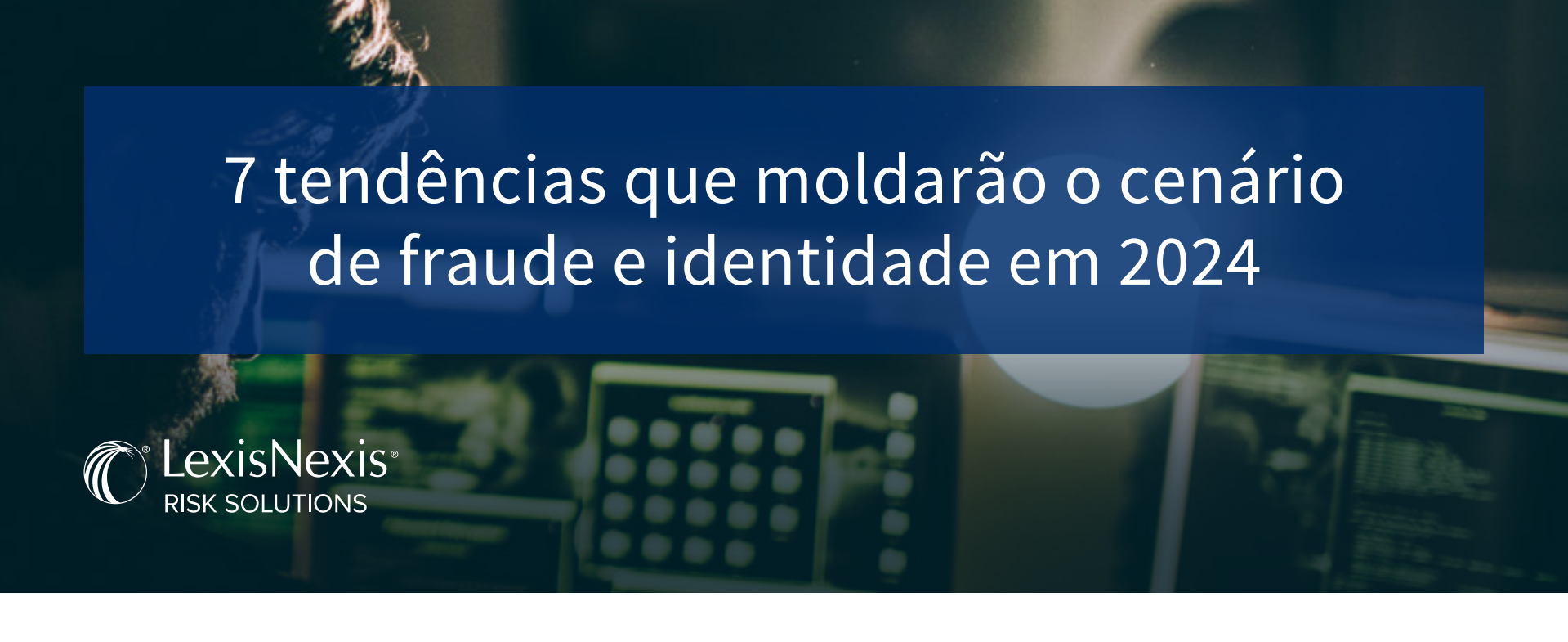


7 tendências que moldarão o cenário de fraude e identidade em 2024

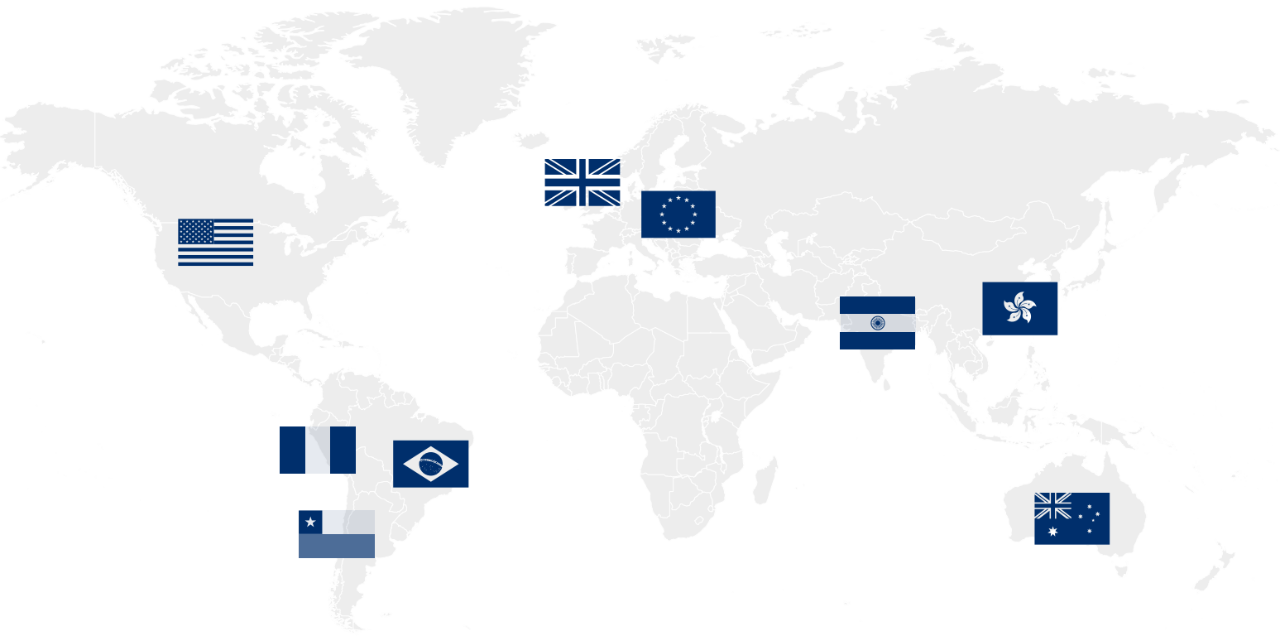
LexisNexis
RISK SOLUTIONS

Os profissionais de fraude e identidade terão de enfrentar desafios crescentes, como o impacto da pressão regulatória adicional em muitas partes do mundo, o problema persistente da fraude de identidade sintética, o uso malicioso de inteligência artificial e a crescente natureza interconectada e transnacional dos ataques de fraudes.

Construir confiança e manter uma experiência positiva do cliente será fundamental. Com oportunidades como a maior adoção da biometria comportamental para combater fraudes complexas, o valor notável de desenvolver uma visão 360 graus do cliente e o vasto potencial de uma abordagem colaborativa para combater a fraude, as organizações podem levar a prevenção de fraudes a novos patamares em 2024.

1 Pressão regulatória adicional provavelmente impactará os custos de gestão de risco

Em 2024, as organizações dedicarão ainda mais recursos para fazer face às crescentes mudanças regulamentares.



EUA: incerteza persistente sobre a responsabilidade por perdas devido a fraudes.

A Lei de Transferência Eletrônica de Fundos poderia ser expandida para incluir fraudes de transferência autorizada. Instituições financeiras com visão de futuro tomam medidas proativas para detectar fraudes e mitigar riscos.

82 %
A maioria dos líderes de serviços financeiros dos EUA responsáveis pelo risco de fraude e estratégias de mitigação acreditam que os consumidores esperam que os bancos os reembolsem por fraudes bem-sucedidas envolvendo as suas contas.[1]

66 %
Os consumidores dos EUA afirmam que provavelmente fechariam as suas contas numa instituição que não os reembolsasse por perdas devido a fraudes de transferências autorizadas.[2]

REINO UNIDO: novos requisitos de pagamento por push autorizado

O regulador do sistema de pagamentos no Reino Unido introduziu um novo sistema de reembolso obrigatório para fraudes de APP, que custou aos consumidores cerca de 630 milhões de dólares no ano passado.[3]

As novas regras exigem que os bancos e outras empresas de pagamento reembolsem as vítimas que foram fraudadas no prazo de alguns dias, com o custo total dividido entre as organizações remetentes e receptoras.

Embora os pagamentos resultantes de fraudes via APP representassem menos de
0,1 %
do volume geral em 2022, métodos de pagamentos mais rápidos são usados em
84 %
dos pagamentos fraudulentos via APP.[4]

Os maiores bancos do Reino Unido relatam até
US$439
perdidos em fraudes via APP para cada US$ 1,26 milhão enviados em transações.[5]

Os pagamentos por push autorizados também são conhecidos como 'golpe de transferência autorizada' nos EUA.

Europa: proposta de nova diretiva sobre serviços de pagamento e serviços em moeda eletrônica (PSD3)

A legislação PSD3 irá desenvolver requisitos para priorizar os interesses, a segurança e a confiança dos consumidores. As propostas incluem:

- Ampliação dos direitos de reembolso para vítimas de fraude.
- Consolidação das instituições de moeda eletrônica e das instituições de pagamento sob um regime regulamentar unificado.
- Garantir que os consumidores tenham uma melhor proteção e compreensão dos seus direitos financeiros.

Embora eficazes na promoção de pagamentos eletrônicos e na redução da fraude, os custos de implementação da PSD2 são estimados em
US$5,41 bilhões de dólares,
e o aumento substancial nas taxas de falha nas transações estimado em
US$36,2 bilhões de dólares,
foram substanciais.[6]

As instituições que não cumprirem os requisitos do PSD2 podem ser multadas até
4 %
dos seus retornos anuais.

América Latina: novas regulamentações sobre jogos e apostas

O mercado regulamentado de jogos de azar online da América Latina deverá quadruplicar de tamanho e atingir US$ 6,75 bilhões em receitas anuais até 2027, atraindo jogadores genuínos e mal-intencionados.[8]

No Brasil, uma nova lei para apostas e jogos de azar online foi aprovada em 2023, regulamentando um mercado informal que gera mais de
US$30 bilhões
todos os anos[9]

O governo chileno apresentou recentemente um projeto de lei para legalizar efetivamente os jogos de azar online. Estima-se que um mercado legalizado poderia gerar receitas de mais de
US$350milhões
de dólares por ano.[10]

No Peru, foram aprovados regulamentos para apostas desportivas e jogos, criando mecanismos para proteger os jogadores de potenciais e reais fraudes.

Hong Kong: segurança aprimorada de e-banking

A Autoridade Monetária de Hong Kong introduziu medidas adicionais que aumentam a segurança bancária online e combatem a fraude digital. Os requisitos são obrigatórios para todas as atividades de e-banking e incluem:

Autenticação adicional do cliente.
- Revisão dos limites de transferência transnacional.
- Controles de gerenciamento de sessão que evitam tentativas fraudulentas de login.
- Adoção de plataforma piloto de compartilhamento de informações entre bancos, que permite aos bancos partilhar informações sobre riscos e tomar medidas de mitigação mais ágeis.

Índia: uma nova direção em segurança cibernética, controles de risco e governança de TI

As entidades bancárias e não-bancárias regulamentadas terão de cumprir o novo conjunto de regras emitido pelo Reserve Bank of India em 2023, incluindo um quadro abrangente de governança de TI para mitigar os riscos do crime cibernético.

Dos quase 53.000 casos de crimes cibernéticos registados em 2021,
60 %
eram fraudes.[11]

Austrália: regulamentação para provedores de pagamento digital

As novas regras propostas pelo governo australiano visam regular os fornecedores de carteiras digitais, permitindo ao Reserve Bank of Australia monitorar estas transações da mesma forma que as redes de cartões de crédito.

Aumento nas transações de carteira móvel na Austrália[12]

US$29,2milhões
2018

US$2,4bilhões
2022

2 Explosão do uso de identidades sintéticas

Os criminosos exploram a popularidade do digital banking e do comércio eletrônico para abrir novas contas fraudulentas com identidades sintéticas, que combinam informações reais e fabricadas. Combater a fraude é um desafio complexo que será uma prioridade crescente em 2024.

48 % dos varejistas e **53 %** das instituições financeiras afirmam que o aumento das identidades sintéticas é o principal fator que contribui para dificultar a verificação de identidade nos canais online[13]

Porcentagem de empresas que relatam um aumento na fraude de identidade sintética por região

52 %
de empresas em todo o mundo relatam um aumento em fraudes de identidade sintética em 2023[14]

US$23bilhões
Valor esperado das perdas devido a fraude de identidade sintética nos EUA até 2030[15]

US$81,000 para US$98,000[16]
É a perda média de uma fraude de identidade sintética não detectada

Porcentagem de executivos de fraude e risco que classificam o aumento das identidades sintéticas como o principal desafio que contribui para a verificação de identidade durante...

55 %	55 %	57 %
Abertura de conta	Login	Transferências / distribuição de fundos [17]

3 O aumento do uso de inteligência artificial por criminosos exigirá novas táticas de mitigação de riscos

A utilização da inteligência artificial (IA) com intenções maliciosas está modificando o cenário da fraude e do risco, aumentando a eficácia dos esforços dos fraudadores e colocando novos desafios para estabelecer e provar a identidade de alguém.

66 %
Dos profissionais de segurança cibernética detectaram ataques deepfake em suas organizações em 2022[18]

90 %
Estima-se que dos conteúdos online serão gerados sinteticamente até 2026[19]

4 Aumento do uso da inteligência comportamental para combater fraudes complexas

A biometria comportamental está se tornando uma ferramenta essencial para empresas e organizações construírem a confiança dos consumidores e reduzirem fraudes cada vez mais sofisticadas. As empresas com visão de futuro que desejam elevar a sua estratégia de prevenção de fraudes e defender-se contra golpes sofisticados estão adotando a biometria comportamental.

A inteligência comportamental pode ser aplicada em qualquer ponto da jornada do usuário, atuando como uma defesa contra algumas das variedades mais desafiadoras de golpes direcionados aos consumidores, como golpes via APP e golpes de acesso remoto, bem como outras formas complexas de fraude.

48 %
Dos executivos da área de fraude classificaram os ataques fraudulentos ao consumidor entre as suas principais preocupações em 2022.[21]

US$612 milhões
Perdas devido a golpes de pagamento push autorizado (APP) no Reino Unido em 2022.[23]

35 %
Das organizações dos entrevistados, em empresas de serviços financeiros dos EUA, implementaram soluções de biometria comportamental até setembro de 2023.[22]

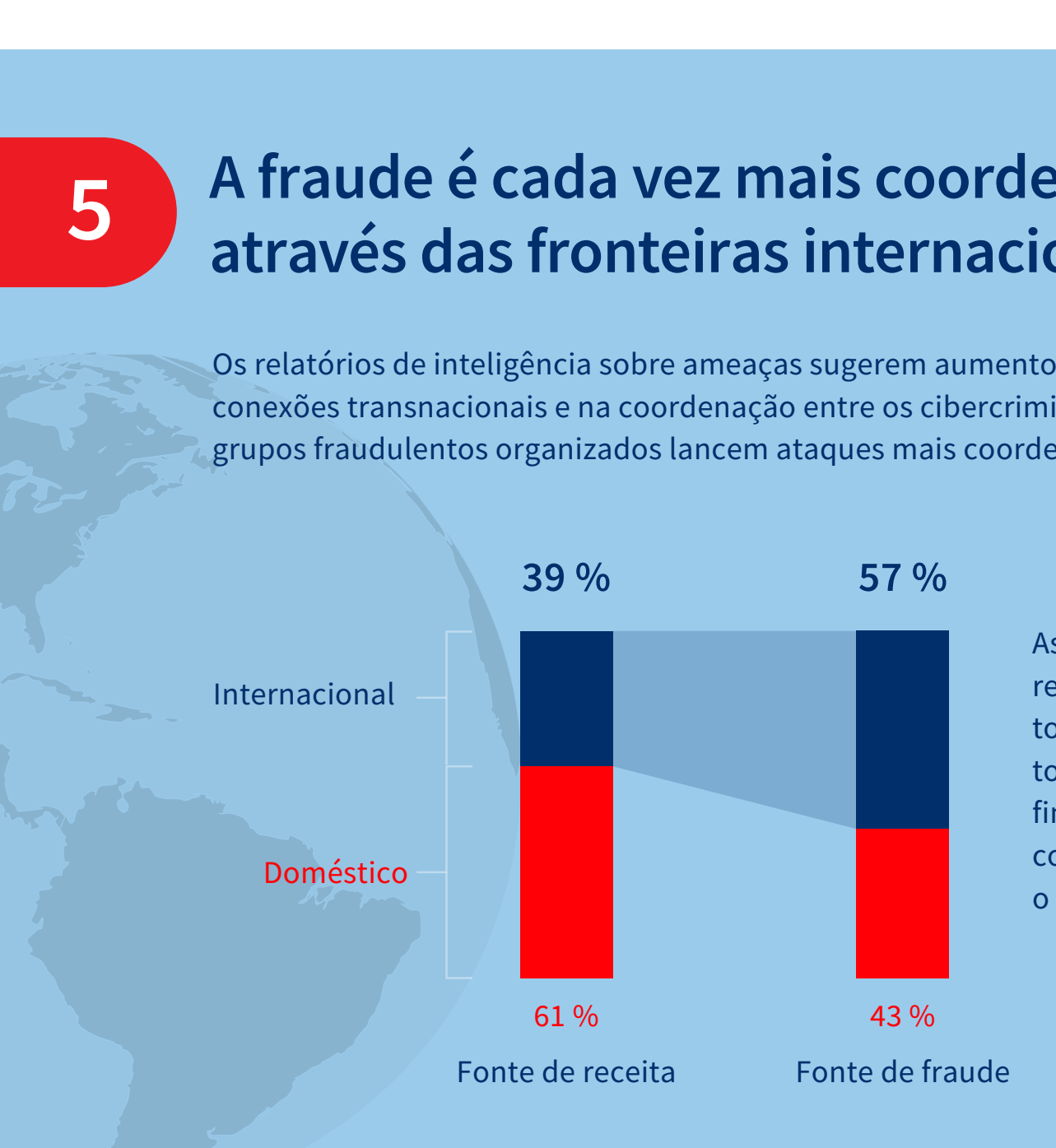
Globalmente,
1/3
das organizações utilizam soluções de biometria comportamental ao longo da jornada do cliente.[24]

Fatores-chave para a adoção de soluções de biometria comportamental[25]

- Acelerando a digitalização
- Fraude na abertura de nova conta.
- Fraude de controle de conta
- Fraudes/golpes de pagamento push autorizado (APP)
- Necessidades fortes de autenticação do cliente
- Conheça seu cliente e as regulamentações contra lavagem de dinheiro
- Mudanças regulatórias na responsabilização
- Melhor experiência do cliente

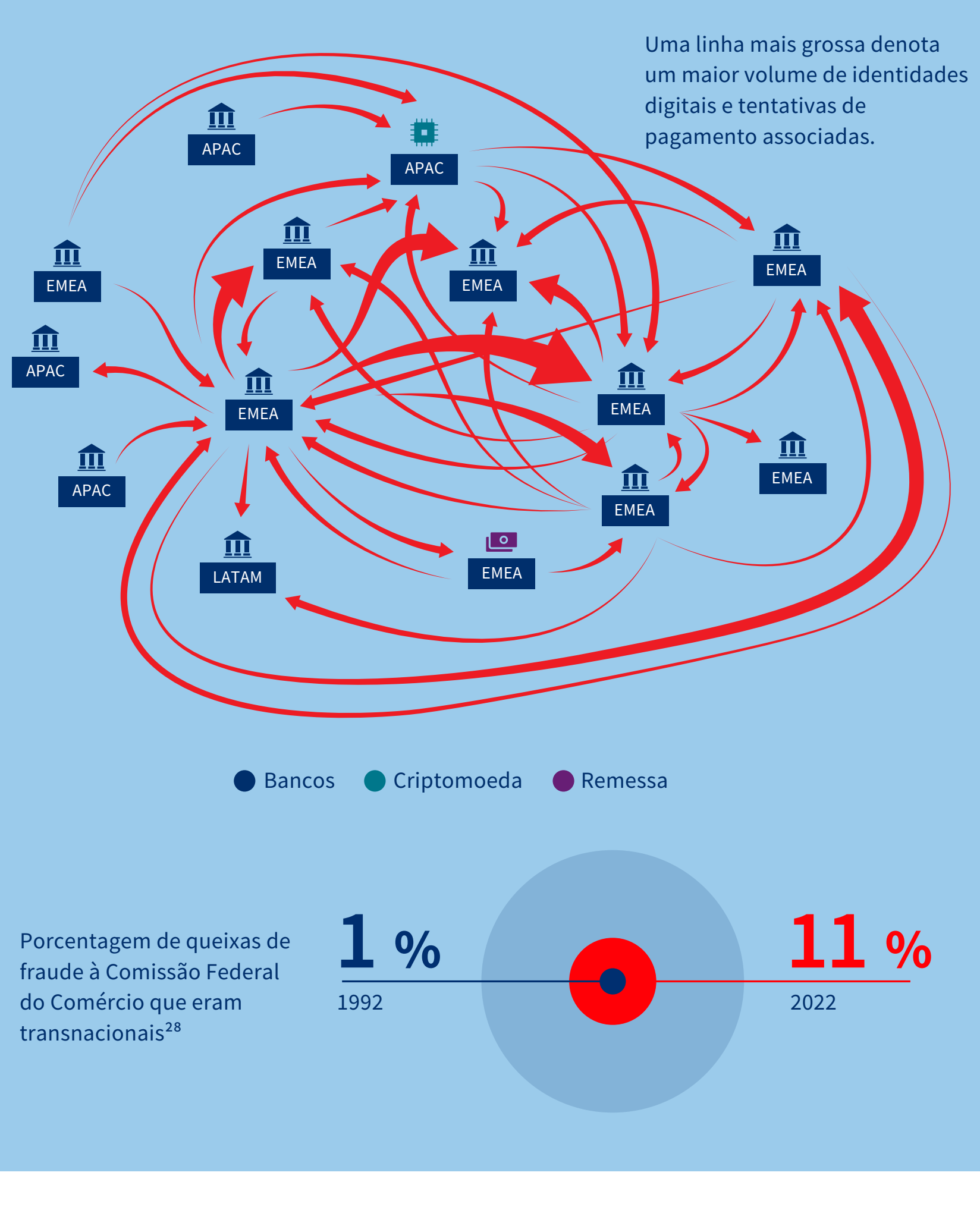
5 A fraude é cada vez mais coordenada através das fronteiras internacionais

Os relatórios de inteligência sobre ameaças sugerem aumentos significativos nas conexões transnacionais e na coordenação entre os cibercriminosos. Esperemos que grupos fraudulentos organizados lancem ataques mais coordenados em 2024.



As receitas internacionais representam 39% da receita total, mas abrigam 57% do total de fraudes para serviços financeiros e organizações de comércio eletrônico em todo o mundo.[26]

As redes de "contas laranjas" ligadas por identidades digitais operam em regiões e instituições financeiras, fazendo tentativas de pagamento a uma organização e depois passando para outras.[27]



Uma linha mais grossa denota um maior volume de identidades digitais e tentativas de pagamento associadas.

Porcentagem de queixas de fraude à Comissão Federal do Comércio que eram transnacionais[28]

1 %
1992

11 %
2022

6 Adotar uma visão 360 graus do cliente está se tornando imperativo para melhorar a avaliação de riscos

Uma abordagem mais integrada e eficaz à gestão de fraudes começa com a compreensão da multiplicidade de canais e interações que os clientes utilizam para interagir com as empresas.

82 %
Dos consumidores que fazem compras on-line com cartão de crédito também são usuários ativos de serviços bancários on-line do mesmo banco que emitiu o cartão de crédito, o que significa que a inteligência de identidade digital pode ser compartilhada entre canais para gerar confiança e evitar fraudes mais complexas.[29]

3/4
Dos entrevistados relatam que a fraude impactou negativamente a sua marca e a experiência de seus clientes.[30]

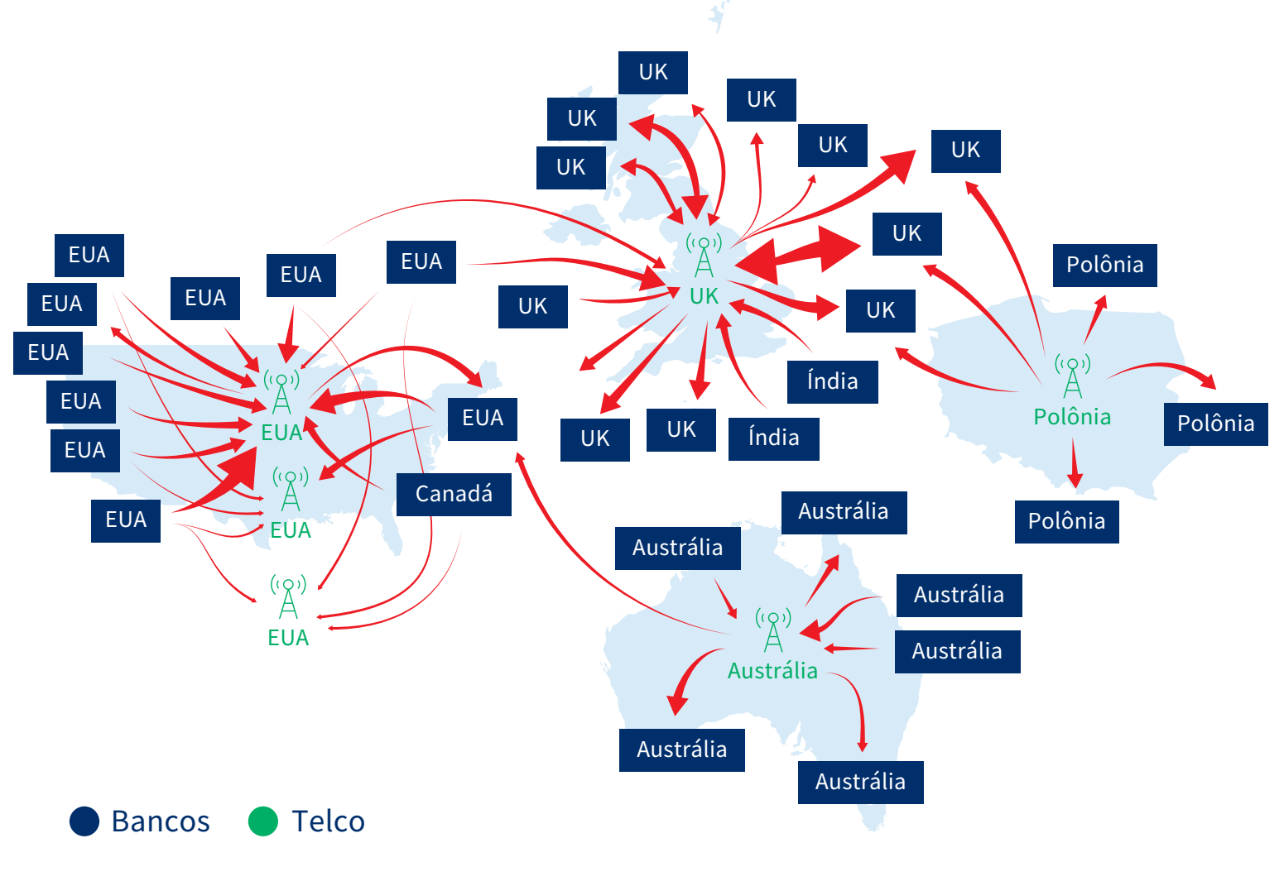
133 %
Aumento no número de bancos que usam LexisNexis® Digital Identity Network® em canais bancários digitais e 3D Secure CNP em 2022 em comparação com 2021.[31]

60 %+
Melhoria na avaliação de risco durante eventos de pagamento subsequentes, reunindo inteligência digital contextual no login.[32]

7 Combate colaborativo à fraude

Iniciativas de compartilhamento de informações, inteligência coletiva, coordenação de remoções e mecanismos de comunicação unificados são a forma como as empresas de segurança cibernética continuarão a colaborar para combater as crescentes ameaças de fraude.

LexisNexis® Risk Solutions analisa aproximadamente 80 bilhões de transações em todo o mundo todos os anos. A LexisNexis® Digital Identity Network® coleta insights de milhares de empresas em todo o mundo, construindo um repositório líder de inteligência de identidade digital que se torna mais poderoso a cada transação.



Esta rede fraudulenta mostra apenas conexões de mais de 10 identidades digitais.

Uma linha mais grossa denota um maior volume de ataques. Esta visualização mostra redes regionais de fraude visando bancos e operadoras de redes móveis.

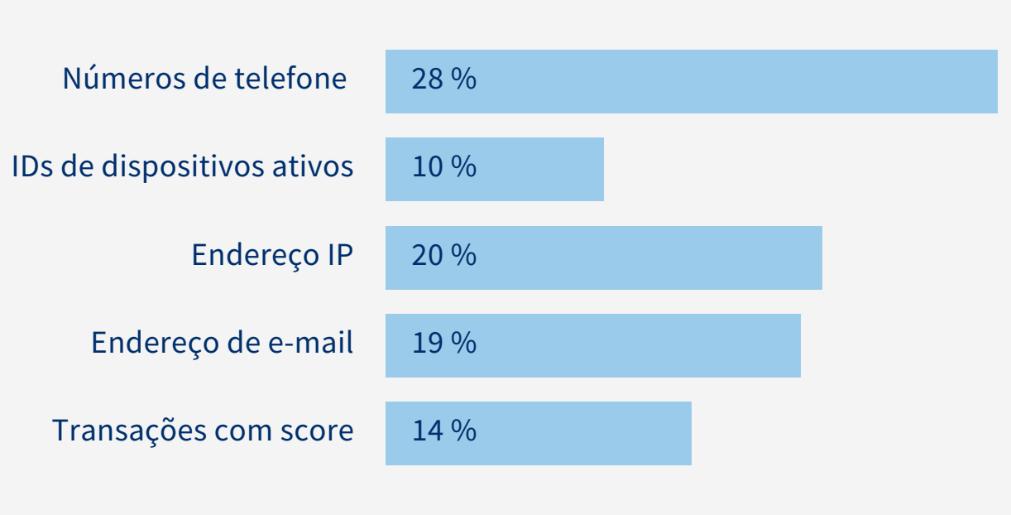
À medida que os ataques ao setor financeiro se tornam mais complexos, os fraudadores iniciarão frequentemente os seus ataques obtendo novos contratos de telefonia móvel ou assumindo o controle de contas de clientes de telefonia móvel existentes para utilização posterior em tentativas de apropriação de contas bancárias ou fraude de novas contas.

Pelo menos
US$2,4milhões
em valor de fraude bloqueado

Pelo menos
US$10,3milhões
foi exposto a fraudes em toda a rede[33]

Os principais elementos de dados da LexisNexis® Digital Identity Network® estão crescendo rapidamente.

Taxa de crescimento anual por elemento de dados[34]



Números de telefone	28 %
IDs de dispositivos ativos	10 %
Endereço IP	20 %
Endereço de e-mail	19 %
Transações com score	14 %

LexisNexis® Digital Identity Network®

Países e territórios vistos na Digital Identity Network®[35]

A cada segundo	90
A cada minuto	193
A cada hora	230
Todos os dias	238
Todo mês	245
Todos	249

LexisNexis
RISK SOLUTIONS

Sobre a LexisNexis Risk Solutions

LexisNexis® Risk Solutions inclui sete marcas que abrangem vários setores e indústrias. Aproveitamos o poder dos dados, plataformas analíticas sofisticadas e soluções tecnológicas para fornecer insights que ajudam empresas e entidades governamentais a reduzir riscos e melhorar decisões para beneficiar pessoas em todo o mundo. Com sede na região metropolitana de Atlanta, Geórgia, temos escritórios em todo o mundo e fazemos parte da RELX (LSE: REL/NYSE: RELX), fornecedora global de análises baseadas em informações e ferramentas de decisão para clientes profissionais e empresariais. Para obter mais informações, visite LexisNexis Risk Solutions e 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 E¬orts 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 Network®