques, hybrides et en personne.⁸**

Moyenne mondiale



Répartition moyenne des volumes de transactions

Répartition moyenne des pertes liées à la fraude

■ En personne ■ Navigateur Web ■ Mobile ■ Centre d'appels/Autres

## INSTAURER LA CONFIANCE, AMÉLIORER L'EXPÉRIENCE ET IDENTIFIER LES RISQUES : LES 5 PRINCIPALES STRATÉGIES POUR RÉUSSIR



**Se préparer à l'évolution des processus de gestion de la fraude à mesure que les paiements en temps réel se mondialisent.**



**Donner la priorité aux solutions d'apprentissage automatique avancé, car elles sont en forte progression.**



**Reprendre les réflexions sur le partage des données à l'heure où l'économie interconnectée évolue.**



**Adopter une approche à plusieurs niveaux pour prévenir la fraude.**



**Investir dans l'éducation et la prévention des consommateurs, car l'individu reste la cible principale des fraudeurs.**



Le rapport sur l'état des fraudes et des identités dans le monde de LexisNexis® Risk Solutions expose nos dernières études et réflexions sur les tendances en matière d'identité, les vecteurs de menaces et les technologies qui ont à l'heure actuelle le plus d'impact sur votre stratégie de défense contre la fraude.

**Pour en savoir plus sur chaque tendance, téléchargez le Rapport 2022 sur l'état des fraudes et des identités dans le monde**

**Télécharger maintenant⁹ >>**