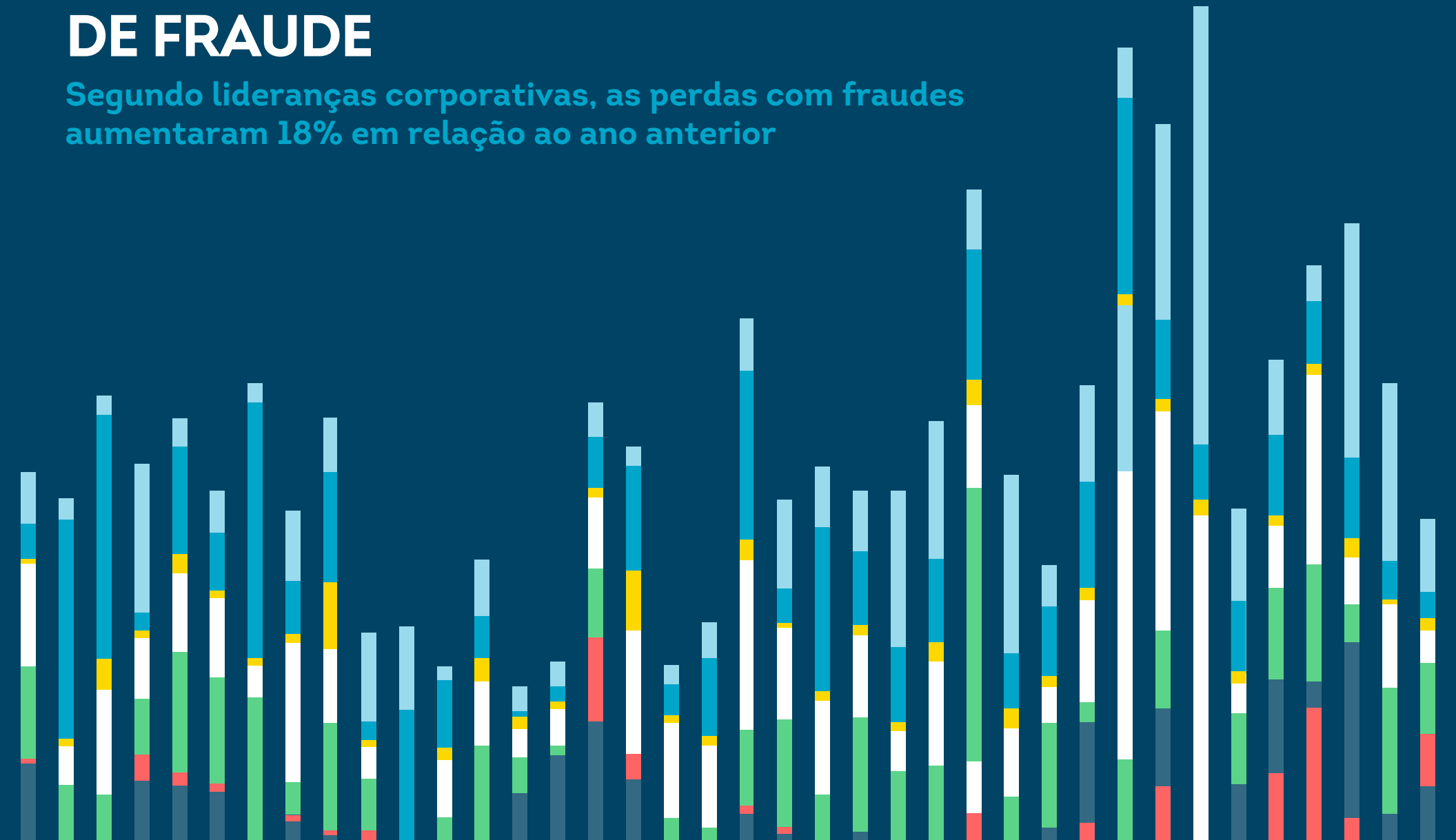
TransUnion

ATUALIZAÇÃO | 2º SEMESTRE DE 2025:

PRINCIPAIS TENDÊNCIAS DE FRAUDE

Segundo lideranças corporativas, as perdas com fraudes aumentaram 18% em relação ao ano anterior



Resumo executivo

Fraudes estão evoluindo rapidamente, e as equipes de prevenção enfrentam desafios para acompanhar esse ritmo. A grande quantidade de dados de identidades comprometidas ameaça sobrecarregar os sistemas de detecção, permitindo que agentes mal-intencionados explorem diferentes etapas da jornada digital do consumidor. Esse cenário crítico foi o pano de fundo das tendências observadas no primeiro semestre de 2025.

O risco crescente de abertura de contas com identidades sintéticas* , roubadas ou adulteradas expõe sua organização a fraudes cada vez mais sofisticadas. Golpes direcionados a consumidores — como aqueles em que o próprio titular autoriza o acesso do fraudador — e invasões de contas aumentaram significativamente, colocando sua marca e seus clientes em risco.

Para se antecipar a essas ameaças, é essencial ter uma visão clara da identidade, garantindo maior proteção contra usuários de risco e, ao mesmo tempo, aprimorando a experiência dos clientes legítimos.

Na atualização do **Relatório de Principais Tendências de Fraude da TransUnion®** – 2º semestre de 2025, reunimos benchmarks e dados da rede global de insights de fraudes da TransUnion. O relatório foi desenvolvido para apoiar profissionais responsáveis por estratégias de mitigação de riscos e melhoria da experiência do cliente, com foco em resultados de negócio.

Aproveite as informações deste relatório para avaliar programas de prevenção a fraudes no contexto do mercado como um todo. Compartilhe com as pessoas da sua organização, aumentando a satisfação de clientes, reduzindo a ocorrência de fraudes e aprimorando o desempenho do negócio.

*Identidade sintética é uma 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.

PRINCIPAIS DESTAQUES

O custo das fraudes para as empresas dispara

7,7%

da receita anual, em média, foi perdida devido a fraudes no ano passado, representando prejuízo de US$ 534 bilhões entre 1.200 líderes empresariais entrevistados em 2025

24%

das lideranças corporativas disseram que golpes foram as maiores fontes de perda por fraude, seguidos por 20% que apontaram a invasão de contas

A invasão de contas aumenta a curto e longo prazo

21%

de aumento no volume de invasões de contas digitais do 1º semestre de 2024 ao 1º semestre de 2025

141%

de aumento no volume de invasões de contas digitais do 1º semestre de 2021 ao 1º semestre de 2025

O onboarding foi a fase mais arriscada no ciclo de vida dos consumidores

8,3%

de todas as tentativas de **onboarding** no 1º semestre de 2025 foram suspeitas de fraude, o que torna essa a fase de maior risco no ciclo de vida do consumidor

26%

de aumento na taxa de **transações com suspeita de** fraude digital **em** tentativas de **onboarding** do 1º semestre de 2024 (quando era 6,6%) ao 1º semestre de 2025

Todos os dados deste relatório combinam insights proprietários da rede de inteligência global da TransUnion, uma pesquisa corporativa especialmente encomendada no Canadá, em Hong Kong, na Índia, nas Filipinas, no Reino Unido e nos EUA, e uma pesquisa com consumidores em 18 países e regiões ao redor do mundo. Na metodologia encontrada na página 21, veja definições de fraude digital e outros tipos de fraude. A primeira metade ou o 1º semestre vai de 1º de janeiro a 30 de junho, e a segunda metade ou o 2º semestre vai de 1º de julho a 31 de dezembro.

Sumário

TransUnion

Anatomia dos riscos ligados à identidade digital

As identidades digitais dos consumidores - fundamentais para decisões de negócio diárias - tornaram-se altamente vulneráveis e, em muitos casos, pouco confiáveis. Por quê? Existe um mercado ativo de roubo de identidade que opera nas áreas mais obscuras da web, sustentando esquemas fraudulentos cada vez mais sofisticados.

As tendências observadas no primeiro semestre de 2025 confirmam essa realidade: vazamentos de dados, golpes por telefone com pressão psicológica e fraudes direcionadas à obtenção de informações pessoais são apenas alguns exemplos. Criminosos utilizam dados roubados ou coletados para criar identidades falsas, explorando vulnerabilidades ao longo de todo o ciclo de vida do consumidor. Entre as práticas mais comuns estão a criação de perfis sintéticos, o uso de deepfakes e a aquisição de credenciais para invasão de contas.

Dependendo do sucesso do ataque inicial, fraudadores podem aplicar estratégias adicionais para contornar autenticações multifator, manter identidades sintéticas ativas ou recorrer a práticas como credit washing para reabilitar perfis aparentemente confiáveis.

Ao longo do último ano, essa "cadeia de suprimentos" criminosa tornou-se altamente especializada. Agentes mal-intencionados passaram a focar no roubo de credenciais de alto valor para viabilizar esquemas específicos. Quando somamos essa dinâmica à evolução da IA generativa, temos um cenário ainda mais preocupante: tecnologia sendo usada para potencializar dados comprometidos, criar identidades sintéticas mais convincentes, deepfakes e ataques de spoofing - tanto contra organizações quanto contra clientes.

Riscos ligados à identidade digital e intensificados por dados comprometidos de consumidores[1]

Captação (Como os golpistas obtêm seus dados)

- Vazamentos de dados
- Ataques de phishing
- Ataques de smishing
- Ataques de vishing
- Infecções por malware
- Engenharia social de *call centers*

Distribuição (Onde os dados roubados vão parar)

- Grupos clandestinos
- Marketplaces na dark web

Preparação (Como eles se preparam para usar os dados)

- Criação de identidade sintética
- Teste de credencial
- Validação de credencial
- Criação de deepfake

Exploração (Quando começam a aplicar os golpes)

- Onboarding
- Invasão de conta
- Transações financeiras
- Troca de SIM/invasão de OTP (senhas de uso único)

Refinamento (Como eles mantêm o golpe funcionando)

- Credit washing
- Manutenção de identidade sintética
- Manipulação de perfil

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

TransUnion

TENDÊNCIAS DE FRAUDE GLOBAIS

Experiências de fraude de empresas e de consumidores

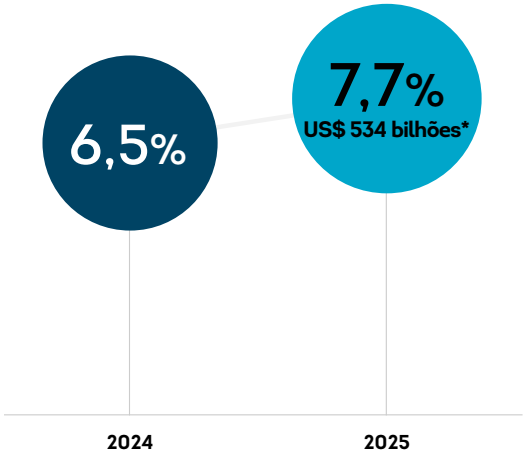
O custo da fraude disparou em todo o mundo

A liderança corporativa entrevistada no Canadá, em Hong Kong, na Índia, nas Filipinas, no Reino Unido e nos EUA afirma que, em média, suas empresas perderam 7,7% da receita por conta de fraudes no ano passado; um aumento em relação aos 6,5% registrados em 2024. Isso representa um total equivalente a US$ 534 bilhões em perdas ligadas a fraudes entre as 1.200 pessoas da liderança corporativa entrevistadas em 2025.

Quase um terço (24%) dos líderes citaram golpe/fraude autorizada como a causa mais proeminente das perdas reportadas, seguido por invasão de conta e fraude de identidade sintética (20% cada). Um número maior da liderança corporativa relatou ter sido alvo de fraudes no último ano. Quando questionados quanto ao aumento dos diversos tipos de fraude no último ano, 82% relataram que todos os tipos de fraude permaneceram iguais ou aumentaram no período (em relação aos 75% de 2024), e mais de 40% relataram aumento nas fraudes em todas as categorias.

Custo total da fraude

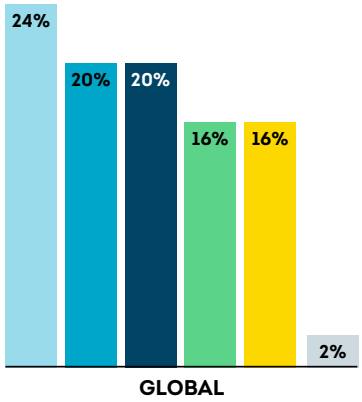
Os líderes corporativos declaram o percentual da receita perdida por suas organizações em decorrência de fraudes no período anterior, juntamente com o valor monetário consolidado dessas perdas entre todos os participantes da pesquisa em nível global



*Conversão para USD com base na taxa de câmbio de 16 de julho de 2025
**Total de 2024 não exibido devido à diferença no número de empresas entrevistadas em âmbito global

Fonte: Pesquisa Corporativa da TransUnion

Causa mais proeminente de perdas por fraude



- **Golpe/fraude autorizada**
  Esquema desonesto de tentativa de enganar uma pessoa para que ela forneça algo de valor (p. ex., acesso à conta, dinheiro, informações)
- **Invasão de conta**
  Pessoas não autorizadas que assumem a conta on-line de alguém (p. ex., banco, redes sociais, e-mail)
- **Fraude de identidade sintética**
  Uso de uma combinação de informações de identificação pessoal para fabricar uma pessoa ou entidade que cometerá um ato desonesto para ganho pessoal ou financeiro
- **Fraude em benefício próprio**
  Representação indevida da identidade ou falsificação de informações com o objetivo de obter ganho financeiro
- **Fraudes de terceiros**
  O uso de identidade roubada para abrir uma conta
- **Outros**

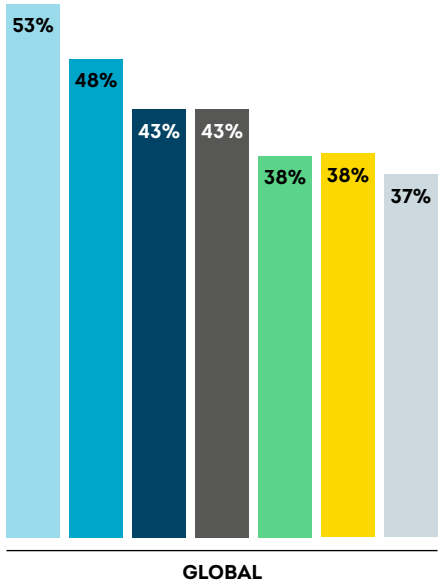
Fonte: Pesquisa Corporativa da TransUnion

TransUnion

As técnicas de prevenção à fraude usam informações sobre identidade e dispositivos

À medida que os riscos de golpes contra consumidores aumentam e ameaçam a integridade das identidades digitais, as organizações passam a utilizar uma combinação de dados, alertas de risco, tecnologias e ferramentas para prevenir fraudes. Mais da metade (53%) dos líderes corporativos entrevistados classificou a verificação de identidade como uma das três principais tecnologias para evitar fraudes, seguida por 48%, que apontaram a reputação do dispositivo como a solução mais eficaz.

Tecnologia classificada como mais eficaz para evitar fraudes
O percentual de líderes corporativos que classificaram essas tecnologias/ soluções entre as três preferidas para evitar fraudes.



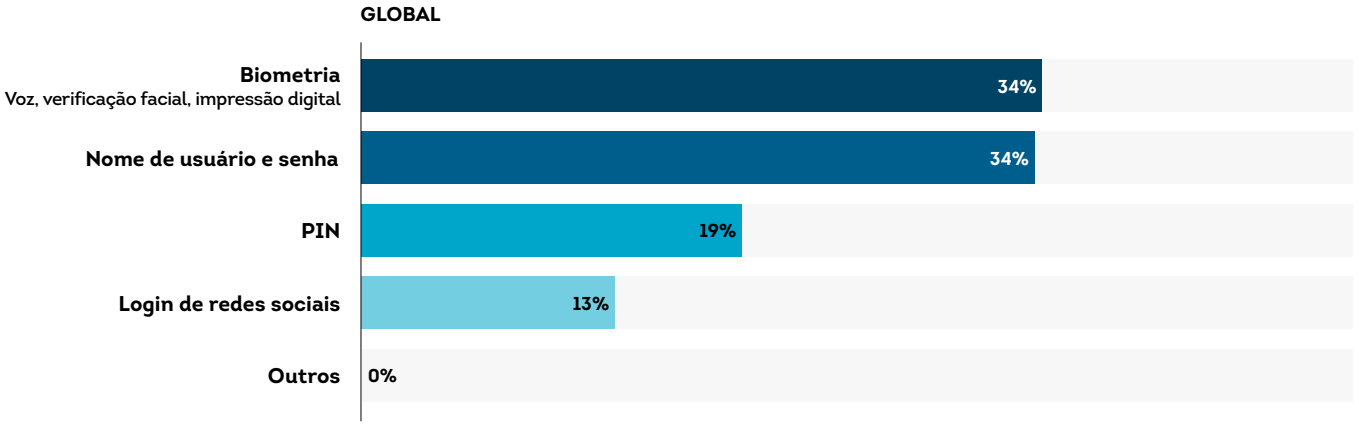
Fonte: Pesquisa Corporativa da TransUnion

Dependência de senhas enfraquece o processo de autenticação de clientes

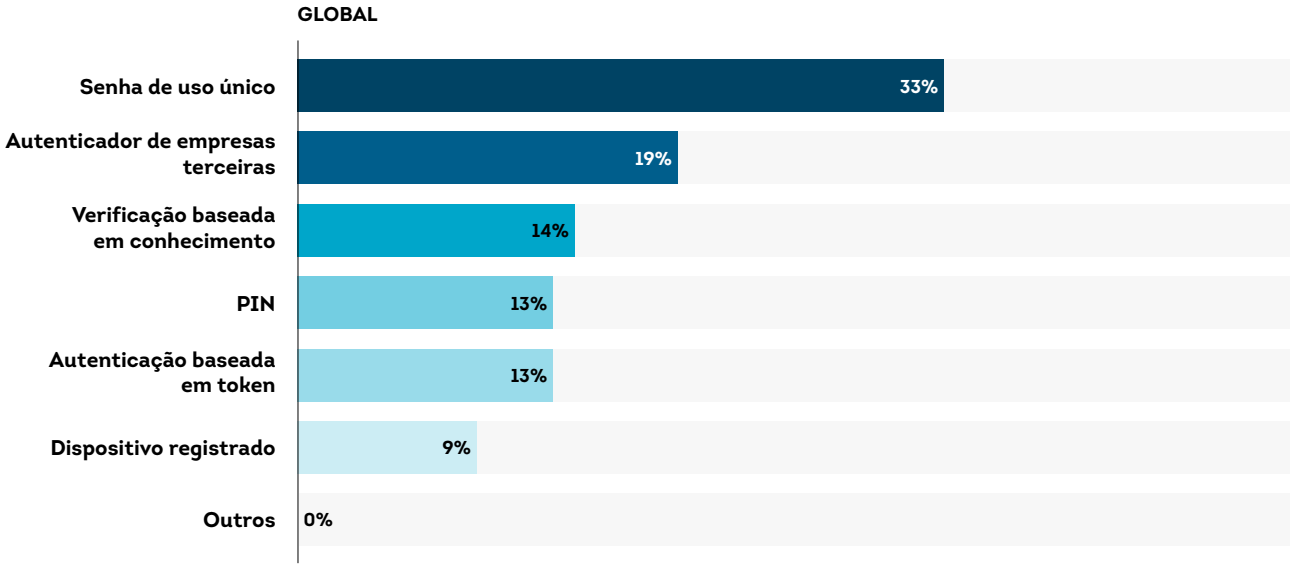
As contas de usuários continuam sendo alvo de ameaças de golpes voltados a consumidores e spoofing de marca. As organizações parecem estar mudando suas abordagens para integrar um segundo fator nos programas de autenticação como uma prática padrão. Embora mais de um terço (34%) da liderança das empresas tenha declarado que usa nomes de usuário e senhas como o principal método de autenticação de clientes, esse índice caiu em cinco pontos percentuais em relação a 2024. Outros 34%disseram usar a biometria como principal método de autenticação, o que representa cinco pontos percentuais a mais em relação a 2024.

No que diz respeito ao segundo fator para a autenticação de clientes, as senhas de uso único (OTPs) continuaram sendo o método mais popular: 33% das lideranças corporativas indicaram que as usam; uma queda em relação aos 35% de 2024. Os aplicativos de autenticação de empresas terceiras ficaram em um segundo lugar distante, mas registraram aumento no uso: de 16% em 2024, para 19% em 2025.

Principal método usado para autenticar clientes



Método secundário usado para autenticar clientes



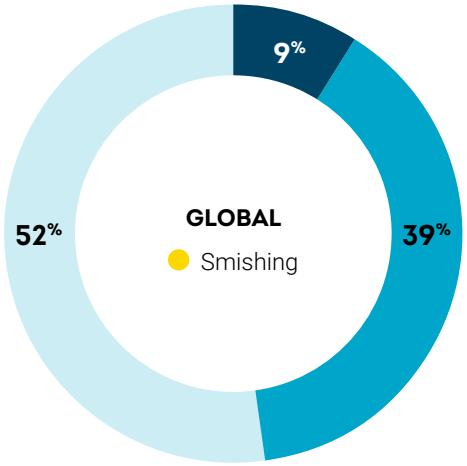
Fonte: Pesquisa Corporativa da TransUnion

Consumidores relataram que os golpes foram o tipo de fraude mais frequente

Quase duas em cada cinco pessoas (39%) afirmaram ter sido alvo de esquemas de fraude por e-mail, on-line, chamadas telefônicas ou mensagens de texto, de fevereiro a maio de 2025. No entanto, uma parte significativa (52%) da população afirmou não ter consciência de que era um alvo. Entre os que disseram ter sido alvo, os principais tipos de fraude foram smishing (36%), phishing (34%) e vishing (33%), conforme relatado pelas pessoas entrevistadas.

Consumidores alvo de fraude

Percentual de pessoas em 18 países e regiões que disseram ter sido alvo de tentativas de fraude on-line, por e-mail, chamadas telefônicas ou mensagens de texto de fevereiro a maio de 2025, e qual o esquema mais comum usado nessas tentativas.



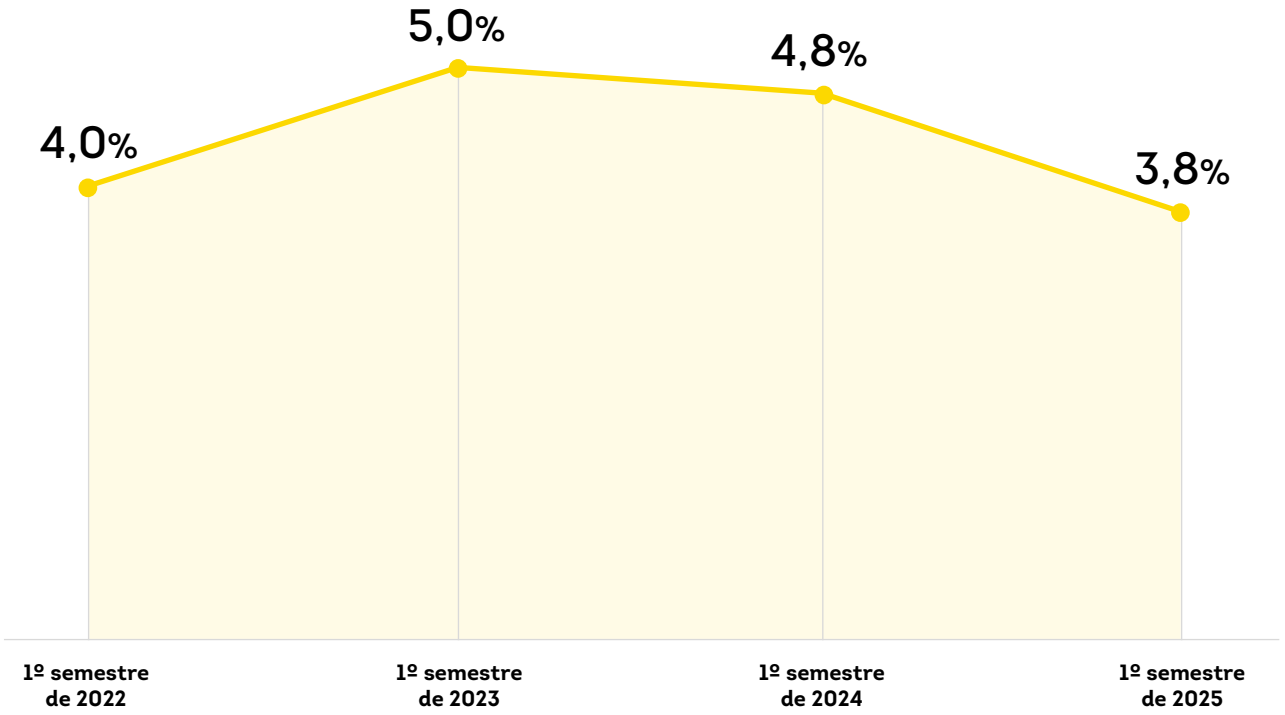
Fonte: Pesquisa da TransUnion com Consumidores

Tendências de fraude digital

As taxas de fraude digital caíram pelo segundo ano consecutivo

As taxas de fraude digital tiveram queda no primeiro semestre de 2025. Globalmente, entre clientes da solução de prevenção à fraude da TransUnion, a taxa caiu para 3,8%, comparada a 4,8% no 2º semestre de 2024, e 5,0% no 1º semestre de 2023. Embora os índices de risco tenham declinado no mundo todo, a República Dominicana (8,6%), a Índia (8,4%) e as Filipinas (4,4%) ficaram no topo do ranking global.

Taxa suspeita de fraude digital em âmbito global

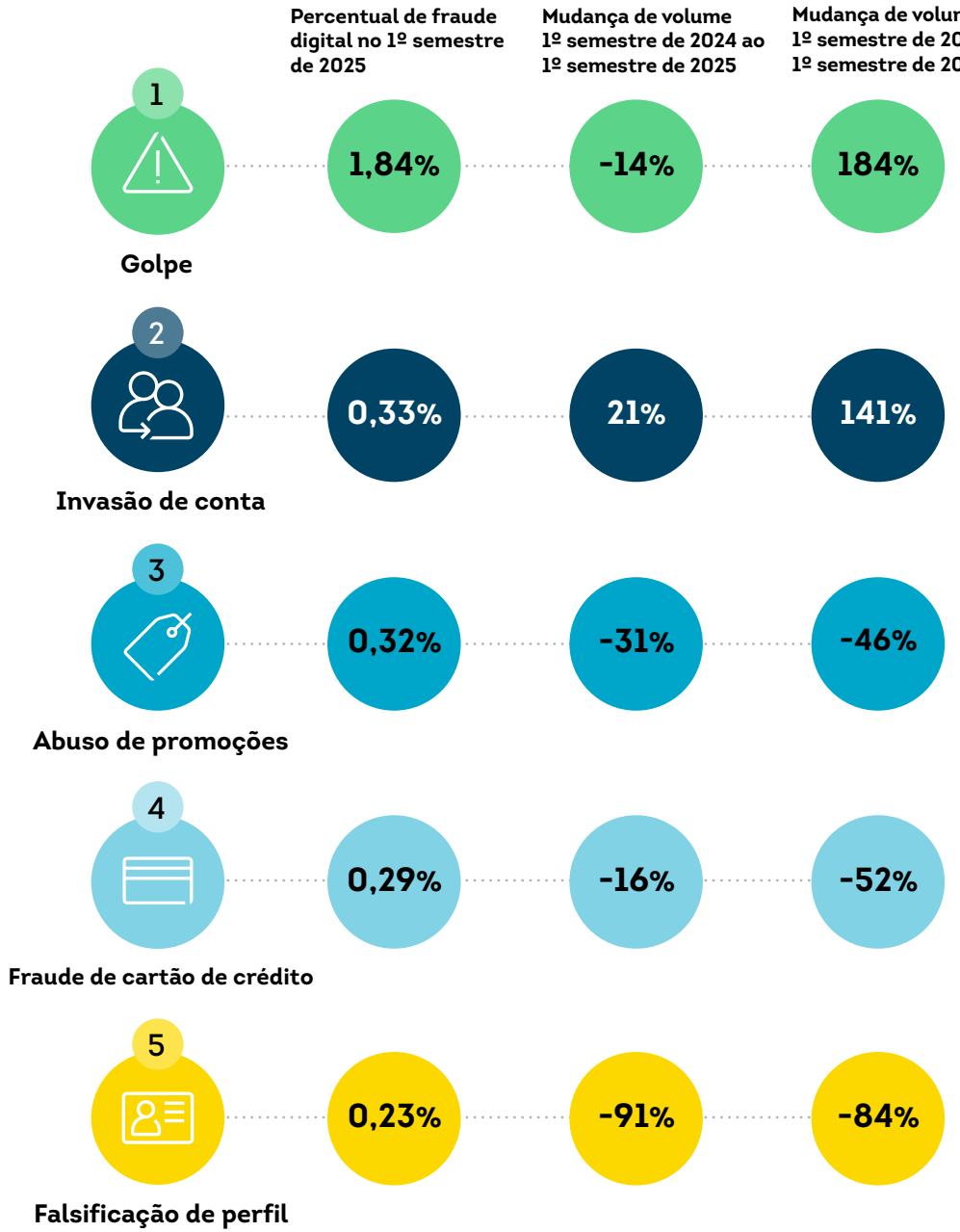


Fonte: Rede de Inteligência Global da TransUnion

Golpes de engenharia social lideraram a lista dos tipos de fraude mais comuns

Em 1,8% de todos os tipos suspeitos de fraude digital reportados à TransUnion por clientes no mundo todo, os golpes de engenharia social (esquema que visa enganar uma pessoa para que ela forneça algo de valor, como acesso à conta, dinheiro, informações) foram os principais tipos de fraude digital no 1º semestre de 2025. No entanto, a invasão de conta (aumento de 21%) foi o tipo de fraude digital com crescimento mais rápido em volume do 1º semestre de 2024 ao 1º semestre de 2025. A fraude por golpe (184%) foi o tipo que mais cresceu desde o 1º semestre de 2021, de acordo com clientes da TransUnion.

Principais tipos de fraude digital e seu crescimento em âmbito global



Fonte: Rede de Inteligência Global da TransUnion

Não é apenas brincadeira de criança – os jogos eletrônicos tiveram os maiores índices de fraude digital

O segmento de jogos eletrônicos, que inclui jogos on-line e para dispositivos móveis, teve o maior percentual (13,5%) de suspeita de fraude digital em âmbito global entre os setores analisados. Dentro deste segmento, 28% das transações foram consideradas suspeitas, representando um aumento de 3% no volume em relação ao mesmo período de 2024. Golpes/solicitações foram o tipo de fraude mais reportado por clientes neste segmento.

Tentativas de fraude digital global por segmento

- **Índice de tentativas suspeitas de fraudes no 1º semestre 2025**
- **Principal tipo de fraude no 1º semestre 2025**
- **Mudança percentual no volume de suspeitas de fraudes digitais do 1º semestre 2024 ao 1º semestre de 2025**

Jogos eletrônicos

1º semestre de 2025
13,5%
Golpes
1º semestre de 2024 ao 1º semestre de 2025
+3%

Comunidades
(encontros on-line, grupos etc.)

1º semestre de 2025
8,3%
Falsificação de perfil
1º semestre de 2024 ao 1º semestre de 2025
-33%

Apostas
(apostas)

1º semestre de 2025
6,8%
Abuso de promoções
1º semestre de 2024 ao 1º semestre de 2025
+24%

Telecomunicações

1º semestre de 2025
4,4%
Golpes
1º semestre de 2024 ao 1º semestre de 2025
+74%

Serviços financeiros

1º semestre de 2025
3,3%
Invasão de conta
1º semestre de 2024 ao 1º semestre de 2025
-20%

Varejo

1º semestre de 2025
2,6%
Fraude de cartão de crédito
1º semestre de 2024 ao 1º semestre de 2025
-64%

Governamental

1º semestre de 2025
2,3%
Fraude de cartão de crédito
1º semestre de 2024 ao 1º semestre de 2025
+52%

Logística

1º semestre de 2025
2,3%
Fraude de envio
1º semestre de 2024 ao 1º semestre de 2025
-42%

Seguro

1º semestre de 2025
1,2%
Fraude de solicitação em benefício próprio
1º semestre de 2024 ao 1º semestre de 2025
-47%

Viagem e lazer

1º semestre de 2025
0,2%
Fraude de cartão de crédito
1º semestre de 2024 ao 1º semestre de 2025
-56%

Fonte: Rede de Inteligência Global da TransUnion

Fraude digital no ciclo de vida dos consumidores

Onboarding é a etapa mais arriscada do ciclo de vida dos consumidores

Analisando o risco por etapa do ciclo de vida do público consumidor, o onboarding é particularmente preocupante. De todas as tentativas de transações globais de onboarding digitais no 1º semestre de 2025 (representando 5% de todo o volume de tráfego), a TransUnion descobriu que 8,3% eram suspeitas de fraude digital; um aumento de 28% em relação ao 1º semestre de 2024.

O risco nesta etapa da jornada dominou a maioria dos segmentos no 1º semestre de 2025, com exceção de serviços financeiros, seguros e governamental, para os quais o maior risco foram as transações financeiras. Os segmentos de comunidades e apostas apresentaram os maiores índices de fraude digital suspeita durante o onboarding entre os setores analisados, com 21,6% e 21,0% respectivamente.

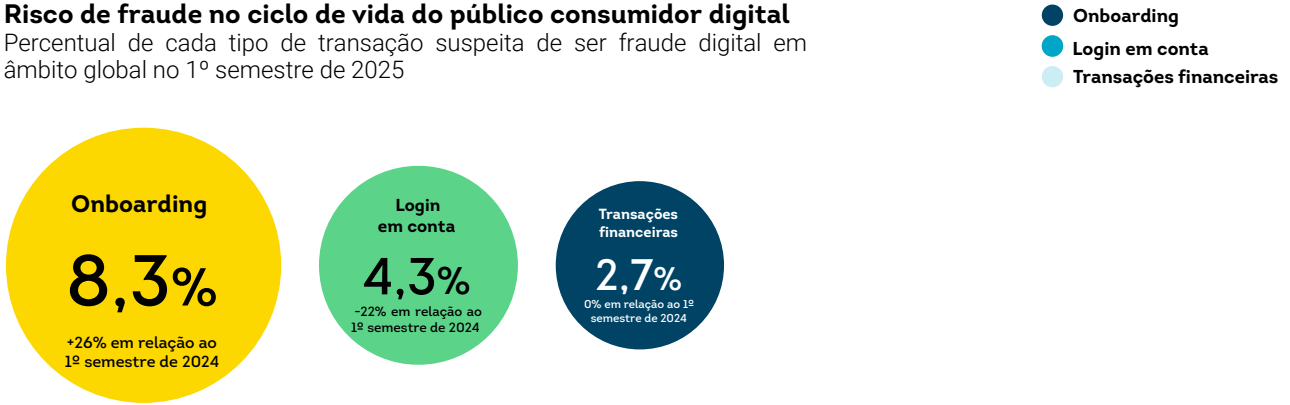
Exemplos de etapas do ciclo de vida do consumidor

Onboarding: Cadastro de conta, registro e originação de empréstimo

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

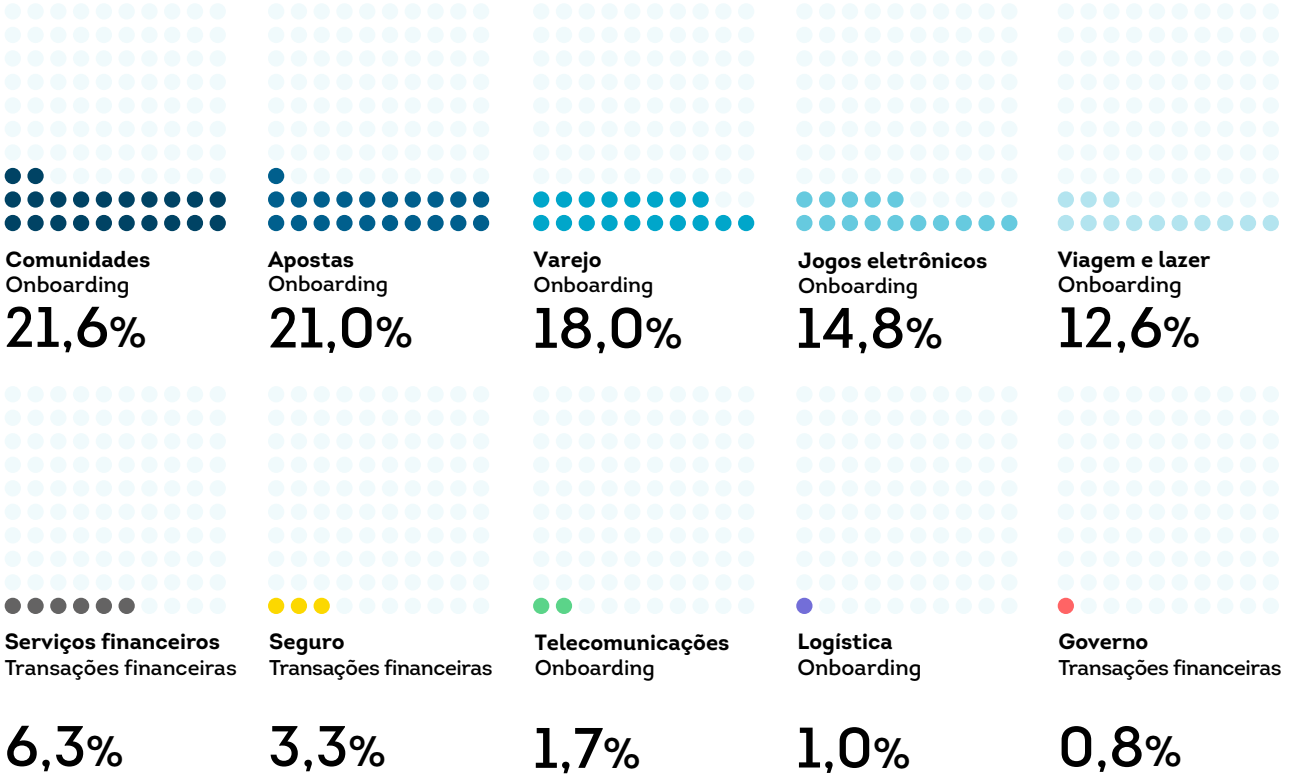
Transações Financeiras: Compras, saques e depósitos

Risco de fraude no ciclo de vida do público consumidor digital
Percentual de cada tipo de transação suspeita de ser fraude digital em âmbito global no 1º semestre de 2025



Fonte: Rede de Inteligência Global da TransUnion

Risco de fraude no ciclo de vida do público consumidor digital por segmento
A etapa do ciclo de vida do consumidor com a maior taxa suspeita de fraude digital por segmento e o percentual correspondente nessa etapa em âmbito global no 1º semestre de 2025



Fonte: Rede de Inteligência Global da TransUnion

TransUnion

AMÉRICA LATINA

Visão geral da América Latina

Graças aos investimentos contínuos das empresas em soluções voltadas à autenticação digital e à prevenção de fraudes na região, o índice de tentativas suspeitas de fraude diminuiu nas transações envolvendo consumidores em todos os países analisados da América Latina, com exceção de Porto Rico, onde houve aumento de apenas 2% no primeiro semestre em comparação ao mesmo período de 2024. No entanto, ainda observamos um percentual elevado de transações suspeitas na criação de novas contas por meio de canais digitais. Os consumidores seguem sendo alvo e vítimas de diversos esquemas fraudulentos, e a população entrevistada na América Latina relatou que os golpes mais frequentes foram smishing e vishing. Diante desse cenário, as estratégias de prevenção à fraude devem manter o consumidor no centro, com ênfase na proteção de credenciais e informações pessoais. Para isso, é fundamental promover educação contínua e campanhas de conscientização, com o objetivo de reduzir a ocorrência de esquemas como invasão de contas.

Os dados da América Latina nesta seção combinam insights sobre fraude digital proprietários da rede de inteligência global 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 e Guatemala.

PONTOS IMPORTANTES

Na mira: consumidores continuam expostos a esquemas fraudulentos

34%

das pessoas entrevistadas em países da América Latina disseram ter sido alvo de fraude por e-mail, on-line, chamada telefônica e mensagens de texto de fevereiro a maio de 2025, sendo que Chile e Colômbia apresentaram as maiores taxas

34%

das pessoas que disseram ter sido alvo na América Latina relataram terem sofrido ataque de vishing, tornando este o esquema de fraude mais mencionado na região

Tentativas incansáveis: transações suspeitas que permanecem em alta

11%

de aumento na taxa **de transações com suspeita de fraude em** tentativas de transações financeiras de países da América Latina analisados no primeiro semestre de 2025 em comparação com o primeiro semestre de 2024

5%

das tentativas de **onboarding** digital de países da América Latina analisadas foram suspeitas de fraude digital no 1º semestre de 2025

O custo continua alto e os fraudadores insistem em explorar as oportunidades

25%

da liderança corporativa que entrevistamos relatou que suas empresas perderam o equivalente a 10% ou mais das receitas no ano passado

42%

da liderança corporativa acha que os ataques de invasão de conta começam **pela web**, seguidos por 20% que acredita que começam com aplicativos para dispositivos móveis

Experiências de fraude de consumidores

Os fraudadores concentram ataques nos canais mais usados pelos consumidores

Embora mais de um terço (34%) dos consumidores entrevistados na América Latina tenha relatado ter sido alvo de algum esquema de fraude por e-mail, canais on-line, chamadas telefônicas ou mensagens de texto nos últimos três meses — percentual inferior à taxa global de 48% — uma parcela significativa da população pode não reconhecer uma tentativa de fraude: 66% afirmaram não saber que estavam sendo alvo. Entre aqueles que disseram ter sido alvo nesse período, os principais tipos de fraude relatados foram vishing (34%) e smishing (31%).

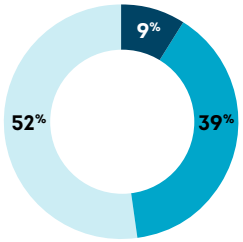
Embora os fraudadores possam atacar a qualquer momento e por qualquer canal, eles tendem a concentrar esforços nos mais populares. No Chile e na Colômbia, onde há maior número de assinaturas de telefonia móvel em comparação a outros países latino-americanos*, o vetor de ataque mais comum relatado pelos entrevistados foi o vishing.

*World Bank Group: Mobile cellular subscriptions (per 100 people) – Colombia, Chile, Dominican Republic, Brazil, Guatemala | Data

Consumidores alvo de fraude

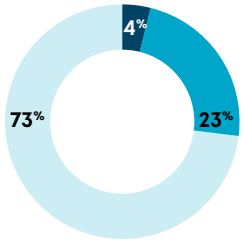
Percentual de pessoas que disseram ter sido alvo de tentativas de fraude on-line, por e-mail, chamadas telefônicas ou mensagens de texto de fevereiro a maio de 2025, e qual o esquema mais comum usado nessas tentativas.

- Foram alvo e foram vítimas
- Foram alvo, mas não foram vítimas
- Não foram alvo
- Tipo de fraude mais relatado



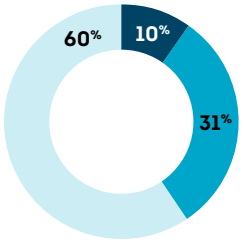
GLOBAL

- Smishing



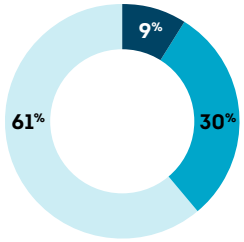
BRASIL

- Vishing



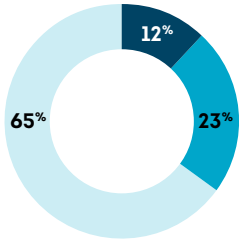
CHILE

- Vishing



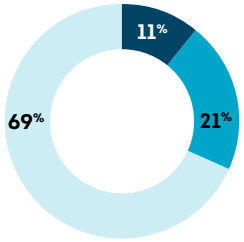
COLÔMBIA (EMPATE)

- Smishing
- Vishing



GUATEMALA (EMPATE)

- Dinheiro/vale-presente
- Esquemas de roubo e venda de identidade em sites legítimos



REPÚBLICA DOMINICANA (EMPATE)

- Dinheiro/vale-presente
- Esquemas de roubo e venda de identidade em sites legítimos

Fonte: Pesquisa da TransUnion com Consumidores

TransUnion

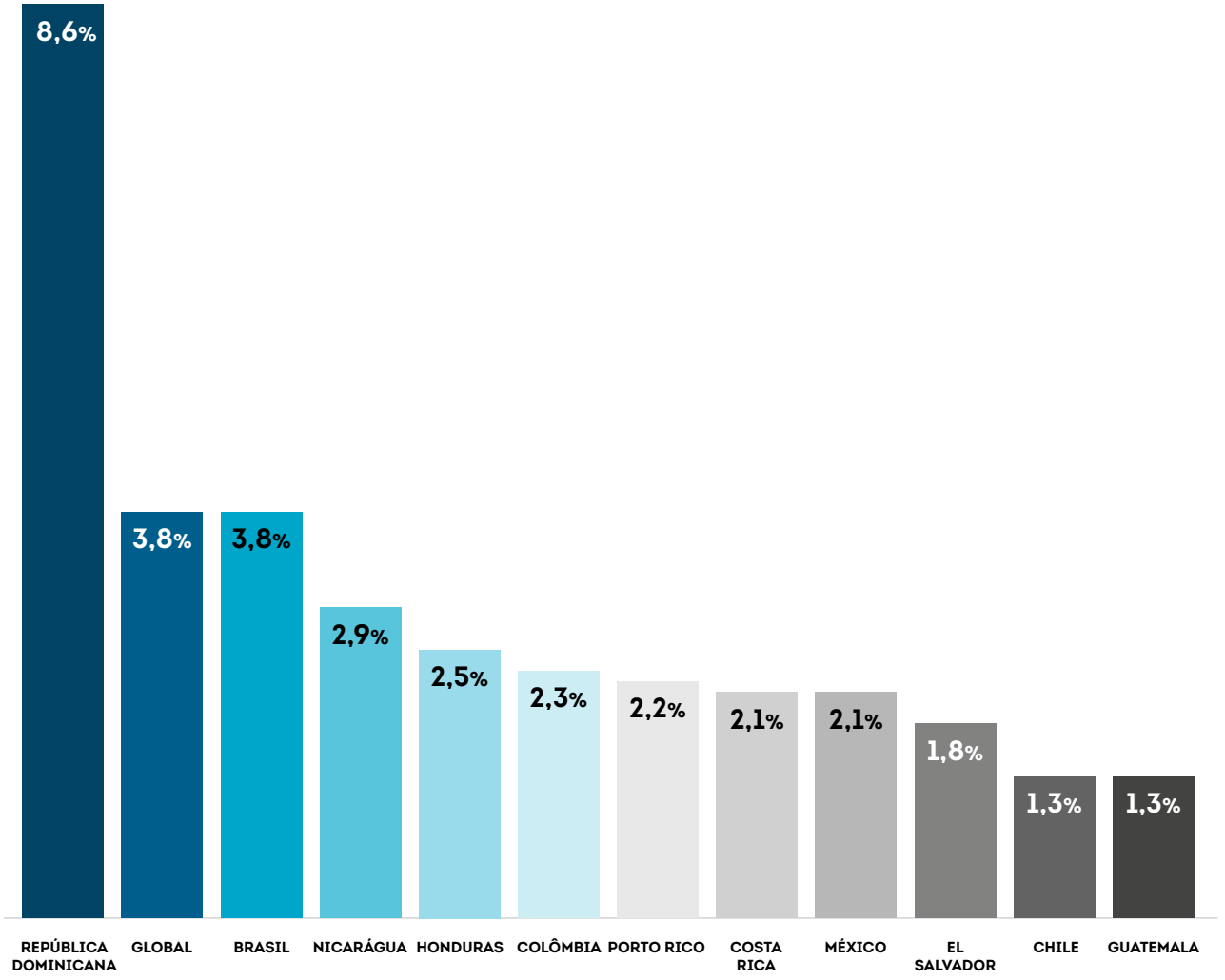
Tendências de fraude digital

Taxas de fraude digital suspeitas se estabilizam, mas permanecem elevadas nos principais mercados da América Latina

A taxa global de tentativas suspeitas de fraude digital entre clientes da TransUnion continuou abaixo de 5% na primeira metade de 2025, registrada em 3,8%. Isso reflete a eficácia contínua das estratégias de prevenção à fraude nos principais mercados. Nos mercados da América Latina que analisamos, três (Brasil, República Dominicana e Nicarágua) relataram taxas acima da média regional de 2,8%, destacando a necessidade de melhores esforços de mitigação de fraude nessas regiões. Esses níveis elevados sugeriram que os fraudadores estão buscando ativamente mercados específicos que ainda possam apresentar vulnerabilidades.

Taxa de transações com suspeitas de fraude digital

1º semestre de 2025



Fonte: Rede de Inteligência Global da TransUnion

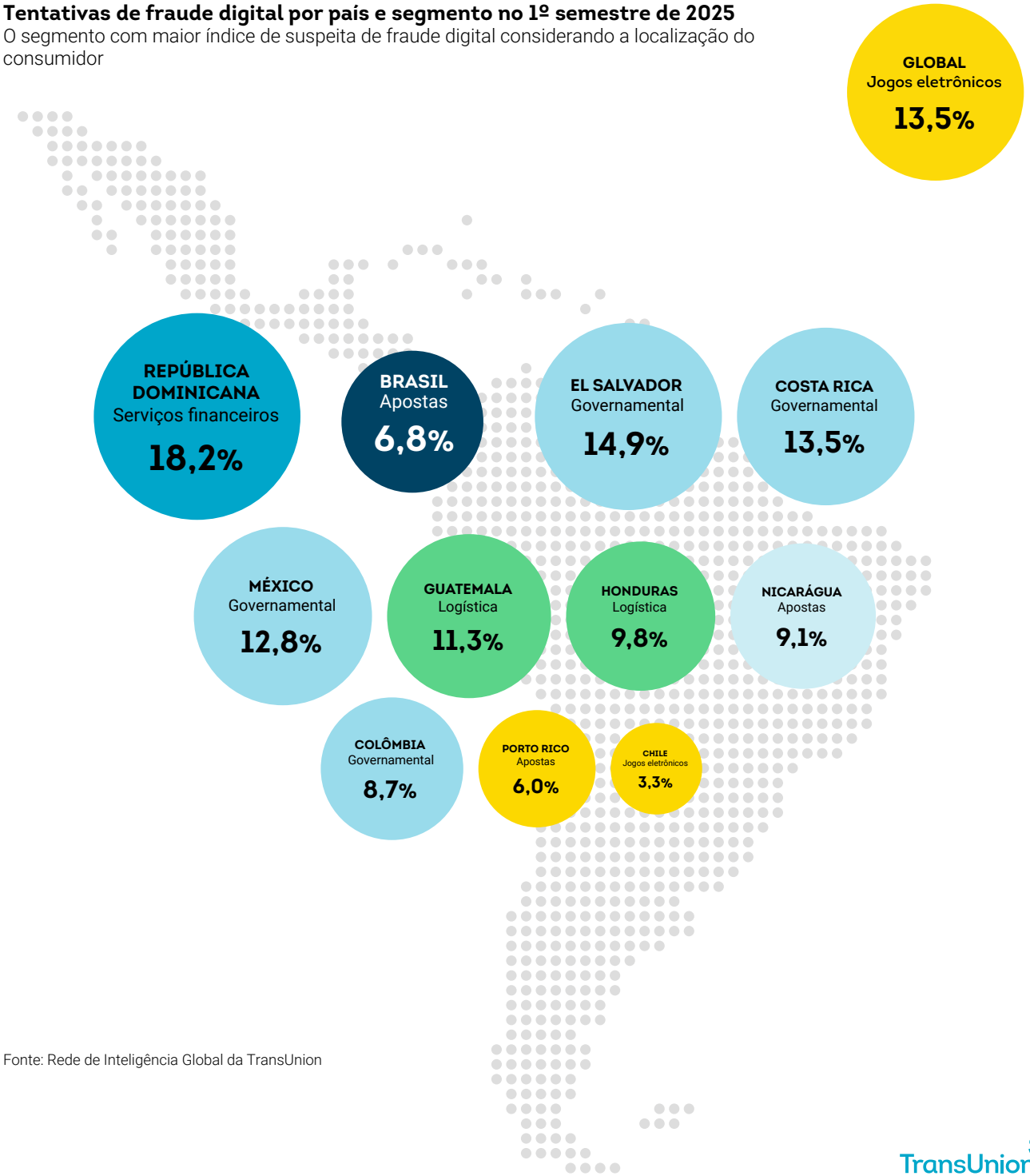
Segmentos específicos são alvo de fraudadores em determinados países

Entre os segmentos analisados globalmente, o setor de jogos eletrônicos registrou o maior percentual de tentativas suspeitas de fraude digital no primeiro semestre de 2025, alcançando 13,5%. Isso representa um aumento significativo de 28% no volume em comparação com o mesmo período em 2024, reforçando a vulnerabilidade crescente desse setor diante de atividades fraudulentas.

Na América Latina, segmentos específicos em mercados individuais também apresentaram taxas de fraude elevadas. Por exemplo, em transações de consumidores na República Dominicana, o setor de serviços financeiros relatou a maior taxa suspeita (18,2%) de fraude digital entre os segmentos analisados no 1º semestre de 2025. No Brasil, o segmento de apostas liderou com uma taxa de 6,8%. Esses valores destacam a necessidade de haver estratégias de prevenção à fraude dentro desses segmentos.

Em muitos outros países analisados na região, o setor governamental apresentou a maior taxa, com um aumento médio de 80% em comparação com o 1º semestre de 2024 na América Latina. Essa tendência reflete os esforços contínuos dos fraudadores de explorar setores que lidam com dados pessoais confidenciais.

Tentativas de fraude digital por país e segmento no 1º semestre de 2025
O segmento com maior índice de suspeita de fraude digital considerando a localização do consumidor



Fonte: Rede de Inteligência Global da TransUnion

TransUnion

Identidades arriscadas impactam todas as etapas do ciclo de vida de consumidores

A fraude baseada em identidade, impulsionada por grandes volumes de dados expostos e pela atuação cada vez mais sofisticada de criminosos cibernéticos, continua a crescer. Esses agentes mal-intencionados têm capacidade para atacar múltiplos pontos simultaneamente.
O onboarding registrou o maior aumento no risco de fraude ao longo do ciclo de vida do consumidor digital, com crescimento de 26% globalmente entre o 1º semestre de 2024 e o 1º semestre de 2025. Para transações envolvendo consumidores na América Latina, a abertura de contas destacou-se como o tipo de transação digital mais arriscado, com 5% dessas operações classificadas como suspeitas de tentativa de fraude digital. Globalmente, o onboarding também se manteve como a etapa mais vulnerável do ciclo de vida do consumidor, apresentando uma taxa de 8,3%.

Na América Latina, Costa Rica e República Dominicana lideraram a região entre os países analisados em risco de fraude no onboarding, relatando taxas de 10,6% e 14,2%, respectivamente. Essas tendências destacam a crescente necessidade de estratégias robustas de verificação de identidade e prevenção a fraudes nos estágios iniciais do engajamento digital.

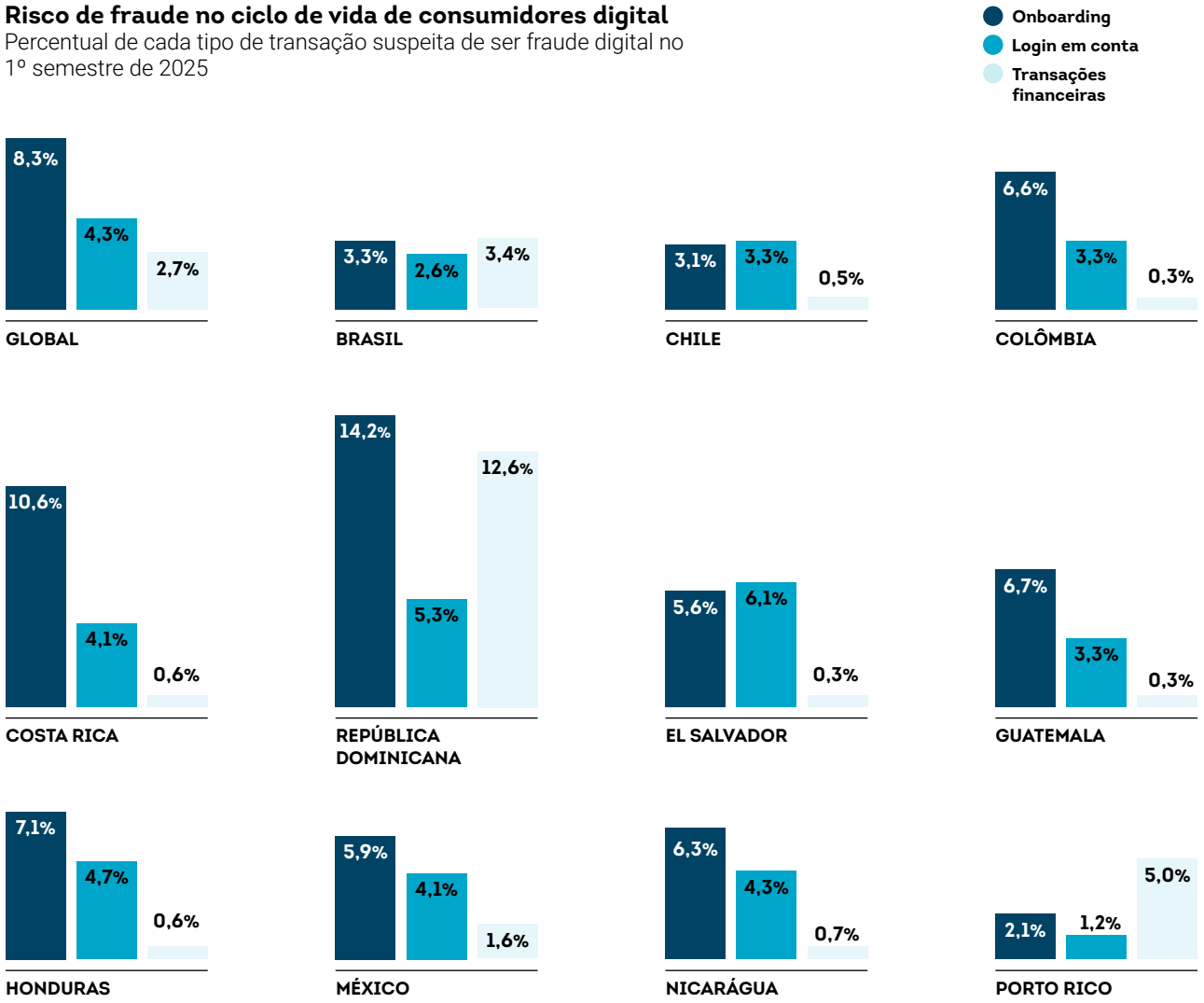
Exemplos de etapas do ciclo de vida do consumidor

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 no ciclo de vida de consumidores digital
Percentual de cada tipo de transação suspeita de ser fraude digital no 1º semestre de 2025



Fonte: Rede de Inteligência Global da TransUnion

AMÉRICA DO NORTE

Visão geral dos Estados Unidos

Os esquemas de fraude estão se tornando cada vez mais sofisticados, e os Estados Unidos enfrentam um risco elevado. A liderança de prevenção à fraude no país reconhece a urgência de fortalecer suas defesas para acompanhar o ritmo, à medida que mais empresas realizam negócios on-line. Não é uma tarefa simples: identidades comprometidas por vazamentos de dados e golpes aumentam o risco em todo o ciclo de vida do consumidor.

No primeiro semestre de 2025, esse desafio se manifestou de diversas formas. A liderança corporativa identificou a invasão de contas (ATO) como a principal causa de perdas relacionadas à fraude. Considerando os golpes de roubo de identidade enfrentados pelos consumidores, combinados às preferências por métodos de autenticação mais vulneráveis, as contas de clientes permanecem como os principais alvos. Além disso, o onboarding foi a etapa mais arriscada do ciclo de vida digital.

Com o uso de ferramentas de IA generativa, fraudadores conseguem criar identidades sintéticas, combinadas com documentos deepfake, históricos de crédito que parecem legítimos e contas adulteradas, tornando difícil distinguir usuários reais. Diante da exposição de dados de consumidores em ocorrências de vazamento e fraude nos Estados Unidos, compreender com clareza o risco associado às identidades digitais está se tornando cada vez mais desafiador.

PONTOS IMPORTANTES

Custo da fraude aumentando para as organizações

9,8%

da receita: essa é a média de perdas decorrentes de fraude, um aumento de 46% em relação a 2024, o que representa US $ 114 bilhões de prejuízos no ano passado entre as 200 pessoas da liderança corporativa entrevistada nos EUA

US$ 2,7 bilhões

na exposição de empresas credoras a identidades sintéticas suspeitas para financiamento de veículos, cartões de crédito bancários, cartões private label e empréstimos pessoais sem garantia nos EUA

A cadeia de suprimentos de identidades roubadas está alimentando uma fraude mais sofisticada

77%

dos vazamentos de dados nos EUA incluíram o número completo do Seguro Social no 1º semestre de 2025, um aumento de 8% em relação ao 1º semestre de 2024 e um recorde histórico desde que a TransUnion começou a reportar esse dado em 2020

51%

dos consumidores dos EUA relataram ter sido alvos de fraudes por e-mail, on-line, chamada telefônica e mensagens de texto, lideradas por phishing, smishing e vishing projetados para roubar credenciais de identidade, de fevereiro a maio de 2025

O onboarding representa o maior risco de fraude em todo o ciclo de vida do consumidor

4,2%

de todas as tentativas de **onboarding digital** nos EUA foram suspeitas de fraude digital; esta foi a fase de maior risco no ciclo de vida do consumidor e superior à taxa geral de suspeita de fraude digital de 3,5% para todas as transações nos EUA

47%

da liderança corporativa dos EUA pesquisada identificou novos tipos de fraude de conta, tanto diretas, como de empresas terceiras e de identidade sintética, como as principais fontes de perdas por fraude no ano passado

Experiências de fraude de empresas e consumidores

O custo do aumento das fraudes

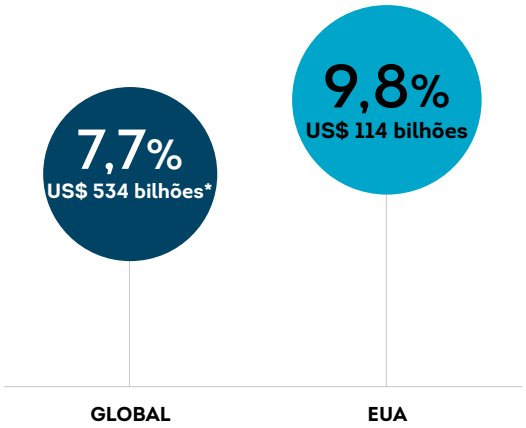
Diminuir o risco de perdas por fraude é uma das funções mais importantes da liderança da área de risco. Seus pares pesquisados nos EUA relataram que suas empresas perderam (em média) o equivalente a 9,8% da receita devido a fraudes no ano passado. Esse é um aumento de 46% em relação a 2024. A liderança dos EUA também relatou perdas por fraude como um percentual da receita que foi 27% maior que a média global de 7,7%. Nos EUA, isso representa um total de US$ 114 bilhões de perdas por fraude entre as 200 líderes entrevistados.

Quase um terço (31%) da liderança corporativa nos EUA citou a invasão de contas como a causa mais proeminente das perdas reportadas, seguida pela fraude de identidade sintética* (24%) e golpe/fraude autorizada (23%).

*Fraude por identidade sintética não é característica do cenário brasileiro

Custo total da fraude

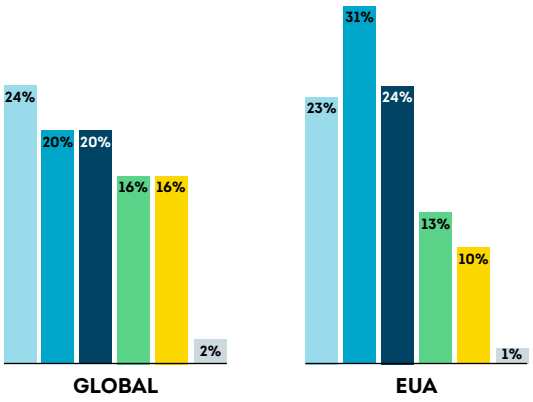
A liderança corporativa declarou o percentual de receitas que suas empresas perderam devido a fraudes no ano passado e o valor monetário total correspondente



*Conversão para USD com base na taxa de câmbio de 16 de julho de 2025.

Fonte: Pesquisa corporativa da TransUnion

Causa mais proeminente de perdas por fraude



- **Golpe/fraude autorizada**
  Esquema desonesto de tentativa de enganar uma pessoa para que ela forneça algo de valor (p. ex., acesso à conta, dinheiro, informações)
- **Invasão de conta**
  Pessoas não autorizadas que assumem a conta on-line de alguém (p. ex., banco, redes sociais, e-mail)
- **Fraude de identidade sintética**
  Uso de uma combinação de informações de identificação pessoal para fabricar uma pessoa ou entidade que cometerá um ato desonesto para ganho pessoal ou financeiro
- **Fraude em benefício próprio**
  Representação indevida da identidade ou falsificação de informações com o objetivo de obter ganho financeiro
- **Fraudes de terceiros**
  O uso de identidade roubada para abrir uma conta
- **Outros**

Fonte: Pesquisa Corporativa da TransUnion

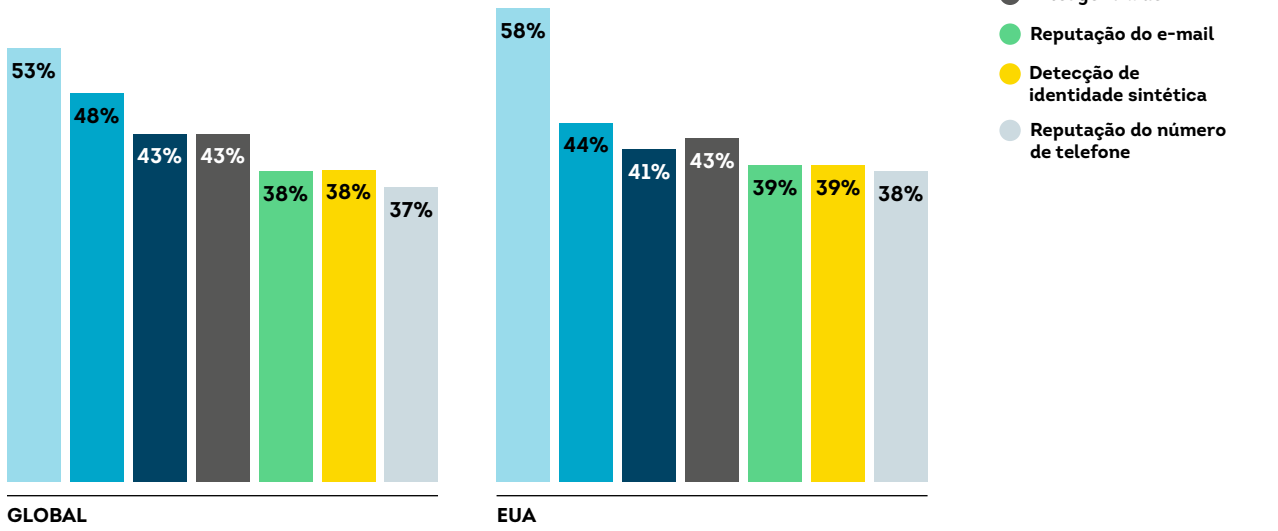
TransUnion

Verificação de identidade é classificada como principal tecnologia de combate a fraudes

A verificação de identidade continua sendo a base da tecnologia de prevenção a fraudes nos EUA. Mais da metade (58%) dos líderes executivos dos EUA entrevistada classificou a verificação de identidade entre as três tecnologias mais eficazes para prevenir fraudes. Após a verificação de identidade, a reputação do dispositivo (44%), a inteligência de IP (43%) e a biometria comportamental (41%) foram classificadas como as mais eficazes.

Tecnologia classificada como mais eficaz para evitar fraudes

O percentual de líderes corporativos que classificaram essas tecnologias/ soluções entre as três preferidas para evitar fraudes



Fonte: Pesquisa Corporativa da TransUnion

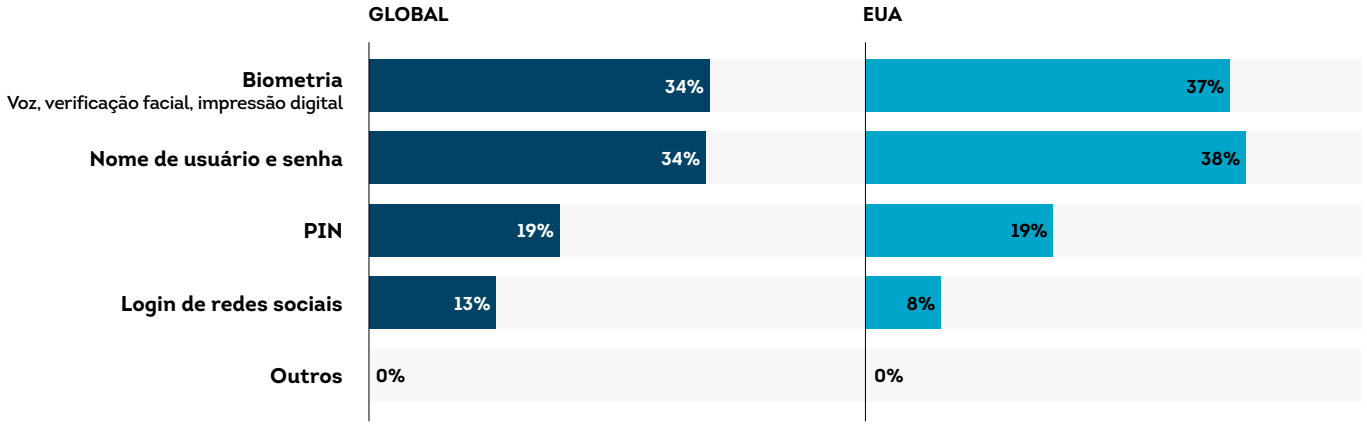
TransUnion

A biometria fica lado a lado com as senhas como principal método de autenticação

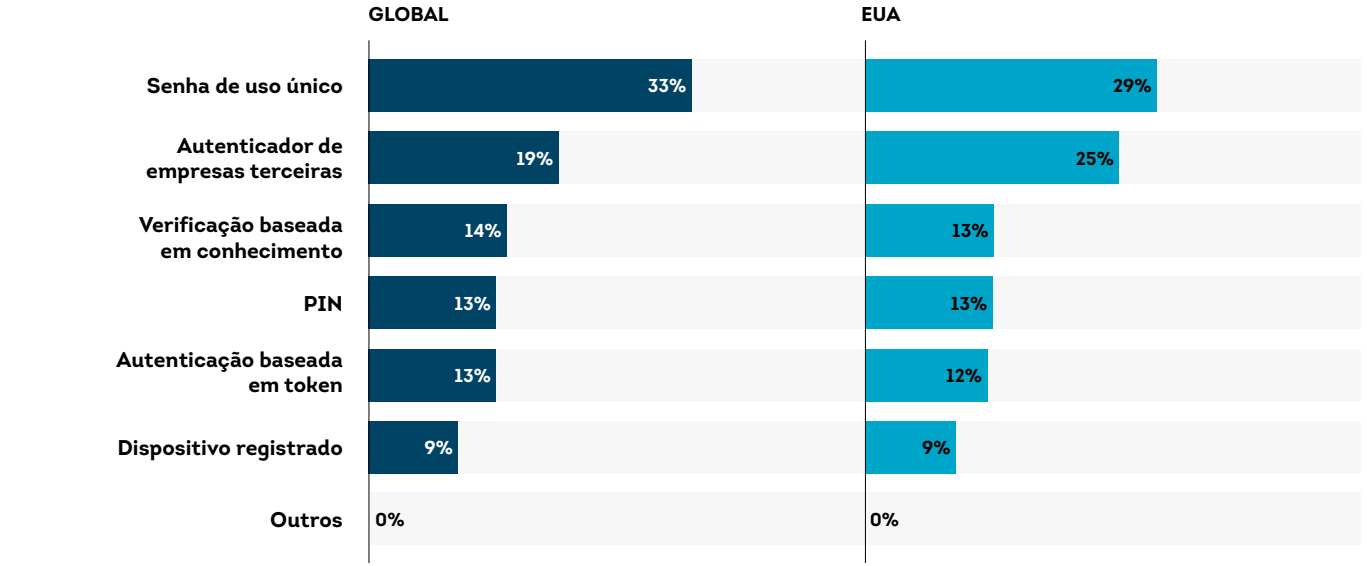
Dados cadastrais de usuários continuam sendo alvo de ameaças de golpes voltados aos consumidores e a vazamentos de dados. Não é à toa que diversos líderes corporativos nos EUA reportaram a invasão de contas como o principal motivo por trás das perdas por fraude. Para conter a maré, eles estão optando por abandonar a autenticação simples de nome de usuário e senha para incorporar a verificação biométrica em seus programas de autenticação. Embora mais de um terço (38%) da liderança corporativa nos EUA tenha declarado que ainda usa nomes de usuários e senhas como o principal método de autenticação de clientes, esse índice caiu 14% em relação a 2024. Outros 37% disseram usar a biometria como principal método de autenticação de clientes, 42% a mais em relação a 2024.

As senhas de uso único continuam sendo o segundo fator mais popular para autenticação de clientes, sendo mencionadas por 29% da liderança corporativa, uma queda em relação aos 35% de 2024. Os aplicativos de autenticação de empresas terceiras (o segundo fator mais popular para autenticação de clientes, segundo a liderança corporativa dos EUA) registraram um aumento no uso, de 20% em 2024 para 25% em 2025.

Principal método usado para autenticar clientes



Método secundário usado para autenticar clientes



Fonte: Pesquisa Corporativa da TransUnion

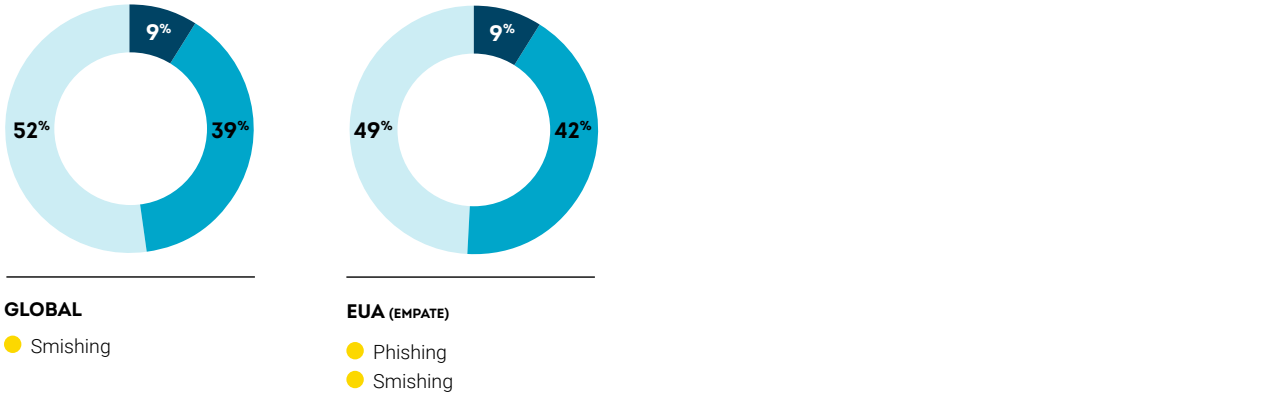
Phishing e smishing empatados como o esquema de fraude mais comum relatado pelos consumidores

Mais da metade (51%) dos consumidores dos EUA afirmou ter sido alvo de esquemas de fraude por e-mail, on-line, chamada telefônica ou mensagens de texto, e 9% foram vítimas no período de fevereiro a maio 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.

Phishing (e-mails, sites, posts em redes sociais, QR codes etc. fraudulentos que visam roubar dados) e smishing (mensagens de texto fraudulentas que tentam enganar alguém a revelar dados) foram relatados, cada, por 46% dos consumidores dos EUA que disseram ter sido alvo de fgraude, o que os torna os principais tipos de fraudes sofridos.

Consumidores alvo de fraude

Percentual de pessoas que disseram ter sido alvo de tentativas de fraude on-line, por e-mail, chamadas telefônicas ou mensagens de texto de fevereiro a maio de 2025, e qual o esquema mais comum usado nessas tentativas.



Fonte: Pesquisa da TransUnion com Consumidores

Tendências de exposição de dados de identidade

Recorde de número e gravidade dos vazamentos de dados nos EUA

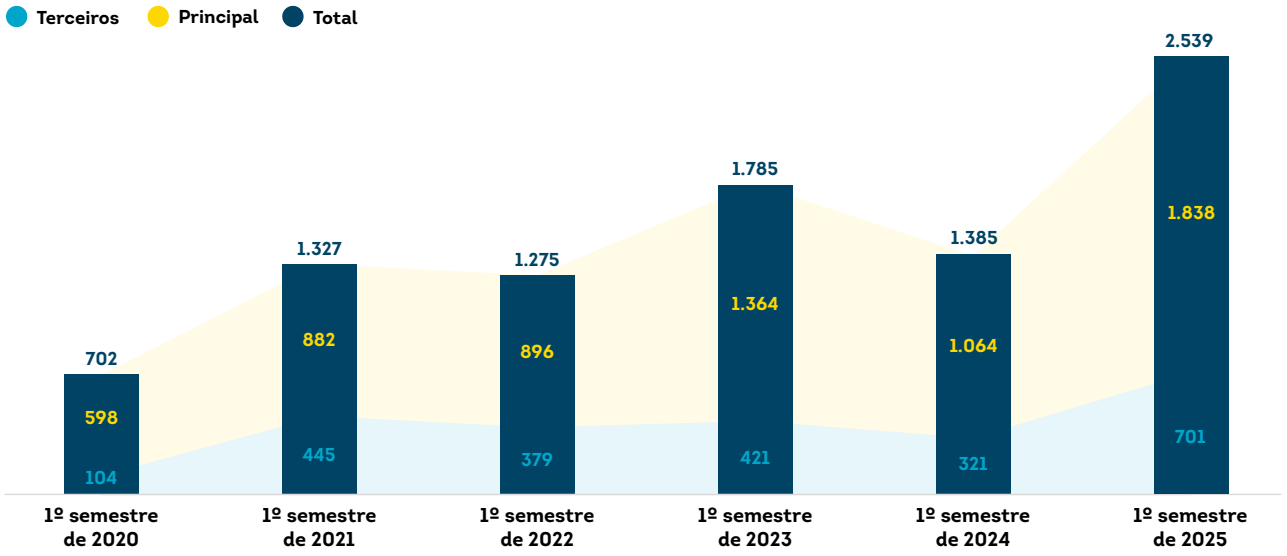
Os criminosos continuam a mudar suas estratégias, passando de ataques voltados a vazamentos de dados para a coleta de credenciais de alta qualidade. Com ataques mais frequentes, porém direcionados a um número menor de indivíduos por incidente, os EUA registraram um aumento de 83% no volume de vazamentos de dados no primeiro semestre de 2025 em comparação ao mesmo período de 2024, atingindo o nível mais alto do período analisado.

No entanto, a quantidade média de pessoas afetadas individualmente por violação caiu para 301 no 1º semestre de 2025, frente a 616 no mesmo período de 2024, e muito abaixo do pico de 5.278 registrado em 2022. Esses ataques buscam dados que não estão prontamente disponíveis, levando criminosos a recorrer ao mercado da dark web para obter informações de identidade usadas em esquemas de fraude.

Essa prática também se alinha a golpes frequentemente relatados contra consumidores, como smishing, phishing e vishing.

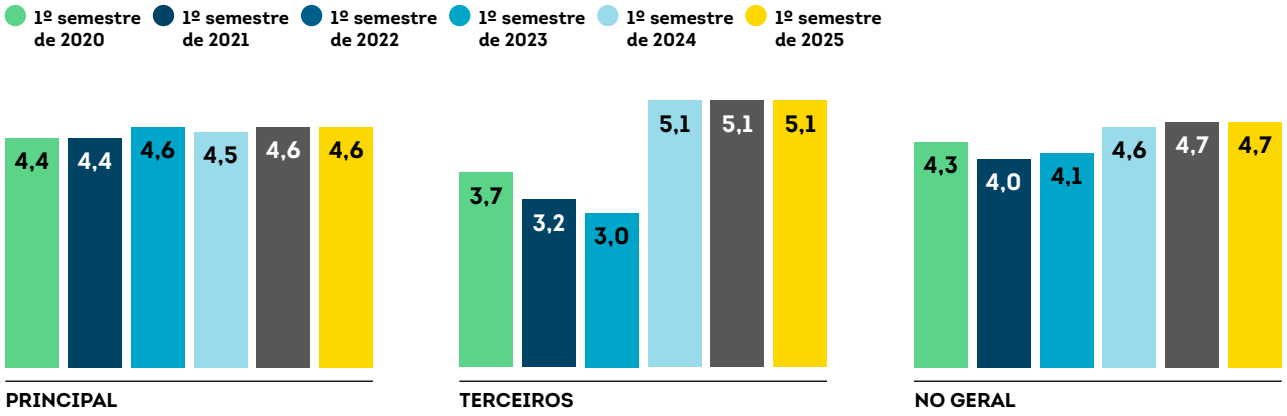
Devido ao foco em credenciais de alto risco, como números de Seguro Social, a gravidade média das violações — medida pela pontuação de risco de violação (BRS) da TransUnion TruEmpower™ — manteve-se no nível mais alto durante o período analisado. Violações de terceiros, envolvendo ataques a organizações que prestam serviços comerciais para marcas, continuaram significativamente mais arriscadas do que aquelas direcionadas a empresas voltadas ao consumidor.

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.

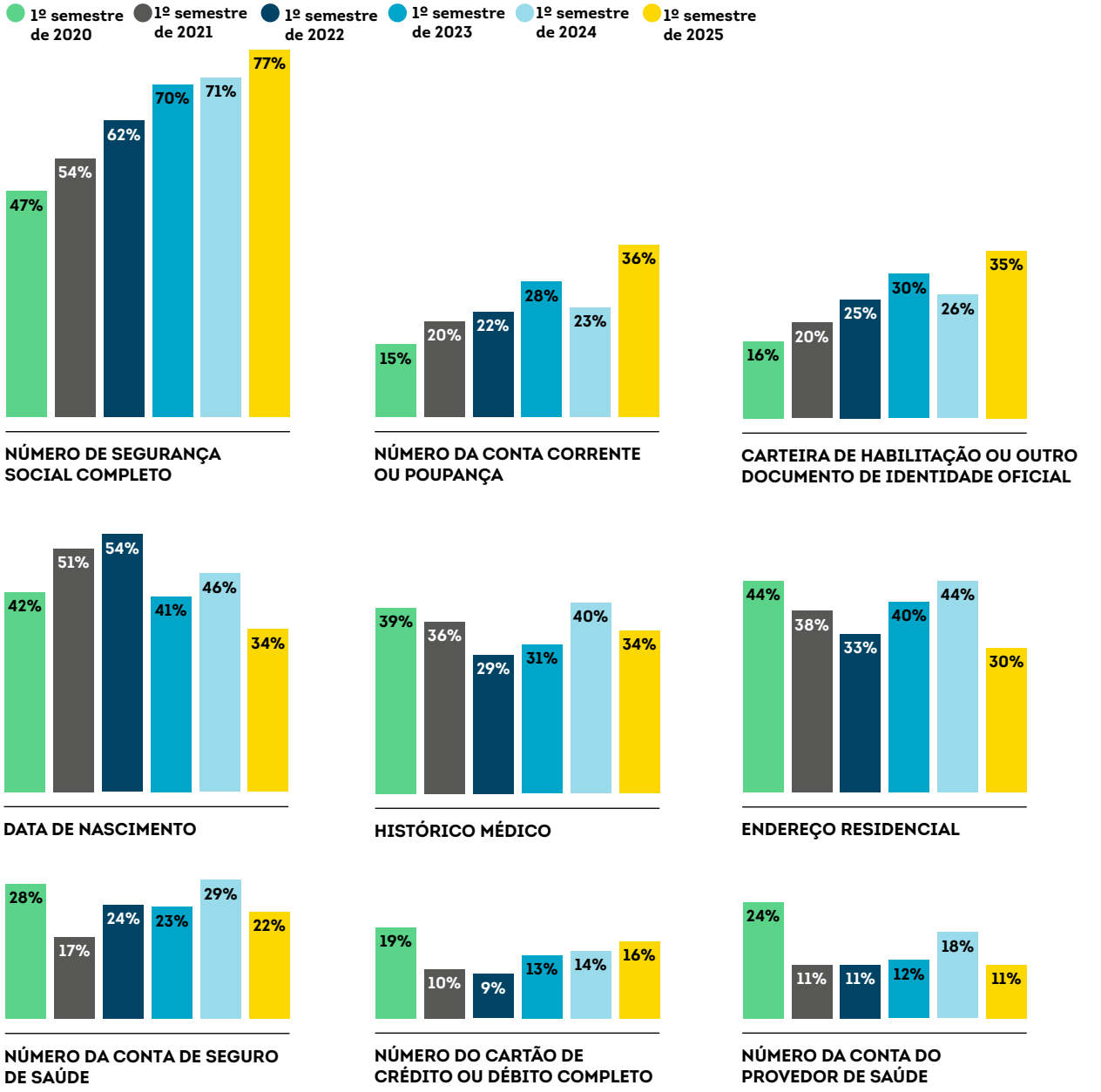
TransUnion

Credenciais de identidade de alto valor são priorizadas por fraudadores

No 1º semestre de 2025, criminosos pareceram se concentrar em credenciais de alto valor para facilitar futuras fraudes e golpes. A TransUnion descobriu que números completos do Seguro Social foram expostos em 77% dos vazamentos de dados nos EUA no 1º semestre de 2025 (um aumento de 8% em relação ao 1º semestre de 2024 e o ponto mais alto desta pesquisa), o que pode dar suporte a novas contas, fraudes sintéticas, de reembolso de impostos e de identidade de benefícios governamentais, entre outros. A exposição de dados de contas correntes/poupança apresentou crescimento significativo, atingindo 36% de 23% no 1º semestre de 2024, possivelmente levando a mais fraudes de invasão de conta ou transações interbancárias/pagamentos. A exposição de dados de carteiras de habilitação também cresceu de 26% no 1º semestre de 2024 para 35% no 1º semestre de 2025, possivelmente alimentando deepfakes de IA de documentos de identificação.

As 10 principais credenciais de identidade expostas em vazamentos de dados nos EUA no 1º semestre de 2025

Percentual de credenciais expostas em um vazamento de dados



Fonte: Rede de Inteligência Global da TransUnion

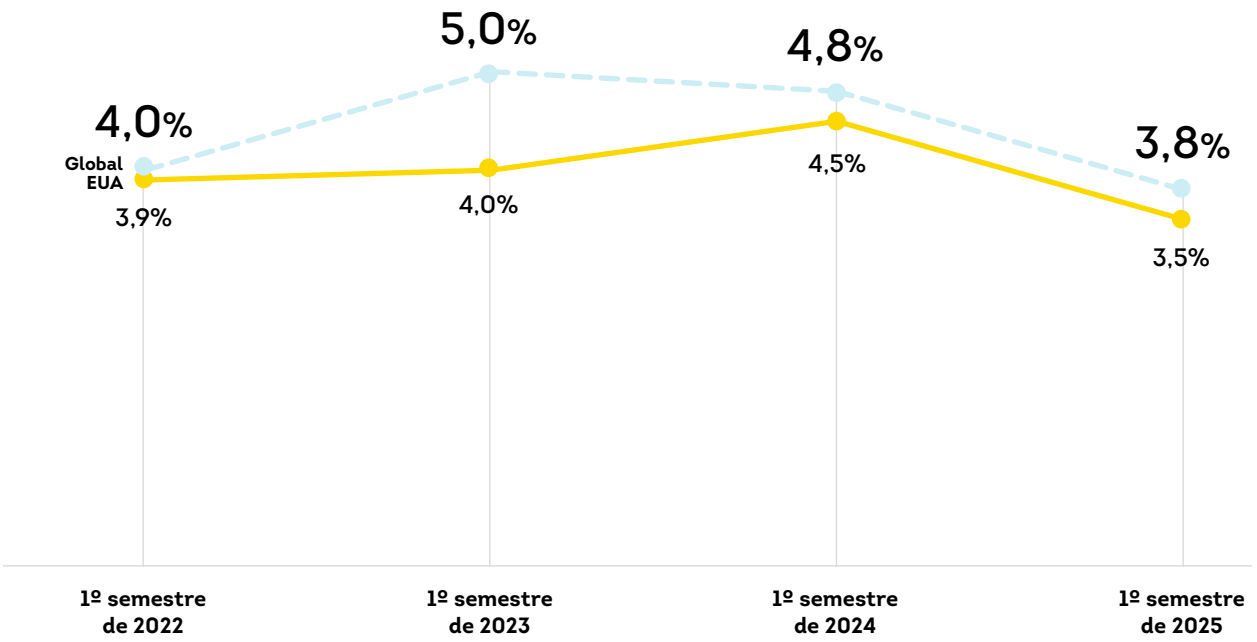
TransUnion

Tendências de fraude digital

Queda na taxa de transações com suspeita de fraudes digitais

O risco de fraude digital nos EUA caiu no 1º semestre do ano pela primeira vez em três anos no 1º semestre de 2025. A taxa de transações com suspeita de fraude digital em tentativas de transação em que o consumidor estava nos EUA caiu para 3,5% no 1º semestre de 2025 após o pico no 1º semestre de 2024 a 4,5%. Isso foi ligeiramente inferior à média global de 3,8% no primeiro semestre de 2025.
A queda na taxa de fraude digital é provavelmente uma combinação do uso crescente de autenticação multifator por parte das organizações para impedir ataques de invasão de contas e dos consumidores estarem mais desconfiadas de esquemas de phishing, vishing e smishing. Ao mesmo tempo, identidades comprometidas estão dando espaço para que ocorram ataques de fraude cada vez mais sofisticados que continuarão a representar riscos para sua organização.

Taxa de transações com suspeita 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 como grupos on-line e sites de relacionamento, experimentou o maior percentual (13,7%) de suspeitas de fraude digital para transações em que o consumidor estava nos EUA no 1º semestre de 2025. Isso representa um aumento de volume de 139% em suspeitas de fraudes digitais do 1º semestre de 2022 ao 1º semestre de 2025 e 64% do 1º semestre de 2024 ao 1º semestre de 2025. Usuários de comunidades on-line contam com as organizações para fornecer confiança e segurança, protegendo-as de esquemas de vendas e outros golpes ao usar suas plataformas. Talvez não seja surpresa que as comunidades clientes da TransUnion tenham relatado falsificação de perfil e golpes como os tipos mais frequentes de fraude digital que testemunharam no 1º semestre de 2025 em todo o mundo, ilustrando o valor dessas plataformas para os fraudadores.

Tentativas de fraude dos EUA por segmento

- **Índice de tentativas suspeitas de fraudes no 1º semestre 2025**
- **Mudança percentual no volume de suspeitas de fraudes digitais do 1º semestre 2024 ao 1º semestre de 2025**

Comunidades
(encontros on-line, grupos etc.)

1º semestre de 2025
13,7%

1º semestre de 2024 ao 1º semestre de 2025
+64%

Apostas
(apostas)

1º semestre de 2025
9,6%

1º semestre de 2024 ao 1º semestre de 2025
-10%

Jogos eletrônicos

1º semestre de 2025
8,3%

1º semestre de 2024 ao 1º semestre de 2025
-38%

Varejo

1º semestre de 2025
3,5%

1º semestre de 2024 ao 1º semestre de 2025
-46%

Serviços financeiros

1º semestre de 2025
3,4%

1º semestre de 2024 ao 1º semestre de 2025
-18%

Logística

1º semestre de 2025
1,9%

1º semestre de 2024 ao 1º semestre de 2025
-70%

Governamental

1º semestre de 2025
0,9%

1º semestre de 2024 ao 1º semestre de 2025
+49%

Seguro

1º semestre de 2025
0,4%

1º semestre de 2024 ao 1º semestre de 2025
-40%

Telecomunicações

1º semestre de 2025
0,4%

1º semestre de 2024 ao 1º semestre de 2025
-32%

Viagem e lazer

1º semestre de 2025
0,2%

1º semestre de 2024 ao 1º semestre de 2025
-35%

Fonte: Rede de inteligência global da TransUnion

Tendências de fraude em *call centers*

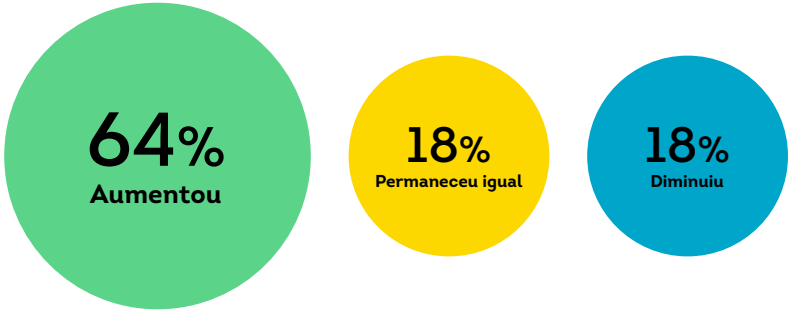
As chamadas recebidas são arriscadas devido ao papel vital que os *call centers* desempenham na experiência de clientes — representando um ponto de contato de alta confiança para os consumidores. Entre líderes corporativos dos EUA participantes da pesquisa, 64% indicaram que os fraudadores aumentaram seus ataques a *call centers* no ano passado, contra 44% em 2024. Mais da metade da liderança corporativa relatou níveis crescentes de táticas criminosas direcionadas a call centers, incluindo falsificação de chamadas para se passar por clientes, uso de serviços de chamadas virtuais e uso de informações de identidade roubadas para passar por perguntas de autenticação baseadas em conhecimento.

As ligações de alto risco nos *call centers* dispararam

A TransUnion documentou um ligeiro aumento (para 6,1%) no percentual de chamadas de alto risco em call centers nos EUA do 1º semestre de 2024 ao 1º semestre de 2025. As chamadas telefônicas de maior risco aumentaram durante esse período em metade dos canais medidos.

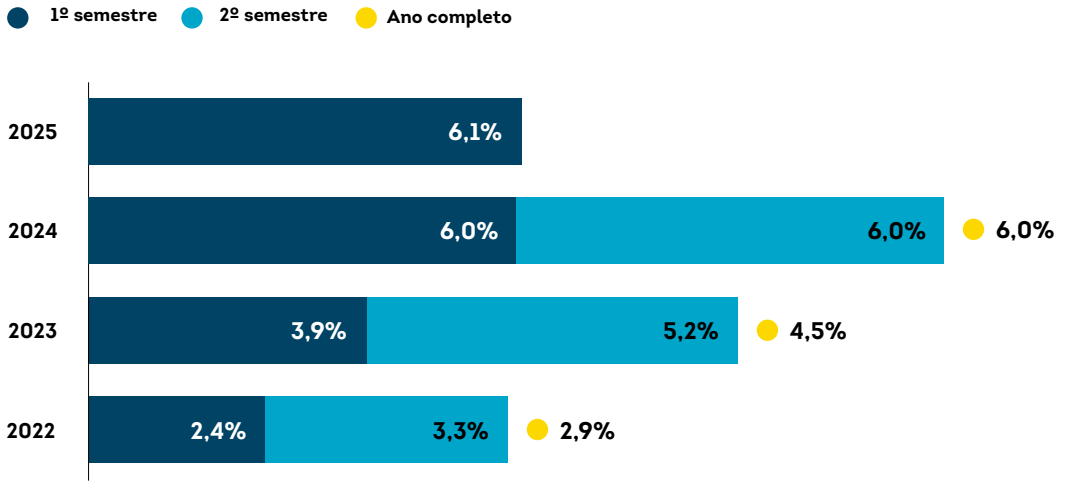
Aumento da frequência de ataques de fraude em *call centers*

A mudança na frequência de ataques de fraude em *call centers* no ano passado foi mencionada pela liderança empresarial, que afirmou ter um conhecimento alto ou extremo sobre atividades relacionadas a fraudes em seus *call centers*.



Fonte: Pesquisa Corporativa da TransUnion

Ligações de alto risco nos *call centers*

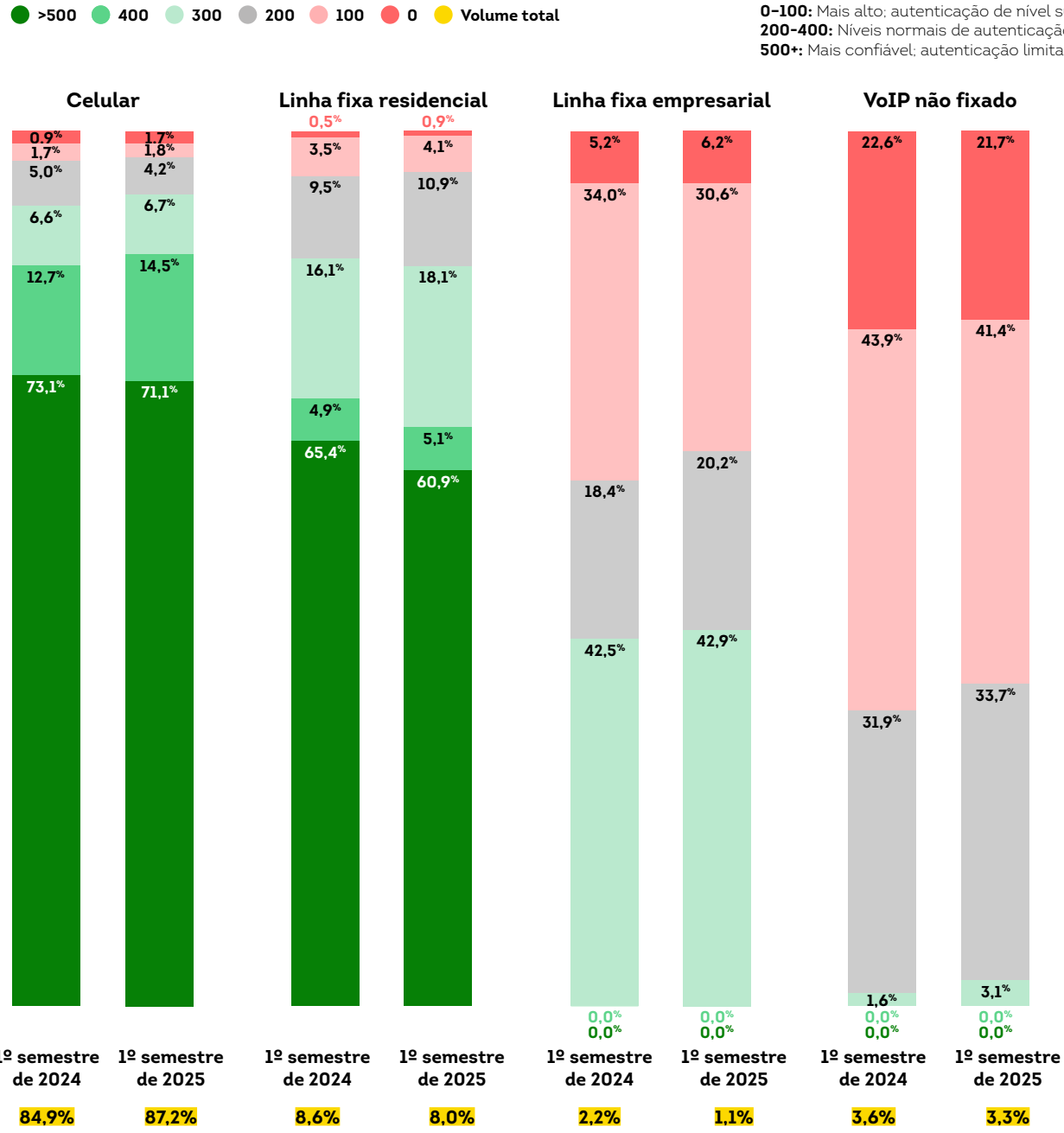


Fonte: Rede de Inteligência Global da TransUnion

O risco de chamadas em dispositivos móveis aumentou; as chamadas virtuais continuaram a ser as mais arriscadas

A TransUnion documentou que a grande maioria (87,2%) das chamadas recebidas por clientes de call centers nos EUA no 1º semestre de 2025 eram de celulares, e essas chamadas estão ficando mais arriscadas. Embora apenas 3,5% das chamadas móveis tenham sido identificadas como de maior risco de fraude, isso representa um aumento de 35% em relação aos 2,6% do 1º semestre 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 3,3% do volume total de chamadas, 63,1% dessas chamadas foram identificadas como de alto risco de fraude no 1º semestre de 2025.

Risco por canal e volume total nos call centers dos EUA



Classificação dos níveis de risco das chamadas

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

Fonte: Rede de inteligência global da TransUnion

TransUnion

Identidades com alto risco podem afetar negativamente cada etapa da jornada do consumidor

Nem toda interação digital com clientes apresenta o mesmo risco para as organizações. No 1º semestre de 2025, o onboarding apresentou um risco particular tanto nos EUA como no restante do mundo. As tentativas de onboarding tiveram a maior taxa (4,2%) de suspeita de fraude digital no ciclo de vida do consumidor para transações em que o usuário estava nos EUA no 1º semestre de 2025; um número consideravelmente menor do que os 8,3% globais. Os logins de contas (um grande problema para a gerência de fraude dos EUA que relatam a invasão de contas como a maior fonte de perdas por fraude) foram os segundos de maior risco no ciclo de vida do consumidor, com uma taxa suspeita de fraude digital de 3,8% para transações em que o usuário estava nos EUA no 1º semestre de 2025.

O risco digital no onboarding está sendo impulsionado por segmentos específicos nos EUA; 37,8% das transações de onboarding em telecomunicações, 24,6% no varejo e 22,9% nas comunidades dos EUA foram suspeitas de fraude digital no 1º semestre de 2025. Ao mesmo tempo, o seguro teve
o maior risco de login de conta, com 29,7% das transações de login dos EUA suspeitas de fraude digital.

Exemplos de etapas da jornada do consumidor

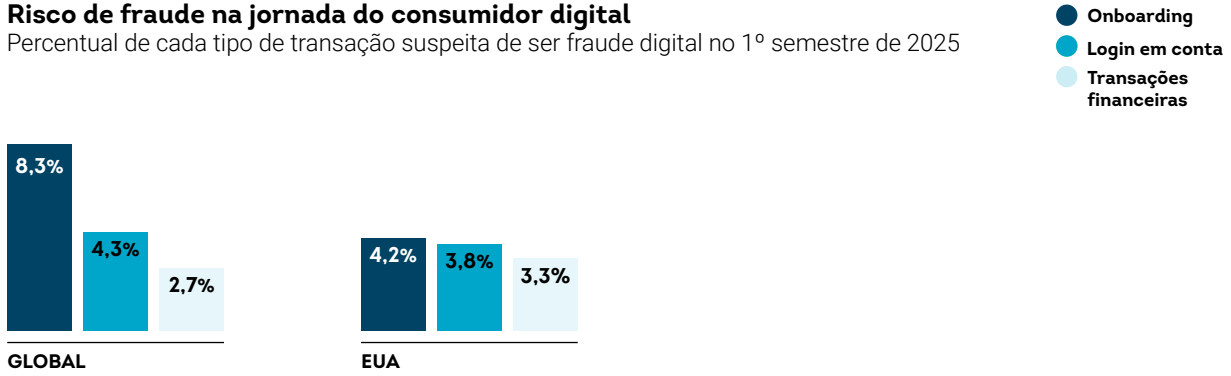
Onboarding: Cadastro de conta, registro e originação de empréstimo

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

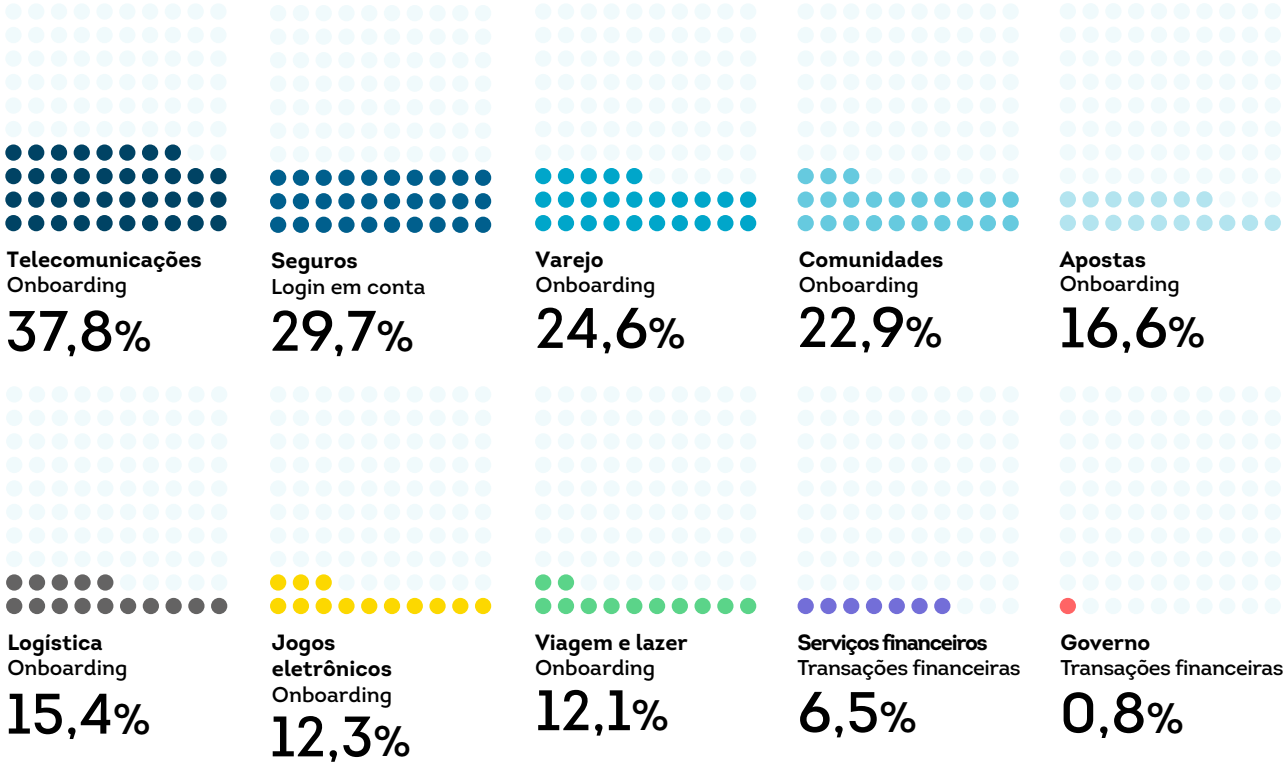
Percentual de cada tipo de transação suspeita de ser fraude digital no 1º semestre de 2025



Fonte: Rede de Inteligência Global da TransUnion

Risco de fraude na jornada do consumidor digital por segmento

A etapa da jornada do consumidor digital com a maior taxa de fraude digital suspeita por segmento e o percentual correspondente nessa etapa nos EUA em 2024



Fonte: Rede de inteligência global da TransUnion

TransUnion

A exposição de identidades sintéticas para obtenção de empréstimos ilustrou o risco de originação de novas contas

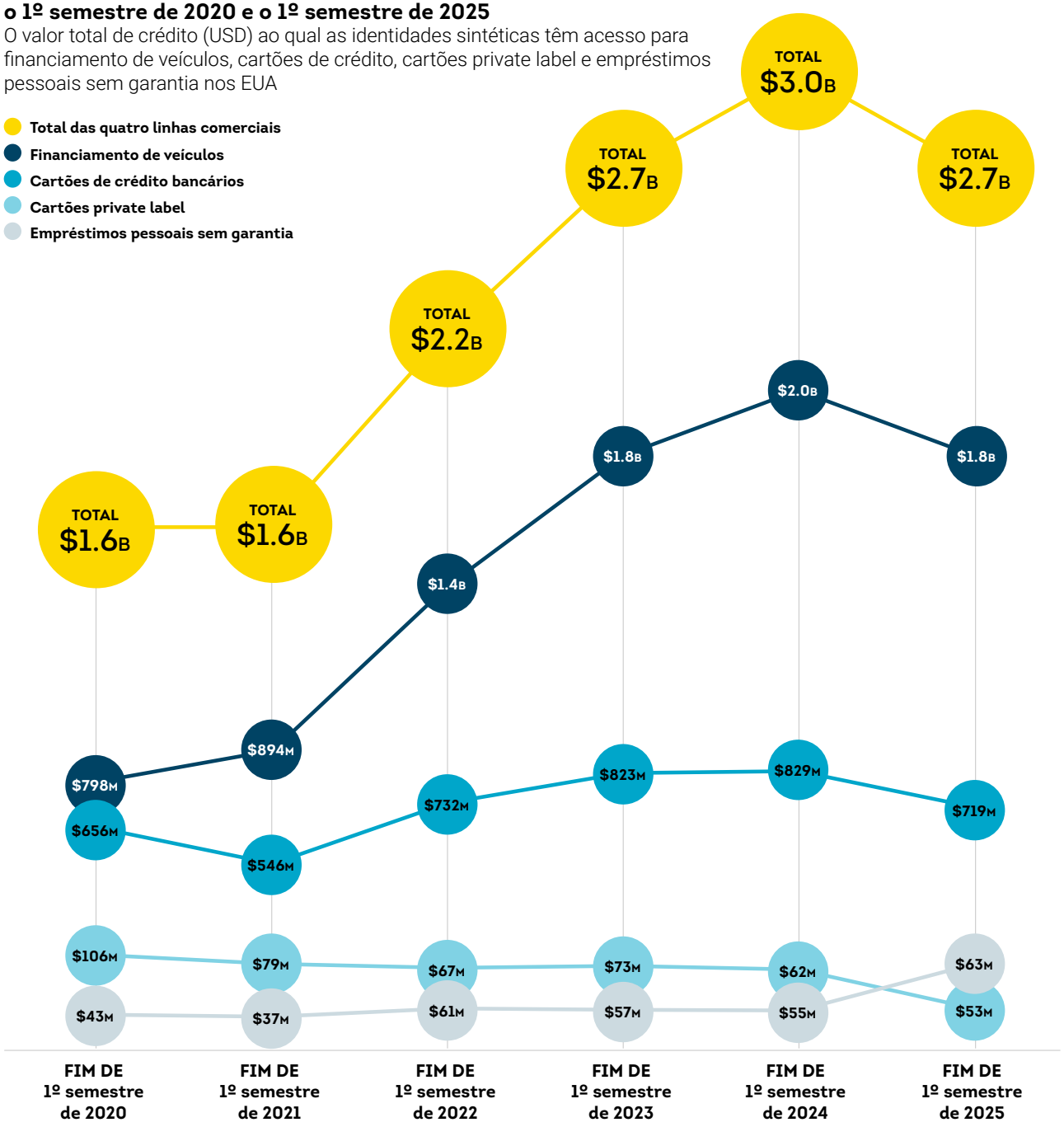
Com uma riqueza de credenciais de identidade roubadas combinadas com a IA generativa, a fraude de identidade sintética é uma ameaça persistente. Quase um quarto (24%) das lideranças corporativas dos EUA pesquisadas pela TransUnion declarou que a fraude de identidade sintética era a principal fonte de perdas por fraude para suas organizações.

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$ 2,7 bilhões em perdas potenciais no fim do 1º semestre de 2025.

Usar contas de crédito para construir um histórico pessoal confiável é uma tática fundamental para identidades sintéticas — uma técnica de proteção de identidade altamente eficaz — o que as torna difíceis de detectar. Com o crescimento das ferramentas de IA generativa para criar documentos deepfake realistas e identidades sintéticas em escala, os criminosos têm meios para cometer fraudes sintéticas em outros segmentos, como varejo, comércio eletrônico, saúde, governo, telecomunicações, FinTech e educação.

Risco de identidade sintética para empresas credoras dos EUA entre o 1º semestre de 2020 e o 1º semestre de 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

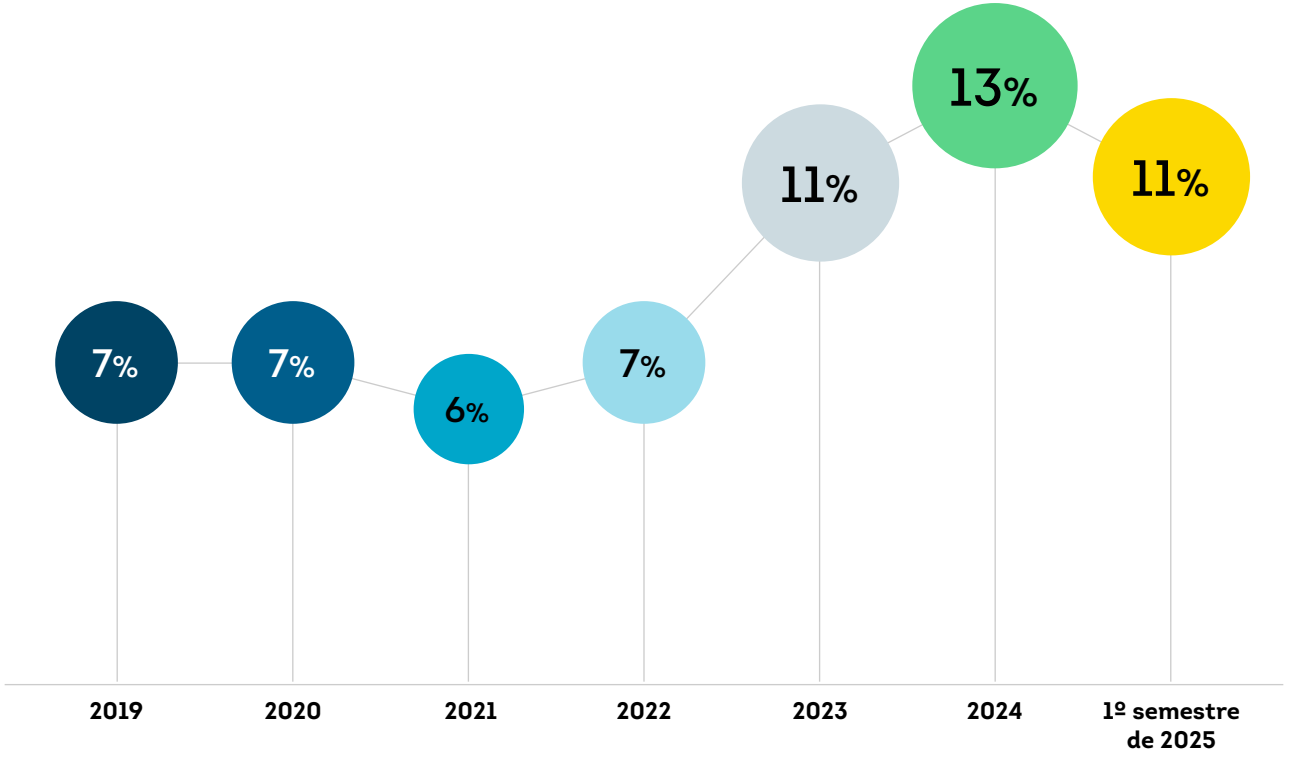
TransUnion

Credit washing amplia o risco de fraude com novas contas

À medida que a fraude de identidade evolui, os criminosos que cometem fraude em benefício próprio ou para terceiros podem tentar reciclar uma identidade através do credit washing. Trata-se de um esquema de manipulação de crédito que consiste em eliminar informações negativas do histórico de crédito de uma identidade, 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 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. No 1º semestre de 2025, as disputas de relatórios de crédito ao consumidor nos EUA alegando fraude representaram 11% de todas as disputas, permanecendo próximas ao máximo durante o período de análise de 13% em todo o ano de 2024.

Litígios no relatório de crédito aos consumidores nos EUA alegando fraude como percentual do total de litígios



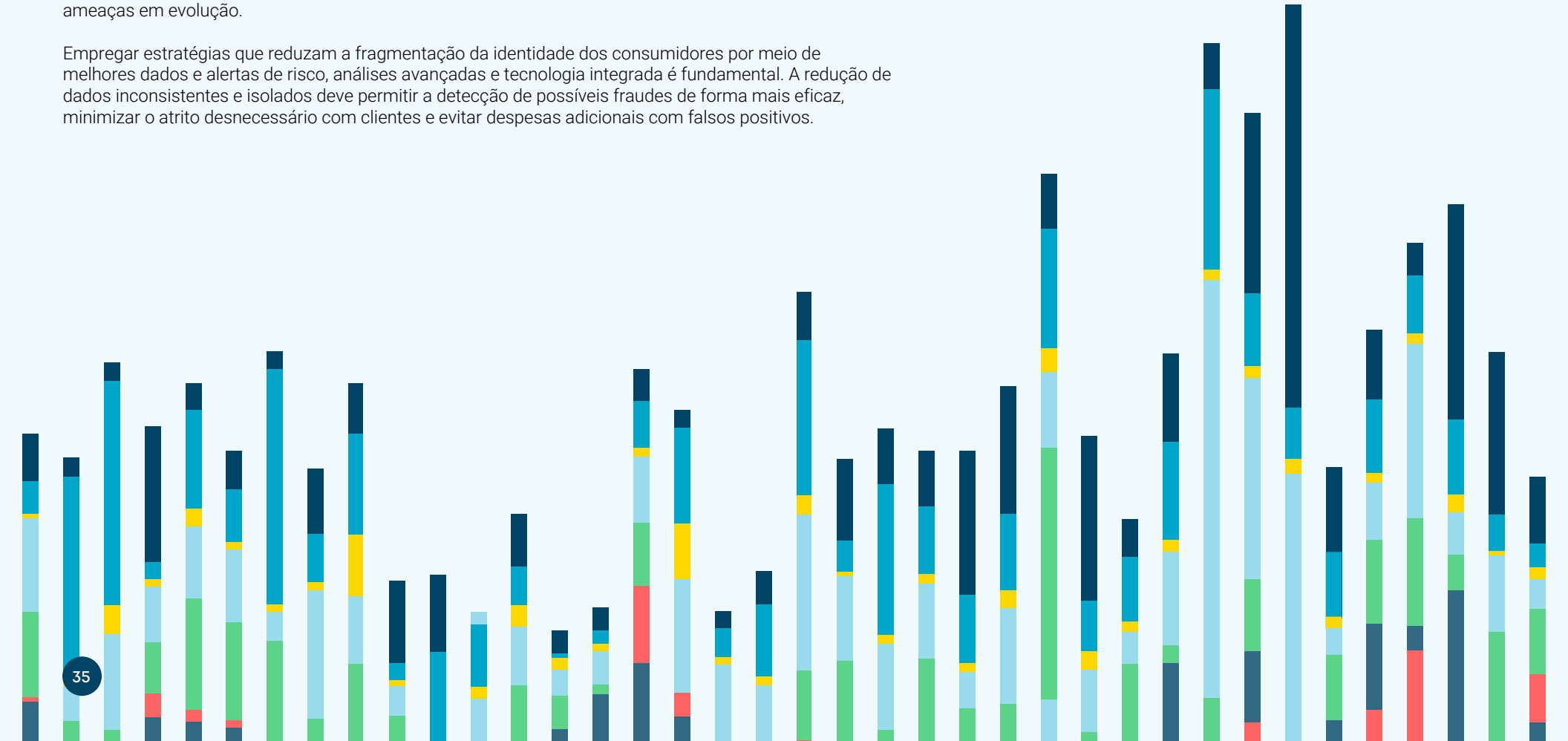
Fonte: Rede de Inteligência Global da TransUnion

Conclusão

Independentemente da localização, o aumento do risco de fraude e das perdas financeiras é uma preocupação crescente para organizações de todos os tamanhos e segmentos. No restante de 2025 e nos anos seguintes, as ameaças a consumidores e organizações continuarão, pois vazamentos de dados graves e golpes levarão a mais identidades e credenciais comprometidas. Proteger a organização e seus clientes não é negociável. É necessário adotar uma postura que assegure que todos os dados de identidade e credenciais apresentados à organização sejam verdadeiros.

À medida que o risco de identidade digital aumenta ao longo da jornada do consumidor, o investimento em detecção de fraudes mais inteligente, capaz de resolver problemas de identidade de forma eficaz, é essencial. Deve-se priorizar uma abordagem corporativa para prevenção à fraude, superando sistemas fragmentados que são mais vulneráveis à exploração. Ao mesmo tempo, é necessário reforçar cada camada das defesas, especialmente diante do vetor de ameaça da IA. Cada camada existente - verificação de identidade, verificação de documentos, autenticação, monitoramento de sessão, entre outras - precisa de alertas aprimorados, melhor pontuação de risco e revisão das estratégias de fraude para adaptação às ameaças em evolução.

Empregar estratégias que reduzam a fragmentação da identidade dos consumidores por meio de melhores dados e alertas de risco, análises avançadas e tecnologia integrada é fundamental. A redução de dados inconsistentes e isolados deve permitir a detecção de possíveis fraudes de forma mais eficaz, minimizar o atrito desnecessário com clientes e evitar despesas adicionais com falsos positivos.



Glossário

Este glossário reúne os principais termos relacionados a golpes digitais, organizados por etapas, para facilitar a compreensão das práticas criminosas e apoiar ações de prevenção.

Captação (Como os golpistas obtêm seus dados)

Vazamentos de dados: Exposição de informações pessoais, como CPF, endereço ou telefone, causada por falhas em sistemas ou ataques cibernéticos.

Phishing: Golpe realizado por e-mails falsos que simulam comunicações legítimas para obter dados sensíveis.

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

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

Infecção por malware: Instalação de programas maliciosos em dispositivos eletrônicos (celulares ou computadores) que coletam senhas e dados sem o conhecimento do usuário.

Engenharia social em call centers: Técnica em que golpistas se passam por clientes e usam persuasão para enganar atendentes e obter informações ou acessos indevidos.

Distribuição (Onde os dados roubados vão parar)

Grupos clandestinos: Comunidades secretas de criminosos que trocam ou vendem informações roubadas.

Marketplaces na dark web: Mercados ocultos na internet onde dados pessoais, senhas e cartões são comercializados entre golpistas.

Preparação (Como eles se preparam para usar os dados)

Criação de identidade sintética: Combinação de dados reais com informações falsas para formar uma identidade aparentemente legítima.

Teste de credencial: Verificação da funcionalidade de logins e senhas roubados em sites ou aplicativos.

Validação de credencial: Confirmação da autenticidade dos dados obtidos, garantindo que possam ser usados em golpes.

Criação de deepfake: Uso de tecnologia para produzir fotos, vídeos ou vozes falsas que imitam pessoas reais, enganando sistemas de segurança.

Exploração (Quando começam a aplicar os golpes)

Criação de conta: Abertura de contas falsas em bancos, e-commerces ou fintechs utilizando dados roubados ou identidades sintéticas.

Invasão de conta: Acesso indevido a contas reais, como bancárias ou de redes sociais, por meio de credenciais roubadas.

Transações financeiras: Realização de compras, transferências ou empréstimos usando contas invadidas ou falsas.

Troca de SIM / invasão de OTP: Golpistas assumem o chip da vítima ou interceptam códigos de autenticação para confirmar operações fraudulentas.

Refinamento (Como eles mantêm o golpe funcionando)

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

Manutenção de identidade sintética: Continuação do uso da identidade falsa sem levantar suspeitas, atualizando dados quando necessário.

Manipulação de perfil: Alteração de informações em contas para parecer legítimo e evitar bloqueios.

Metodologia de fornecimento de dados

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

Pesquisa corporativa

Esta pesquisa on-line foi realizada no Canadá (200 pessoas entrevistadas), em Hong Kong (200), na Índia (200), nas Filipinas (200), no Reino Unido (200) e nos EUA (200) de 29 de maio a 6 de junho de 2025 pela TransUnion em parceria com a empresa provedora de pesquisa terceirizada, Dynata. A pesquisa foi direcionada a funções gerenciais com responsabilidade por risco e/ou fraude em empresas cujas principais bases de clientes eram pessoas consumidoras e com receitas anuais mínimas de CA$ 300 milhões no Canadá, HK$ 200 milhões em Hong Kong, ₹1 bilhão na Índia, ₱1 bilhão nas Filipinas, £ 200 milhões no Reino Unido e US$ 200 milhões nos EUA. Os entrevistados responderam usando um método de pesquisa painel on-line em uma combinação de desktops, celulares e tablets. Tenha em mente que alguns percentuais dos gráficos podem não somar 100% devido a arredondamentos ou aceitação de diversas respostas.

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 pessoas 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 foi realizada de 5 a 25 de maio de 2025 em Botswana (251 pessoas entrevistadas), Brasil (949), Canadá (982), Chile (888), Colômbia (933), República Dominicana (601), Guatemala (478), Hong Kong (968), Índia (999), Quênia (433), Namíbia (291), Filipinas (943), Ruanda (345), África do Sul (922), Espanha (957), Reino Unido (1.000), EUA (2.998) e Zâmbia (325) pela TransUnion em parceria com a empresa provedora de pesquisa terceirizada, 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, Guatemala e Espanha). Para garantir a representatividade na metodologia para adquirir os dados demográficos de residentes, a pesquisa incluiu cotas para equilibrar as respostas entre as principais demografias, como idade, gênero e renda familiar. Tenha em mente que alguns percentuais dos gráficos podem não somar 100% devido a arredondamentos ou aceitação de diversas respostas.

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 do consumidor 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. O índice ou o percentual de tentativas de fraudes digitais suspeitas refletem os valores que os clientes da TransUnion determinaram que atendia a uma das seguintes condições: 1) negação em tempo real devido a indicadores fraudulentos; 2) negação em tempo real por violações da política corporativa; 3) fraude após investigação da pessoa cliente; ou 4) violação da política corporativa após investigação da pessoa cliente, em comparação com todas as transações avaliadas. 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 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 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 30 de junho 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. Nós tornamos a confiança possível ao garantir que cada pessoa seja representada de maneira confiável no mercado. Fazemos isso com uma imagem Tru™ de cada pessoa: um olhar multidimensional das pessoas, que cuidamos com bastante carinho. Através das nossas aquisições e investimentos em tecnologia, desenvolvemos soluções inovadoras que vão além da nossa sólida base em crédito central, abrangendo áreas como marketing, fraude, risco e análises avançadas. Como resultado, as pessoas e as empresas podem realizar transações com confiança, auxiliando na conquista por resultados. Chamamos isso de Informação para o Bem ® – e isso leva a oportunidades econômicas, ótimas experiências e empoderamento pessoal para milhões de pessoas em todo o mundo.

transunion.com.br/business

TransUnion