10 tendências que irão moldar o cenário de fraudes em 2022.

LexisNexis® RISK SOLUTIONS

Muitas organizações enfrentam obstáculos cada vez maiores com relação à detecção e prevenção a fraudes. Os consumidores continuam migrando para os canais digitais e, mesmo que as organizações estejam lucrando com isso, ela também tem um custo.

Os fraudadores vão aonde as operações ocorrem, em busca de novos pontos vulneráveis a serem explorados.

Seguem aqui as nossas previsões para as 10 principais tendências a serem observadas por apresentarem maior probabilidade de impactar os orçamentos e as ações relacionadas a fraudes no ano que se inicia.

01 A transformação digital não deve desacelerar

Os efeitos da pandemia aceleraram anos na digitalização das interações dos clientes. Ao mesmo tempo em que as empresas disponibilizam os seus serviços no espaço digital, os clientes também se sentem mais à vontade e confiantes em consumi-los de maneira online.

Embora a transformação digital estivesse em alta antes da pandemia, ela assumiu uma nova urgência com a sua chegada. A pandemia basicamente mudou como as pessoas interagem com as empresas, colocando todo um grupo inexperiente de usuários digitais à disposição dos fraudadores.

A média global da participação das interações dos clientes que são digitais cresceu 22%[1].

21% APAC

23% Europa

24% EUA

02 Maior automação

Automação é uma faca de dois gumes. Embora simplifique a jornada do cliente ao oferecer preenchimento automático e outras mordomias, também facilita os ataques por parte dos fraudadores, gerando maiores volumes de investidas. Metodologias automatizadas também podem causar mais danos mais rapidamente.

1,2 bilhões
Número de ataques de bots na primeira metade de 2021

representando **41%** do crescimento global a.a.

O volume de ataques de bots subiu **28%** nos serviços financeiros

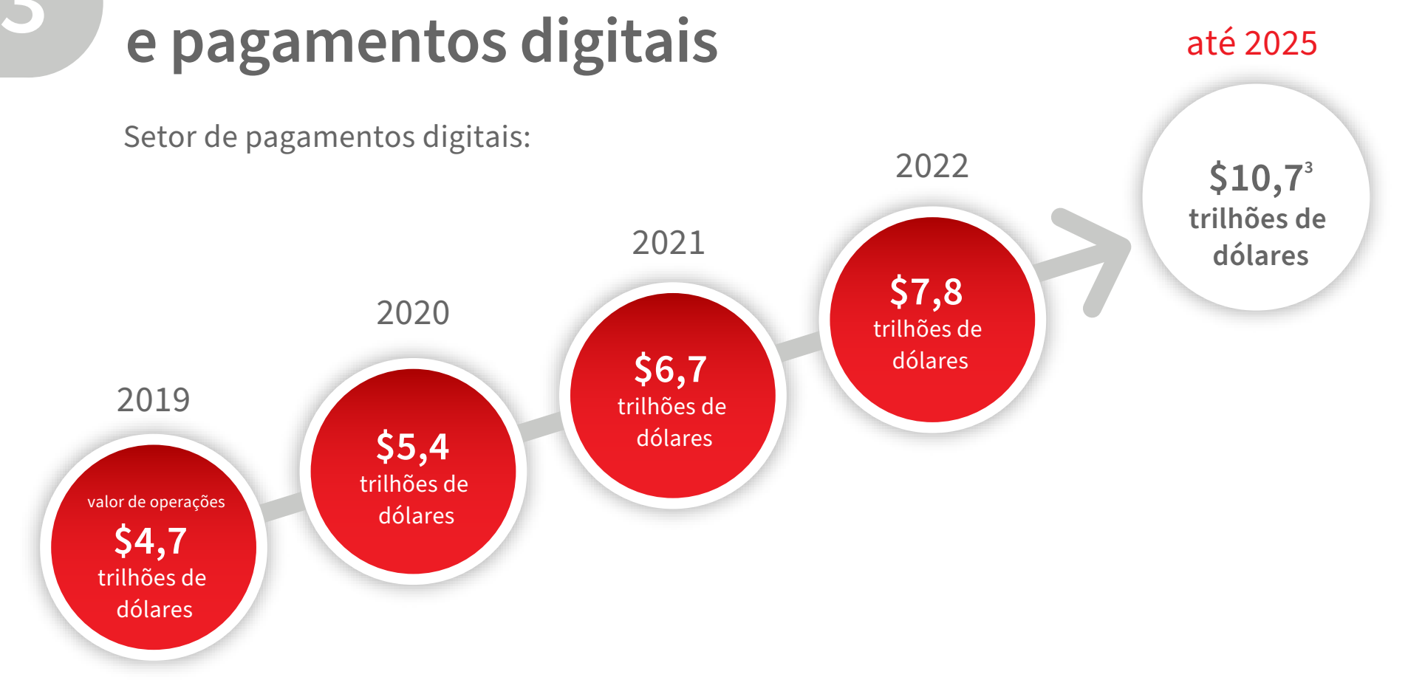
A Mídia foi bastante atingida com o volume de bots disparando **174%**

Os ataques de bots na jornada do cliente também estão em ascensão:

Logins	Pagamentos	Criação de novas contas
52%	18%	8,9%
Crescimento nas tentativas de invasão a contas.	Crescimento (provavelmente testes de credenciais roubadas de cartão de crédito).	Ocorrências de ataques, a maior entre todos os casos de uso.[2]

03 Adoção de novos métodos e pagamentos digitais

Setor de pagamentos digitais:



Novas opções de pagamentos digitais oferecem criação de contas sem esforço e rápido acesso a crédito, o que abre as portas para ataques de fraudadores usando credenciais roubadas.

Os consumidores amam comprar agora e pagar depois (BNPL)...

Mais de **17 milhões**
Número de consumidores que usaram BNPL no Reino Unido.[4]

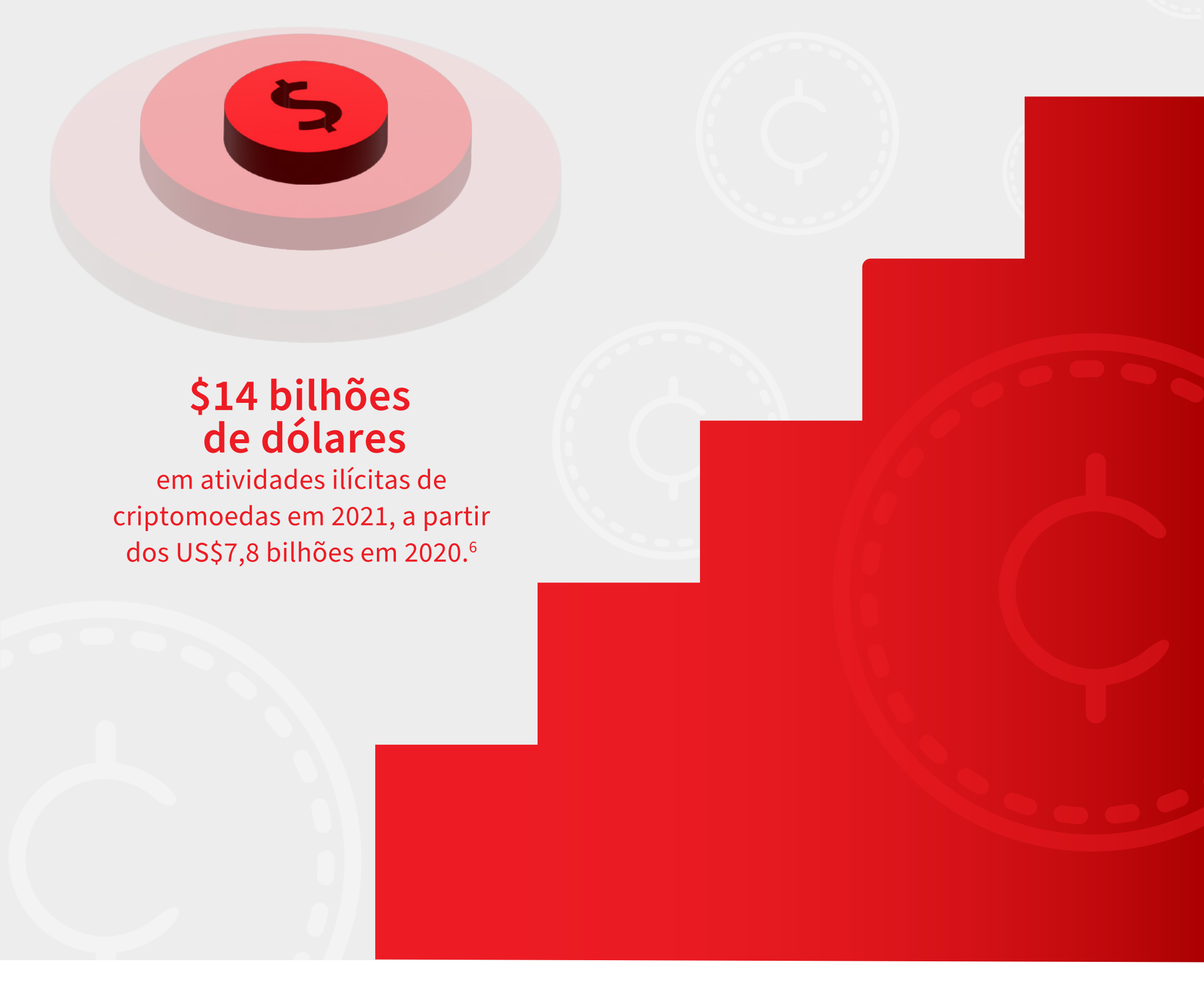
Mais de **400 %**
Crescimento de BNPL de 2020 a 2021 nos EUA.

U.S. **$ 1 trilhão**
Volume bruto global previsto de mercadorias do setor de BNPL até 2025.[5]

...e os fraudadores também.

As maiores plataformas de BNPL divulgaram um aumento acentuado de fraudes, principalmente em criação de novas contas, invasão a contas e reembolsos com cartões de crédito roubados.

As criptomoedas também representam um desafio cada vez maior, já que a falta de transparência que proporcionam faz com que sejam a moeda de escolha para golpes, pagamentos de resgate, lavagem de dinheiro e outras atividades ilícitas.



$14 bilhões de dólares
em atividades ilícitas de criptomoedas em 2021, a partir dos US$7,8 bilhões em 2020.[6]

04 Maior risco de fraudes de pagamento

Os clientes adoram a conveniência das operações digitais. No mundo todo, estima-se que o mercado de pagamentos digitais supere os US$ 236 bilhões até 2028, uma taxa de crescimento anual composta (CAGR) de 19,4%.[7]

Entretanto, um aumento na atividade das operações digitais também atrai os fraudadores, já que a consciência sobre segurança de dados não cresce na mesma velocidade. Por exemplo, as tentativas de fraudes digitais saltaram quase 150% nos serviços financeiros.[8]

Prejuízo global estimado para o comércio eletrônico por conta de fraudes de pagamento online em 2021:

$20 bilhões de dólares
o que representa um aumento de 14% em relação a 2020.[9]

70%
das operações fraudulentas de internet banking tiveram origem nos canais móveis durante o segundo trimestre de 2021, 63% a mais que no ano anterior. As fraudes de aplicativos bancários móveis foram responsáveis pelo maior aumento.[10]

Enquanto prejuízos por fraudes ocorrem por toda a jornada do cliente, a criação de novas contas e os pontos de distribuição parecem ser os mais suscetíveis às fraudes nos EUA.[11]

05 A crescente prevalência de golpes

Golpes de invasão a contas (ATO) e de engenharia social, inclusive pagamento push autorizado (APP), romances, fraudes de investimento e de falsificação de identidade, estão se tornando os crimes financeiros que crescem com maior velocidade.
Na realidade, 98%[12] dos ataques cibernéticos são baseados em engenharia social.
Esses golpes representam um desafio global emergente pela dificuldade em detectá-los.

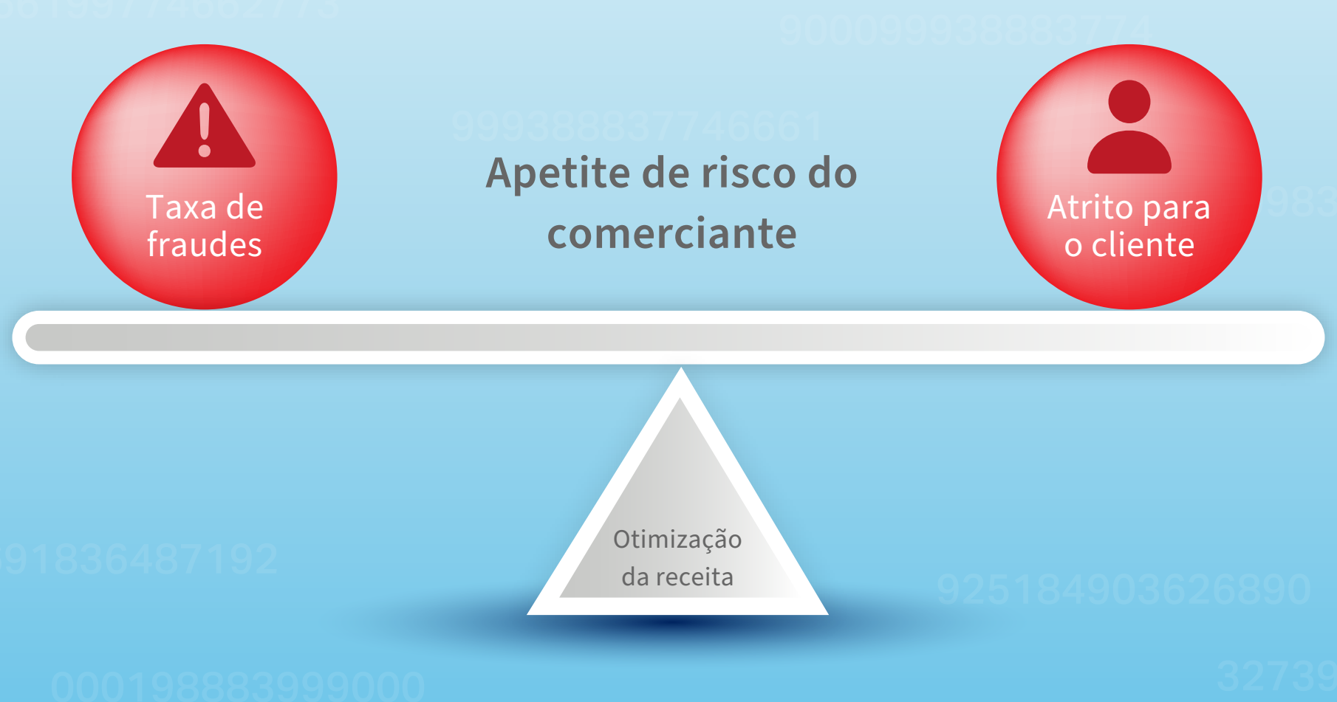
Reino Unido
As fraudes de APP saltaram **71%** no primeiro semestre de 2021, com prejuízo somado em mais de US$482.[13] Isso, em comparação aos US$648 (£479) milhões em todo o ano de 2020.[14]

Austrália
Prejuízo de mais de **$126 milhões de dólares** somente em golpes de investimento, o mais alto entre as categorias.[15]

EUA
Prejuízo de quase **$1,2 bilhões de dólares** em golpes de falsificação de identidade em 2020, impactando aproximadamente uma em cada cinco pessoas.[16]

06 Desafio contínuo para equilibrar fraudes e atrito

As empresas continuam lutando para encontrar um equilíbrio entre oportunidade e risco. Embora cada informação pessoal adicional fornecida pelos consumidores possa ajudar a diminuir o volume de fraudes, ela também adiciona atrito à jornada do usuário, o que pode afastá-lo de uma operação. É ainda mais difícil alcançar o equilíbrio entre fraudes e atrito nos diversos canais (ex.: móvel, internet, ponto de venda).



A correspondência incorreta dos métodos de autenticação com o risco da operação pode gerar atritos na jornada do cliente, causando queda nas conversões. Para manter a ocorrência de fraudes baixa e fornecer o volume certo de atrito, os comerciantes e emissores buscam por soluções alternativas de autenticação para maximizar a experiência do cliente e minimizar atrito desnecessário durante os processos de *onboarding* e de finalização de compra.

07 A ascensão das identidades sintéticas

A criação de novas identidades combinando elementos de informações reais e falsificadas é um dos crimes online que mais crescem nos EUA.[17]
Incentivados pelo aumento no uso de internet banking e de outros serviços financeiros digitais, as fraudes de identidade sintética tornaram-se um desafio multimilionário. É também um dos tipos mais difíceis de roubo de identidade para empresas e instituições financeiras detectarem porque não há uma pessoa real para denunciar a fraude.

Como as identidades sintéticas funcionam

Os fraudadores pegam trechos de dados legítimos + adicionam informações fictícias = criam uma nova identidade

Como o crédito de informações de dados legítimos é construído

- Solicitação de cartões de crédito
- Tomada de empréstimos
- Abertura de contas bancárias
- Inscrição a benefícios fornecidos pelo governo

08 O aumento no custo das fraudes

A pandemia levou, mais do que nunca, os consumidores para os canais online e móveis. Os fraudadores foram logo atrás, o que resultou no aumento do volume de ataques e, consequentemente, do custo das fraudes, ambos significativamente mais altos agora do que antes do início da pandemia.

$5,4 trilhões de dólares
Custo global das fraudes[18]

9,9%
Aumento do custo das fraudes para as empresas de serviços financeiros nos EUA. Cada US$ 1 perdido em fraudes custa US$4,00 às empresas de serviços financeiros nos EUA. (Comparado a US$3,25 em 2019 e US$3,64 em 2020).[19]

Na APAC, as operações fraudulentas custaram até 3,87 vezes o valor da operação perdida, acima dos 3,40 de 2019.[20]

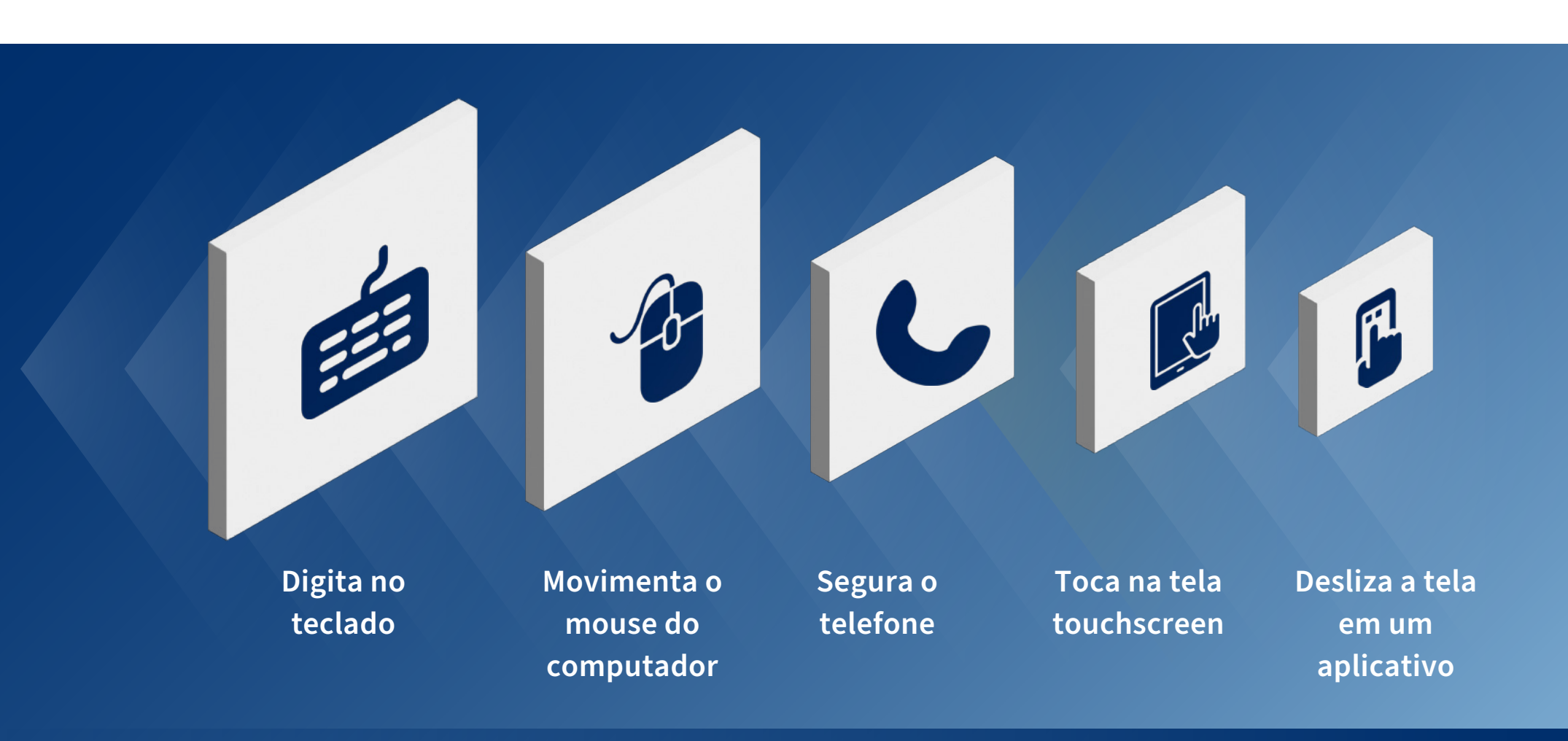
As operações fraudulentas na LATAM custaram até 3,68 vezes o valor da operação perdida em 2020, acima dos 3,46 de 2019.[21]

No Reino Unido, estima-se que o prejuízo por fraudes seja de **$185 bilhões de dólares.**[22]

09 Maior necessidade por avaliação de fraudes em multicamadas

Os fraudadores de hoje aplicam golpes complexos e de múltiplos vetores, além de estarem sempre desenvolvendo novas estratégias para burlar os controles e explorar as vulnerabilidades. Uma abordagem em multicamadas que inclua identidade física, inteligência de identidade digital e biometria comportamental é uma das melhores defesas para diminuir o risco de fraudes.

A biometria comportamental analisa como um usuário:

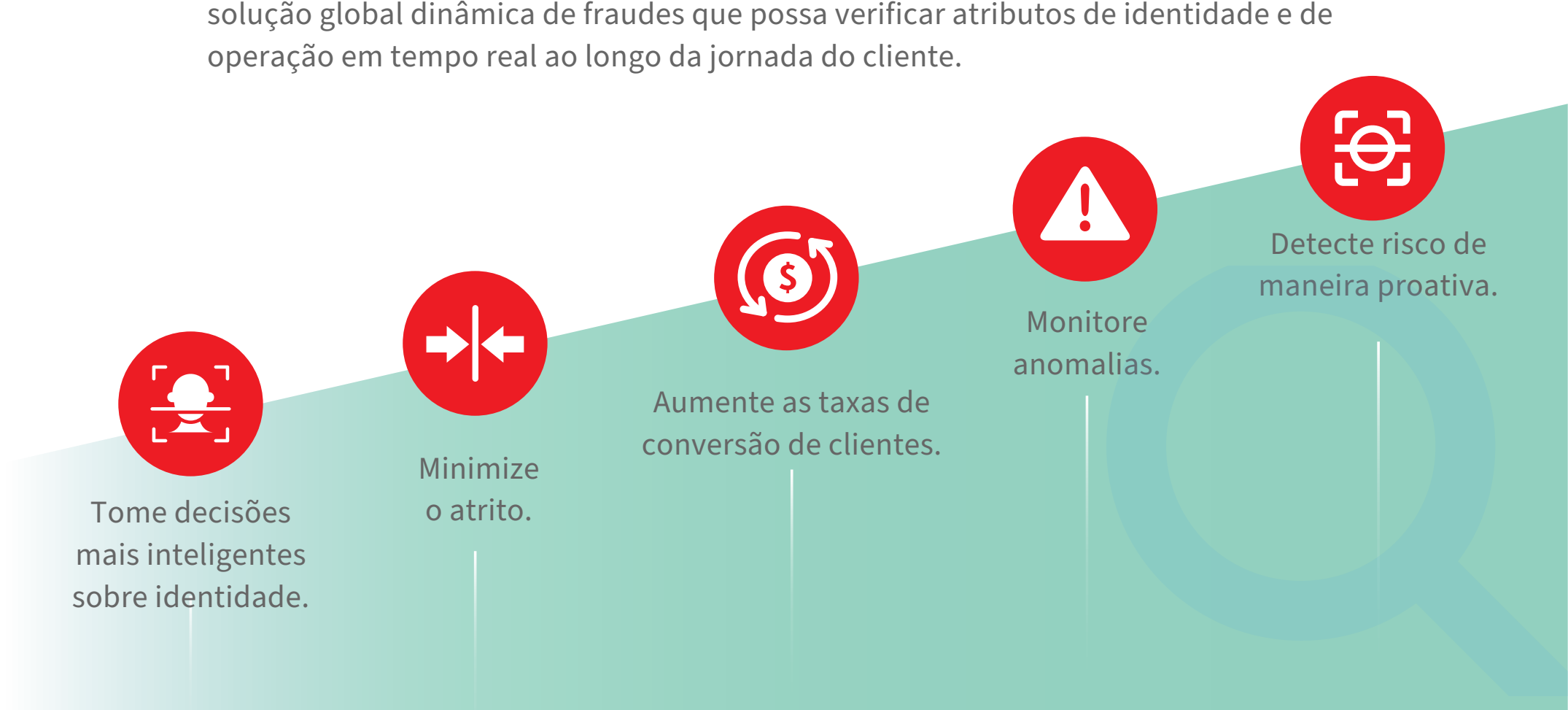


O Behavioral Biometrics pode ser usado para:

- **Detectar bots e agregadores;**
- **Identificar perfis dos verdadeiros clientes;**
- **Definir o perfil de fraudadores com confiança;**
- **Reconhecer interações incomuns;**
- **Fortalecer a confiança dos verdadeiros clientes.**

10 Maior necessidade da avaliação dos riscos em tempo real

A tendência de alta das atividades online e móvel ressalta a necessidade de uma solução global dinâmica de fraudes que possa verificar atributos de identidade e de operação em tempo real ao longo da jornada do cliente.



Aproveitar as mais novas ferramentas, inteligência e tecnologia pode ajudar as organizações a reduzir o risco de fraudes e ficar à frente das estratégias criminosas em rápida evolução.

Veja como a LexisNexis® Risk Solutions reúne gestão de fraudes, verificação de identidade e informações sobre risco utilizando inteligência de rede, cobertura global reconhecida pelo setor e propriedade intelectual para permitir que a sua empresa diferencie, com confiança, entre um verdadeiro cliente e uma ameaça, ao mesmo tempo em que mantém a experiência do cliente ininterrupta.

LexisNexis® RISK SOLUTIONS

Fontes:

[1] https://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
[2] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf
[3] https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide#transaction-value
[4] https://www.bbc.com/news/business-59433904
[5] https://www.cbinsights.com/research/report/buy-now-pay-later-outlook/#today
[6] https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
[7] https://www.businesswire.com/news/home/20211124006042/en/Global-Digital-Payment-Market-Report-2021-Transactions-Worth-7-Trillion-is-Expected-to-Shift-from-Cash-to-Card-and-Digital-Payments-by-2023---Forecast-to-2028---ResearchAndMarkets.com#:~:text=The%20global%20digital%20payment%20market,the%20fintech%20sector's%20technological%20developments
[8] https://www.propertycasualty360.com/2021/06/22/fraudsters-targeting-financial-services-more-than-any-other-industry-in-2021-414-204577/?slreturn=20220117094312
[9] https://www.businesswire.com/news/home/20210425005002/en/Juniper-Research-eCommerce-Losses-to-Online-Payment-Fraud-to-Exceed-20-Billion-Annually-in-2021/
[10] https://www.outseer.com/wp-content/uploads/Outseer-Fraud-Report-Q32021.pdf
[11] https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices
[12] https://purplesec.us/resources/cyber-security-statistics/
[13] https://www.finextra.com/newsarticle/38884/app-fraud-losses-overtake-card-crime-in-h1-2021
[14] https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
[15] https://www.scamwatch.gov.au/scam-statistics
[16] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
[17] https://www.fbi.gov/audio-repository/ftw-podcast-synthetic-ids-010220.mp3/view
[18] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf
[19] https://risk.lexisnexis.com/about-us/press-room/press-release/20220106-annual-true-cost-of-fraud-study
[20] https://risk.lexisnexis.com/global/en/insights-resources/research/apac-true-cost-of-fraud-study#:~:text=Depending%20on%20the%20market%2C%20the,other%20APAC%20markets%20at%203.40
[21] https://www.prnewswire.com/news-releases/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
[22] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf

---

Sobre a LexisNexis® Risk Solutions

A LexisNexis® Risk Solutions explora o poder dos dados e da análise avançada para fornecer informações a empresas e entidades governamentais com a finalidade de reduzir riscos e auxiliar na tomada de decisões que beneficiem pessoas ao redor do mundo. Fornecemos soluções de dados e tecnologia para uma ampla gama de setores, incluindo seguros, serviços financeiros, assistência médica e governo. Com sede na área metropolitana de Atlanta, Geórgia, temos escritórios em todo o mundo e fazemos parte da RELX (LSE: REL/NYSE: RELX), uma fornecedora global de análises baseadas em informação e ferramentas para tomada de decisões voltada para profissionais e empresas.

Para maiores informações, acesse www.risk.lexisnexis.com e www.relx.com. Nossas soluções ajudam as organizações a prevenir crimes financeiros, assegurar o compliance regulatório, mitigar riscos empresariais, melhorar a eficiência operacional e aumentar a rentabilidade.