TransUnion

ATUALIZAÇÃO | 1º SEMESTRE DE 2026:

PRINCIPAIS TENDÊNCIAS DE FRAUDE

Mais de um quarto dos consumidores alegou ter perdido dinheiro em fraudes digitais no último ano

Resumo executivo

A fraude digital está mudando de perfil. Cada vez mais, os criminosos deixam de explorar apenas falhas técnicas e passam a se passar por pessoas ou empresas confiáveis para enganar consumidores e acessar contas ou dados sensíveis. Com isso, a fraude deixa de ser apenas um custo operacional e passa a representar um risco direto para a receita, o crescimento e a confiança nas empresas.

Esse impacto já é percebido pelos consumidores. Em 2025, as fraudes digitais geraram perdas estimadas em US$ 99 bilhões nos Estados Unidos. Além disso, cerca de 1 em cada 6 consumidores (16%) disse ter sido vítima de algum tipo de golpe — um sinal claro de que o problema já faz parte do dia a dia das pessoas.

Ao mesmo tempo, as empresas enfrentam um cenário aparentemente paradoxal. A taxa global de tentativas suspeitas de fraude digital recuou para 3,8% em 2025, o menor nível dos últimos anos. Ainda assim, os ataques estão mais sofisticados, mais direcionados e mais difíceis de identificar.

Um dos principais sinais dessa mudança é o aumento da invasão de contas (ATO). Esse tipo de fraude cresceu 37% em um ano e passou a representar 3,14% das transações suspeitas de fraude digital em 2025. Esse movimento reflete uma mudança mais ampla na forma como os fraudadores atuam.

Os criminosos estão explorando cada vez mais vazamentos de dados, phishing e engenharia social para obter acesso a informações reais e enganar consumidores. Assim, aplicam golpes mais difíceis de detectar — invadem contas com dados roubados, criam perfis falsos que parecem legítimos ou convencem a própria vítima a autorizar uma transação acreditando estar falando com uma empresa confiável.

Ao mesmo tempo, os consumidores estão mais atentos e exigentes. A segurança dos dados pessoais se tornou um dos fatores mais importantes na escolha de uma empresa para realizar transações online.

Nesse cenário, o desafio das empresas vai além de bloquear tentativas de fraude. É preciso verificar, de forma consistente e ao longo de toda a jornada digital, se o usuário é realmente quem diz ser. Estratégias que combinam dados de identidade, comportamento e dispositivos, apoiadas por inteligência artificial, permitem reduzir atrito, fortalecer a confiança e identificar riscos com mais precisão.

PONTOS IMPORTANTES

Golpes cada vez mais convincentes afetam a confiança – e o bolso dos consumidores

26%
dos consumidores disseram ter perdido dinheiro em fraudes digitais no último ano.

77%
dos consumidores mencionaram que a confiança na segurança de seus dados pessoais é o fator mais importante ao escolher com quem farão transações on-line.

O risco de fraude está presente em toda a jornada do consumidor

8,3%
das transações de onboarding digital em 2025 foram classificadas como suspeitas de fraude, tornando essa a etapa de maior risco na jornada do consumidor.

37%
de aumento no índice de suspeitas de fraude por invasão de contas (ATO) de 2024 a 2025.

O comprometimento de credenciais aumenta o risco de ataques de fraude sofisticados

33%
dos consumidores que afirmaram ter sido alvo de fraude digital disseram ter sofrido ataque de phishing; o maior índice entre todos os tipos de golpe.

47%
de aumento no volume de vazamentos de dados nos EUA de 2024 a 2025.

TransUnion

Sobre a pesquisa

O relatório visa fornecer à liderança em prevenção à fraude, riscos, identidade e autenticação as informações atuais para avaliar suas táticas preventivas no contexto das tendências globais e ajustar suas estratégias com confiança. Ele considera duas fontes de inteligência: insights de uma pesquisa global envolvendo 12.730 consumidores em 18 países e regiões e aqueles que ganharam em bilhões de transações dentro da rede de inteligência global proprietária da TransUnion. Quando essas duas perspectivas são analisadas em conjunto, elas permitem entender não apenas como a fraude acontece, mas também como ela está mudando. O resultado é uma leitura mais completa do cenário atual, marcada por ataques cada vez mais dinâmicos. de ameaças atual que muda em ritmo acelerado.

Como aplicar esses insights

Use este relatório como um guia estratégico para:

- Comparar o seu ambiente de negócios com as tendências globais, regionais e do segmento
- Identificar vulnerabilidades no ciclo de vida do consumidor
- Avaliar o nível de maturidade do seu conjunto de soluções antifraude na detecção de fraudes em constante evolução
- Alinhar com as áreas internas da sua empresa sobre os principais riscos e das expectativas dos consumidores
- Apoiar as decisões de investimento em soluções de prevenção a fraudes

Consulte a metodologia de fornecimento de dados completa na página 41 para saber mais informações.

Como interpretar dos dados

Achados da pesquisa com consumidores

Os insights dos consumidores refletem as experiências com fraude digital (on-line, por e-mail, telefone e mensagens de texto) e os comportamentos e preferências sobre as experiências digitais. Embora esses relatos frequentemente estejam alinhados com os padrões reais de ataque, eles devem ser interpretados com cautela, pois representam percepções individuais. Por isso, esses dados são mais úteis como indicadores de sentimento, nível de confiança, mudanças de comportamento e expectativas dos consumidores — e não como medidas exatas da incidência de fraude.

Métricas de fraude digital

Todos os dados de fraude digital representam fraudes digitais suspeitas com base em indicadores de risco de dispositivos usados por clientes da TransUnion. Como as organizações estão constantemente ajustando os controles e o apetite de risco, os índices de fraude podem mudar ao longo do tempo ou nos diversos segmentos e regiões. As mudanças podem refletir os níveis de atividade, os volumes de transação ou limites de risco atualizados. Encare esses valores como indicadores-guia da atividade de fraude digital.

Comparações geográficas: A fraude digital por localização geográfica se baseia na localização do consumidor durante uma transação, e não na localização da empresa. Os níveis de fraude regional podem mudar conforme os limites de risco que as empresas aplicam a certas localizações ou transações. Use essas comparações como indicadores-guia, e não como medidas absolutas de segurança regional.

Referências do segmento: Os índices de fraude digital no nível do segmento representam fraudes contra empresas nesse setor, e não fraudes cometidas por ou contra consumidores nessa categoria especificamente. As diferenças entre os segmentos costumam refletir na variação de suas tolerâncias ao risco, jornadas de clientes e estratégias de prevenção a fraude.

Considerações sobre dados específicos dos EUA

Vazamentos de dados: Os volumes das violações se baseiam nas informações de conhecimento público; a exposição real pode ser maior. A pontuação de risco de violação (BRS) mede a facilidade com que credenciais expostas podem se tornar alvo de fraude de identidade.

Fraude em call centers: Os índices de chamadas de alto risco são influenciados pela forma como cada instituição configura seus limites de pontuação.

Exposição a identidades sintéticas: As estimativas de fraude sintética refletem somente as categorias de crédito que a TransUnion mediu; a exposição real pode ser maior.

Disputas de relatórios de crédito: Essas métricas dependem das disputas de relatório de crédito em que os consumidores alegaram ter sido alvo de fraude e podem oscilar conforme a orientação e o comportamento do consumidor.

Sumário

TransUnion

Seus clientes são legítimos?

O futuro das fraudes impulsionadas pela IA

Se os dados de identidade passaram a ser o principal alvo na fraude digital, a inteligência artificial tornou-se uma ferramenta tanto para fraudadores quanto para quem atua na sua prevenção. A IA não reinventa a fraude, mas torna as práticas existentes mais rápidas, acessíveis e escaláveis.

Na prática, isso reduz drasticamente as barreiras de entrada. Um esquema que antes exigia uma operação estruturada, com várias pessoas, hoje pode ser conduzido por um único indivíduo. Com o uso de dados roubados e ferramentas de automação baseadas em IA, atividades passam a ser executadas de forma simples e em larga escala.

Fica claro o impacto: distinguir clientes legítimos de fraudadores se torna cada vez mais difícil ao longo de toda a jornada do cliente. A IA viabiliza invasões de contas (ATO) com facilidade, explorando credenciais comprometias e também viabiliza a criação de novas contas com dados falsos, apoiados por documentos manipulados e simulações biométricas cada vez mais sofisticadas.

Além disso, amplia a capacidade de fraude permitindo que criminosos se passem por empresas reais e utilizem canais digitais falsificados para enganar consumidores.

Para equilibrar esse cenário, é essencial adotar uma estratégia de prevenção à fraude centrada em identidade e orientada por IA, capaz de elevar a detecção sem aumentar o atrito. A capacidade de analisar, conectar e validar dados ao longo da jornada do cliente torna-se essencial. Ao combinar informações de dispositivos, padrões de comportamento e dados compartilhados entre organizações, é possível construir uma visão mais confiável sobre quem está por trás de cada interação, com o apoio de modelos avançados de machine learning.

[1]As expressões e conceitos mencionados nesta página estão detalhados no glossário.

TENDÊNCIAS DE FRAUDE GLOBAIS

Experiências de fraude do público consumidor

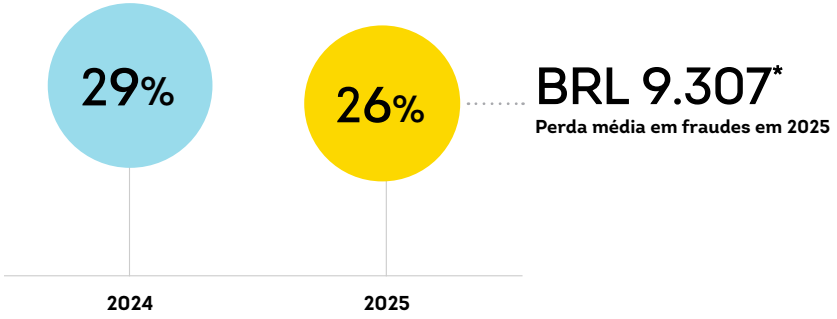
A geração Z é a mais suscetível a sofrer perdas com esquemas de fraude baseados em confiança

Entre os consumidores pesquisados em 18 países e regiões, 26% relataram ter perdido dinheiro com fraudes digitais no último ano, com uma perda média de USD 1.671, o equivalente a R$ 9.307. Os consumidores mais jovens demonstraram maior propensão a sofrer perdas financeiras em comparação com a população geral. Entre a geração Z, 39% afirmaram ter sido impactados por fraudes digitais no último ano — o maior índice observado entre todas as gerações.

O uso intensivo de plataformas de redes sociais, jogos on-line e criptomoedas pode contribuir para essa maior exposição ao risco. Entre os tipos de fraude relatados pela Geração Z, os esquemas baseados em confiança figuraram entre os mais recorrentes, incluindo fraudes de roubo e comercialização de identidade em plataformas legítimas de comércio eletrônico (27%) e esquemas de "conta laranja" (26%).

Esses percentuais superam o índice geral de 24%, também o mais elevado entre as categorias analisadas.Na sequência, 23% dos consumidores em geral relataram perdas financeiras decorrentes de golpes de vishing — chamadas telefônicas fraudulentas que induzem à divulgação de informações pessoais —, possivelmente associados à personificação de empresas legítimas ou de organizações governamentais.

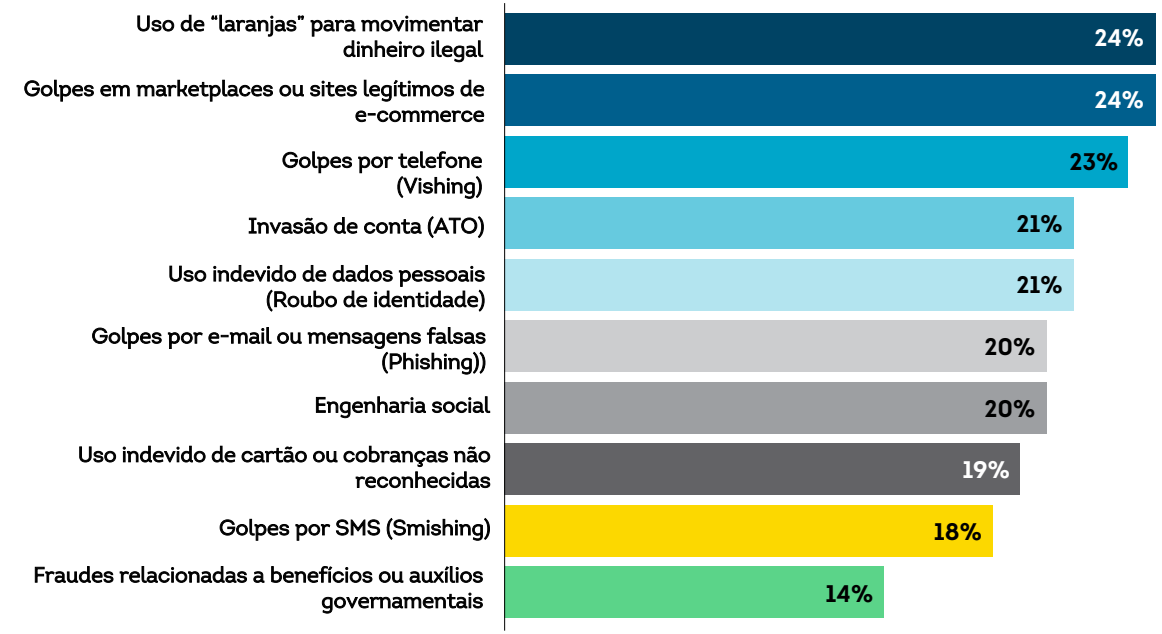
Perdas por fraude relatadas por consumidores
O percentual de consumidores em 18 países e regiões que disseram ter perdido dinheiro por fraude digital no último ano e o valor médio que alegaram ter perdido



*Conversão para USD com base na taxa de câmbio de 29 de dezembro de 2025

Fonte: Pesquisa da TransUnion com consumidores

Principal causa das perdas por fraude
Percentual por tipo de golpe entre consumidores que relataram perda financeira com fraude digital no último ano



Fonte: Pesquisa da TransUnion com consumidores

As expressões e conceitos mencionados nesta página estão detalhados no glossário.

Golpes que expõem dados de identidade predominam nas fraudes relatadas pelos consumidores

Mais da metade (53%) dos consumidores relataram ter sido alvo de esquemas de fraude digital entre agosto e dezembro de 2025, e 10% disseram ter sido vítimas. Ainda assim, uma parcela significativa (47%) dos entrevistados afirmou desconhecer que estavam sendo alvo dessa prática.

Entre aqueles que disseram ter sido alvo de golpes, os principais tipos de fraude relatados pelos consumidores tinham como objetivo expor identidades: phishing (33%), smishing (28%) e vishing (27%).

Consumidores alvo de fraude
Percentual de consumidores que afirmaram ter sido alvo de tentativas de fraude digital entre agosto e dezembro de 2025, e o esquema mais frequente relatado

Fonte: Pesquisa da TransUnion com consumidores

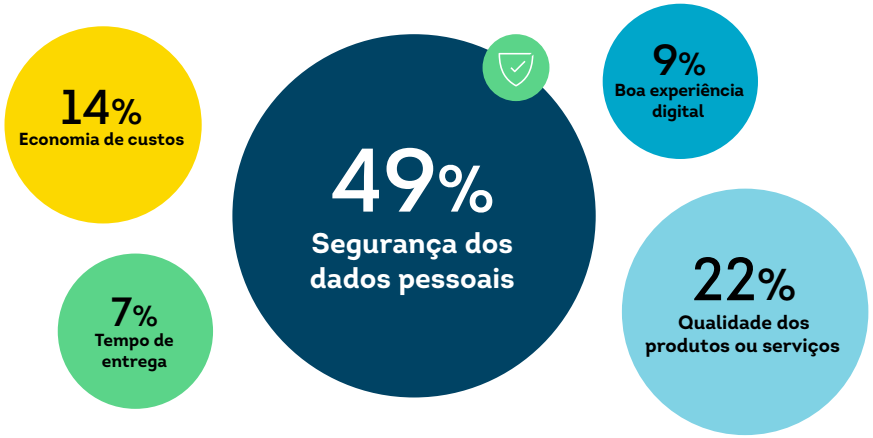
Transações on-line seguras e fluidas motivam a preferência dos consumidores por uma marca

Com o aumento do uso de serviços digitais, as preferências relacionadas à segurança e à proteção de dados tornaram-se críticas para o crescimento dos negócios. Mais de um terço dos consumidores (37%) afirmou realizar mais da metade de suas transações de varejo e comerciais por canais on-line, ante 34% no ano anterior, enquanto 39% disseram conduzir a maior parte do gerenciamento de contas digitalmente (38% anteriormente). Entre famílias de alta renda, o uso é ainda mais intenso: cerca de metade informou utilizar canais on-line para comércio (55%) e gestão de contas (50%).

As expectativas por experiências digitais seguras, protegidas e convenientes são elevadas, especialmente em transações financeiras. Mais da metade dos consumidores (56%) afirmou que provavelmente trocaria de empresa em busca de uma experiência superior. Ao apontarem fatores que impediriam o retorno a um site, a preocupação com fraudes foi a mais citada, por 65% dos respondentes.

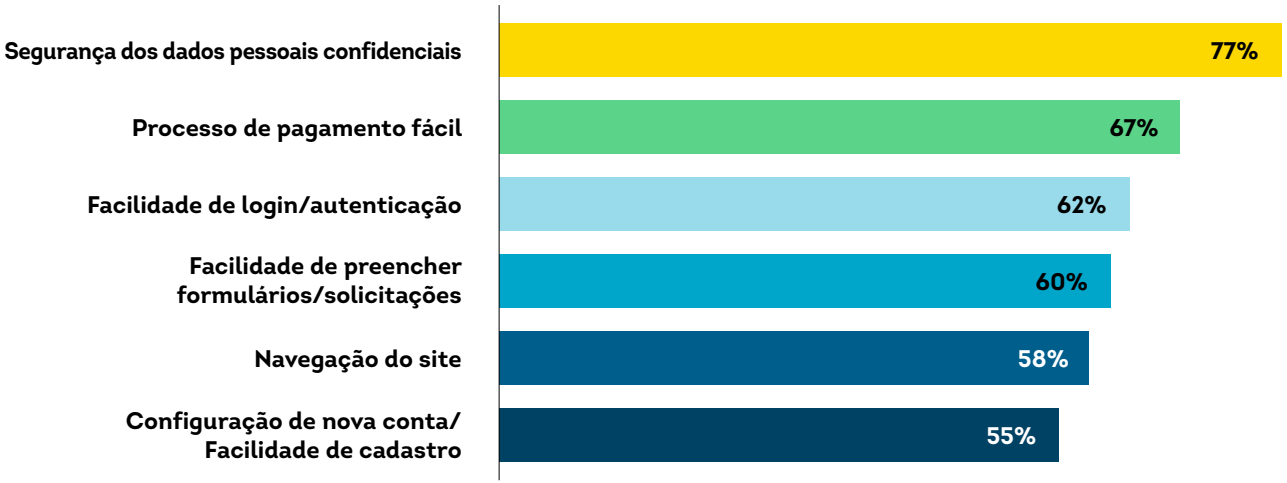
Para atrair e reter clientes, as organizações precisam demonstrar confiança no uso dos dados. Quase metade dos consumidores (49%) classificou a segurança das informações pessoais como o atributo mais importante em empresas on-line. Além disso, 77% afirmaram que a garantia de que seus dados não serão comprometidos é um fator decisivo ao escolher com quem transacionar, sendo o aspecto mais bem avaliado.

Prioridades dos consumidores ao escolher empresas on-line preferidas
Principais respostas escolhidas



Fonte: Pesquisa da TransUnion com consumidores

Características importantes informadas ao escolher com quem fazer negócios on-line
Percentual que respondeu "muito importante"



Fonte: Pesquisa da TransUnion com consumidores

Tendências de fraude digital

Queda no índice geral de fraudes digitais suspeitas

A taxa global de tentativas suspeitas de fraude digital foi de 3,8% em 2025, o menor nível desde 2022.

Mas essa queda não significa que a fraude está menor. Um dos motivos é o aumento no volume de transações digitais. Com mais pessoas comprando, acessando serviços e realizando operações online, a proporção de casos suspeitos tende a parecer menor.

Além disso, as empresas podem estar priorizando os casos mais críticos de fraude. Nesse cenário, golpes menos evidentes podem acabar passando com mais facilidade e ficando fora dessa contagem.

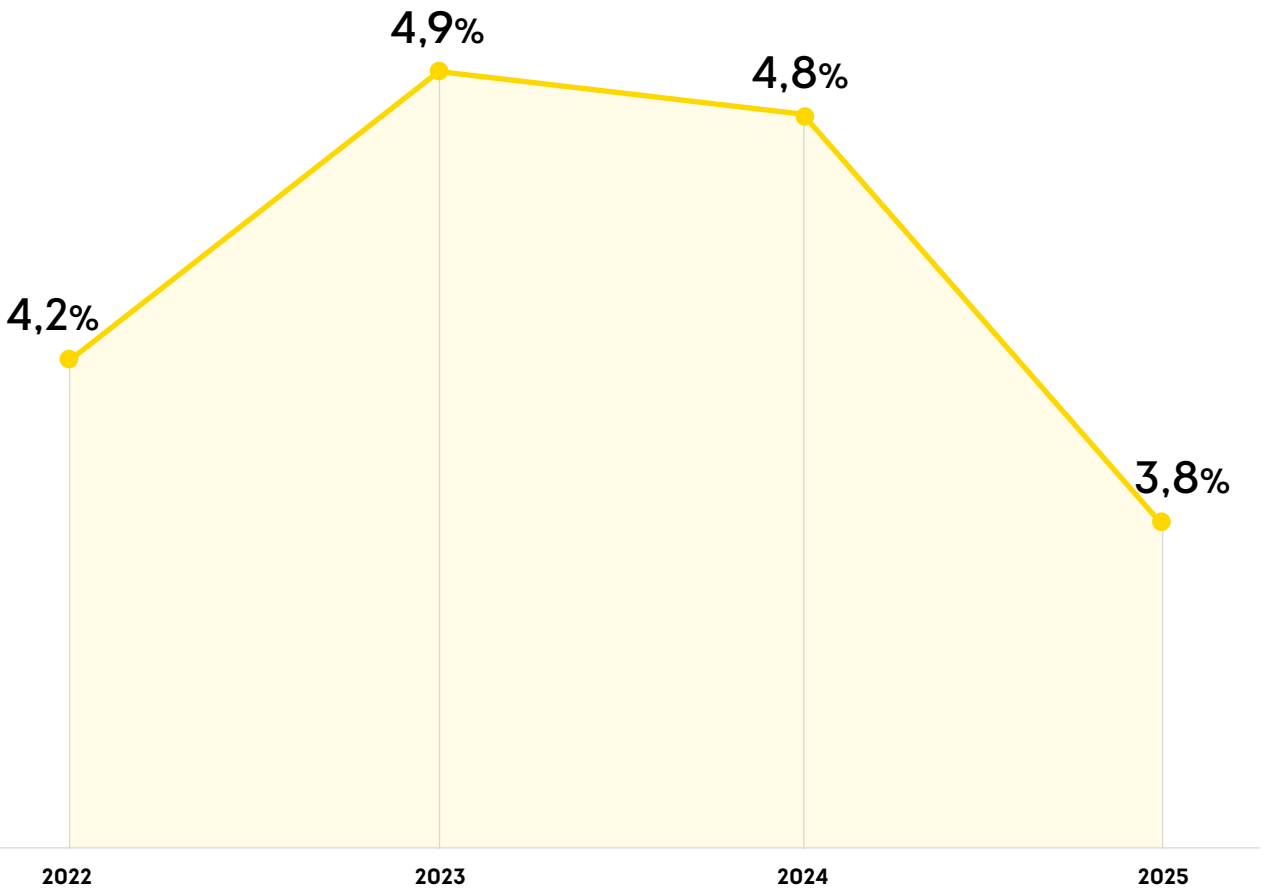
Ao mesmo tempo, os fraudadores também mudaram sua forma de agir. Eles usam dados vazados, credenciais roubadas e engenharia social para acessar contas ou criar acessos que parecem legítimos.

Outro ponto importante é que os ataques estão cada vez mais focados nos consumidores — e não nos sistemas das empresas — o que dificulta a identificação pelas ferramentas tradicionais de detecção.

Por isso, mesmo com a queda na taxa geral, o cenário continua mais complexo.

Essa variação também aparece entre as regiões analisadas. Em 2025, a Ásia registrou a maior taxa de fraude digital suspeita, com 5,9%, enquanto a Europa apresentou a menor, com 2,1%.

Taxa de fraude digital suspeita em âmbito global



Fonte: Rede de inteligência global da TransUnion

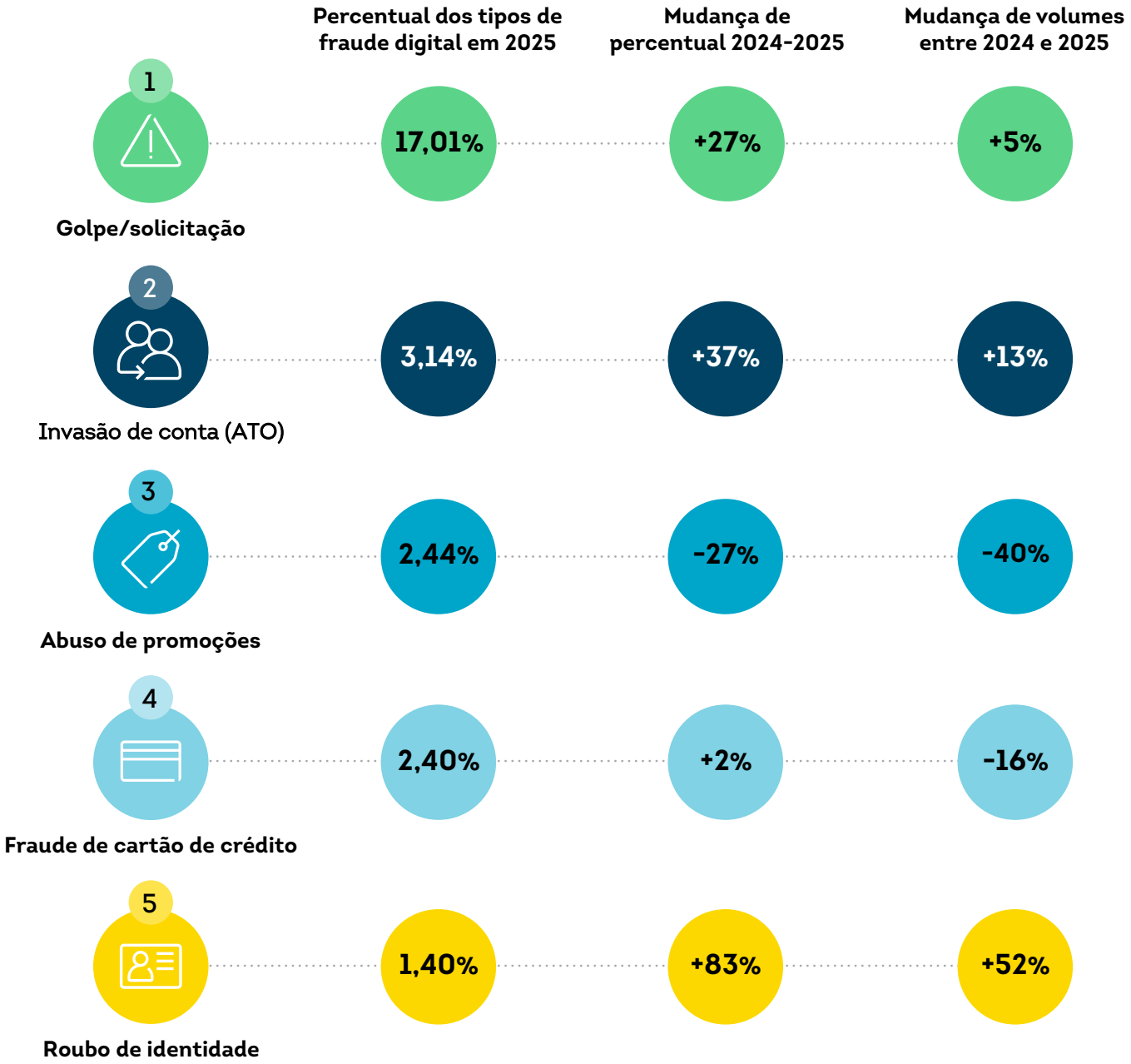
Os ataques de ATO crescem em frequência e volume

As contas de consumidores continuam sob ataque. Em 2025, a invasão de contas (ATO) representou 3,14% das suspeitas de fraude digital, acima dos 2,3% registrados em 2024. Isso equivale a um crescimento de 37% no período. Além disso, o número total de transações associadas a ATO também aumentou 13%.

Outro destaque são os golpes baseados em contato direto com o consumidor — como ofertas falsas de produtos ou serviços — usados para roubar dados de acesso. Esse tipo de fraude respondeu por 17,01% das suspeitas de fraude digital em 2025, voltando a liderar o ranking e registrando aumento de 27% em relação a 2024.

Esses dois tipos de fraude estão diretamente conectados. Em muitos casos, o golpe é o primeiro passo para invadir a conta da vítima, seja obtendo credenciais de acesso ou induzindo o próprio usuário a fornecer informações.

Principais tipos de fraude digital e sua evolução



Fonte: Rede de inteligência global da TransUnion

TransUnion

Os segmentos de entretenimento são os mais suscetíveis ao risco de fraude digital

Entre os segmentos analisados, a indústria de jogos eletrônicos registrou o maior percentual de tentativas suspeitas de fraude digital em âmbito global, alcançando 12,8% em 2025, um aumento de 7% em relação a 2024. Na sequência, o segmento de comunidades apresentou uma taxa de 8,1%. Em ambos os segmentos, o tipo de fraude mais frequentemente relatado pelos clientes da TransUnion foi o de golpes/solicitações.

Os jogos eletrônicos se destacam como um alvo relevante para fraudes digitais por fatores que vão além do perfil tradicionalmente associado a esse público. Esse cenário não se limita a adolescentes, uma vez que, de acordo com pesquisa global realizada pela Entertainment Software Association, a idade média dos jogadores é de 41 anos, sendo a maior concentração etária entre 25 e 36 anos. Além disso, mais da metade dos jogadores indicou o celular como seu principal dispositivo de jogo. Em plataformas da economia da atenção, onde o uso de nomes de usuário fictícios é comum, os fraudadores encontram um ambiente propício para enganar usuários menos atentos.

Criminosos exploram o caráter social e interativo desses ambientes, incluindo videogames e comunidades on-line, criando perfis falsos para aplicar golpes e ofertas enganosas aos consumidores. Em alguns casos, o objetivo é a fraude direta, mas, com maior frequência, essas abordagens são utilizadas para coletar informações pessoais, que posteriormente viabilizam tentativas de invasão de contas (ATO) ou a abertura de novas contas fraudulentas.

Tentativas de fraude digital por segmento

- **Taxa de tentativas suspeitas de fraude em 2025**
- **Principal tipo de fraude em 2025**
- **Mudança percentual no volume de suspeitas de fraude digital de 2024 a 2025**

Jogos eletrônicos

2025
12,8%
Golpe/solicitação

2024-2025
+7%

Comunidades
(namoro on-line, grupos etc.)

2025
8,1%
Golpe/solicitação

2024-2025
-36%

Jogos
(apostas, pôquer etc.)

2025
7,7%
Abuso de promoções

2024-2025
+27%

Telecomunicações

2025
4,2%
Golpe/solicitação

2024-2025
+66%

Serviços financeiros

2025
3,2%
Invasão de conta (ATO)

2024-2025
-21%

Varejo

2025
2,8%
Invasão de conta (ATO)

2024-2025
-60%

Governo

2025
2,2%
Fraude de cartão de crédito

2024-2025
+28%

Logística

2025
1,6%
Fraude de envio

2024-2025
-55%

Seguro

2025
1,3%
Fraude do corretor fantasma

2024-2025
-39%

Viagem e lazer

2025
0,2%
Fraude de cartão de crédito

2024-2025
-58%

Fonte: Rede de inteligência global da TransUnion

Fraude digital na jornada do consumidor

O onboarding é a etapa mais arriscada na jornada do consumidor

Em 2025, o onboarding digital concentrou o maior risco de fraude ao longo da jornada do consumidor. Fraudadores utilizaram dados de identidade comprometidos, falsos, allterados ou roubados em 8,3% de todas as transações suspeitas de fraude digital, tornando essa etapa significativamente mais arriscada do que o login em conta, que registrou 4,3%.

Na maioria dos segmentos analisados, o onboarding permaneceu como o principal ponto de vulnerabilidade. As exceções foram os setores de serviços financeiros, seguros, telecomunicações e governo, nos quais as transações financeiras representaram a etapa de maior risco.

Os segmentos de comunidades e varejo apresentaram as maiores taxas de fraude digital suspeita durante o onboarding, com 22,5% e 22,3%, respectivamente.

Exemplos de etapas na jornada do consumidor

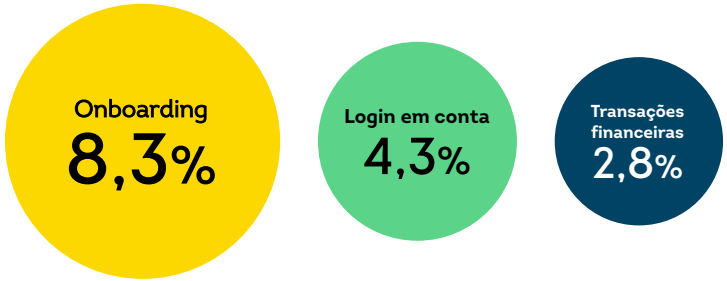
Onboarding: Cadastro de conta, registro e originação de empréstimo

Login em conta: Tentativas de login com falha e bem-sucedidos

Transações financeiras: Compras, saques e depósitos

Risco de fraude na jornada do consumidor digital

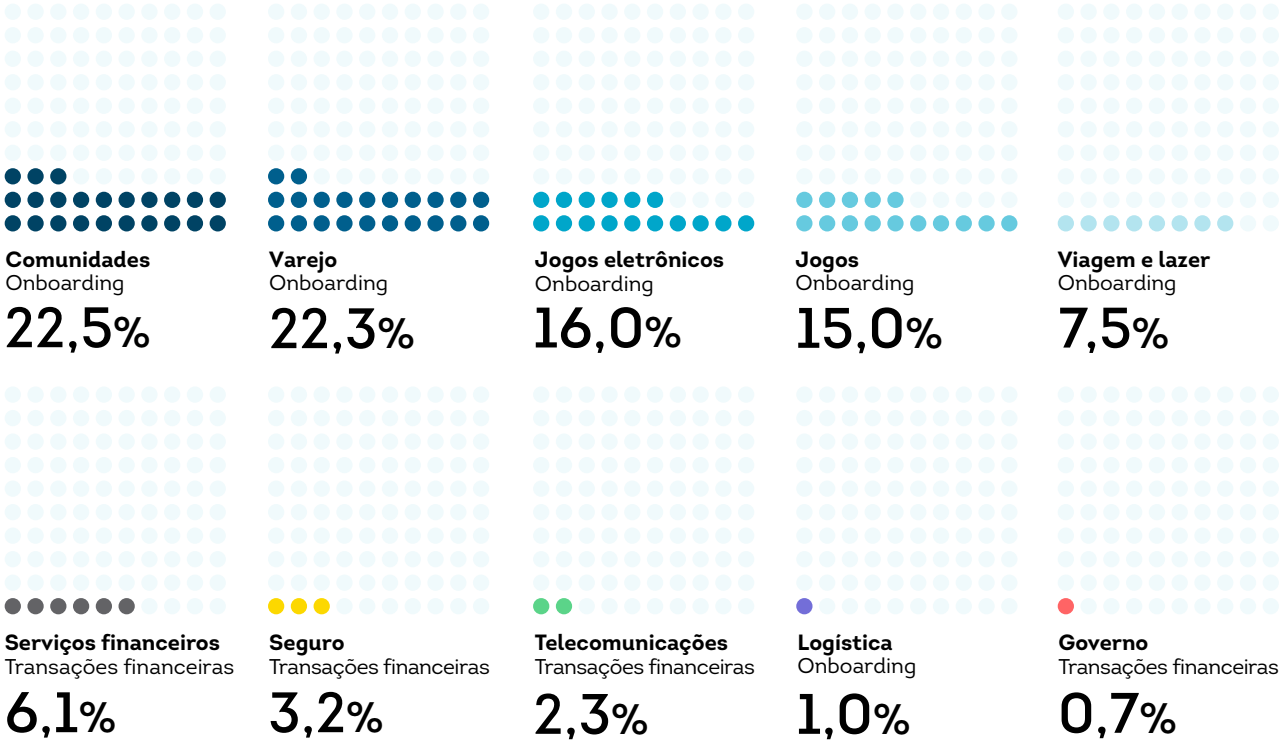
Percentual de cada tipo de transação suspeita de ser fraude digital em 2025



Fonte: Rede de inteligência global da TransUnion

Risco de fraude na jornada do consumidor digital por segmento

A etapa da jornada do consumidor com a maior taxa suspeita de fraude digital por segmento e o percentual correspondente nessa etapa em 2025



Fonte: Rede de inteligência global da TransUnion

TransUnion

AMÉRICA LATINA

Visão geral da América Latina

Em 2025, os investimentos em prevenção a fraude contribuíram para uma redução de 46% nas tentativas suspeitas de fraude digital nos países latino-americanos analisados, em comparação com 2024.

Apesar desse avanço, o onboarding e o login continuam concentrado uma parte relevante das transações suspeitas, mantendo-se como pontos críticos de risco ao longo da jornada do consumidor. Entre os consumidores da região que relataram perdas financeiras com fraudes digitais no último ano, a média foi de US$ 1.973 (cerca de R$ 10.989), com impactos significativos sobre as finanças pessoais e a confiança no uso de canais digitais. O vishing se destacou como o golpe mais frequente, reforçando a necessidade de estratégias que combinem tecnologia com ações contínuas de educação do consumidor sobre proteção de dados e credenciais.

No Brasil, o impacto é ainda mais relevante. A perda média chegou a R$ 10.699, um aumento de 60% em relação a 2024. Entre os consumidores que perderam dinheiro com fraudes digitais no Brasil, 32% apontaram o vishing como o principal tipo de golpe. Além disso, a taxa geral de fraude digital no país alcançou 3,8%, acima da média regional, indicando maior exposição a riscos.

Para sustentar a confiança, as empresas precisam fortalecer continuamente seus controles, garantindo a proteção e o uso adequado dos dados. Esse fator segue como um dos principais critérios considerados pelos consumidores ao decidir com quais empresas transacionar on-line.

Os dados da América Latina nesta seção combinam insights exclusivos sobre fraudes digitais da rede global de inteligência da TransUnion no Brasil, Chile, Colômbia, Costa Rica, República Dominicana, El Salvador, Guatemala, Honduras, México, Nicarágua e Porto Rico, e uma pesquisa com consumidores no Brasil, Chile, Colômbia, República Dominicana, México e Porto Rico.

PONTOS IMPORTANTES

Os fraudadores se concentram em vishing

41%
dos adultos latino-americanos afirmaram ter sido alvo de fraudes digitais entre agosto e dezembro de 2025.

27%
dos consumidores latino-americanos que disseram ter sido alvo de fraude indicaram que foram vítimas de vishing, tornando-o o esquema de fraude mais comum na região.

Os fraudadores persistem, pressionando cada vez mais o onboarding

5,7%
das tentativas de onboarding digital realizadas por consumidores da América Latina em 2025 foram suspeitas de fraude, tornando essa etapa a mais arriscada da jornada do consumidor

83%
dos consumidores latino-americanos consideram 'muito importante' a confiança na proteção de seus dados pessoais ao escolher com quem realizar transações on-line.

Digitalização em curso – fraudadores à espreita

37%
dos latino-americanos afirmaram realizar a maior parte de suas atividades de gerenciamento de contas on-line, um aumento de dois pontos percentuais em relação ao ano anterior.

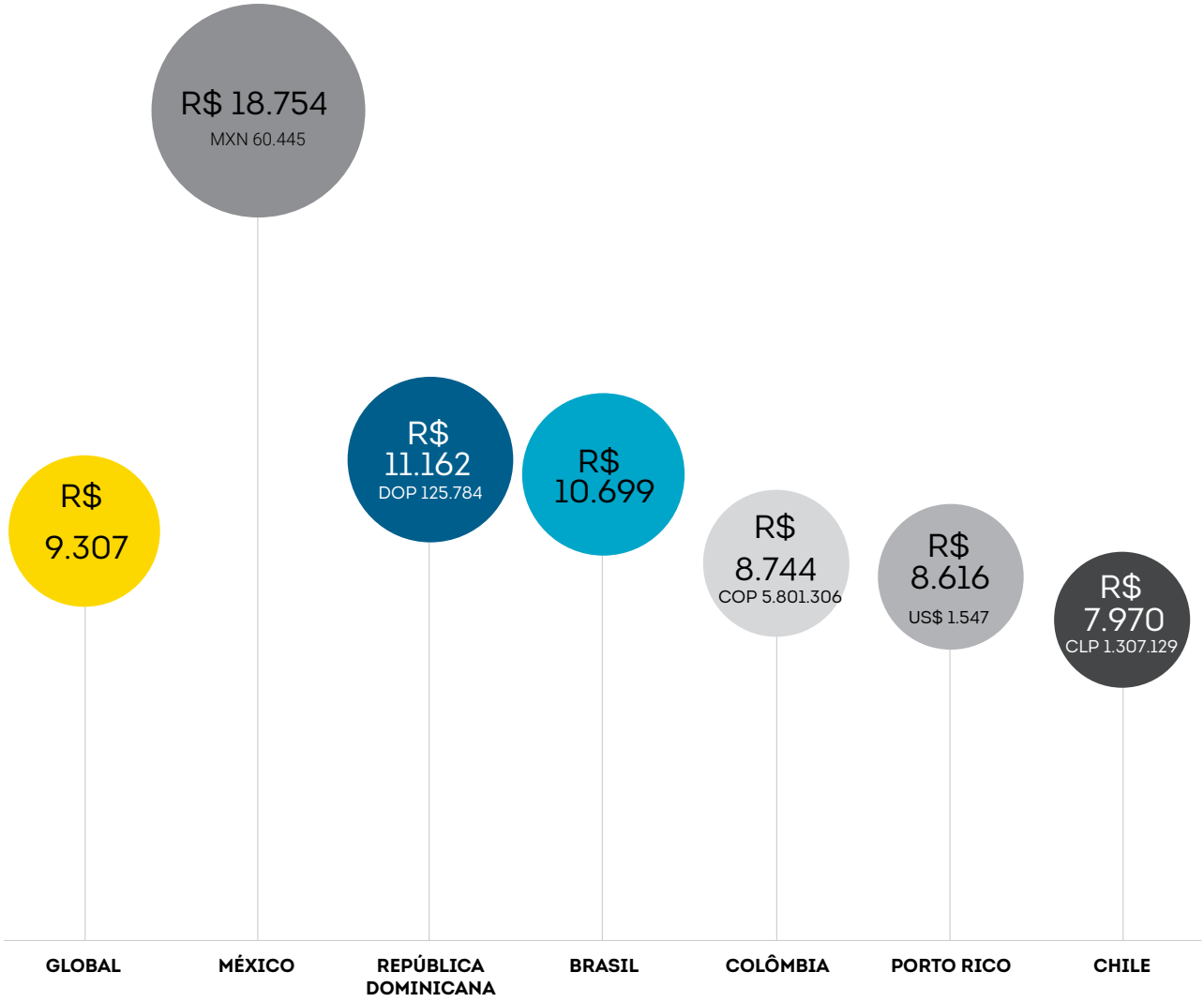
33%
dos entrevistados da geração Z da América Latina disseram ter perdido dinheiro devido a fraudes digitais no último ano, tornando-os a geração com o maior percentual, provavelmente devido à sua extensa presença on-line.

Experiências de fraude do público consumidor

O impacto significativo da fraude nos consumidores

A perda média relatada por consumidores latino-americanos que afirmaram ter prejuízo com fraudes digitais no último ano foi de R$ 10.989 - acima da média global e superior à de países como Canadá e Espanha. Esses impactos tendem a ser duradouros, já que a recuperação financeira e de crédito exige processos longos e graduais. O vishing foi o golpe mais relatado entre consumidores da região que sofreram perdas financeiras, em contraste com o cenário global, onde predominam esquemas de roubo e uso indevido de informações em sites de e-commerce e contas laranja. Na América Latina, o vishing foi citado por mais de um quarto dos consumidores no Brasil (32%), Chile (29%), República Dominicana (40%), México (37%) e Porto Rico (42%), significativamente acima da média global de 23%. Quando analisados no contexto econômico de cada país, esses valores ganham outra dimensão. Em economias em desenvolvimento, o impacto da fraude sobre a renda é proporcionalmente maior. Enquanto uma perda média de cerca de US$ 2.307 nos Estados Unidos representa aproximadamente dois salários mínimos, valores próximos a US$ 1.921* no Brasil podem equivaler a mais de seis salários mínimos. Essa diferença evidencia que a fraude não afeta apenas o valor absoluto perdido, mas compromete de forma mais profunda a capacidade financeira do consumidor, ampliando seus efeitos ao longo do tempo.

Perdas por fraude relatadas por consumidores
Perda média relatada por fraude (em BRL) entre consumidores que afirmaram ter perdido dinheiro devido a fraudes digitais no último ano

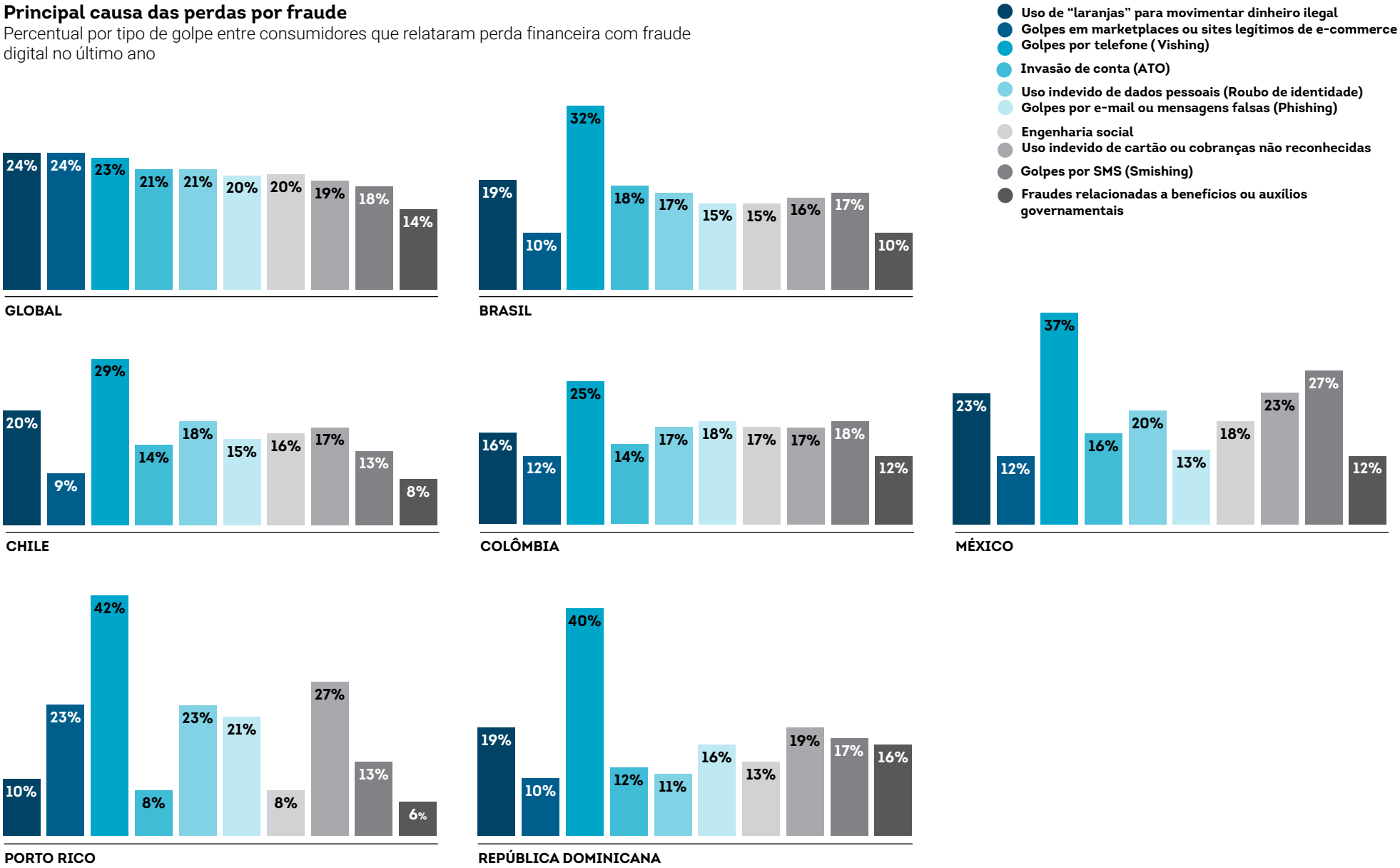


*Conversão para USD com base na taxa de câmbio de 29 de dezembro de 2025
**A média global é a média dos 18 países entrevistados

Fonte: Pesquisa da TransUnion com consumidores

Principal causa das perdas por fraude

Percentual por tipo de golpe entre consumidores que relataram perda financeira com fraude digital no último ano



Fonte: Pesquisa da TransUnion com consumidores

Os fraudadores continuam tendo consumidores como alvos, embora muitos possam não estar cientes disso

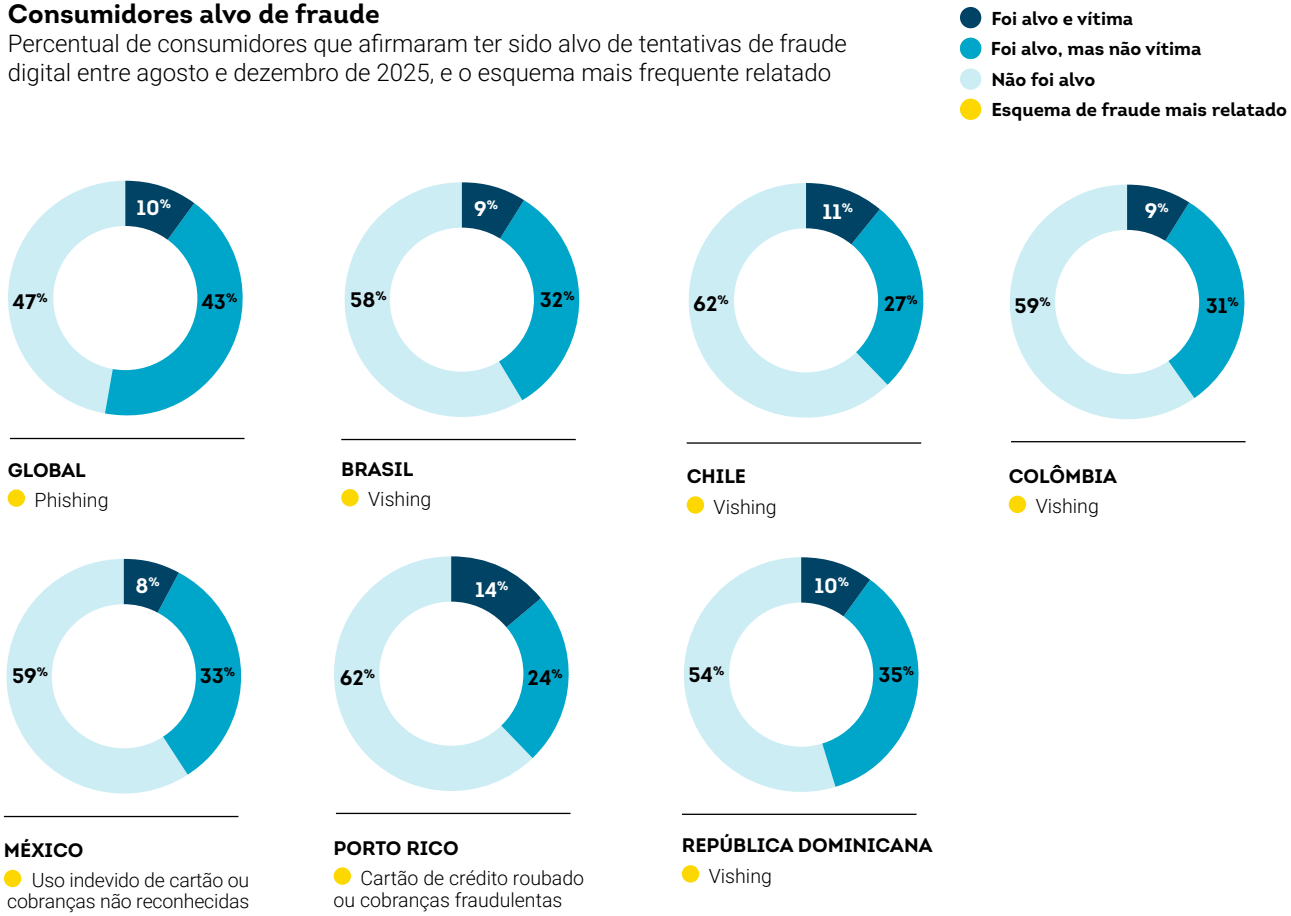
Na América Latina, 41% dos consumidores entrevistados relataram ter sido alvo de algum esquema de fraude digital nos últimos três meses, percentual inferior à média global de 53%. Ainda assim, há uma lacuna relevante de percepção de risco, uma vez que quase 6 em cada 10, ou seja 59% dos consumidores afirmaram não ter consciência de que estavam sendo alvo de tentativas de fraude.

Globalmente, o phishing foi o esquema de fraude mais frequentemente relatado entre os consumidores que afirmaram ter sido alvo desse tipo de ataque. Na América Latina, no entanto, o vishing destacou-se como o principal esquema relatado, especialmente no Brasil, Chile, Colômbia e República Dominicana. Fraudes relacionadas a cartões de crédito roubados ou cobranças fraudulentas também tiveram peso relevante na região, sendo apontadas como o principal esquema por consumidores no México e em Porto Rico.

Considerando o conjunto dos países latino-americanos analisados, o vishing emergiu como o esquema de fraude mais recorrente, reforçando a necessidade de estratégias de mitigação que priorizem a educação do consumidor e a proteção centrada no usuário, com foco na prevenção de apropriação indevida de contas e no uso indevido de credenciais pessoais.

Consumidores alvo de fraude

Percentual de consumidores que afirmaram ter sido alvo de tentativas de fraude digital entre agosto e dezembro de 2025, e o esquema mais frequente relatado



Fonte: Pesquisa da TransUnion consumidores

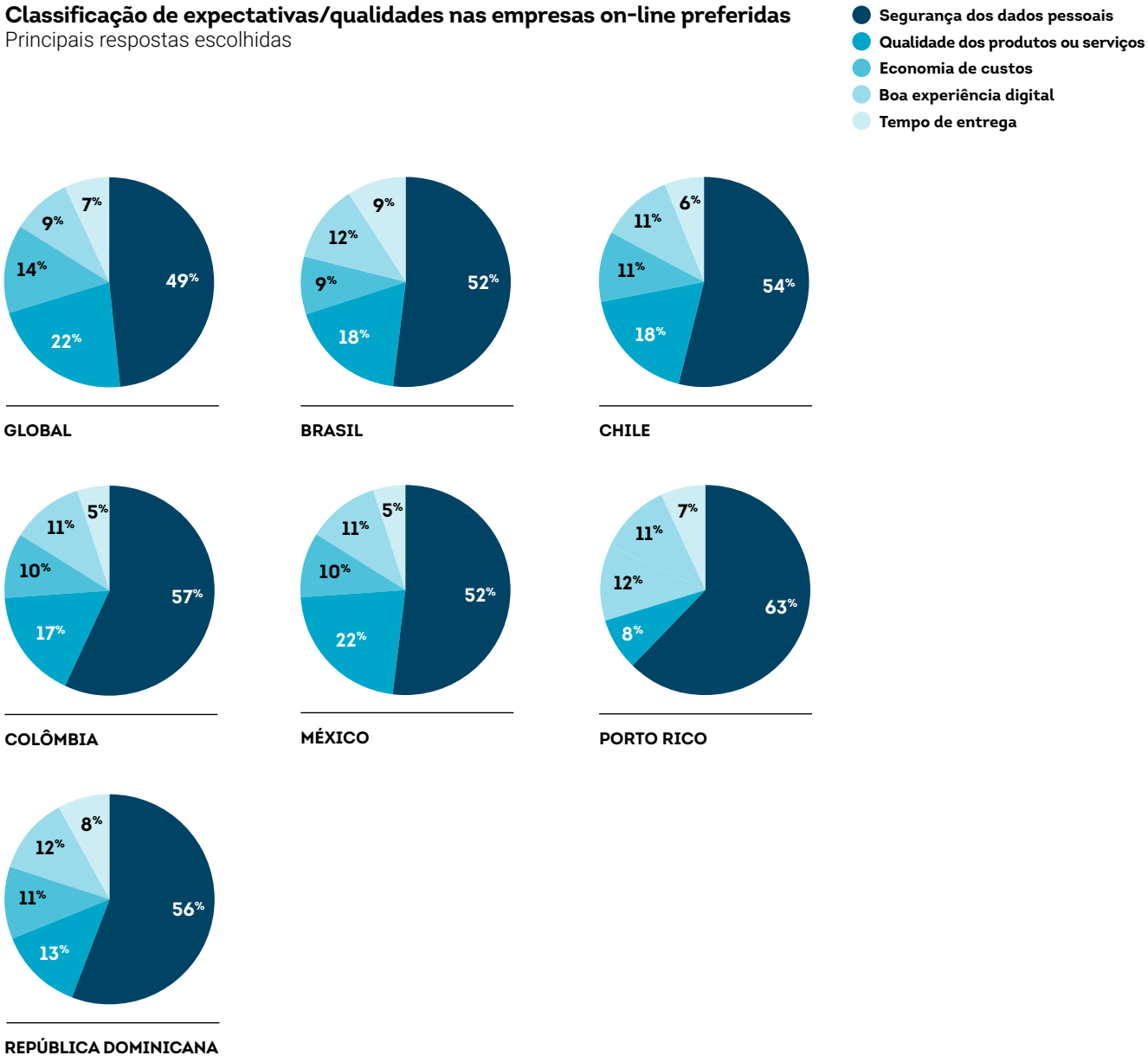
A segurança dos dados pessoais on-line é uma das principais expectativas dos consumidores

Os consumidores em todo o mundo têm expectativas claras em relação às transações on-line. Ao serem questionados sobre as qualidades ou expectativas que consideram ao escolher uma empresa on-line para fazer negócios, a segurança de seus dados pessoais foi a principal escolha para 49% e a qualidade dos produtos e serviços foi a principal escolha para 22%.

Apesar da importância atribuída aos prazos de entrega e às experiências digitais, os consumidores da América Latina estão alinhados com as expectativas globais; a segurança dos dados pessoais continua sendo a prioridade máxima em toda a região, especialmente em mercados como Porto Rico e Colômbia.

Ao serem questionados sobre a importância que atribuem a determinados recursos na escolha de com quem realizar transações on-line, a confiança na segurança de seus dados pessoais foi, mais uma vez, a principal preocupação dos países latino-americanos. Os consumidores em Porto Rico disseram que a confiança de que seus dados pessoais não serão comprometidos é muito importante (93%), a maior porcentagem entre os países da América Latina, seguida pela República Dominicana (86%). Um processo de pagamento fácil foi classificado como o segundo fator mais importante para todos os países latino-americanos pesquisados, em consonância com a opinião dos consumidores em todo o mundo.

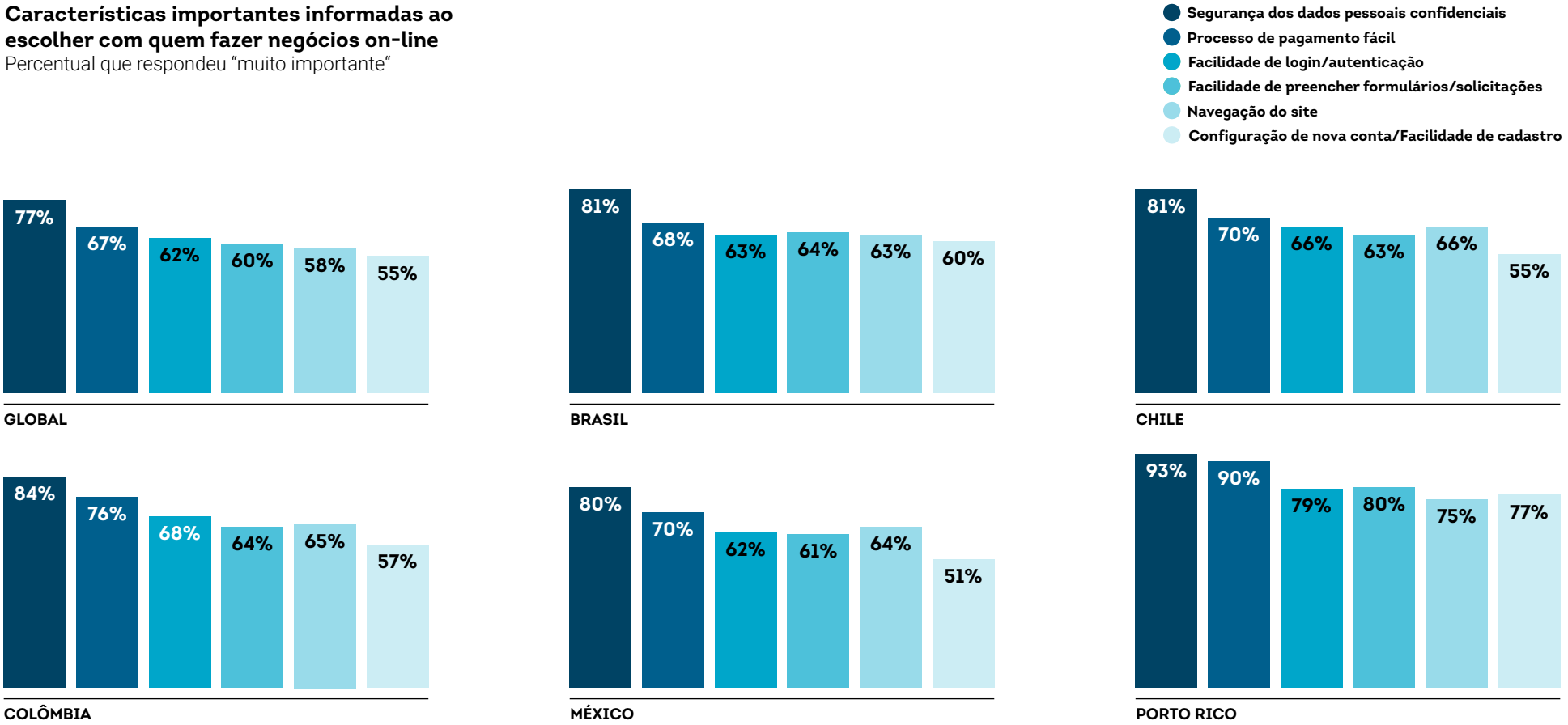
Classificação de expectativas/qualidades nas empresas on-line preferidas
Principais respostas escolhidas



Fonte: Pesquisa da TransUnion com consumidores

Características importantes informadas ao escolher com quem fazer negócios on-line

Percentual que respondeu "muito importante"



Fonte: Pesquisa da TransUnion com consumidores

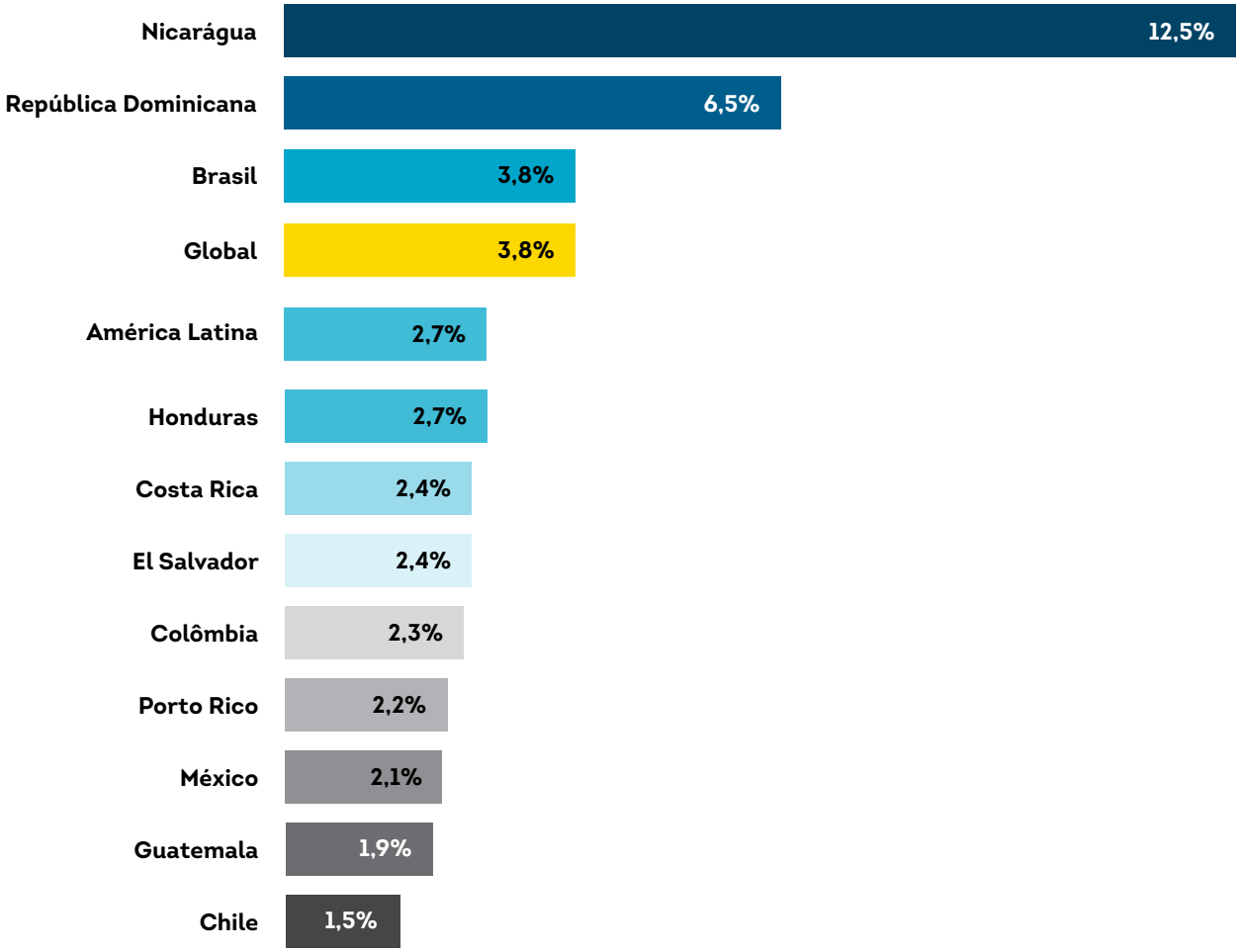
Tendências de fraude digital

Aumento das fraudes digitais suspeitas nos principais mercados da América Latina

A taxa global de tentativas de fraude digital suspeita entre clientes da TransUnion foi de 3,8% em 2025. Isso reflete a eficácia contínua das estratégias de prevenção à fraude nos principais mercados. Para os países latino-americanos analisados, a taxa média foi de 2,7%, com variações consideráveis entre os países. Três mercados — Brasil, República Dominicana e Nicarágua — registraram taxas acima da média regional. Esses níveis elevados sugerem que os fraudadores estão mais ativos nesses mercados específicos porque as vulnerabilidades nesses locais podem ser maiores do que em outros.

Todos os mercados analisados na América Latina, com exceção da Nicarágua, registraram uma queda anual nas tentativas de fraude digital suspeitas, o que destaca a importância e a eficácia dos esforços coordenados de mitigação de fraudes nesses países.

Taxa de suspeitas de fraude digital em 2025



Fonte: Rede de inteligência global da TransUnion

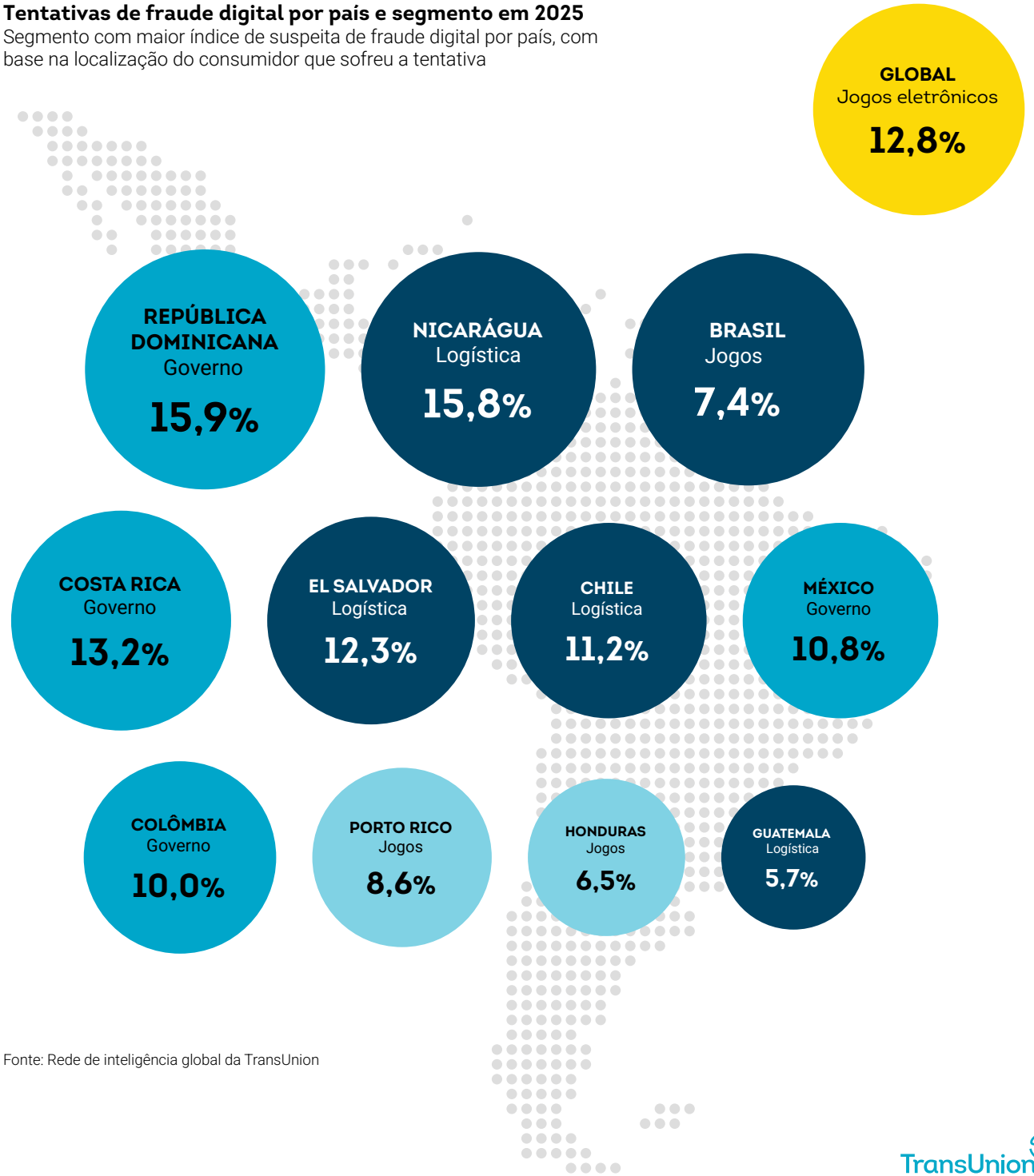
Os segmentos de governo e logística apresentam a maior taxa de suspeita de fraude digital na maioria dos países da América Latina

Entre os segmentos analisados globalmente, o setor de jogos eletrônicos registrou o maior percentual (12,8%) de tentativas suspeitas de fraude digital em 2025. O volume de suspeitas de fraude digital neste setor cresceu significativamente 7% de 2024 para 2025, sublinhando a crescente vulnerabilidade do setor à atividade fraudulenta.

Na América Latina, diferentes segmentos dentro de mercados individuais apresentaram taxas elevadas de fraude. Em tentativas de transação em que o consumidor estava na Nicarágua, por exemplo, o setor de logística apresentou a maior taxa de suspeita de fraude digital entre todos os segmentos analisados, com 15,8%.

Em praticamente todos os mercados da região, os setores de governo e logística emergiram como os que apresentaram a maior taxa de suspeita de fraude digital. Essa tendência reflete os esforços contínuos dos fraudadores de explorar setores que lidam com dados pessoais confidenciais e outros dados, como endereços ou registros de compras. Esses valores destacam a necessidade de haver estratégias de prevenção à fraude dentro desses segmentos.

Tentativas de fraude digital por país e segmento em 2025
Segmento com maior índice de suspeita de fraude digital por país, com base na localização do consumidor que sofreu a tentativa



Fonte: Rede de inteligência global da TransUnion

TransUnion

Credenciais em risco impactam todas as etapas da jornada do consumidor

Em 2025,o onboarding registrou o maior crescimento no risco de fraude ao longo da jonrada do consumidor, com um aumento global de 18% em relação a 2024. O login de contas também permaneceu como uma etapa de risco elevado, apresentando uma taxa de fraude digital suspeita de 4,3%, acima da média global de 3,8% para todas as tentativas de transações digitais.

Na América Latina, o onboarding destacou-se como a etapa mais visada da jornada digital, com uma taxa de fraude digital suspeita de 5,7% em 2025 entre os países analisados. Nicarágua e República Dominicana lideraram a região nesse indicador, com taxas de 65,3% e 15,8%, respectivamente.

A etapa de login de contas em El Salvador e no México apresentou taxas semelhantes de suspeita de fraude digital em comparação com o onboarding no ano passado. Em alguns mercados, como o Brasil, as taxas de fraude digital suspeita ficaram abaixo da média global no onboarding
(3,7% vs. 8,3%) e no login (2,6% vs. 4,3%), mas superaram a média global nas transações financeiras, alcançando 3,2% em 2025, frente a 2,8% globalmente.

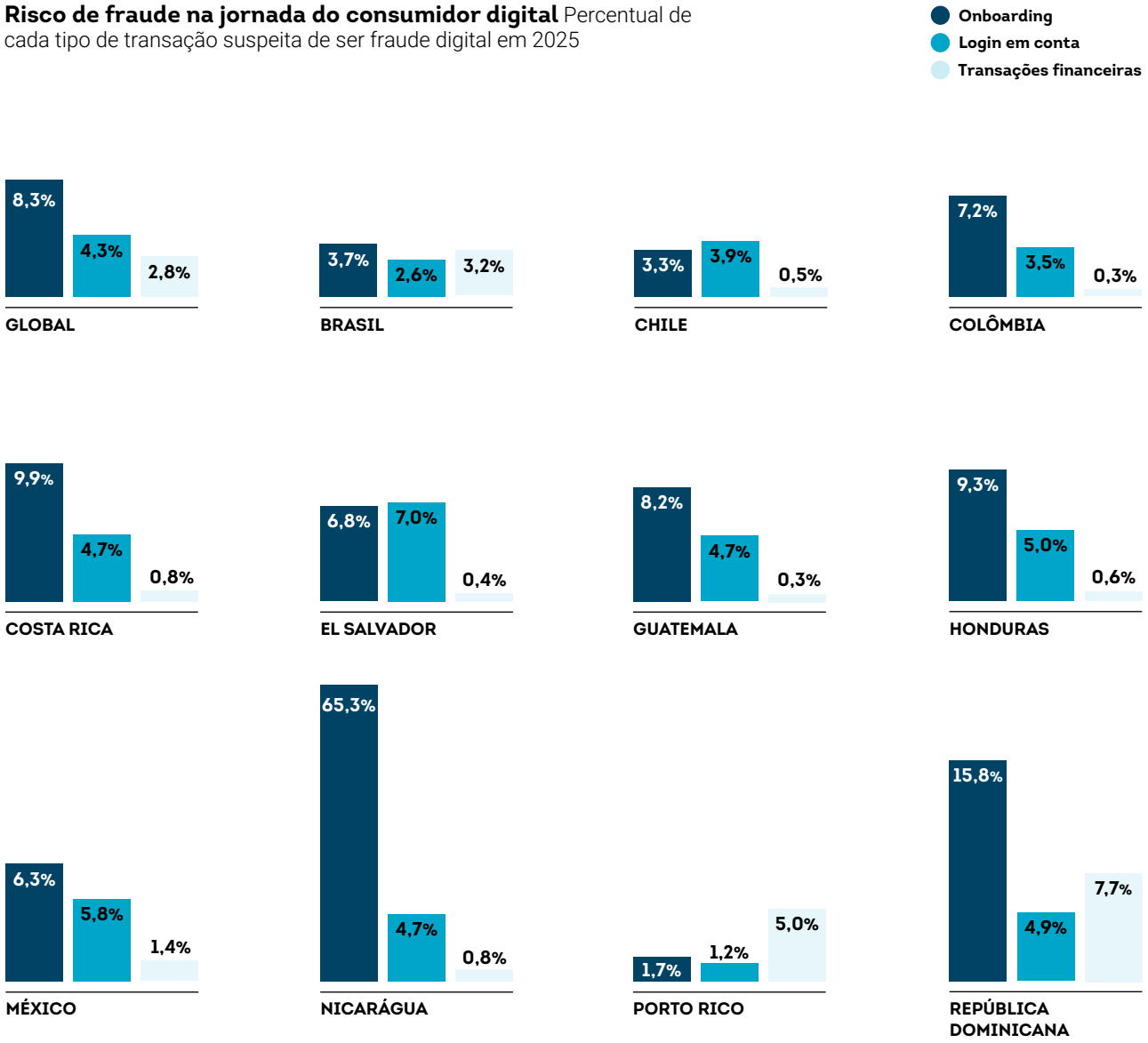
Exemplos de etapas da jornada do consumidor

Onboarding: Cadastro de conta, registro e originação de empréstimo

Login em conta: Eventos de login com falha e bem-sucedidos

Transações financeiras: Compras, saques e depósitos

Risco de fraude na jornada do consumidor digital Percentual de cada tipo de transação suspeita de ser fraude digital em 2025



Fonte: Rede de inteligência global da TransUnion

AMÉRICA DO NORTE

Visão geral dos Estados Unidos

Os esquemas de fraude são mais sofisticados e mais difíceis de detectar. O que está se tornando evidente é como os criminosos estão conseguindo contornar as defesas. Em 2025, os criminosos pareciam estar explorando duas estratégias paralelas de fraude digital, ambas dependentes da utilização indevida de informações pessoais comprometidas de consumidores. Primeiro, o alvo são consumidores ingênuos, com golpes cada vez mais convincentes para obter lucro imediato, evitando assim completamente as defesas contra fraudes. Em segundo lugar, roubar informações pessoais confiáveis por meio de vazamentos de dados, golpes contra consumidores e engenharia social de agentes de call center para burlar sistemas de autenticação ou enganar ferramentas de detecção de fraudes na criação de novas contas.

Em 2025, essas estratégias resultaram em perdas significativas para os consumidores devido a fraudes relacionadas a uso indevido de dados pessoais e invasão de contas (ATO). O estudo também revelou um paradoxo: uma taxa geral de fraude digital mais baixa, acompanhada por uma taxa crescente de invasão de contas (ATO), visto que os fraudadores visavam pagamentos de alto valor. A alta taxa de golpes e fraudes de solicitação relatadas dentro de uma comunidade credenciada, plataforma de jogos ou videogames indica que agentes mal-intencionados estão criando suas próprias contas. E as identidades sintéticas são um problema significativo para qualquer organização, ainda mais para empresas credoras com a instrumentalização de credit washing. Nada disso ficará mais fácil em um ambiente de fraude digital impulsionado por IA, exigindo maior foco na detecção de fraudes de identidade em todos os canais e em cada etapa do ciclo de vida do consumidor.

PONTOS IMPORTANTES

Golpes contra consumidores resultam em grandes prejuízos por fraude

USD 2.307

Perda média relatada no último ano entre os 16% dos consumidores americanos que afirmaram ter perdido dinheiro devido a fraudes digitais nesse período.

29%

dos consumidores americanos que relataram perdas com fraude digital no último ano apontaram o roubo de identidade como a segunda principal causa, atrás apenas de uso indevido do cartão ou cobranças fraudulentas (33%).

Credenciais comprometidas aumentam o risco de fraudes futuras

78%

dos vazamentos de dados nos EUA expuseram números completos do Seguro Social em 2025, o maior desde o início da pesquisa da TransUnion em 2020.

39%

dos consumidores americanos que relataram ter sido alvo de fraude digital entre agosto e dezembro de 2025 indicaram o phishing como o tipo de golpe mais frequente.

Riscos sofisticados de fraude de identidade estão se tornando cada vez mais evidentes

13%

de aumento nas chamadas de alto risco recebidas em call centers de clientes da TransUnion nos Estados Unidos entre 2024 e 2025, incluindo um crescimento de 41% nas chamadas feitas por dispositivos móveis.

USD 2,6 bilhões

em exposição de empresas credoras a identidades sintéticas nos EUA para financiamentos de veículos, cartões de crédito, cartões private label e empréstimos pessoais sem garantia no final de 2025.

Experiências de fraude do público consumidor

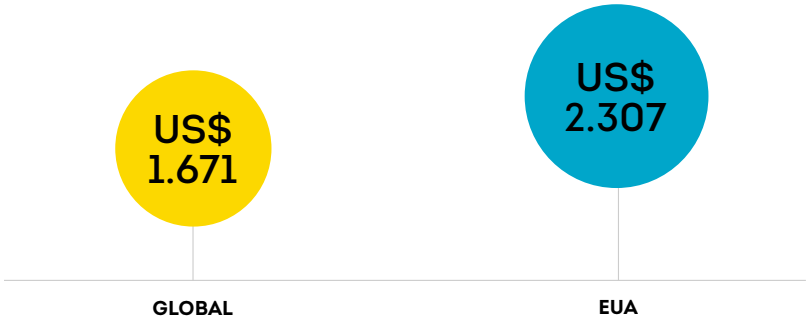
Fraudes baseadas em identidade impulsionam perdas por fraude ao consumidor

Em 2025, os consumidores americanos sofreram perdas por fraude que pareciam estar intimamente relacionadas a vazamentos de dados e golpes contra consumidores, fornecendo aos criminosos as credenciais necessárias para perpetrar fraudes. Quase um em cada seis (16%) consumidores adultos dos EUA disseram ter perdido dinheiro devido a algum tipo de fraude digital no último ano, com uma perda média relatada de US$ 2.307.

Extrapolando para a população adulta dos EUA (268,3 milhões em 1º de julho de 2025, segundo o Departamento do Censo dos Estados Unidos [United States Census Bureau]), isso reflete uma perda estimada de US$ 99 bilhões por parte dos consumidores americanos devido a fraudes digitais no último ano.

Um terço (33%) dos consumidores americanos relataram que o motivo da perda foi o roubo do cartão de crédito ou cobrança fraudulenta, 29% uso indevido de dados pessoais (roubo de identidade) e 27% a invasão de contas (ATO).

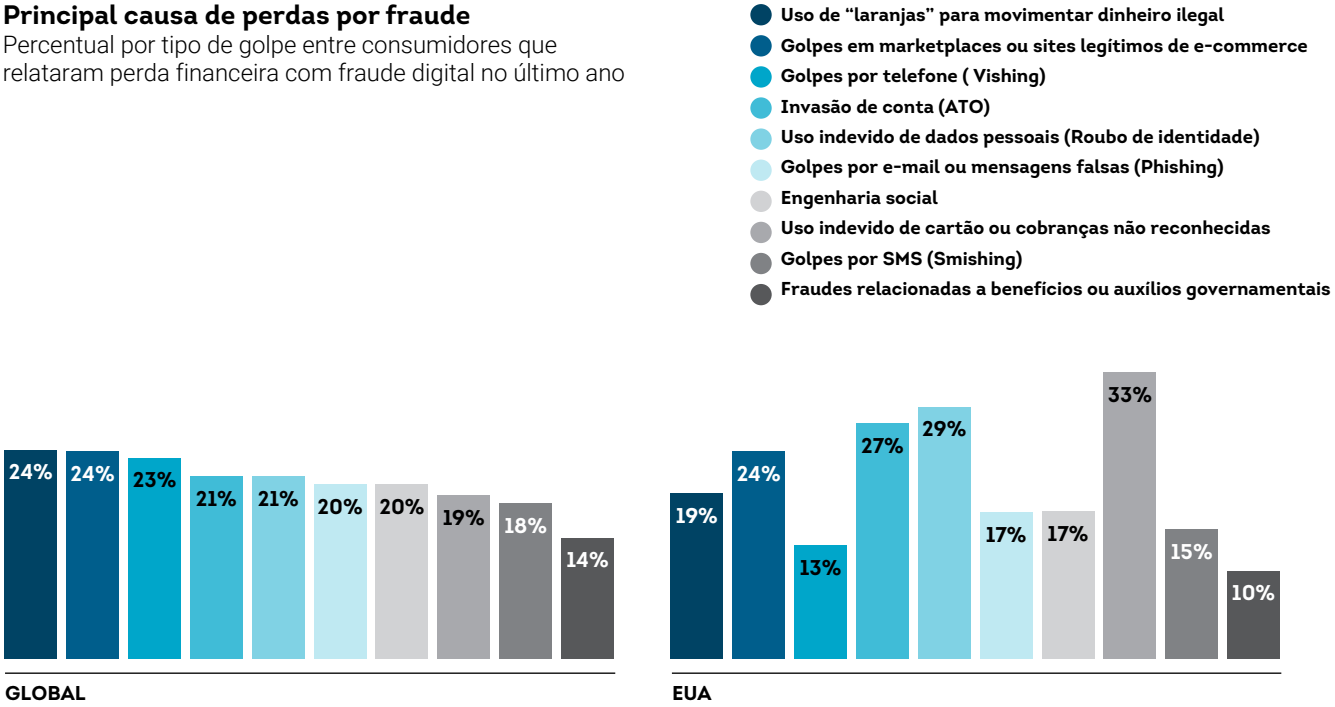
Perdas por fraude relatadas por consumidores
Perda média relatada por fraude (em USD) entre consumidores que afirmaram ter perdido dinheiro devido a fraudes digitais no último ano



*Conversão para USD com base na taxa de câmbio de 29 de dezembro de 2025
**A média global é a média dos 18 países entrevistados

Fonte: Pesquisa da TransUnion com pessoas consumidoras

Principal causa de perdas por fraude
Percentual por tipo de golpe entre consumidores que relataram perda financeira com fraude digital no último ano



Fonte: Pesquisa da TransUnion com consumidores

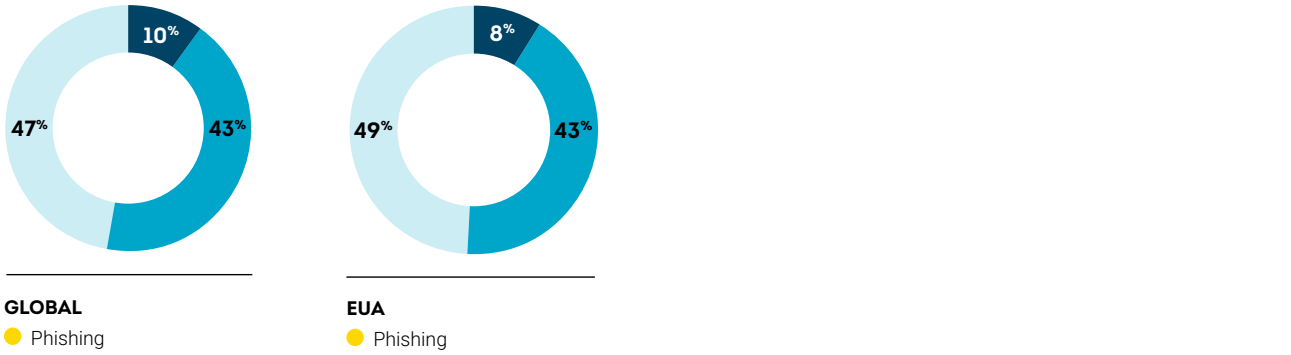
Phishing é o esquema de fraude mais relatado por consumidores

Mais da metade (51%) dos consumidores dos EUA relataram ter sido alvo de um esquema de fraude digital, e 8% disseram ter sido vítima entre agosto e dezembro de 2025. No entanto, uma parte significativa da população não reconheceu a fraude em potencial; 49% disseram não saber que estavam sendo alvo de esquemas de fraude. Esses números têm se mantido constantes nos últimos dois anos.

Phishing (e-mails, sites, posts em redes sociais, QR codes etc. fraudulentos que visam roubar dados) foi o esquema mais relatado; 39% dos consumidores americanos disseram ter sido alvo desse tipo de fraude. Em seguida, veio o smishing (mensagens de texto fraudulentas destinadas a enganar alguém para que revele dados), com 36%.

Consumidores alvo de fraude

Percentual de consumidores que afirmaram ter sido alvo de tentativas de fraude digital entre agosto e dezembro de 2025, e o esquema mais frequente relatado



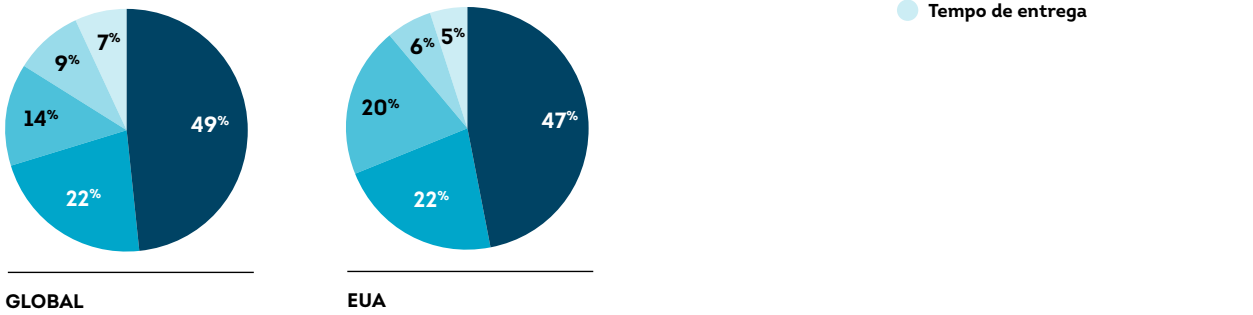
Fonte: Pesquisa da TransUnion com consumidores

Os consumidores preferem marcas que oferecem experiências digitais seguras e protegidas

Os americanos parecem entender os riscos de fazer negócios on-line, mas a conveniência é grande demais para ser ignorada. Quarenta e três por cento afirmaram realizar mais de 50% de suas transações on-line e 57% disseram que fazem mais de 50% da gestão de suas contas on-line. Mas, com a adoção dos canais digitais, as pessoas esperam que as experiências digitais das marcas sejam seguras e fáceis. As expectativas são altas — e os riscos são ainda maiores. Quarenta e dois por cento dos consumidores americanos trocariam de empresa por uma experiência digital melhor e 70% não retornariam a um site se percebessem qualquer risco de fraude.

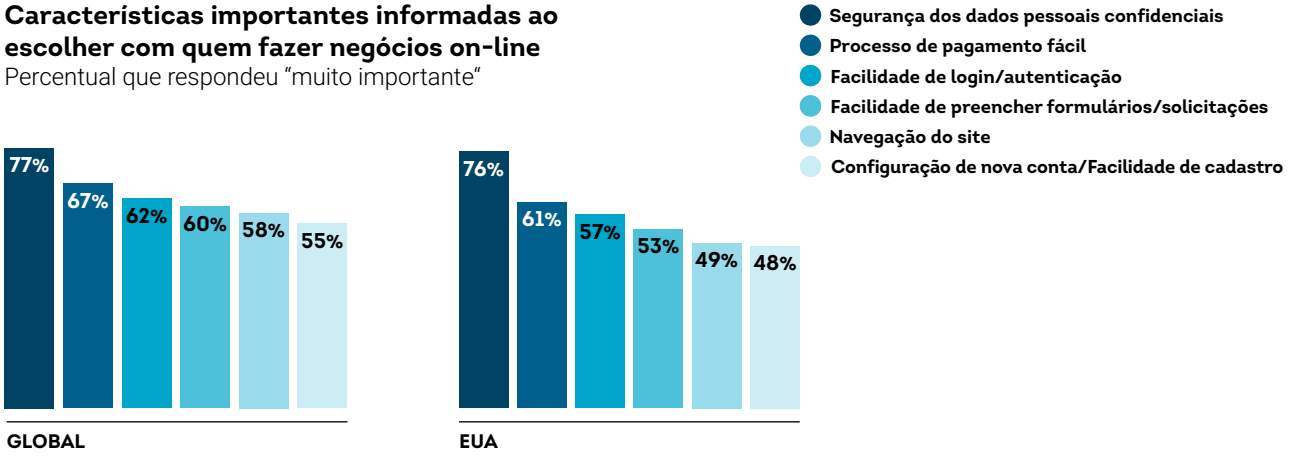
Conquistar a confiança é fundamental. Quase metade (47%) dos consumidores classificou a forte segurança de dados como sua principal expectativa em relação às empresas on-line, sendo essa a resposta mais frequente, e 76% afirmaram que a confiança de que seus dados pessoais estão protegidos é muito importante ao decidir onde fazer negócios, sendo essa a característica mais importante para eles. Além disso, 44% afirmaram que a preocupação com fraudes era um dos principais motivos para abandonar o carrinho de compras on-line, perdendo apenas para os custos de envio.

Classificação de expectativas/qualidades nas empresas on-line preferidas
Principais respostas escolhidas



Fonte: Pesquisa da TransUnion com consumidores

Características importantes informadas ao escolher com quem fazer negócios on-line
Percentual que respondeu "muito importante"



Fonte: Pesquisa da TransUnion com consumidores

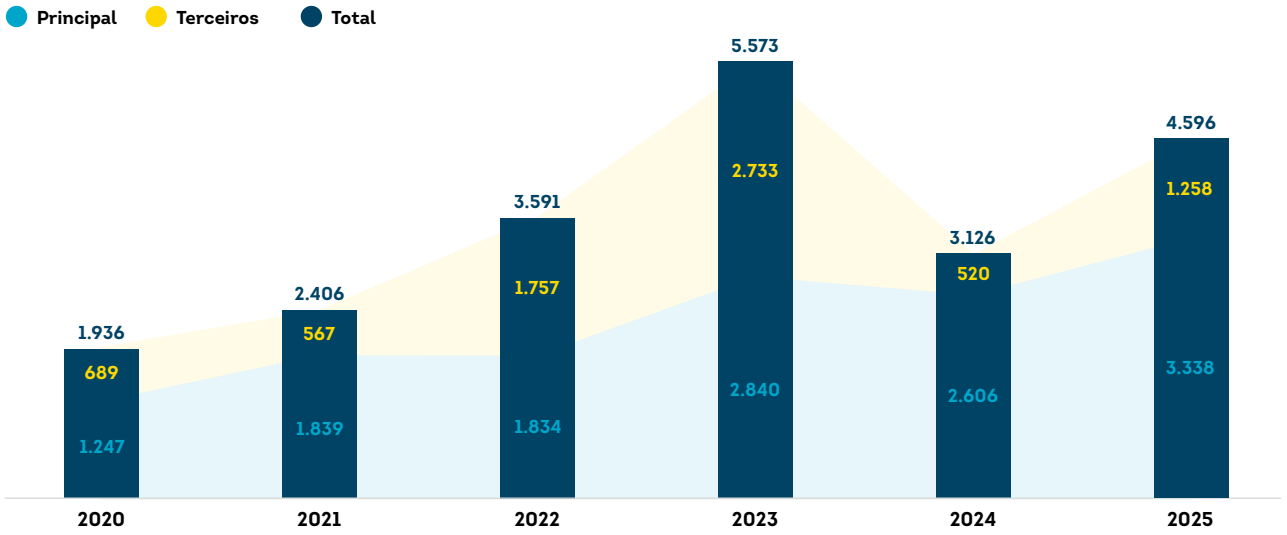
Tendências de exposição de dados pessoais

A gravidade dos vazamentos de dados nos EUA atinge níveis recordes

Os EUA registraram um aumento de 47% no volume de vazamentos de dados em 2025 em comparação com 2024. Os ataques pareciam buscar dados que não estavam prontamente disponíveis em mercados de dados da dark web para obter credenciais de dados pessoais para esquemas de fraude.

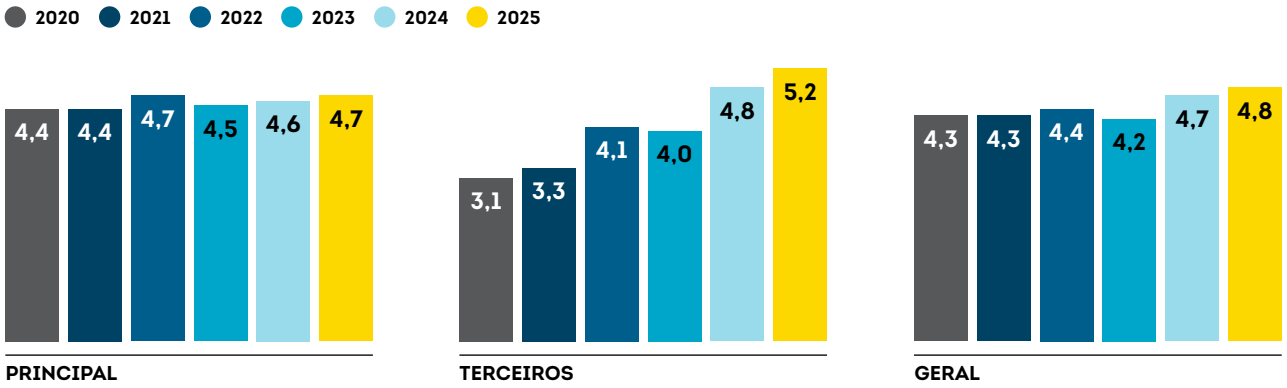
Criminosos visaram credenciais de alto risco, incluindo números completos do Seguro Social (SSN), o que elevou a gravidade média das violações (a capacidade de uma violação permitir fraude de identidade), medida pela pontuação de risco de violação (BRS) da TransUnion TruEmpower™, um indicador importante de fraudes futuras, ao seu nível mais alto desde que nossa análise começou em 2020. Violações de terceiros envolvendo ataques a organizações que fornecem serviços comerciais para marcas foram significativamente mais arriscadas do que aquelas direcionadas a organizações principais.

Volume de vazamentos de dados nos EUA



Fonte: Rede de inteligência global da TransUnion

Média da pontuação de risco de violação para vazamentos de dados nos EUA



Fonte: Rede de inteligência global da TransUnion

Um vazamento de dados primário representa um ataque direto a uma organização. Um vazamento de dados de empresas terceiras, também conhecido como "ataque à cadeia de suprimentos", "ataque à cadeia de valor" ou "violação de backdoor", ocorre quando um fraudador tem acesso à rede de uma entidade através de empresas fornecedoras ou prestadoras de serviços, como processamento de folha de pagamento ou cobrança médica, por exemplo.

O setor de saúde continua registrando altos níveis de comprometimentos de dados

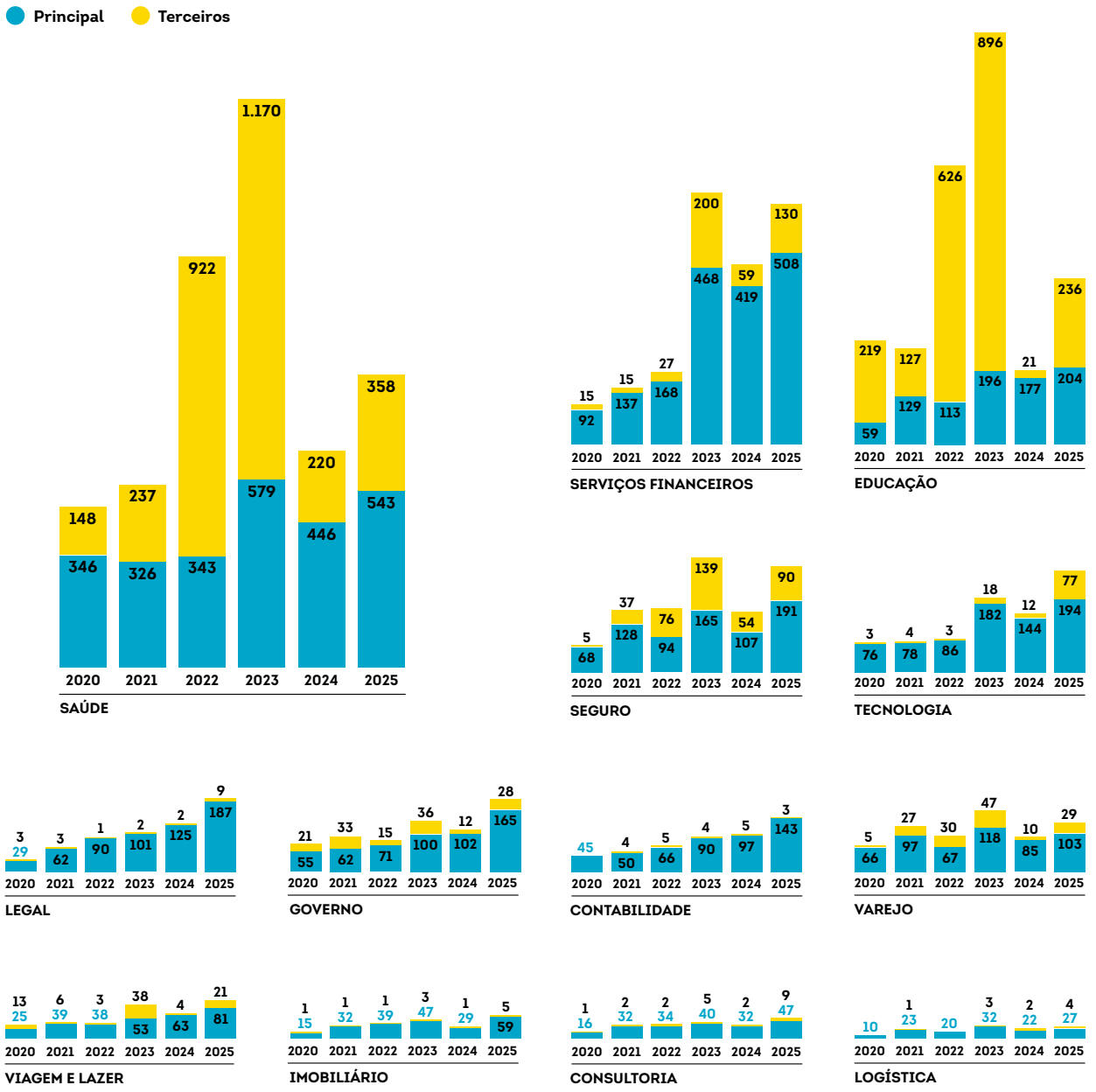
O maior número de violações de segurança em 2025 foi observado no segmento de saúde, seguido pelo de serviços financeiros. Entretanto, os segmentos de saúde e contabilidade empataram como os que apresentaram o maior BRS (5,1).

Tanto os ataques diretos quanto os indiretos na área da saúde têm como alvo credenciais de identidade valiosas, incluindo o número

o completo do Seguro Social (SSN), histórico médico, números de pagamento e informações de contato — todos importantes para perpetrar golpes contra consumidores e verificar dados já comprometidos.

Mais de 84% das violações de segurança em cada um dos quatro principais segmentos com alto índice BRS (saúde, contabilidade, direito e viagens e lazer) estavam relacionadas a ataques cibernéticos, em oposição a outros tipos de violações, como erros de sistema e erros humanos. Entretanto, os serviços financeiros e o governo registraram uma proporção abaixo da média de violações de segurança decorrentes de ataques cibernéticos.

Volume de vazamentos de dados nos EUA



Fonte: Rede de inteligência global da TransUnion

Criminosos visam credenciais de alto valor para invasão de contas (ATO) e onboarding

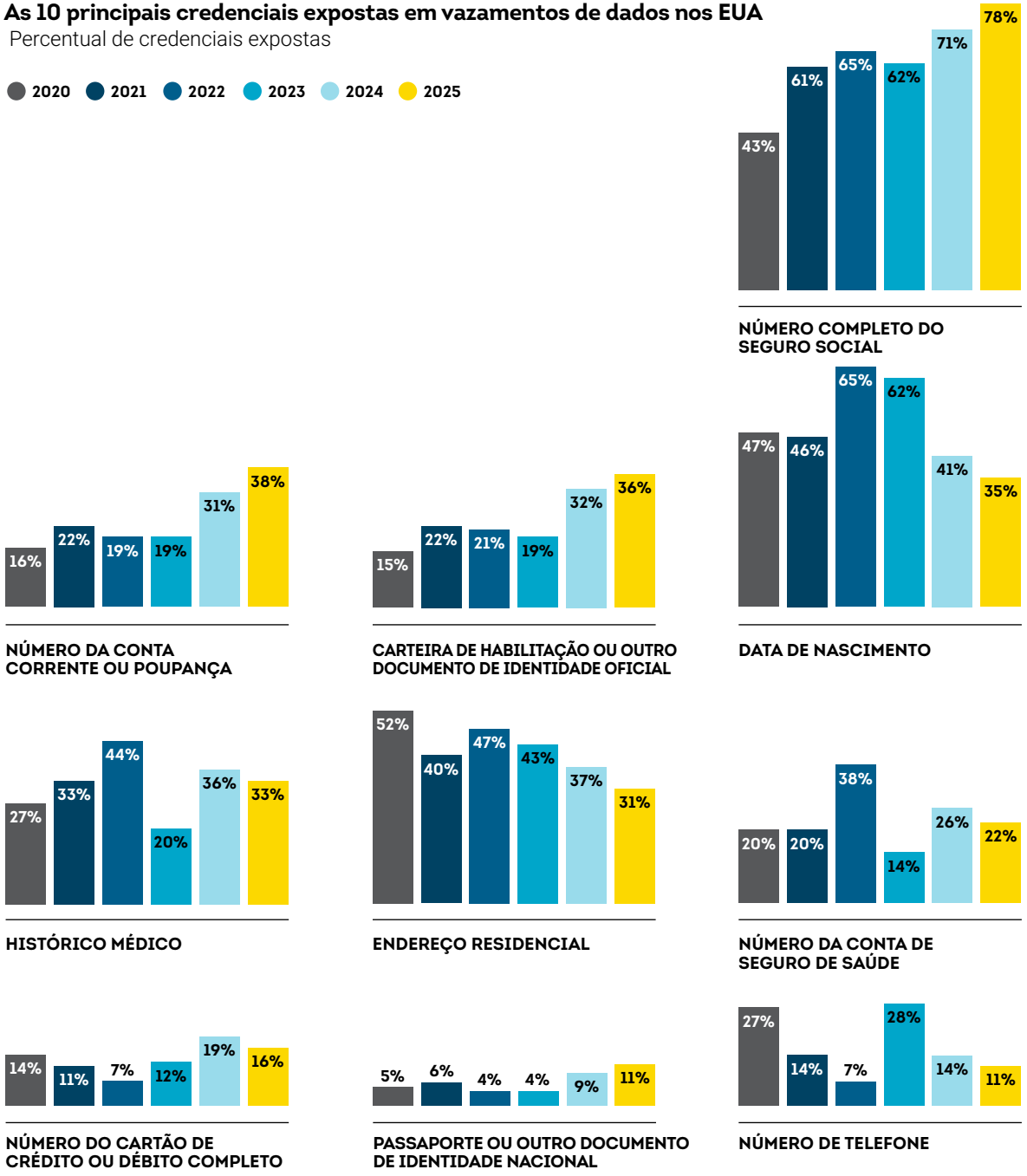
Os números de segurança social completos foram expostos em 78% de todas as vazamentos de dados em 2025, sendo consistentemente a credencial mais procurada desde 2021 e representando um aumento de 10% em relação a 2024. Essa é uma credencial vital para perpetrar fraudes de novas contas, ATO, em restituições de impostos e em benefícios governamentais.

Em 2025, pela primeira vez desde o início de nossa análise em 2020, a exposição de números de contas correntes e de poupança foi a segunda credencial mais exposta, aparecendo em 38% das vazamentos de dados em geral e em 41% das violações de terceiros. Essas exposições de credenciais de contas de depósito apresentaram um crescimento significativo, aumentando 138% no geral nos últimos seis anos e impressionantes 356% em violações de terceiros.

À medida que os criminosos cibernéticos procuram utilizar deepfakes da IA generativa para contornar sistemas de autenticação biométrica, a exposição de credenciais de identificação governamentais aumenta. A exposição de carteiras de motorista e outros documentos de identidade emitidos pelo estado cresceu 140% nos últimos seis anos, e a de passaportes, 120% no mesmo período. Históricos médicos (incluindo diagnósticos e médicos) foram incluídos em 33% das violações no geral, um aumento de 22% em seis anos, e em 45% das violações de terceiros, um aumento de 400%.

As 10 principais credenciais expostas em vazamentos de dados nos EUA

Percentual de credenciais expostas



Fonte: Rede de inteligência global da TransUnion

TransUnion

Tendências de fraude digital

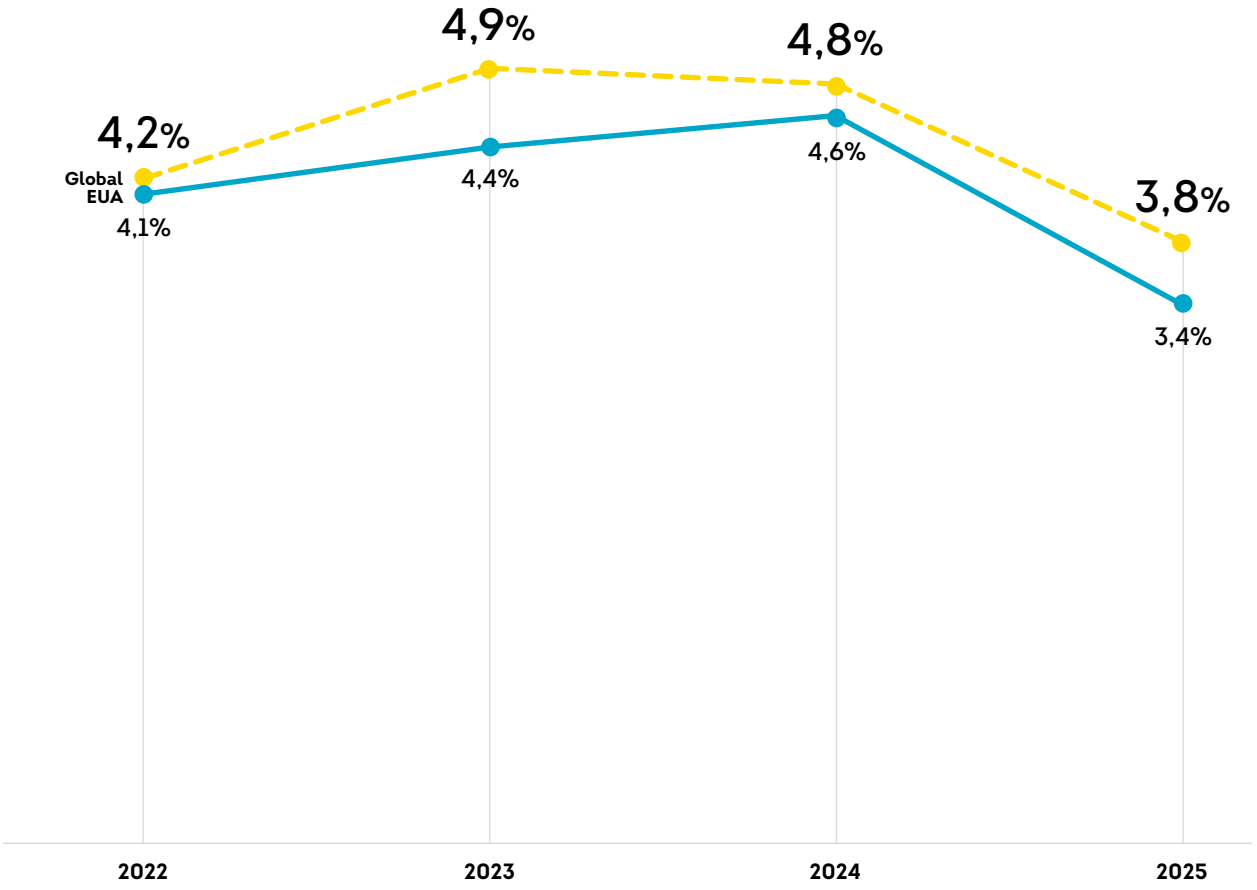
A taxa de fraudes digitais suspeitas diminuiu à medida que os ataques se tornam mais sofisticados

A taxa de suspeita de fraude digital em tentativas de transações em que o consumidor estava nos EUA caiu 26% em 2025 em comparação com 2024. A taxa caiu para 3,4% em 2025, ligeiramente abaixo da média global de 3,8%.

Os criminosos tendem a concentrar seus ataques de fraude nos alvos mais fáceis, ao mesmo tempo que utilizam ferramentas de IA para burlar sistemas de detecção de fraude desatualizados ou fragmentados. As tendências de risco de fraude digital parecem refletir isso, já que os fraudadores evitam tentar contornar diretamente sistemas de autenticação multifatorial mais robustos, optando, em vez disso, por usar golpes de phishing e vishing com IA generativa direcionados aos consumidores.

O acesso às credenciais de login dos consumidores encoraja os fraudadores a cometerem invasão de contas (ATO) com sucesso, utilizando técnicas para burlar senhas de uso único e aproveitar métodos de autenticação secundários, resultando em perdas médias maiores, como as prevalentes nos EUA. Além disso, o roubo de informações de identidade pessoal geralmente leva os criminosos a usar técnicas de IA generativa, como identidades sintéticas ou credenciais de identidade deepfake, e pode estar mascarando ataques de fraude sofisticados na abertura de novas contas — sem levantar suspeitas até que as perdas ocorram dias ou meses depois.

Taxa de suspeitas de fraude digital



Fonte: Rede de inteligência global da TransUnion

O segmento de comunidades apresentou os maiores riscos de fraude digital

O segmento de comunidades, que inclui propriedades da Web e aplicativos como grupos on-line e sites de namoro, experimentou o maior percentual (11,7%) de fraude digital suspeita para transações em que o consumidor estava nos EUA em 2025. Isso representa um aumento de 15% de 2024 para 2025 e um crescimento de 7% no volume de suspeitas de fraude digital entre esses dois períodos.

Outros segmentos ligados ao entretenimento também apresentaram taxas de risco de fraude acima da média. O segmento de jogos, incluindo sites e aplicativos de apostas on-line, continuou a registrar tentativas suspeitas de fraude digital em quase 1 a cada 10 transações (9,8%). Os jogos eletrônicos apresentaram uma taxa de suspeita de fraude digital de 8,3%. Vale destacar que o segmento de governo apresentou o maior aumento anual (19%) no número de tentativas suspeitas de fraude digital, dentre todos os segmentos analisados.

Tentativas de fraude digital nos EUA por segmento

- **Taxa de tentativas suspeitas de fraude em 2025**
- **Mudança percentual no volume de suspeitas de fraude digital de 2024 a 2025**

Comunidades
(namoro on-line, grupos etc.)

2025
11,7%

2024-2025
+7%

Jogos
(apostas, pôquer etc.)

2025
9,8%

2024-2025
0%

Jogos eletrônicos

2025
8,3%

2024-2025
-32%

Varejo

2025
3,8%

2024-2025
-41%

Serviços financeiros

2025
3,2%

2024-2025
-23%

Logística

2025
1,6%

2024-2025
-70%

Governo

2025
0,8%

2024-2025
+19%

Seguro

2025
0,5%

2024-2025
-19%

Telecomunicações

2025
0,4%

2024-2025
-22%

Viagem e lazer

2025
0,2%

2024-2025
-47%

Fonte: Rede de inteligência global da TransUnion

Riscos de fraude digital impactam todas as etapas da jornada do consumidor

Nos EUA, todas as etapas da jornada do consumidor apresentaram níveis semelhantes de risco de fraude digital. Em 2025, o onboarding era ligeiramente mais arriscada do que o login em contas existentes e as transações financeiras.

As tentativas de onboarding tiveram a maior taxa (3,8%) de fraude digital suspeita no ciclo de vida da pessoa consumidora para transações em que o usuário estava nos EUA em 2025; um valor consideravelmente menor do que os 8,3% globais. Em 2025, os logins de contas e as transações financeiras (3,6% e 3,3%, respectivamente) apresentaram riscos semelhantes quando o usuário estava nos EUA.

O risco digital no onboarding foi impulsionado por segmentos específicos: 35,2% de tentativas de onboarding em telecomunicações, 28,1% em varejo 21,3% nas comunidades foram suspeitas de fraude digital em 2025. Ao mesmo tempo, o seguro teve o maior risco de login de conta, com 42,7% das transações de login dos EUA suspeitas de fraude digital.

Exemplos de etapas da jornada do consumidor

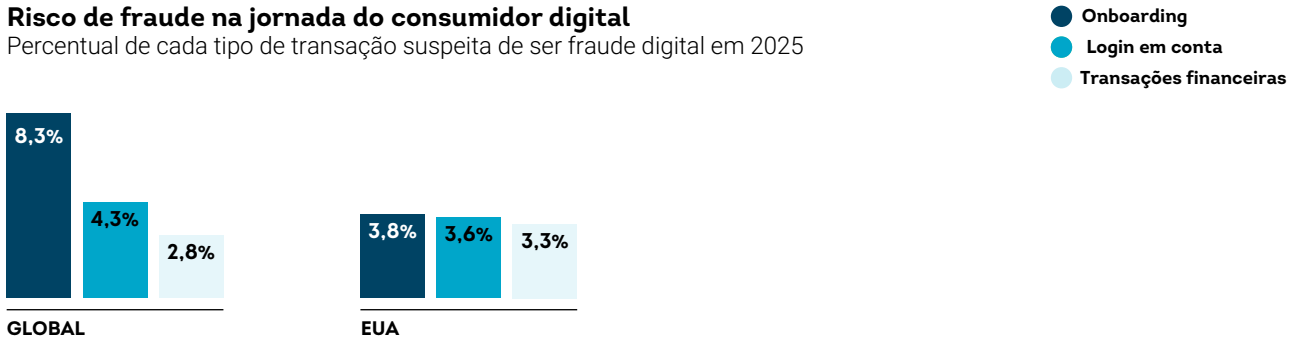
Onboarding: Cadastro de conta, registro e originação de empréstimo

Login em conta: Eventos de login com falha e bem-sucedidos

Transações financeiras: Compras, saques e depósitos

Risco de fraude na jornada do consumidor digital

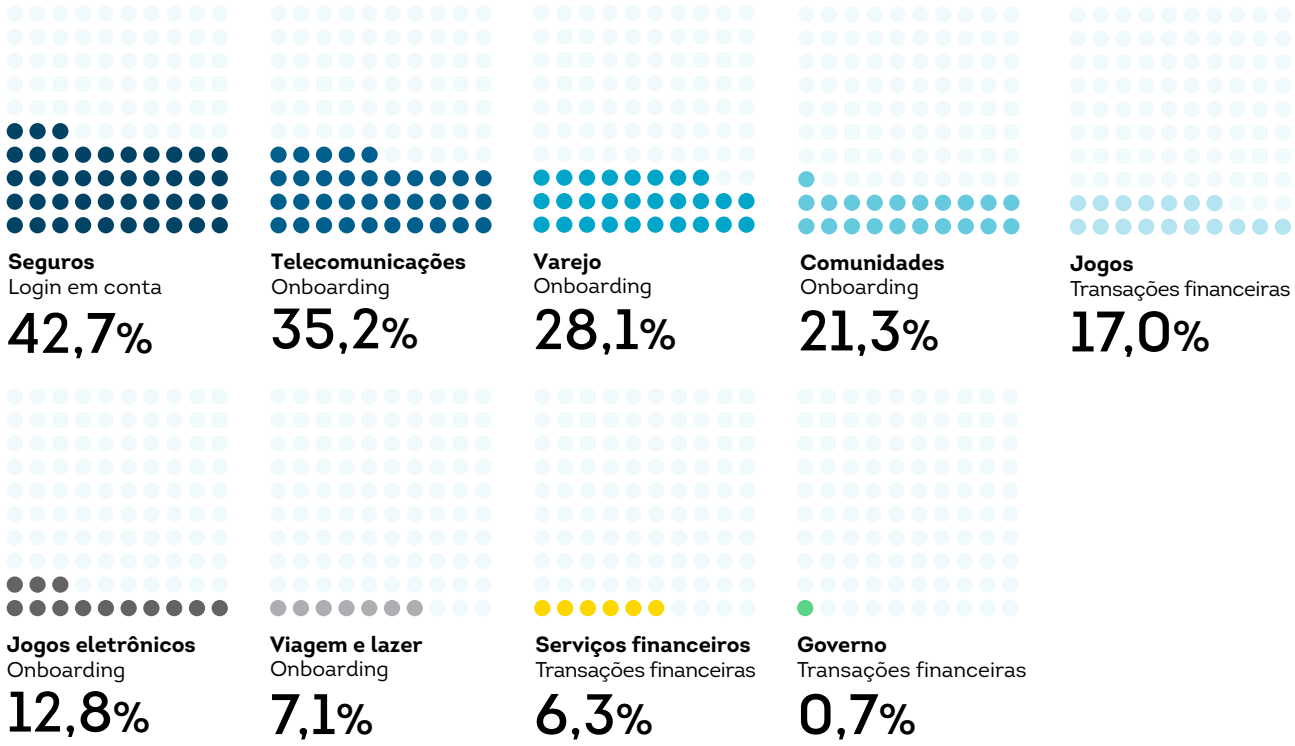
Percentual de cada tipo de transação suspeita de ser fraude digital em 2025



Fonte: Rede de inteligência global da TransUnion

Risco de fraude na jornada do consumidor digital por segmento

A etapada jornada do consumidor com a maior taxa de fraude digital suspeita nos EUA por segmento e o percentual correspondente nessa etapa em 2025



Fonte: Rede de inteligência global da TransUnion

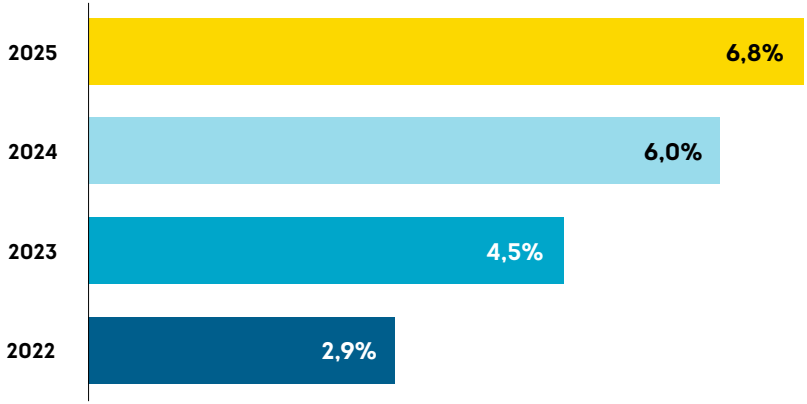
Tendências de fraude em call centers

As chamadas de alto risco para call centers continuam aumentando

Os call centers das organizações representam um canal de alta confiança do qual os consumidores dependem. Os call centers também são alvos de criminosos que visam facilitar a invasão de contas (ATO) por meio de engenharia social, induzindo os agentes a revelar dados de clientes ou alterar informações de contas.

Ao medir o risco de chamadas recebidas em call centers nos EUA, a TransUnion documentou um aumento de 13% (para 6,8%) no percentual de chamadas de alto risco entre 2024 e 2025. Chamadas de alto risco são aquelas que obtêm uma pontuação de 0 ou 100. As chamadas telefônicas de maior risco aumentaram em três dos quatro canais monitorados durante esse período.

Chamadas de alto risco para call centers nos EUA



Fonte: Rede de inteligência global da TransUnion

O risco de chamadas recebidas por dispositivos móveis aumenta nos call centers

A grande maioria (87%) das chamadas recebidas pelos clientes do call center da TransUnion nos EUA em 2025 foram feitas por meio de telefones celulares e apresentaram maior risco do que em 2024. Embora apenas 3,8% das chamadas móveis tenham sido identificadas como de maior risco de fraude, isso representa um aumento de 41% em relação aos 2,7% de 2024.

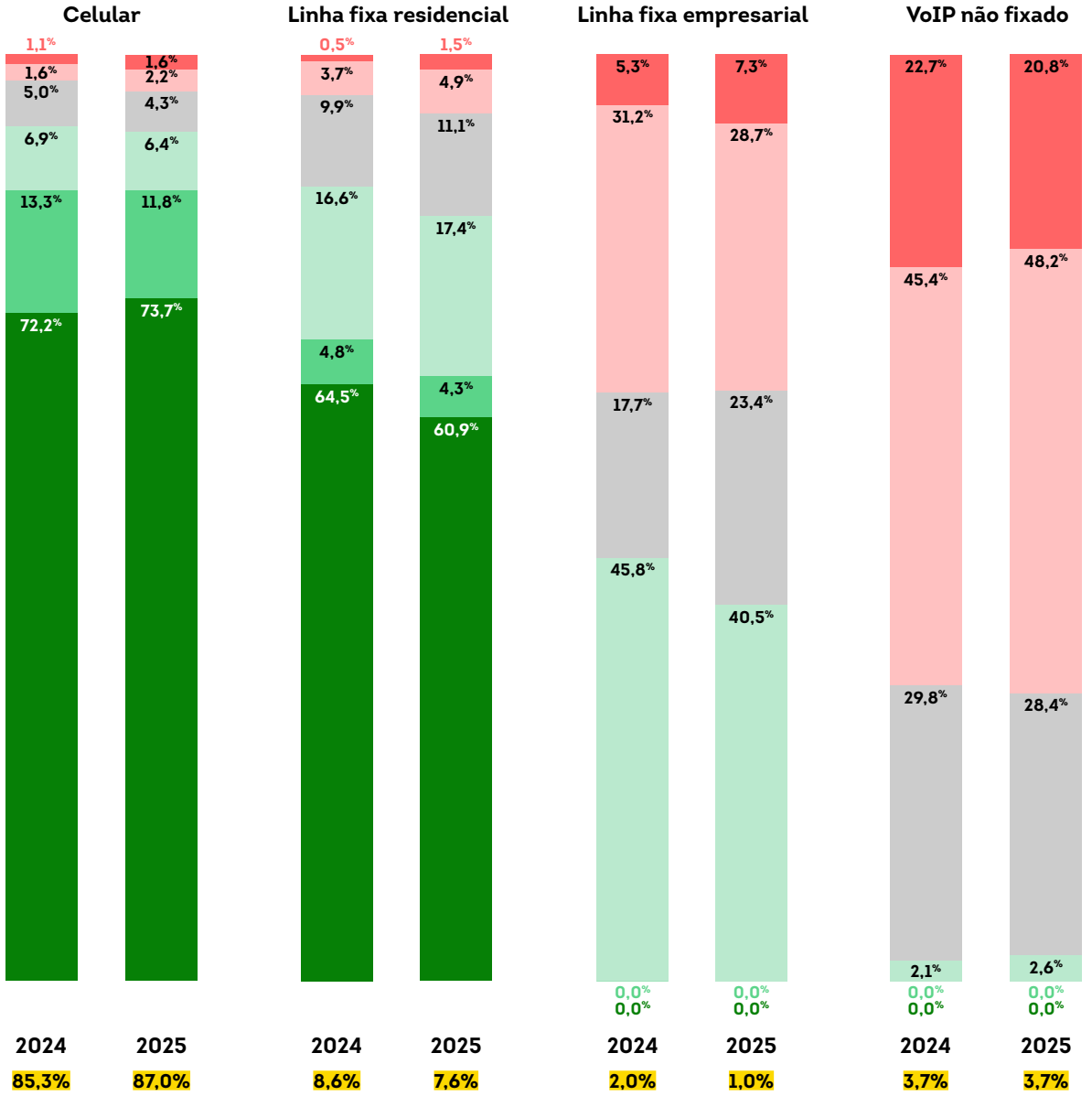
O canal mais arriscado para o call center era o Voz sobre Protocolo de Internet (Voice over Internet Protocol - VoIP) não fixo, um número de telefone que não está associado a um dispositivo físico. Embora esse canal representasse apenas 3,7% do volume total de chamadas, 69% dessas chamadas foram identificadas como de alto risco de fraude em 2025.

Risco por canal e volume total nos call centers dos EUA

>500 400 300 200 100 0 Volume geral

Classificação dos níveis de risco das chamadas

0 e 100: Mais alto; autenticação de nível superior
200-400: Níveis normais de autenticação
500+: Mais confiável; autenticação limitada



Fonte: Rede de inteligência global da TransUnion

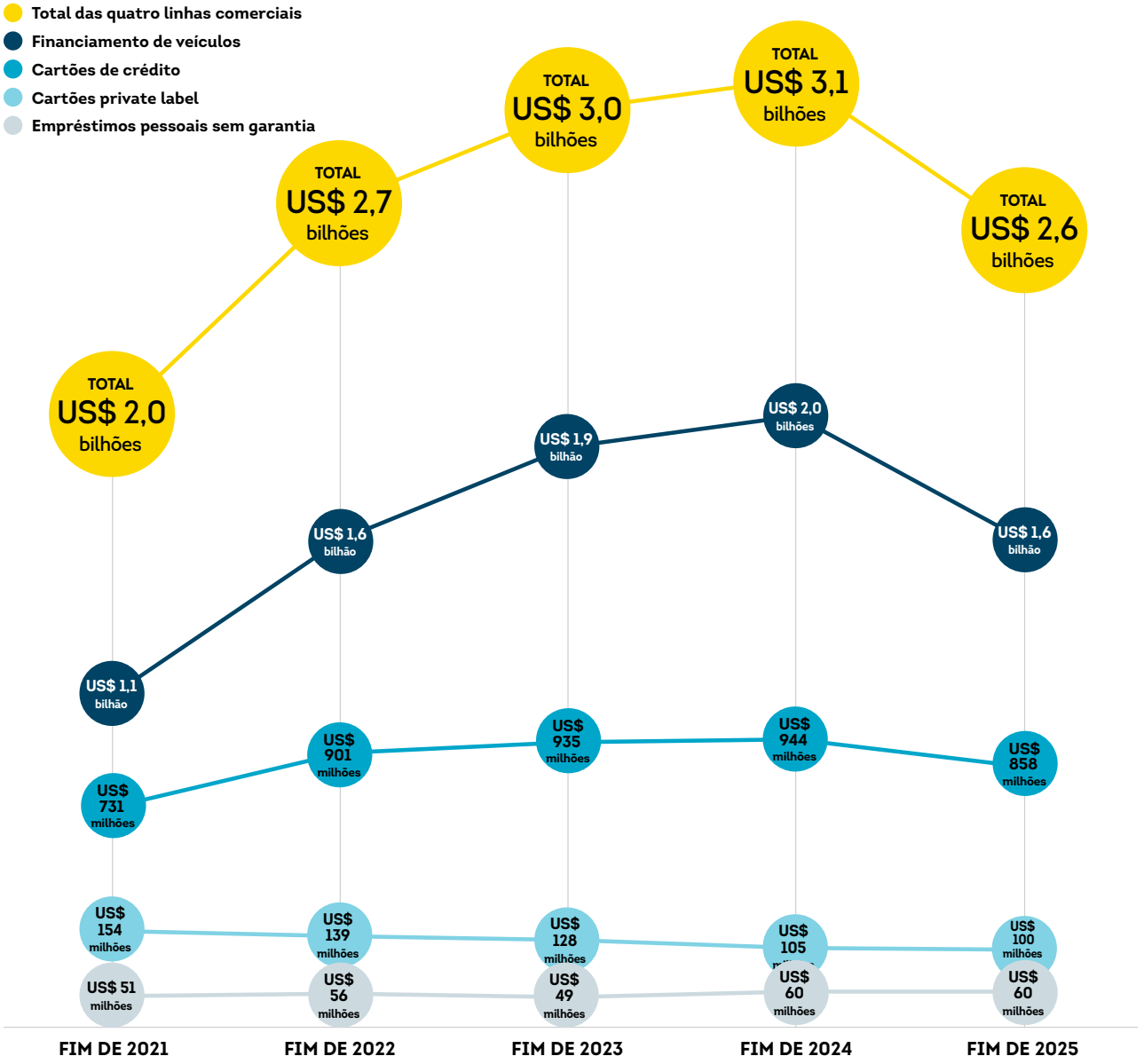
Tendências de fraude de identidade sintética e credit washing*

A exposição à identidade sintética em empréstimos permanece persistentemente alta

Identidades sintéticas continuam sendo um vetor de ataque de alto risco para os processos de criação de novas contas nas organizações, impulsionadas por credenciais comprometidas e potencializadas pela IA generativa. De acordo com os dados de crédito aos consumidores da TransUnion, a exposição total a identidades sintéticas entre contas abertas por empresas credoras dos EUA para financiamentos de veículos, cartões de crédito, cartões private label e empréstimos pessoais não garantidos atingiu US$ 2,6 bilhões em perdas potenciais no fim de 2025.

A criação de um histórico de crédito para estabelecer uma história pessoal verossímil continua sendo uma tática fundamental para identidades sintéticas, conferindo legitimidade e dificultando a detecção de perfis falsos. À medida que as ferramentas de IA generativa facilitam a geração de documentos deepfake realistas e a criação de identidades sintéticas em larga escala, os criminosos expandem suas atividades para além dos serviços financeiros. A queda na exposição ao crédito para empresas credoras nos EUA pode prenunciar uma mudança no uso de títulos sintéticos para segmentos menos preparados, como educação, FinTech, governo, saúde, varejo e telecomunicações, ampliando a área de atuação para fraudes com títulos sintéticos.

Risco de identidade sintética para empresas credoras dos EUA entre 2021 e 2025
O valor total de crédito (USD) ao qual as identidades sintéticas têm acesso para financiamento de veículos, cartões de crédito, cartões private label e empréstimos pessoais sem garantia nos EUA



Fonte: Rede de inteligência global da TransUnion
*As expressões e conceitos mencionados nesta página estão detalhados no glossário.

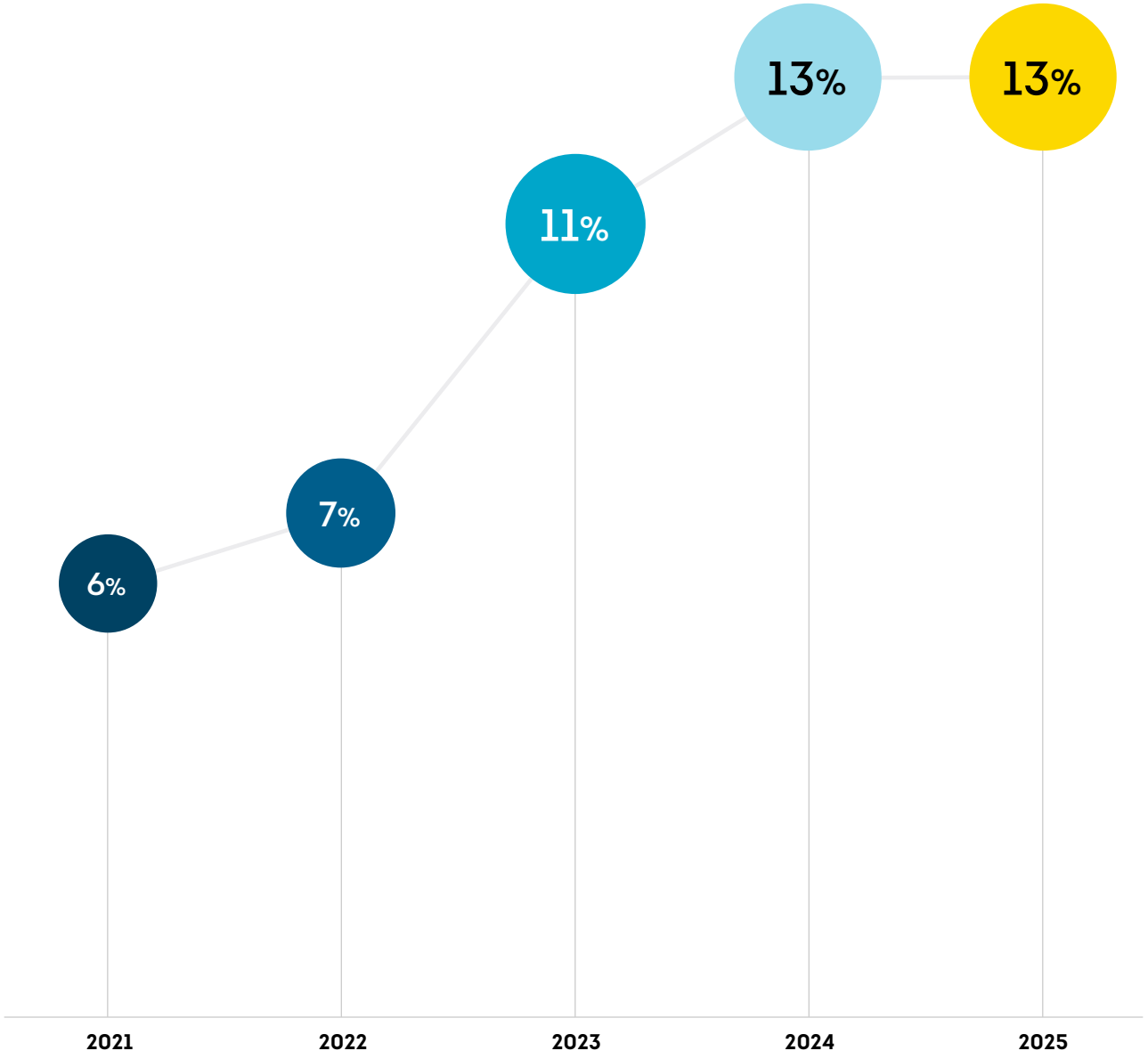
O credit washing permite reutilizar dados comprometidos

Criminosos utilizam dados manipulados ou sintéticos combinados com históricos de crédito construídos de forma legítima, tornando essas identidades difíceis de diferenciar de pessoas reais. Após serem utilizados, esses perfis podem ser abandonados ou reutilizados em novas fraudes. É aí que entra o credit washing.

Credit washing é um golpe de manipulação de crédito que visa remover informações negativas legítimas do histórico de crédito de uma pessoa, fazendo uma falsa alegação de fraude de identidade. Estas disputas de relatórios de crédito falsos podem ser feitas contra contas abertas usando uma identidade roubada de um consumidor ou uma identidade sintética, ou transações não autorizadas na conta de crédito legítima.

Os consumidores nos EUA (ou seus representantes autorizados) têm o direito legal de contestar itens imprecisos em seus relatórios de crédito, e a TransUnion segue um processo de resolução de disputas altamente regulamentado. Em 2025, as contestações de relatórios de crédito do consumidor nos EUA, alegando fraude, representaram 13% de todas as contestações, sem alterações em relação a 2024.

Percentual do total de litígios de consumidores nos EUA sobre relatórios de crédito que envolvem alegações de fraude



Fonte: Rede de inteligência global da TransUnion

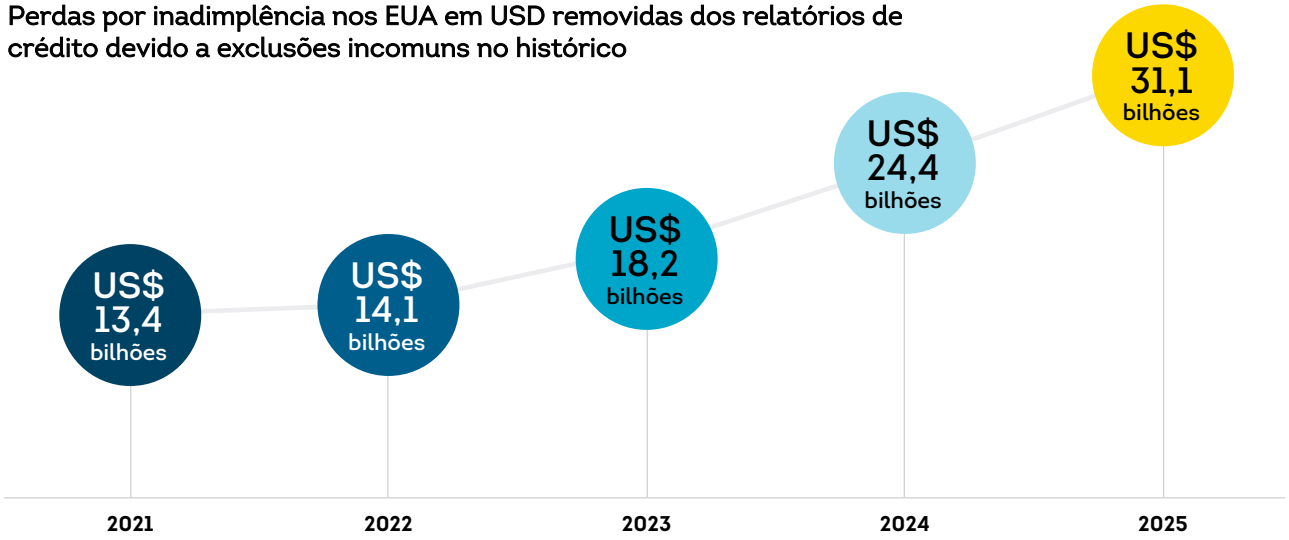
O crescimento atípico das baixas contábeis por supressão de crédito ilustra o risco de credit washing

Se uma dívida não for paga após um determinado período, as instituições financeiras normalmente a consideram como perda, denominando-a "baixa por inadimplência". As perdas por inadimplência são um risco conhecido no setor de empréstimos. Ao mesmo tempo, as dívidas não pagas resultam em um registro negativo no relatório de crédito de uma pessoa, afetando sua pontuação de crédito. No entanto, quando um relatório de crédito negativo — seja referente a um empréstimo, conta de crédito ou transação — é contestado com sucesso pelo consumidor como fraude, o resultado ainda é uma baixa contábil, mas o item é suprimido dos modelos de pontuação de crédito como se nunca tivesse ocorrido; o que é chamado de "supressão atípica" ou exclusão incomum.

Supressões atípicas podem ser relatadas às agências de crédito por instituições financeiras ou diretamente pelos consumidores através do processo de contestação de crédito. Embora seja uma ferramenta importante para os consumidores se protegerem contra fraudes, também pode ser um método usado por criminosos para reciclar identidades usadas para cometer fraudes, o chamado "credit washing".

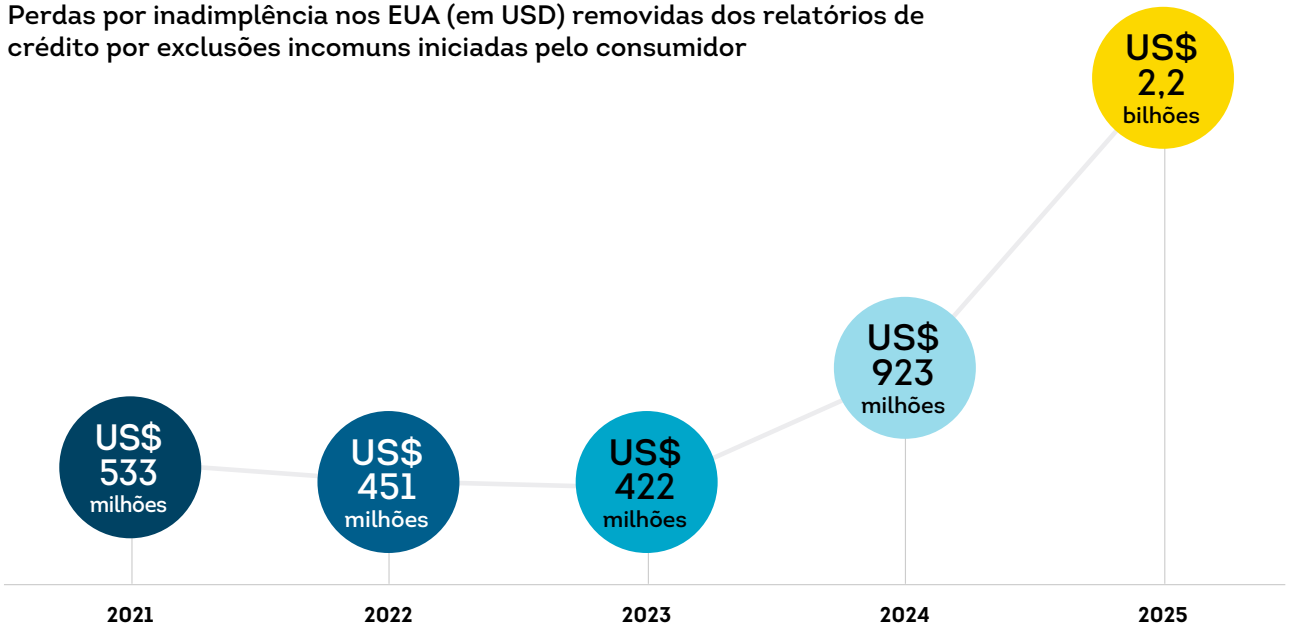
A dimensão do potencial de credit washing tem sido dramática, especialmente devido às supressões iniciadas pelos consumidores. As perdas por inadimplência apagadas dos relatórios de crédito dos EUA devido a supressão atípica cresceram 28% de 2024 para mais de US$ 31 bilhões no final de 2025. As supressões de baixas contábeis iniciadas pelo consumidor, que representam cerca de 7% de todas as supressões atípicas de baixas contábeis no final de 2025, aumentaram 138% desde o final de 2024, ultrapassando US$ 2 bilhões pela primeira vez.

Perdas por inadimplência nos EUA em USD removidas dos relatórios de crédito devido a exclusões incomuns no histórico



Fonte: Rede de inteligência global da TransUnion

Perdas por inadimplência nos EUA (em USD) removidas dos relatórios de crédito por exclusões incomuns iniciadas pelo consumidor



Fonte: Rede de inteligência global da TransUnion

TransUnion

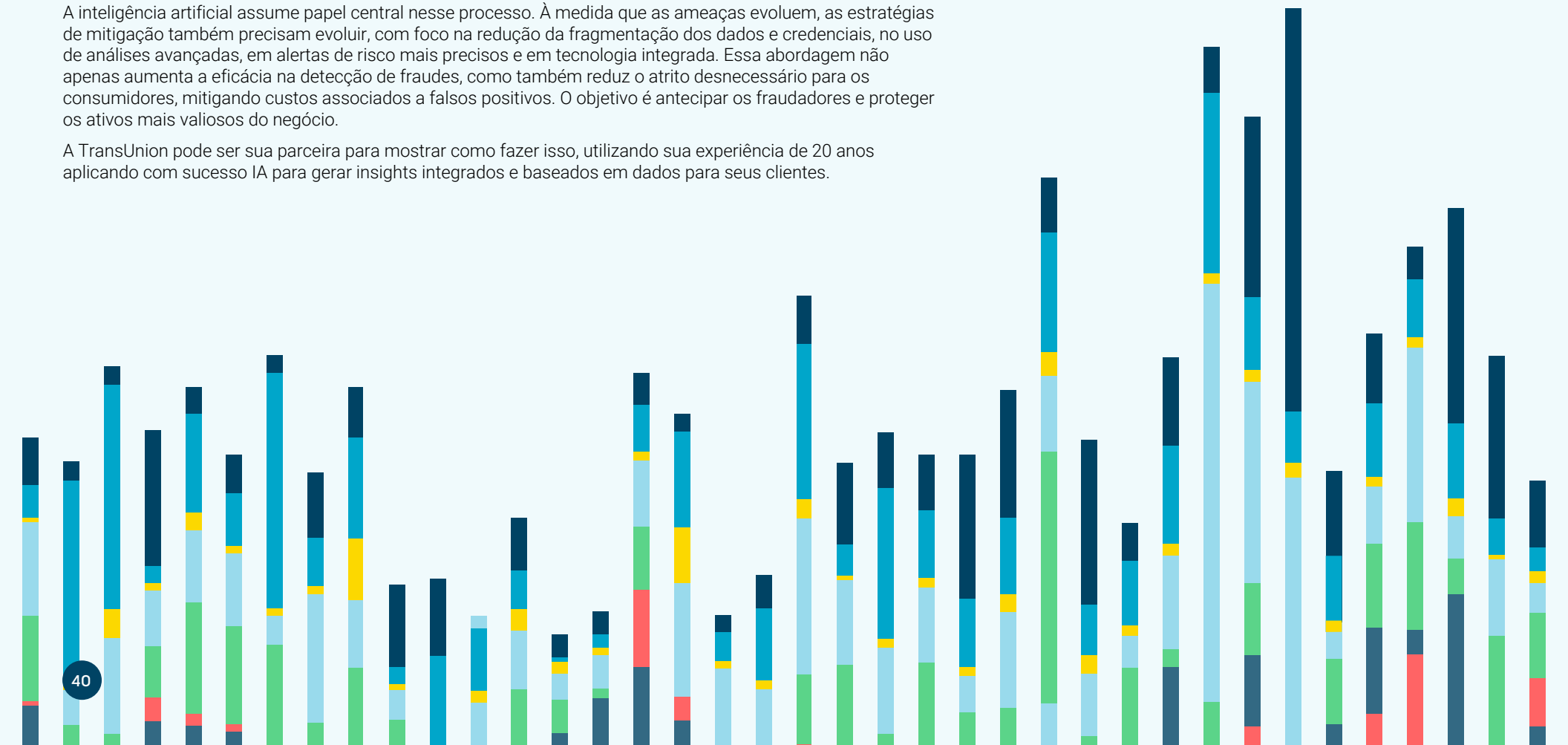
Conclusão

A fraude vem se consolidando como um desafio crescente para organizações de todos os portes e segmentos. Olhando para 2026 e além, os riscos tendem a se intensificar, à medida que os fraudadores aprimoram suas técnicas para evitar, contornar ou enganar os mecanismos de defesa existentes. Vazamentos de dados e golpes continuarão a comprometer credenciais, tornando essencial proteger simultaneamente a organização e seus consumidores. O desafio central passa a ser inspirar confiança sem reduzir os níveis de controle, preservando, ao mesmo tempo, uma experiência fluida para o cliente.

Com riscos associados aos dados pessoais e credenciais de alto valor presentes em todo a jornada do consumidor, investir em detecção de fraudes mais inteligente deixou de ser um diferencial competitivo e passou a ser uma necessidade operacional e estratégica. Isso exige uma abordagem holística e integrada de prevenção a fraudes em toda a organização. Ambientes fragmentados ampliam a exposição ao risco, o que reforça a importância de eliminar silos e fortalecer todas as camadas de defesa — da verificação de dados e documentos à autenticação e ao monitoramento de sessões — com maior adaptabilidade, inteligência e capacidade de avaliação de risco.

A inteligência artificial assume papel central nesse processo. À medida que as ameaças evoluem, as estratégias de mitigação também precisam evoluir, com foco na redução da fragmentação dos dados e credenciais, no uso de análises avançadas, em alertas de risco mais precisos e em tecnologia integrada. Essa abordagem não apenas aumenta a eficácia na detecção de fraudes, como também reduz o atrito desnecessário para os consumidores, mitigando custos associados a falsos positivos. O objetivo é antecipar os fraudadores e proteger os ativos mais valiosos do negócio.

A TransUnion pode ser sua parceira para mostrar como fazer isso, utilizando sua experiência de 20 anos aplicando com sucesso IA para gerar insights integrados e baseados em dados para seus clientes.



Glossário

Táticas de fraude baseadas em identidade potencializadas pela IA

Credit Washing: Manipulação do histórico de crédito para que a identidade falsa pareça confiável.

Deepfakes: Mídias sintéticas realistas que manipulam rostos/vozes para enganar.

Identidade Sintética: Tipo de fraude que combina dados reais com informações falsas para criar uma identidade fictícia. Essa prática é comum em países que não possuem um identificador único nacional, pois a ausência de um dado central dificulta a validação cruzada. No Brasil, esse risco é significativamente reduzido devido à existência do CPF como identificador único, aliado a mecanismos avançados de validação e integração de bases governamentais e privadas. Por isso, a ocorrência de fraude por identidade sintética é considerada pouco provável no contexto brasileiro.

Injeção: Envio de imagens ou vídeos manipulados diretamente aos sistemas de verificação para enganar biometria ou prova de vida.

Personificação: Fingir ser organização/entidade confiável para enganar e obter acesso/dados.

Spoofing: Falsificação de identidade/endereços digitais para se passar por fonte legítima.

Principais causas das perdas por fraude

Fraudes relacionadas a benefícios ou auxílios governamentais: Golpe em que criminosos se passam por programas oficiais para enganar vítimas e obter dados pessoais ou dinheiro, prometendo falsos benefícios governamentais.

Golpes em marketplaces ou sites legítimos de e-commerce: Uso de plataformas reais para roubar ou revender identidades.

Golpes por e-mail ou mensagens falsas (Phishing): Golpe realizado por e-mails falsos que simulam comunicações legítimas para obter dados sensíveis.

Golpes por SMS (Smishing): Fraude por mensagens SMS contendo links falsos que direcionam para páginas fraudulentas ou instalam softwares maliciosos.

Golpes por telefone (Vishing): Golpe por ligações telefônicas fraudulentas, em que criminosos se passam por representantes de instituições (ex. Bancos) para obter informações pessoais.

Golpes que manipulam o comportamento do consumidor (Engenharia social): Técnica em que golpistas se passam por clientes e usam persuasão para enganar atendentes e obter informações ou acessos indevidos.

Invasão de contas (ATO): Acesso indevido a contas reais, como bancárias ou de redes sociais, por meio de credenciais roubadas.
Roubo de identidade: Uso indevido de dados pessoais para se passar por alguém.

Uso de "laranjas" para movimentar dinheiro ilegal: Uso de terceiros para movimentar dinheiro ilícito.

Uso indevido de cartão ou cobranças não reconhecidas: Uso não autorizado de cartão para compras ou cobranças indevidas.

Metodologia de fornecimento de dados

Este relatório combina dados proprietários da rede de inteligência global da TransUnion e pesquisas com consumidores.

Call center

As conclusões sobre call center da TransUnion foram baseadas predominantemente em dados de instituições financeiras de grande e pequeno porte com sede nos EUA. A taxa ou percentual de chamadas consideradas de alto risco foi determinada com base na avaliação de vários fatores de risco.

Disputas de relatórios de crédito de consumidores

As conclusões sobre disputa do relatório de crédito de consumidores da TransUnion foram baseadas em dados de crédito de consumidores dos EUA dos estados, territórios, protetorados e bases militares dos EUA e no exterior. Eles são frequentemente extraídos de mais de 50 anos de dados de crédito de consumidores e contêm informações de crédito de cerca de 400 milhões de pessoas.

Pesquisa com consumidores

Esta pesquisa on-line com foi realizada de 20 de novembro a 9 de dezembro de 2025 no Brasil (1.000 pessoas entrevistadas), Canadá (999), Chile (499), Colômbia (853), República Dominicana (415), Hong Kong (1.000), Índia (950), Quênia (495), México (500), Namíbia (308), Filipinas (821), Porto Rico (218), Ruanda (308), África do Sul (1.000), Espanha (999), Reino Unido (1.000), EUA (1.000) e Zâmbia (365) pela TransUnion em parceria com o provedor de pesquisa terceirizado, Dynata. Pessoas adultas de 18 anos ou mais foram entrevistadas por meio de um método de pesquisa painel on-line em uma combinação de computador, celular e tablet. As perguntas da pesquisa foram administradas em chinês (Hong Kong), inglês, francês (Canadá), português (Brasil) e espanhol (Colômbia, República Dominicana, México, Porto Rico e Espanha). Para garantir a representatividade na metodologia de fornecimento de dados entre os dados demográficos de residentes, a pesquisa incluiu cotas para equilibrar as respostas entre as principais demografias, como idade, gênero e renda familiar. Observe que alguns percentuais do gráfico podem não somar 100% devido ao arredondamento ou à variedade das respostas aceitas.

Vazamentos de dados

A TransUnion obtém seus próprios dados sobre violações em parceria com o Identity Theft Resource Center (ITRC). A equipe do ITRC monitora todos os eventos de exposição de dados reportados publicamente, desde fontes que incluem órgãos estaduais de procuradores-gerais, comunicados de imprensa de entidades violadas, escritórios de advocacia, especialistas em segurança cibernética, entre outros. A TransUnion expande os dados do ITRC com um processo que calcula os principais riscos de cada violação, as etapas apropriadas da pessoa consumidora e a pontuação de risco de violação (BRS). A BRS se baseia na quantidade e na gravidade das credenciais de identidade específicas que a entidade afetada considerou terem sido expostas. Dentre as 60 possíveis escolhas de credenciais de identidade, cada violação passa pelo perfil de ameaça de identidade TruEmpower da TransUnion para produzir um padrão e uma pontuação de risco e ações prescritas às pessoas consumidoras. A BRS usa uma escala de 1 a 10, em que 1 representa a menos grave e 10 representa a mais grave.

Fraude digital

A TransUnion usa a inteligência de bilhões de transações originadas de mais de 40.000 sites e aplicativos. As tentativas de fraudes digitais suspeitas refletem aqueles que os clientes da TransUnion disseram atender a uma das seguintes condições com base nos indicadores de risco de dispositivos: 1) negação em tempo real devido a indicadores fraudulentos; 2) negação em tempo real por violações da política corporativa; 3) fraude após investigação do cliente; ou 4) uma violação da política corporativa mediante condições de investigação do cliente. As análises nacionais e regionais examinaram transações em que o consumidor ou o fraudador suspeito estavam em determinado país ou região ao conduzir uma transação.
A estatística global representa todos os países do mundo, e não apenas países e regiões selecionados.

Fraude sintética

As conclusões sobre fraudes sintéticas da TransUnion foram baseadas em dados de crédito de pessoas consumidoras dos EUA dos estados, territórios, protetorados e bases militares dos EUA e no exterior. Eles são frequentemente extraídos de mais de 50 anos de dados de crédito de pessoas consumidoras e contêm informações de crédito de cerca de 400 milhões de pessoas. A análise de fraudes sintéticas abrange atividades de crédito dos EUA registradas entre 1º de janeiro de 2009 e 31 de dezembro de 2025. As medidas de exposição do credor se baseiam na fórmula proprietária da TransUnion para capturar uma possível perda total em risco para as empresas credoras.

SOBRE A TRANSUNION (NYSE: TRU)

A TransUnion é uma empresa global de informações e insights com mais de 13.000 colaboradores que opera em mais de 30 países. Tornamos a confiança possível assegurando que cada pessoa seja representada de forma confiável no mercado. Fazemos isso com uma imagem real de cada pessoa: uma visão prática dos consumidores, administrada com cuidado. Por meio de nossas aquisições e investimentos em tecnologia, desenvolvemos soluções inovadoras que vão além de nossa sólida base em crédito, expandindo para áreas como marketing, fraude, risco e análise avançada. Como resultado, as empresas e as pessoas podem realizar transações com confiança e alcançar grandes resultados. Chamamos isso de Informação para o Bem®, que ajuda a criar oportunidades econômicas, experiências incríveis e empoderamento pessoal para milhões de pessoas em todo o mundo.

transunion.com/business

TransUnion