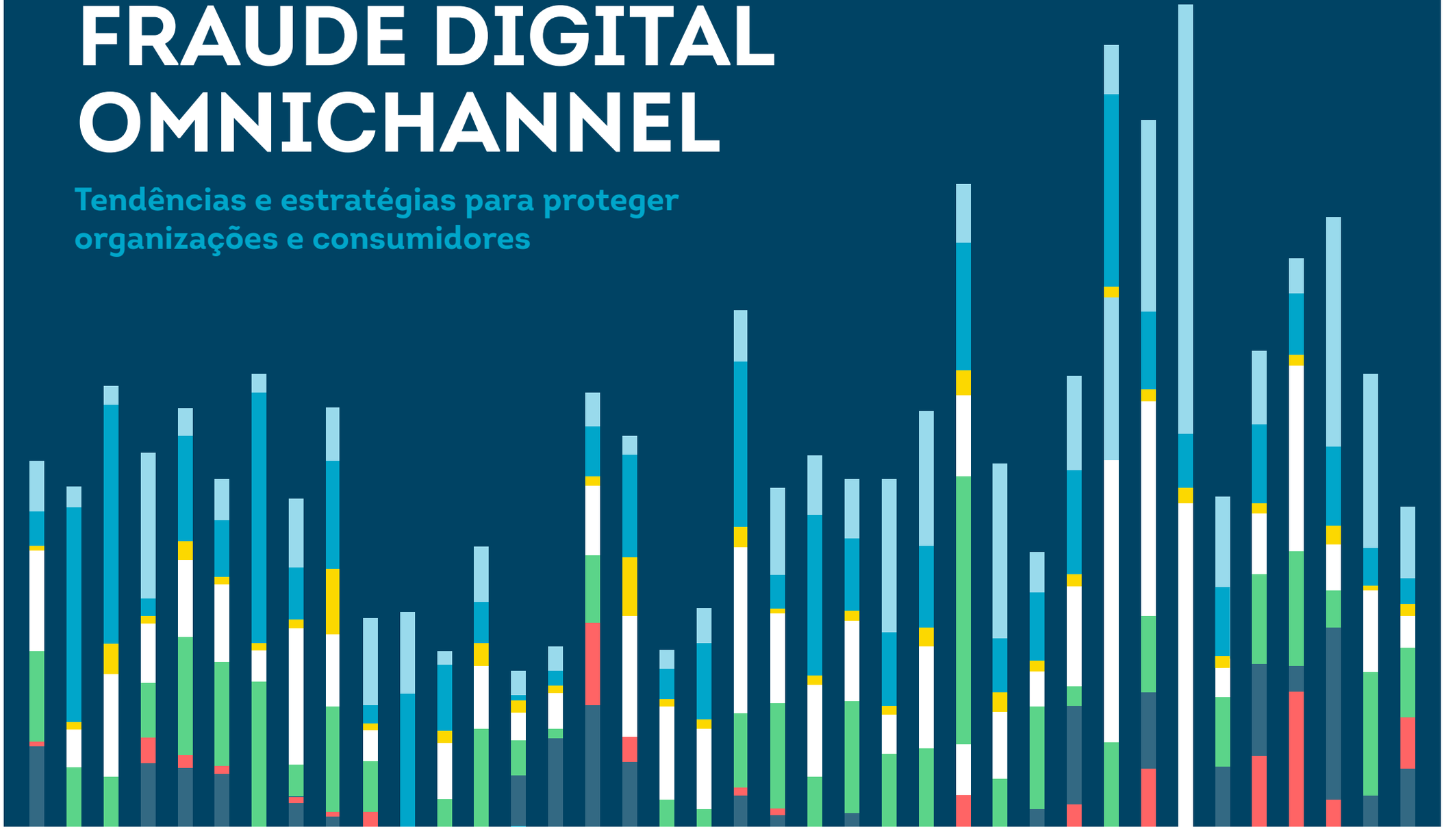
TransUnion

ATUALIZAÇÃO DO 2º SEMESTRE DE 2024

# TENDÊNCIAS DE FRAUDE DIGITAL OMNICHANNEL

## Tendências e estratégias para proteger organizações e consumidores



# Introdução

Os líderes de negócios reconhecem que podem estar enfrentando perdas consideráveis na receita e aumento do custo operacional a cada ano devido às fraudes. As pessoas que cometem crimes cibernéticos estão acessando de forma ilícita mais informações de identidade de organizações e pessoas físicas para abrir novas contas no nome de consumidores, criar contas fraudulentas, incluindo um número recorde de identidades sintéticas, ou para enganar os consumidores e fazê-los compartilhar seus dados de acesso. Diante de ameaças, ganharão as organizações que adotarem uma postura que pressupõe que as informações dos consumidores estão comprometidas, promovendo a confiança ao aprimorar a experiência omnichannel desse público com recursos fluidos de prevenção e detecção de fraude. Isso significa usar dados aprimorados de alerta de risco e identidade, regras de fraude centralizadas e tecnologia integrada para garantir a confiança na autenticidade das pessoas com quem se interage, independentemente do canal.

Neste relatório global sobre as Tendências de Fraude Digital Omnichannel, a TransUnion reúne tendências, benchmarks e toda sua expertise em fraude e identidades. O relatório apresenta insights para as pessoas responsáveis pelas áreas de prevenção contra fraudes e melhoria da experiência do cliente com o intuito de entregar melhores resultados de negócios. 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, a fim de melhorar a satisfação de clientes, reduzir a ocorrência de fraudes e aprimorar o desempenho do negócio.

Todos os dados deste relatório combinam insights proprietários da rede de inteligência global da TransUnion, uma pesquisa corporativa com pessoas consumidoras especialmente encomendada pela TransUnion no Canadá, na Índia, no Reino Unido e nos EUA, e uma pesquisa com pessoas consumidoras especialmente encomendada pela TransUnion em 18 países e regiões ao redor do mundo. Neste relatório, o 1º semestre (a primeira metade do ano) vai de 1º de janeiro a 30 de junho, e o 2º semestre (a segunda metade do ano) vai de 1º de julho a 31 de dezembro.



## PONTOS IMPORTANTES

### O custo das fraudes representa um risco financeiro significativo para as organizações

**6,5%**
da receita equivalente na média de perdas decorrentes de fraude, o que representa US$ 359 bilhões de perdas em fraude no ano passado entre os 801 líderes de negócios entrevistados no Canadá, na Índia, nos EUA e no Reino Unido

**75%**
dos líderes de negócios indicaram que as fraudes aumentaram ou permaneceram iguais no ano passado

### A preocupação com fraudes permanece alta entre as empresas e os consumidores

**5,2%**
de todas as tentativas de transações digitais globais foram suspeitas de fraude digital no 1º semestre de 2024, de acordo com a rede global de inteligência da TransUnion

**49%**
dos adultos em 18 países e regiões disseram terem sido alvo de golpes por e-mail, on-line, chamada telefônica e mensagens de texto no 2º trimestre de 2024, segundo a pesquisa da TransUnion com consumidores

### Maior risco de fraude na criação de novas contas

**6,5%**
de todas as tentativas de abertura de contas digitais globais foram suspeitas de fraude digital, de acordo com a rede global de inteligência da TransUnion; essa foi a fase de maior risco na jornada do cliente

**US$ 3,2 bilhões**
em exposição de empresas credoras a identidades sintéticas suspeitas para financiamentos de veículos, cartões de crédito, cartões private label e empréstimos pessoais sem garantia no final de junho de 2024 (nível mais alto de todos os tempos); o percentual de identidades sintéticas entre contas abertas no 1º semestre de 2024 também é o mais alto segundo a rede de inteligência global da TransUnion

# Sumário


**Experiências de fraude da liderança corporativa** 4

O custo da fraude

Tecnologia mais eficaz de prevenção a fraude

Utilização do método de autenticação de identidade

**Tendências de exposição de dados de identidade** 7

Os vazamentos de dados nos EUA atingiram recorde de gravidade

Os segmentos de serviços financeiros e de saúde foram os maiores alvos de violações

As principais credenciais de identidade foram o maior alvo dos vazamentos de dados

Os consumidores disseram ser alvo frequente de golpes fraudulentos

**Tendências globais de fraude digital** 11

O risco de suspeitas de fraude digital continuou elevado

O abuso de promoções está no topo da lista dos tipos de fraude mais comuns

O segmento da comunidade apresentou as maiores taxas de fraude digital

**Tendências de fraude em call centers** 15

As ligações de alto risco nos call centers disparam

Chamadas virtuais apresentam os riscos mais elevados para call centers

**Risco de fraude em novas contas ameaça as experiências digitais** 17

A abertura de novas contas apresenta a fase de risco mais elevado na jornada do cliente

Alta histórica em expor identidades sintéticas para obtenção de empréstimos

Financiamentos de veículos de alto valor atraindo fraudadores

Credit Washing amplia o risco de fraude na abertura de novas contas

**Conclusão** 22

**Metodologia de fornecimento de dados** 23

# Experiências de fraude da liderança corporativa

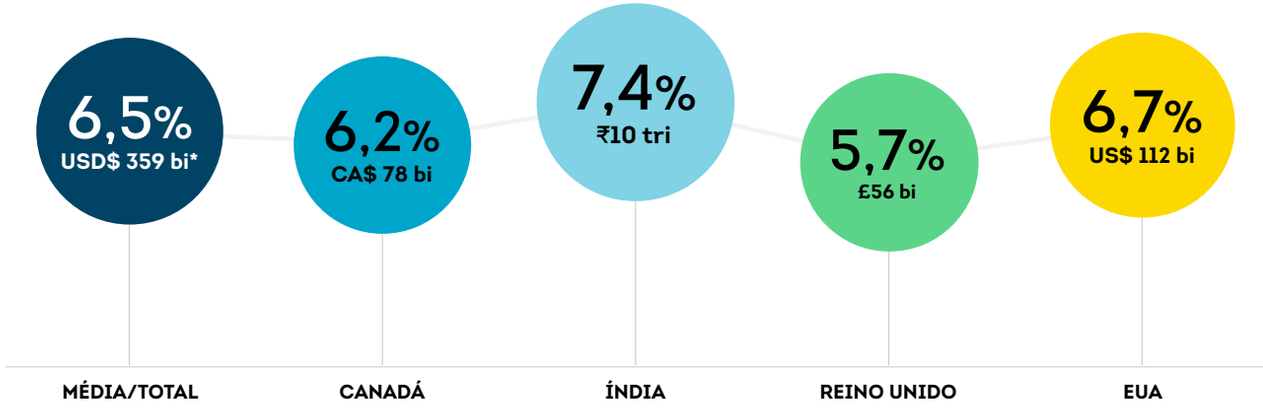
## O custo da fraude

Proteger os clientes e suas empresas de fraudes é essencial para a integridade e o sucesso das organizações. A liderança corporativa entrevistada no Canadá, na Índia, nos EUA e no Reino Unido afirma que, em média, suas empresas perderam o equivalente a 6,5% da receita por conta de fraudes no ano passado. Isso representa um total de US$ 359 bilhões de perdas de fraudes entre os 801 líderes corporativos entrevistados.

Quase um terço (31%) da liderança corporativa citou golpe/fraude autorizada como a causa mais proeminente das perdas reportadas, seguido por fraudes de terceiros (17%). Enquanto 75% afirmaram que todos os tipos de fraude avaliados permaneceram iguais ou aumentaram no ano passado, quase metade (49%) disseram que golpes/fraudes autorizadas aumentaram mais; 10 pontos percentuais a mais do que qualquer outro tipo de fraude.

### Custo total da fraude

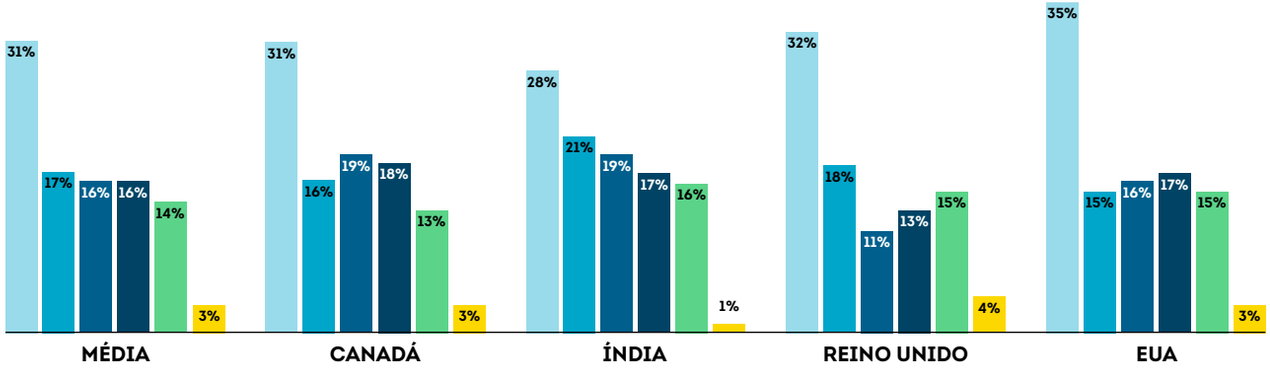
A liderança corporativa declarou o percentual de receitas que suas empresas perderam devido a fraudes no ano passado e o valor monetário correspondente




*Conversão para USD com base na taxa de câmbio de 5 de agosto de 2024

### 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)
- **Fraudes de terceiros**
  O uso de identidade roubada para abrir uma conta
- **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
- **Outros**



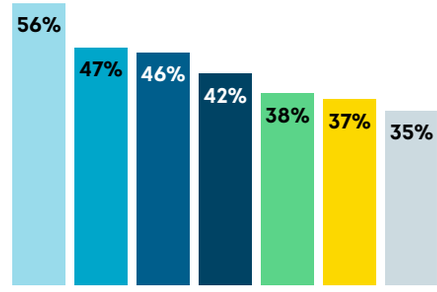

Fonte: Pesquisa corporativa da TransUnion

## Tecnologia mais eficaz de prevenção a fraude

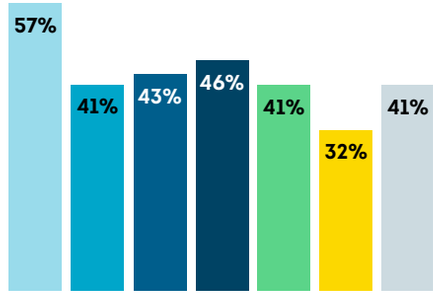
Dada a complexidade das fraudes e do risco de comprometimento das identidades dos consumidores, as organizações usam uma variedade de dados, alertas de risco, tecnologias e ferramentas para evitá-las. Mais da metade (56%) da liderança corporativa entrevistada classificou a verificação de identidade de modo geral como a tecnologia mais eficaz para evitar fraudes, e quase dois terço (64%) da liderança corporativa nos EUA disse o mesmo (ambos o maior percentual declarado).

### Tecnologia classificada como mais eficaz para evitar fraudes

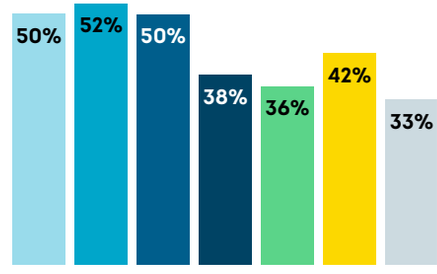
- Verificação de identidade
- Inteligência de IP
- Reputação do dispositivo
- Detecção de identidade sintética
- Biometria comportamental
- Reputação do número de telefone
- Reputação do e-mail



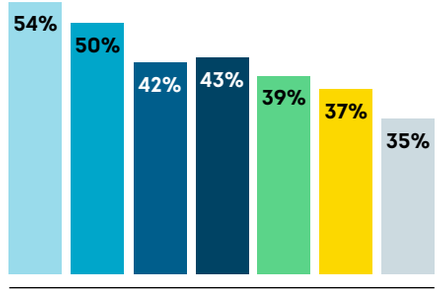

MÉDIA



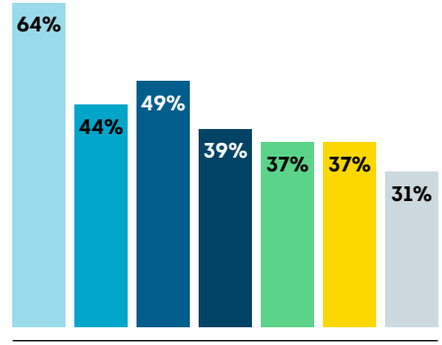

CANADÁ




ÍNDIA




REINO UNIDO



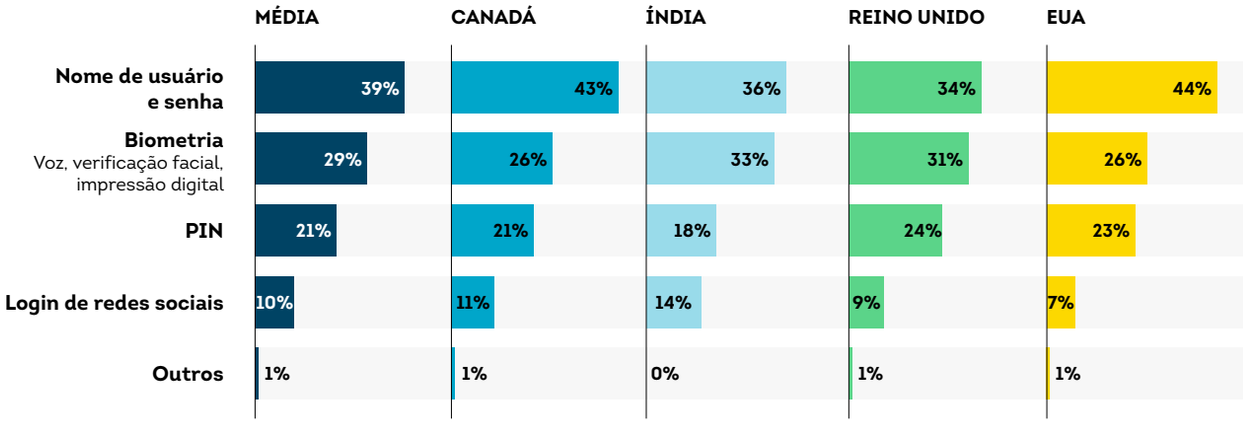

EUA

Fonte: Pesquisa corporativa da TransUnion

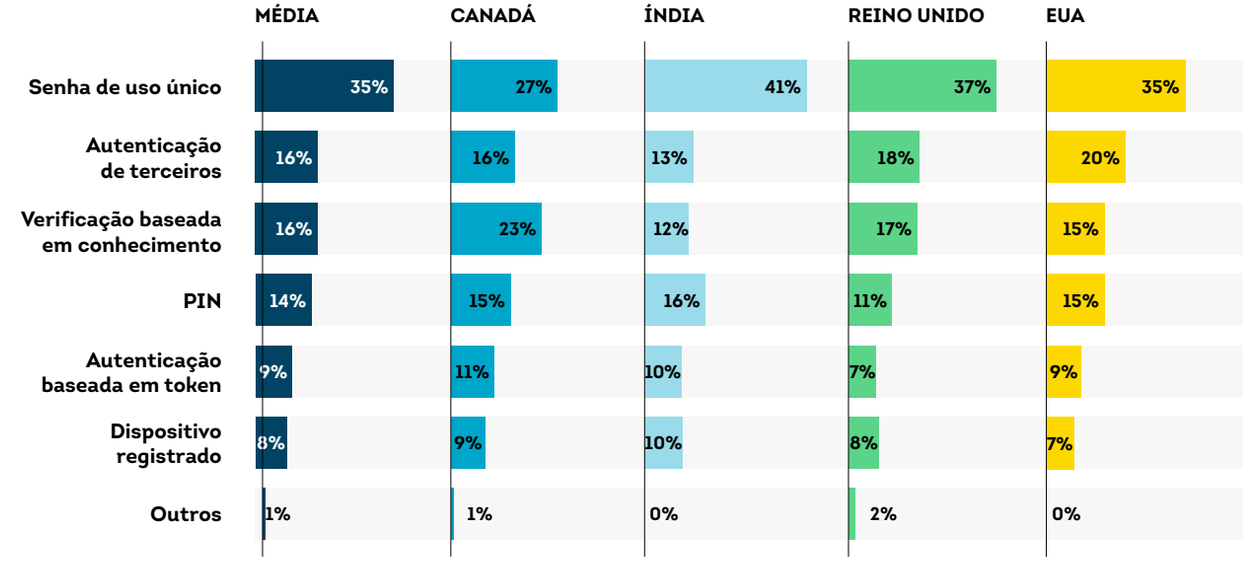
## Utilização do método de autenticação de identidade

Embora as credenciais de usuários estivessem sob ameaça de vazamentos de dados e golpes de consumidores, 39% da liderança corporativa declarou usar nomes de usuário e senhas como o principal método de autenticação de clientes; o maior percentual. Outros 29% disseram usar a biometria como principal método de autenticação. As senhas de uso único foram o segundo fator mais popular para autenticação de clientes, sendo mencionadas por 35% da liderança corporativa.

### Principal método usado para autenticar clientes




### Método secundário usado para autenticar clientes




Fonte: Pesquisa corporativa da TransUnion

# Tendências de exposição de dados de identidade

Criminosos continuaram determinados a adquirir dados de identidade de consumidores, tomando como alvo organizações e consumidores para abastecer seus esquemas de fraude. Mais da metade (49%) de todos os consumidores entrevistados em 18 países e regiões no 2º trimestre de 2024 disseram que foram alvo de golpes por e-mail, on-line, chamadas telefônicas ou mensagens de texto nos últimos três meses. Além disso, a gravidade dos vazamentos de dados nos EUA atingiu níveis históricos na primeira metade de 2024.

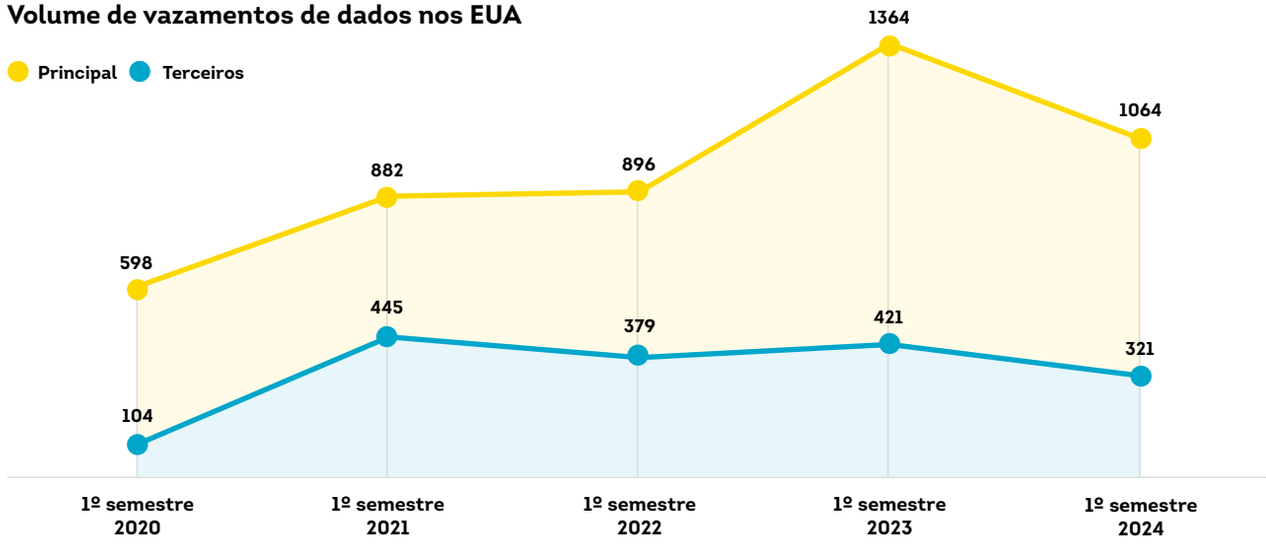
## Os vazamentos de dados nos EUA atingiram recorde de gravidade

Com vazamentos de dados sendo o principal indicador de fraudes futuras, as organizações dos EUA reportaram centenas de violações físicas e digitais na primeira metade do ano. Enquanto o volume de vazamentos de dados nos EUA diminuiu 22% ano após ano (YoY) no 1º semestre de 2024, a gravidade média do risco de violação (a capacidade de uma violação permitir fraude de identidade), medida pela pontuação de risco de violação (BRS) da TransUnion® TruEmpower™, aumentou 3% nesse mesmo período. Esse foi o maior valor já medido no 1º semestre deste que a TransUnion começou as análises em 2020.

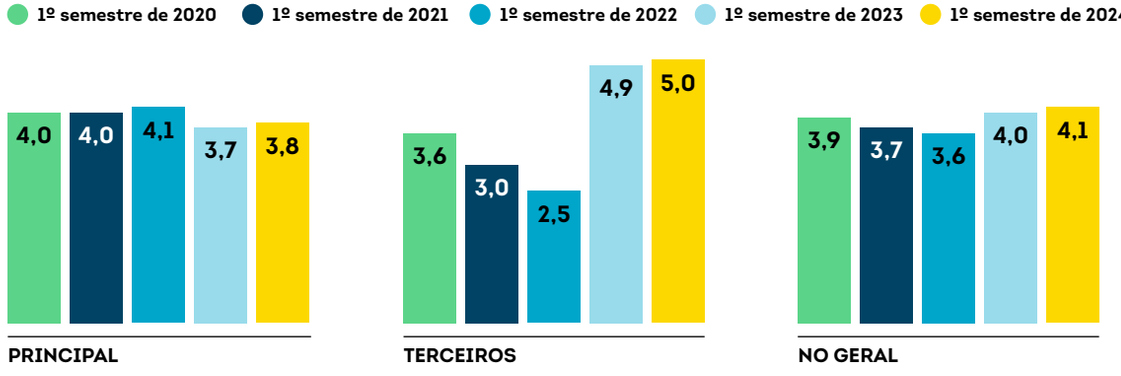
Os criminosos continuam a focar em provedores de serviços terceirizados como fonte de diversas credenciais de consumidores. Segundo os dados da TransUnion, as violações de terceiros foram mais graves no 1º semestre de 2024, com uma média de BRS 32% superior às violações internas.



### Volume de vazamentos de dados nos EUA




### Média da pontuação de risco de vazamento de dados para vazamentos de dados nos EUA




Um vazamento de dados primário representa um ataque direto a uma organização. Um vazamento de dados de terceiros, 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 fornecedores ou prestadores de serviços, como processamento de folha de pagamento ou cobrança médica, por exemplo.

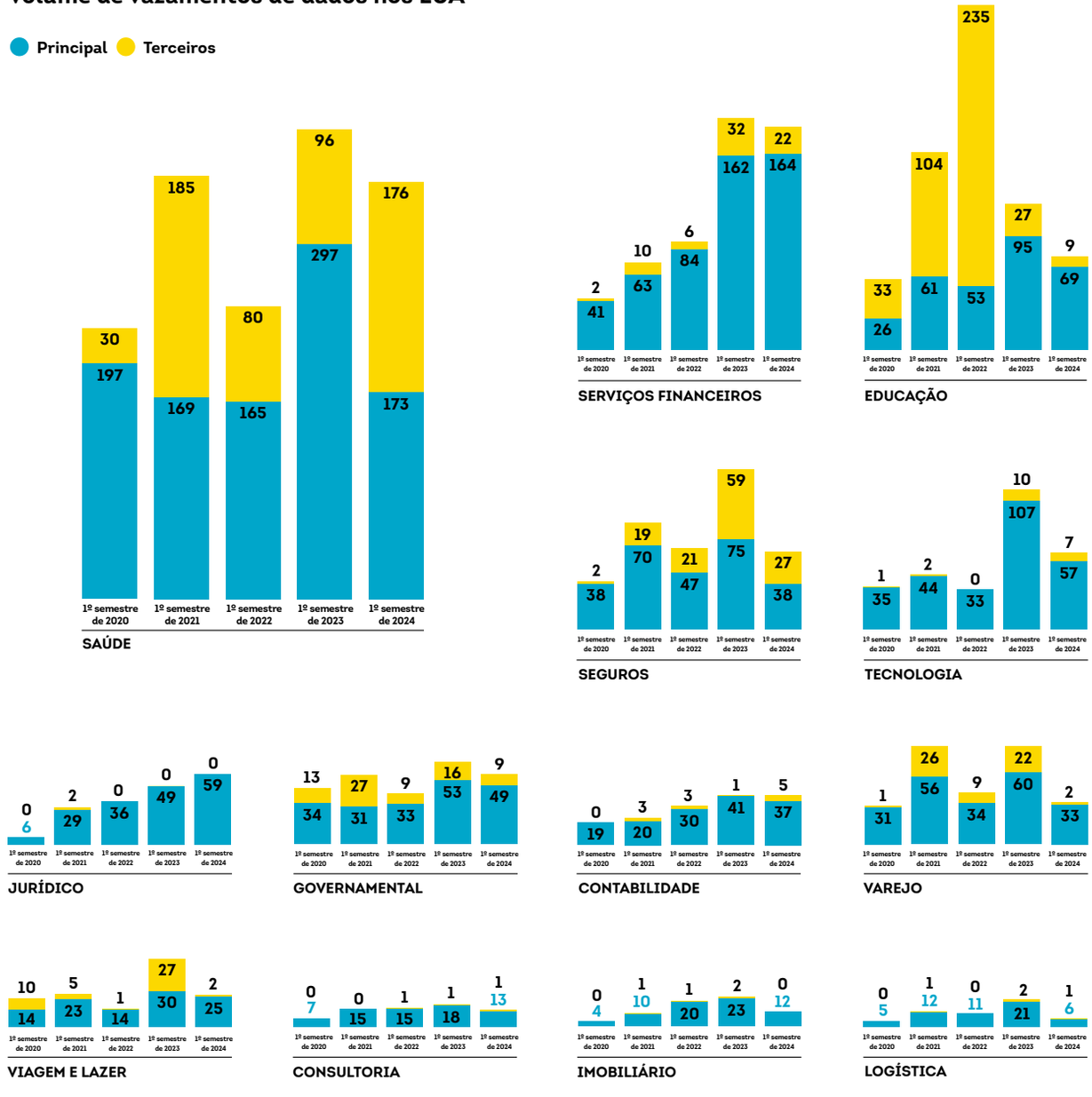
Fonte: TransUnion TruEmpower

TransUnion

## Os segmentos de serviços financeiros e de saúde foram os maiores alvos de violações

Segundo a TransUnion, no 1º semestre de 2024, o segmento de saúde sofreu o maior número de violações, seguido pelo de serviços financeiros e educação. Não apenas o setor de saúde teve o maior volume de violações, mas a TransUnion constatou que elas foram as mais graves nesse período, com um BRS de 5,4, seguido por contabilidade (4,0) e governo (4,0).

### Volume de vazamentos de dados nos EUA



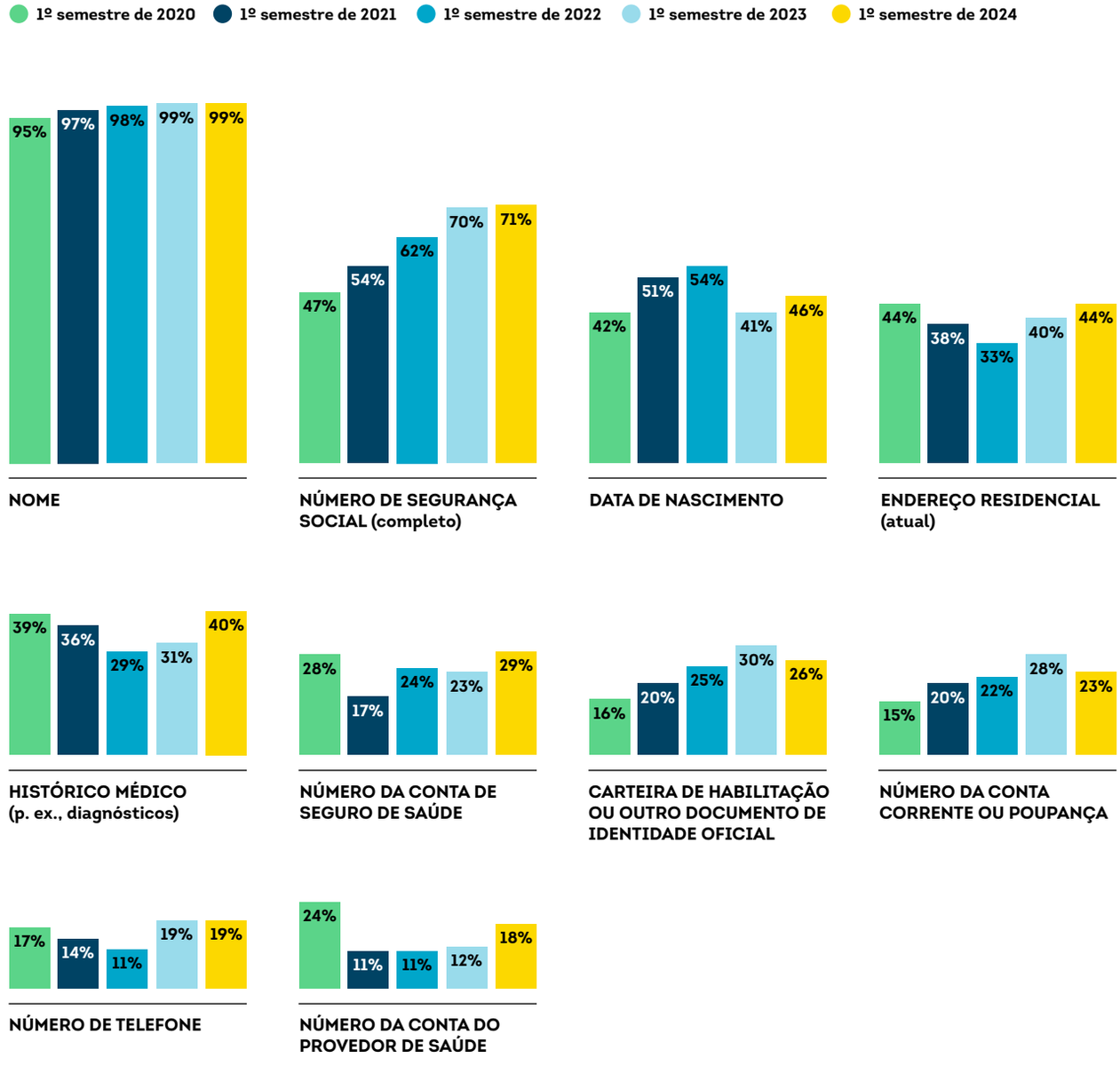

Observação: Os relatórios de mudanças no Gabinete do Procurador-Geral do Estado de Nova York aumentaram o número de violações relatadas nos serviços financeiros em 2023.

Fonte: TransUnion TruEmpower

## As principais credenciais de identidade foram o maior alvo dos vazamentos de dados

Os criminosos violaram os sistemas das organizações para roubar credenciais de identidade de consumidores, necessárias para abrir contas fraudulentas e criar identidades sintéticas. No 1º semestre de 2024, a TransUnion constatou que números de Segurança Social completos foram expostos em 71% dos vazamentos de dados, datas de nascimento em 46% e endereços residenciais em 44%. A exposição de dados no segmento de saúde mostrou um crescimento significativo no 1º semestre de 2024. Históricos médicos foram incluídos em 40% das violações gerais, um aumento de 29% ano após ano, e 71% das violações de terceiros, um aumento de 58%. Também houve um aumento no roubo de dados no segmento de cartões de pagamento (PCI) de organizações de serviços financeiros: a exposição de números de cartões de crédito ou débito aumentou 69%, de datas de vencimento até 136%, de códigos de segurança 79% e de nomes de titulares 85%.

**As 10 principais credenciais de identidade expostas em violações de dados nos EUA no 1º semestre de 2024**
Percentual de credenciais expostas em um vazamento de dados




Fonte: TransUnion TruEmpower

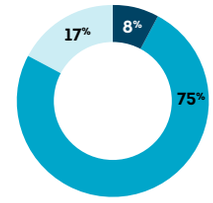
## Os consumidores disseram ser alvo frequente de golpes fraudulentos

Quase metade (49%) dos consumidores afirmou ter sido alvo de esquemas de fraude por e-mail, on-line, chamadas telefônicas ou mensagens de texto e 9% disseram ter sido vítima no período de janeiro a maio de 2024, segundo a Pesquisa Consumer Pulse da TransUnion do 2º trimestre de 2024. No entanto, uma parte significativa da população não reconheceu a fraude em potencial; 51% disseram não saber que estavam sendo alvo de esquemas de fraude. Entre os que disseram ter sido alvo, os principais tipos de fraude foram 37% de smishing, 34% de phishing, 33% de vishing, conforme relatado pelos consumidores em âmbito global.

### Consumidores que foram alvo de fraude

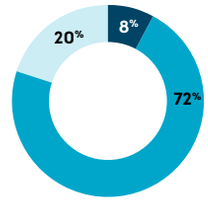
Percentual de consumidores que disseram ter sido alvo de tentativas de fraude on-line, por e-mail, chamadas telefônicas ou mensagens de texto de janeiro a maio de 2024, e qual o esquema mais comum usado nessas tentativas.

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



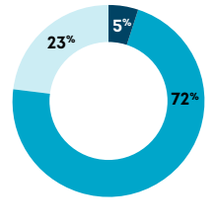

**ZÂMBIA**

Golpe de dinheiro/ vale-presente



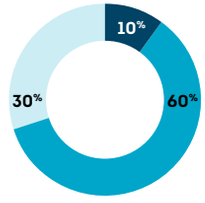

**QUÊNIA**

Vishing



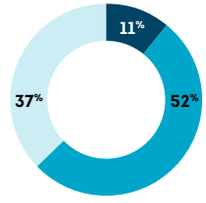

**BOTSUANA**

Vishing



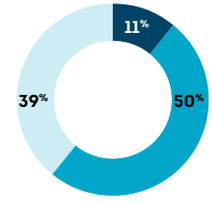

**FILIPINAS**

Phishing



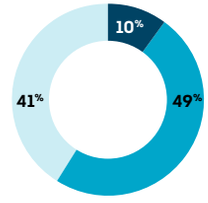

**NAMÍBIA**

Golpe de dinheiro/ vale-presente



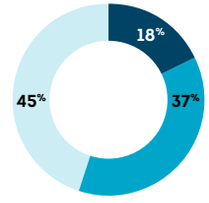

**RUANDA**

Golpe de dinheiro/ vale-presente



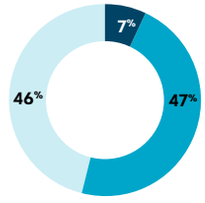

**ÁFRICA DO SUL**

Golpe de dinheiro/vale-presente



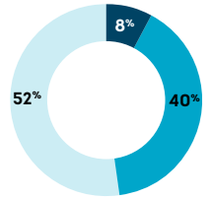

**ÍNDIA**

Phishing



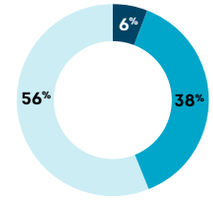

**CANADÁ**

Phishing



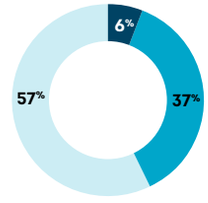

**ESTADOS UNIDOS**

Phishing



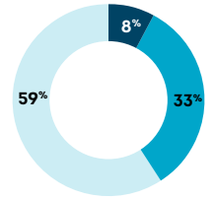

**HONG KONG**

Smishing



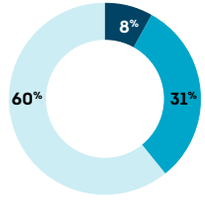

**REINO UNIDO**

Phishing



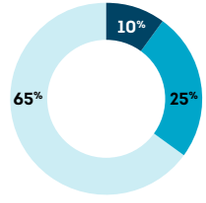

**COLÔMBIA**

Smishing



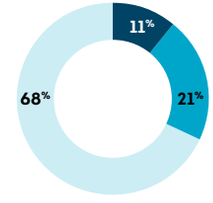

**CHILE**

Smishing



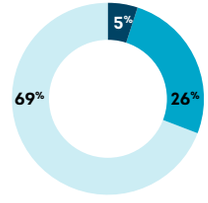

**GUATEMALA**

Esquemas de roubo e venda de identidade/Smishing



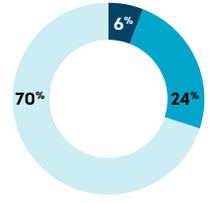

**REPÚBLICA DOMINICANA**

Cartão de crédito roubado




**ESPANHA**

Smishing




**BRASIL**

Golpe do PIX

Fonte: Pesquisa Consumer Pulse da TransUnion do 2º trimestre de 2024

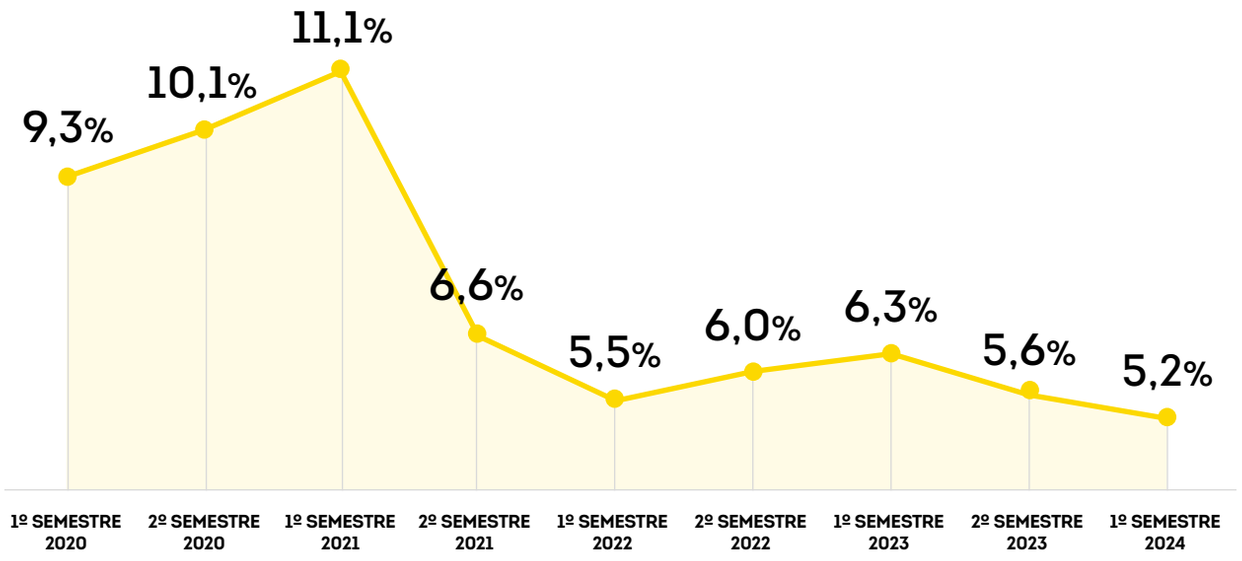
# Tendências globais de fraude digital

## O risco de suspeitas de fraude digital continuou elevado

A fraude digital continuou seu padrão oscilante histórico, mas consistentemente alto. A taxa de suspeita de fraude digital globalmente entre clientes do TransUnion TruValidate™ caiu para 5,2% no 1º semestre de 2024, de 5,6% no 2º semestre de 2023 e 6,3% no 1º semestre de 2023. Como visto nos relatórios anteriores, o risco de fraude digital variou conforme o país em que o consumidor estava durante a tentativa de transação, o segmento e o tipo de transação.

Dos 19 mercados onde fornecemos detalhamentos por país e região, sete (Brasil, Canadá, Chile, Colômbia, Índia, México e Filipinas) apresentaram um aumento na taxa de suspeita de fraude digital ano após ano no 1º semestre de 2024. Além disso, sete mercados (Brasil, Canadá, Colômbia, República Dominicana, Hong Kong, Índia e Filipinas) tinham taxas suspeitas de fraude digital acima da média global de 5,2% no 1º semestre de 2024.

**Taxa de suspeitas de fraude digital**

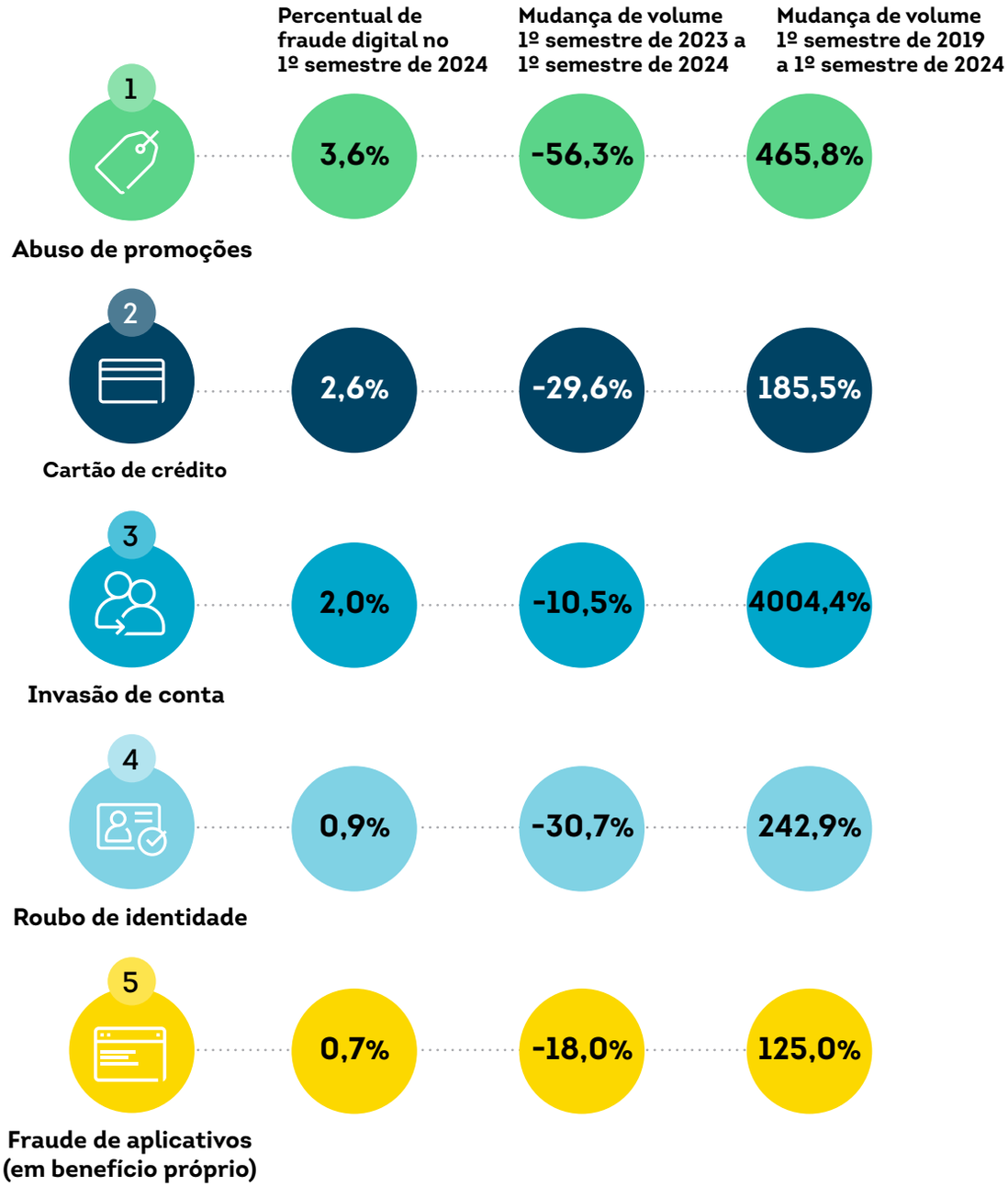



Fonte: TransUnion TruValidate

## O abuso de promoções está no topo da lista dos tipos de fraude mais comuns

Em 3,6%, o abuso de promoções (consumidores ou fraudadores se aproveitando de ofertas de marketing para receber incentivos financeiros não previstos) foi o principal tipo de fraude digital relatado à TransUnion por seus clientes em âmbito global no 1º semestre de 2024; cerca de um terço a mais do que a fraude de cartão de crédito (2,6%). No entanto, a fraude de identidade sintética (aumento de 153%) foi o tipo de fraude digital com crescimento mais rápido em termos de volume do 2º semestre de 2023 ao 1º semestre de 2024, e a fraude de pagamentos de transações interbancárias/débito (aumento de 113%) foi a que mais cresceu ano após ano (YoY) no 1º semestre de 2024, de acordo com clientes da TransUnion.

### Principais tipos de fraude e sua evolução




Fonte: TransUnion TruValidate

## O segmento de comunidades apresentou as maiores taxas de fraude digital

O setor de comunidades, que inclui propriedades da Web como fóruns on-line e sites de namoro, experimentou a maior percentual (11,5%) de suspeita de fraude digital em âmbito global no 1º semestre de 2024, de acordo com dados do TransUnion TruValidate, representando uma taxa de 23% e um aumento de 22% no volume de suspeita de fraude digital em relação ao 1º semestre de 2023. Os usuários de comunidades on-line contam com as organizações para fornecer confiança e segurança ao usar suas plataformas. No entanto, clientes de comunidades da TransUnion relataram a falsificação de perfil como o tipo mais frequente de fraude que testemunharam no primeiro semestre de 2024. Não é de surpreender que as comunidades tenham sido o segmento com a maior taxa de suspeita de fraude digital em 7 dos 19 países e regiões para os quais fornecemos detalhamentos no 1º semestre de 2024.

### Tentativas de fraude digital global por segmento

- **Índice de tentativas de fraudes digitais suspeitas – 1º semestre 2024**
- **Principais tipos de fraudes – 1º semestre 2024**
- **Mudança percentual no volume de fraudes digitais suspeitas do 1º semestre 2023 ao 1º semestre 2024**

### Comunidades
(encontros on-line, fóruns etc.)

1º SEMESTRE DE 2024
**11,5%**
**Falsificação de perfil**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**+22,3%**

### Jogos eletrônicos

1º SEMESTRE DE 2024
**11,4%**
**Scam/Solicitação**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-6,3%**

### Varejo

1º SEMESTRE DE 2024
**7,3%**
**Abuso de promoções**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-61,1%**

### Apostas
(apostas on-line, pôquer etc.)

1º SEMESTRE DE 2024
**7,2%**
**Abuso de promoções**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-9,2%**

### Serviços financeiros

1º SEMESTRE DE 2024
**4,6%**
**Invasão de conta**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-3,6%**

### Logística

1º SEMESTRE DE 2024
**2,9%**
**Fraude de envio**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**+120,7%**

### Telecomunicações

1º SEMESTRE DE 2024
**2,4%**
**Roubo de identidade**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-89,2%**

### Seguros

1º SEMESTRE DE 2024
**1,8%**
**Agente fantasma**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-32,4%**

### Governamental

1º SEMESTRE DE 2024
**1,6%**
**n/a***

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**+13,3%**

*N/A - o número de clientes que relataram tipos de fraude digital não tem relevância estatística o suficiente para constar no relatório

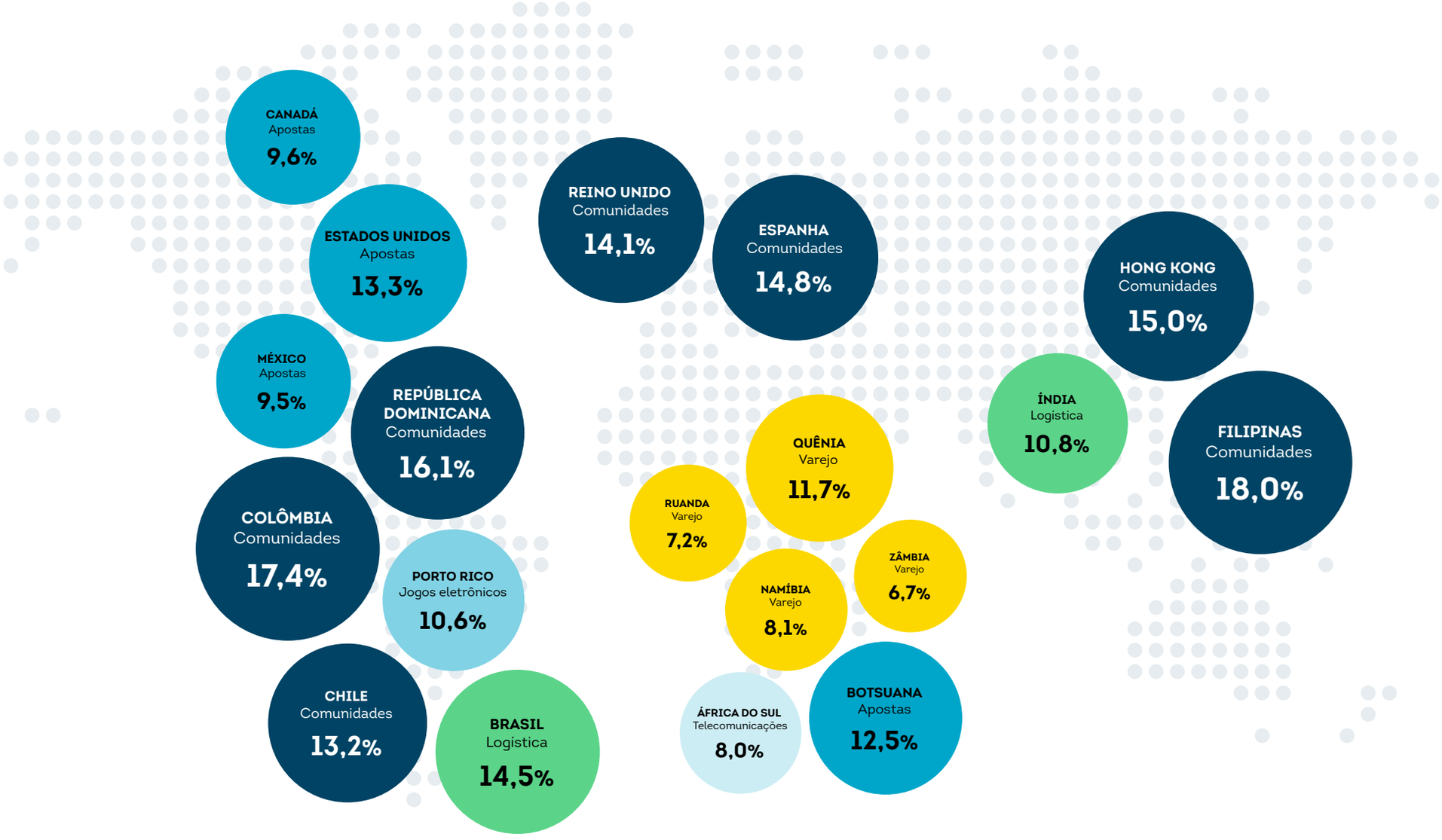
### Viagem e lazer

1º SEMESTRE DE 2024
**1,0%**
**Fraude de cartão de crédito**

1º SEMESTRE DE 2023
A 1º SEMESTRE DE 2024
**-33,2%**

Fonte: TransUnion TruValidate

**Tentativas de fraudes por região e segmento no 1º semestre de 2024**
O segmento com maior índice de suspeita de fraude digital considerando a localização do consumidor na região em que houve tentativa de transação






Fonte: TransUnion TruValidate

# Tendências de fraude em call centers

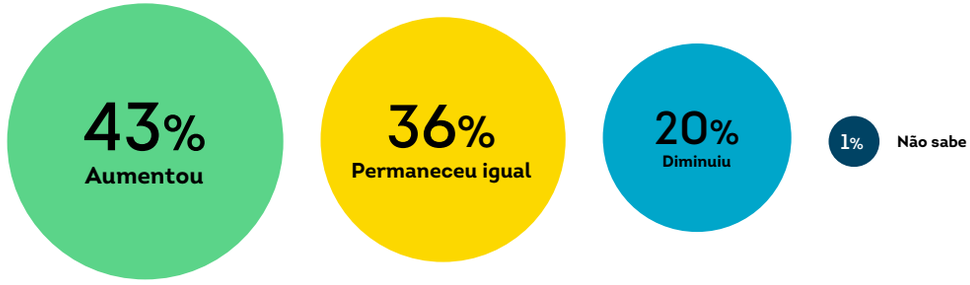
Os call centers desempenham um papel importante na experiência omnichannel de clientes, representando um ponto de contato de alta confiança para consumidores que podem ser abordados/acessados de diversas maneiras. Entre a liderança empresarial que participou da pesquisa patrocinada pela TransUnion e afirmou ter um conhecimento alto ou extremo sobre atividades relacionadas a fraudes em seus call centers, 43% indicaram que os fraudadores aumentaram seus ataques aos call centers no ano passado. Também entre esses líderes empresariais, mais da metade indicou que informações pessoais roubadas para passar pela autenticação baseada em conhecimento (59%), o uso de spoofing para se passar por um cliente (54%) e serviços de chamadas virtuais para ser anônimo ou não rastreável (53%) aumentaram no ano passado.

## As ligações de alto risco nos call centers disparam

A TransUnion documentou o aumento de 54% no percentual de chamadas de alto risco em call centers nos EUA do 1º semestre de 2023 ao 1º semestre de 2024, de 3,9% para 6,0%.

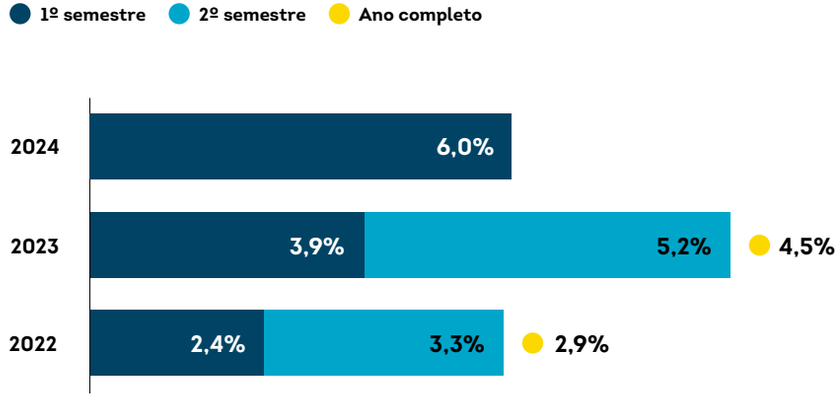
### Aumento da frequência de ataques de fraude em call centers

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

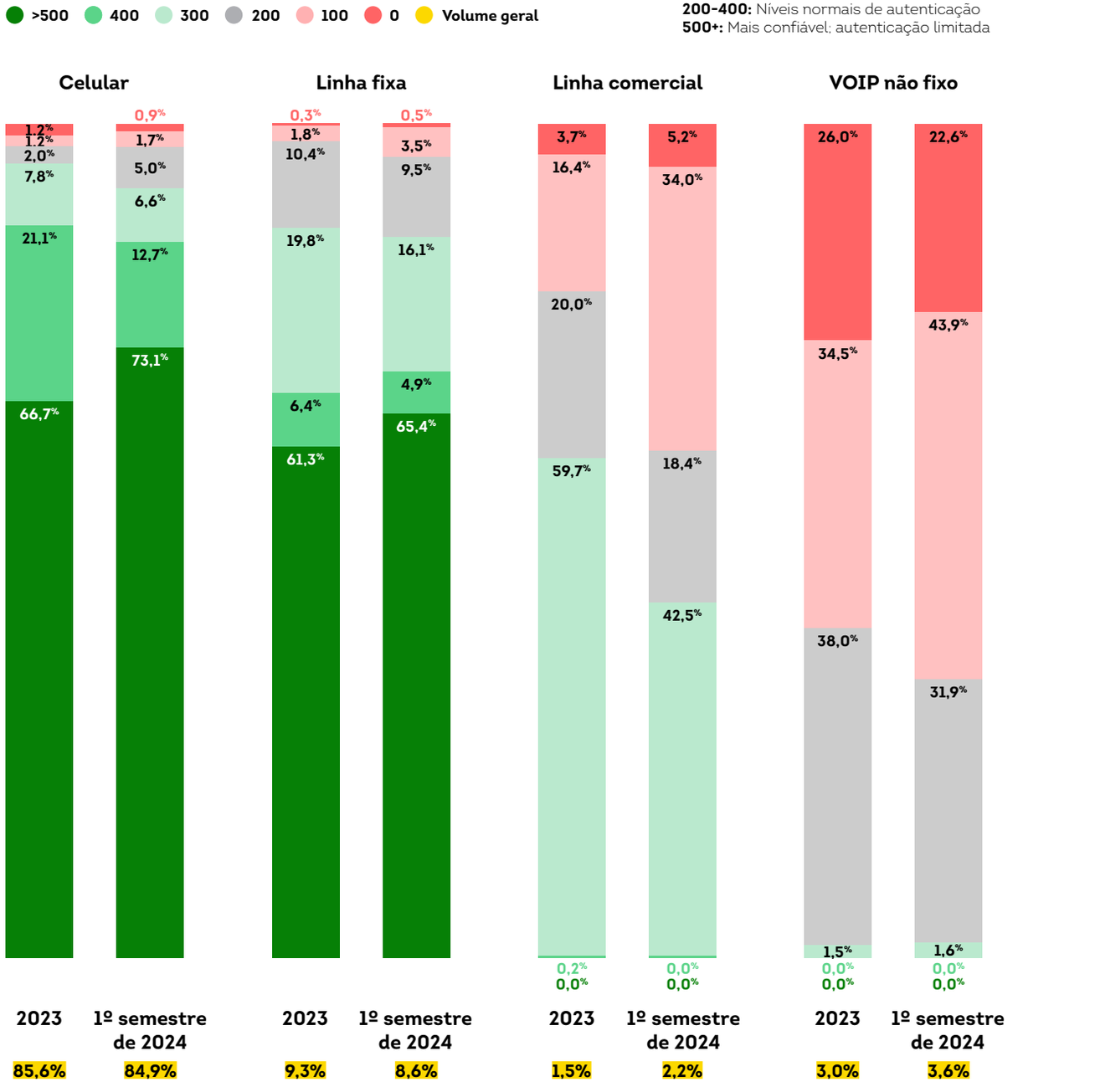



Fonte: TransUnion TruValidate

## Chamadas virtuais apresentam os riscos mais elevados para call centers

Embora a TransUnion tenha documentado que a grande maioria (85%) das chamadas recebidas por seus clientes de call center nos EUA eram de celulares no 1º semestre de 2024, apenas 2,6% dessas chamadas foram identificadas como sendo de alto risco de fraude. O percentual de ligações arriscadas de dispositivos móveis subiu de 2,4% durante todo o ano de 2023. 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 3,6% do volume total de chamadas, 67% dessas chamadas foram identificadas como de alto risco de fraude; um aumento em relação ao ano de 2023.

### Risco por canal e volume total nos call centers dos EUA




**Classificação dos níveis de risco das chamadas**

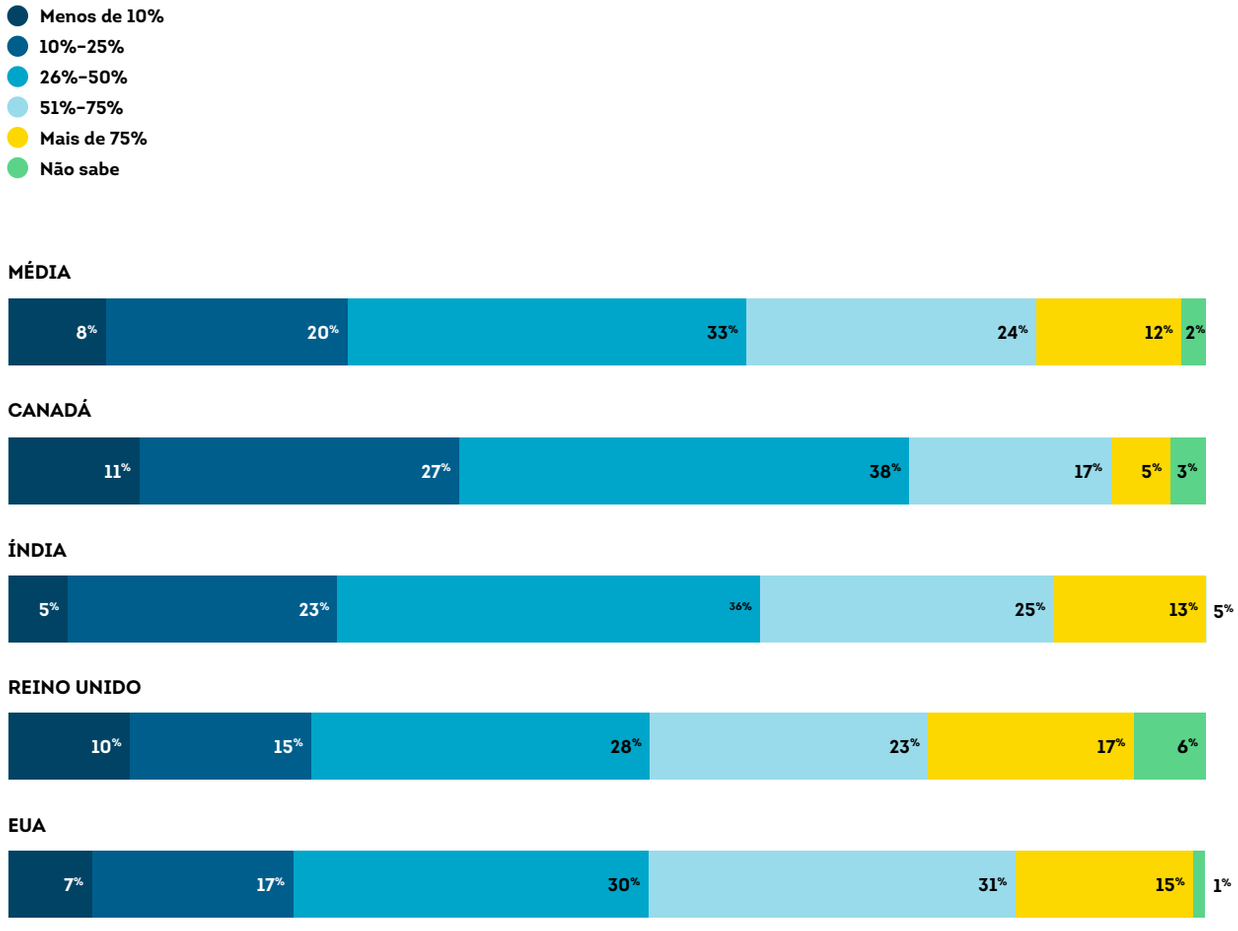
**0–100:** Mais alto; autenticação de nível superior
**200–400:** Níveis normais de autenticação
**500+:** Mais confiável; autenticação limitada

Fonte: TransUnion TruValidate

# Risco de fraude em novas contas ameaça as experiências digitais

À medida que as organizações confiam mais nos canais digitais e móveis para entregar experiências rápidas e convenientes para os clientes, a criação de novas contas on-line passa a representar um risco ainda maior. Mais de dois terços da liderança corporativa entrevistada pela TransUnion indicou que pelo menos 25% das aberturas de novas contas em suas organizações eram feitas on-line; mais de um terço indicou que era 51% ou mais. Embora quase três quartos (72%) dos líderes empresariais tenham indicado que uma alta taxa de detecção era extremamente ou muito importante para suas soluções contra fraudes, com tantas informações de identidade comprometidas no mercado, eles muitas vezes têm dificuldade para proteger seus negócios e, ao mesmo tempo, garantir experiências rápidas e contínuas aos clientes, especialmente na abertura de novas contas.

**Novas contas abertas on-line**
Percentual de novas contas de clientes abertas on-line




Fonte: Pesquisa corporativa da TransUnion

## A abertura de novas contas apresenta a fase de risco mais elevado na jornada do cliente

Analisando o cenário por fase da jornada do cliente, é particularmente preocupante o risco de criação de novas contas, impulsionado por maus atores que usam identidades sintéticas ou roubadas para abrir contas. De todas as tentativas de transações globais de criação de contas digitais TruValidate da TransUnion no 1º semestre de 2024 (representando 7% de todo o volume de tráfego), a TransUnion descobriu que 6,5% eram suspeitas de fraude digital; a maior taxa de risco de qualquer fase da jornada do cliente.

**Exemplos de fase da jornada do cliente**

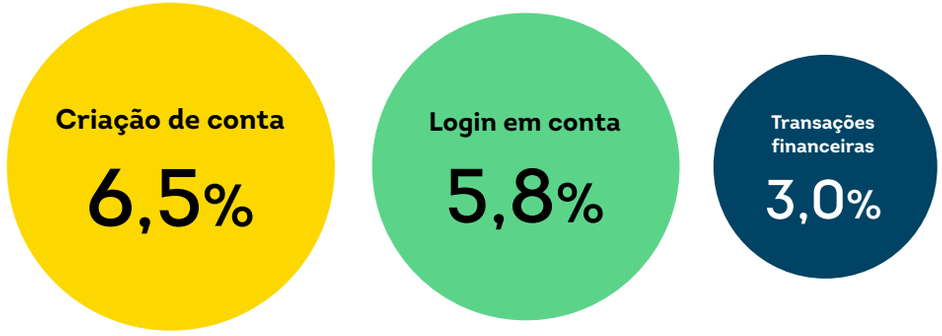
**Criação de conta:** Cadastro de conta, registro e originação de empréstimo

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

**Transações financeiras:** Compras, saques e depósitos

### Risco de fraude digital por tipo de transação da jornada do cliente

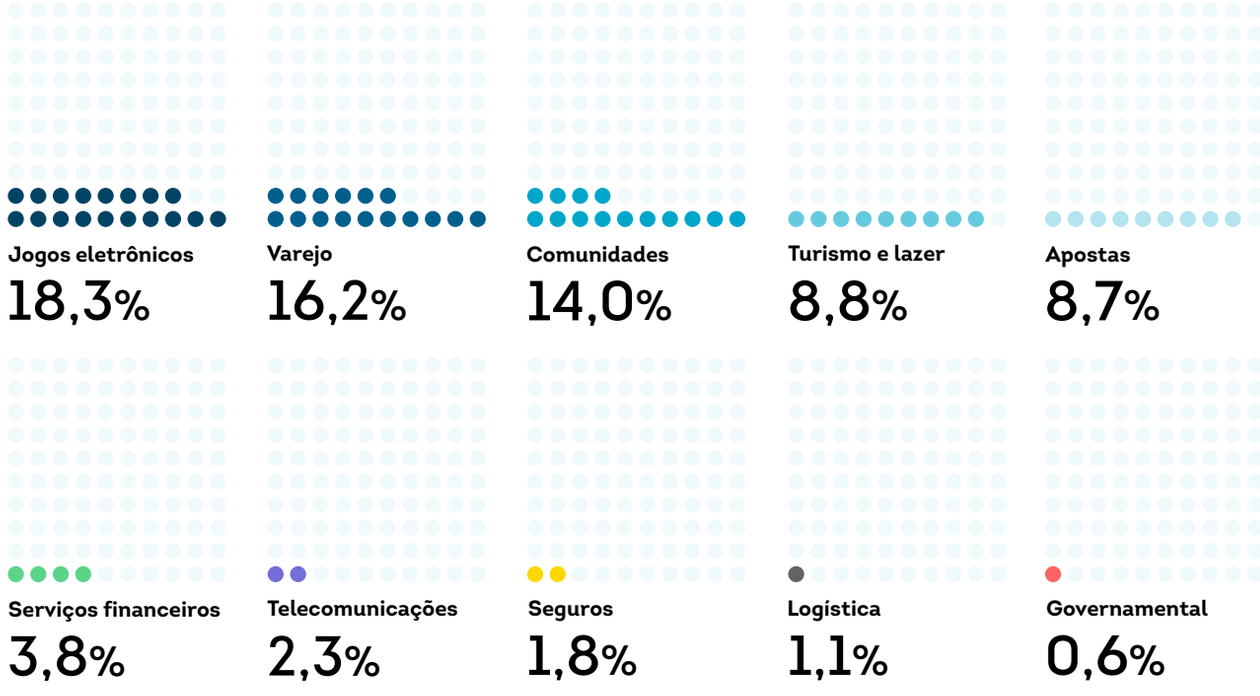
Percentual de cada tipo de transação suspeita de ser fraude digital em âmbito global no 1º semestre de 2024




Fonte: TransUnion TruValidate

### Fraude digital de criação de conta por segmento

Percentual de tentativas de transações de criação de contas digitais com suspeita de serem fraude digital por cada segmento em âmbito global no 1º semestre de 2024



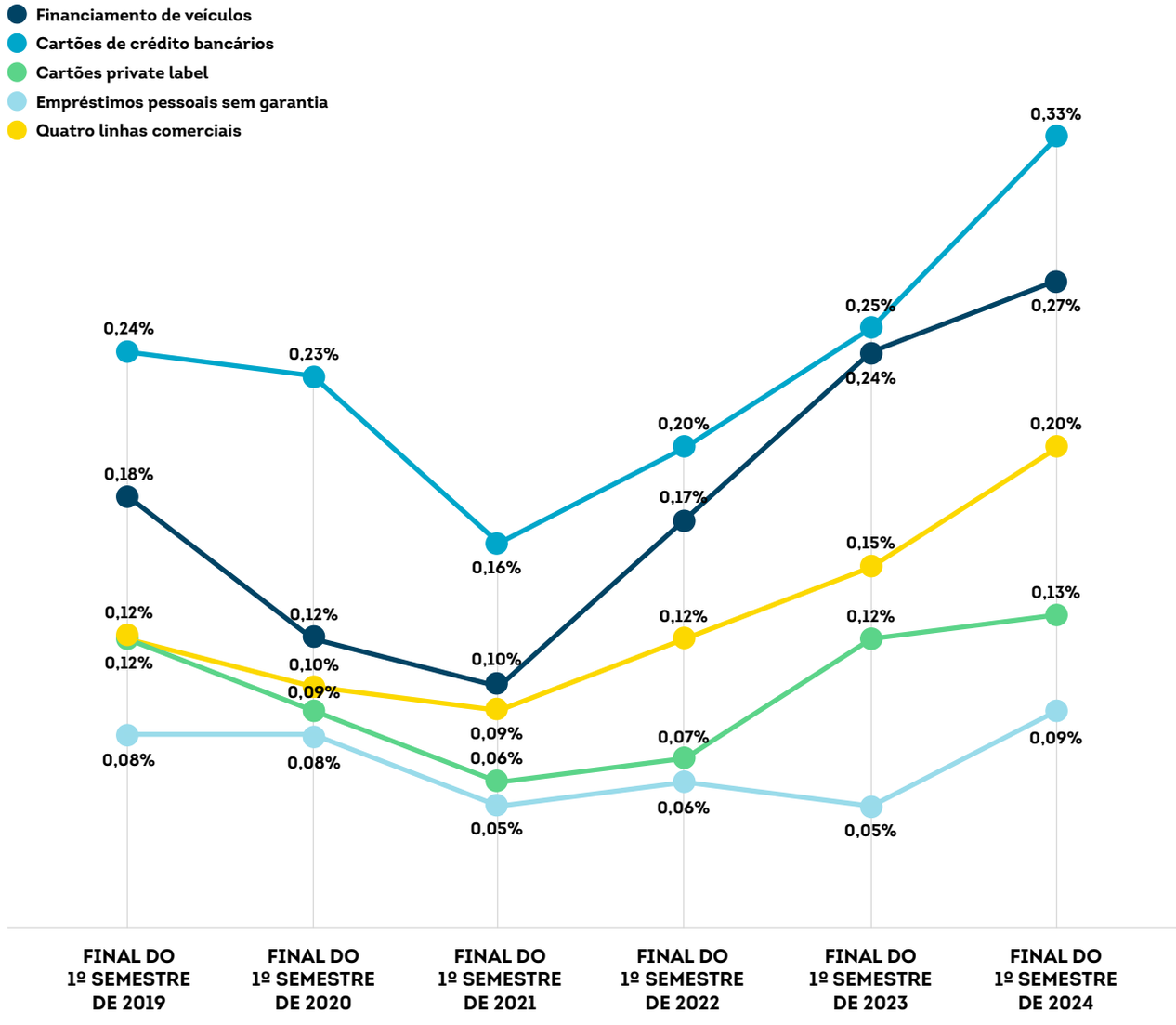

Fonte: Pesquisa da TransUnion sobre fraudes

## Alta histórica em expor identidades sintéticas para obtenção de empréstimos

Com uma grande variedade de credenciais de identidade roubadas prontamente disponíveis, a TransUnion constatou que os criminosos estão se tornando muito bons na fabricação de identidades. De acordo com os dados de crédito de consumidores da TransUnion, o percentual de identidades sintéticas entre contas abertas por credores dos EUA para financiamentos de veículos, cartões de crédito bancários, cartões private label e empréstimos pessoais sem garantia atingiu uma máxima histórica no final do 1º semestre de 2024, deixando os credores expostos a US$ 3,2 bilhões em potenciais perdas, também uma máxima histórica e 7% a mais que o final do 1º semestre de 2023. As identidades sintéticas entre contas abertas aumentaram 18% (chegando a 0,20%) no 1º semestre de 2024, em comparação com o 1º semestre de 2023. Com base no percentual de tentativas de abertura de contas com identidades sintéticas, o mercado enfrenta uma ameaça crescente de baixas no futuro. A aplicação de identidades sintéticas para financiamentos de veículos pareceu particularmente interessante para que os fraudadores acumulassem saldos. A exposição total dos credores a identidades sintéticas para financiamento de veículos apresentava saldos quase duas vezes maiores do que o setor de cartões bancários, que ocupa o segundo lugar entre as modalidades de crédito analisadas.

**Identidades sintéticas na abertura de conta**

Percentual de contas recém-abertas nos EUA associadas a identidades sintéticas



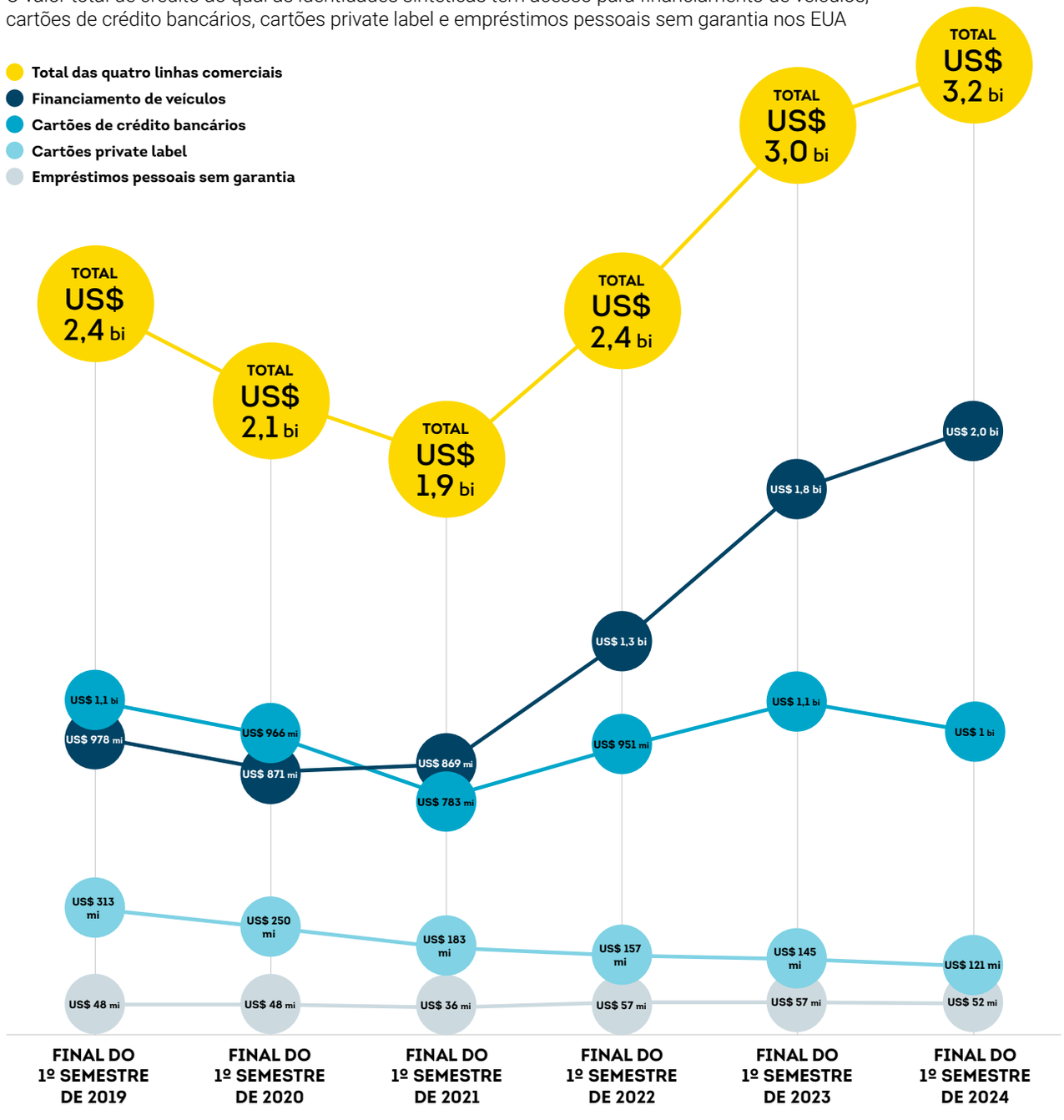

Fonte: TransUnion TruValidate

## Financiamentos de veículos de alto valor atraindo fraudadores

Com base no percentual de tentativas de abertura de contas com identidades sintéticas, o mercado enfrenta uma ameaça crescente de baixas no futuro. Entre as contas abertas com identidades sintéticas, os financiamentos de veículos pareciam ser mais atraentes para os fraudadores acumularem saldos. Ao final do 1º semestre de 2024, a exposição total dos credores a identidades sintéticas para financiamento de veículos apresentava saldos 100% maiores que o setor de cartões bancários.

**Identidades sintéticas: Exposição total de credores**

O valor total de crédito ao qual as identidades sintéticas têm acesso para financiamento de veículos, cartões de crédito bancários, cartões private label e empréstimos pessoais sem garantia nos EUA




Fonte: TransUnion TruValidate



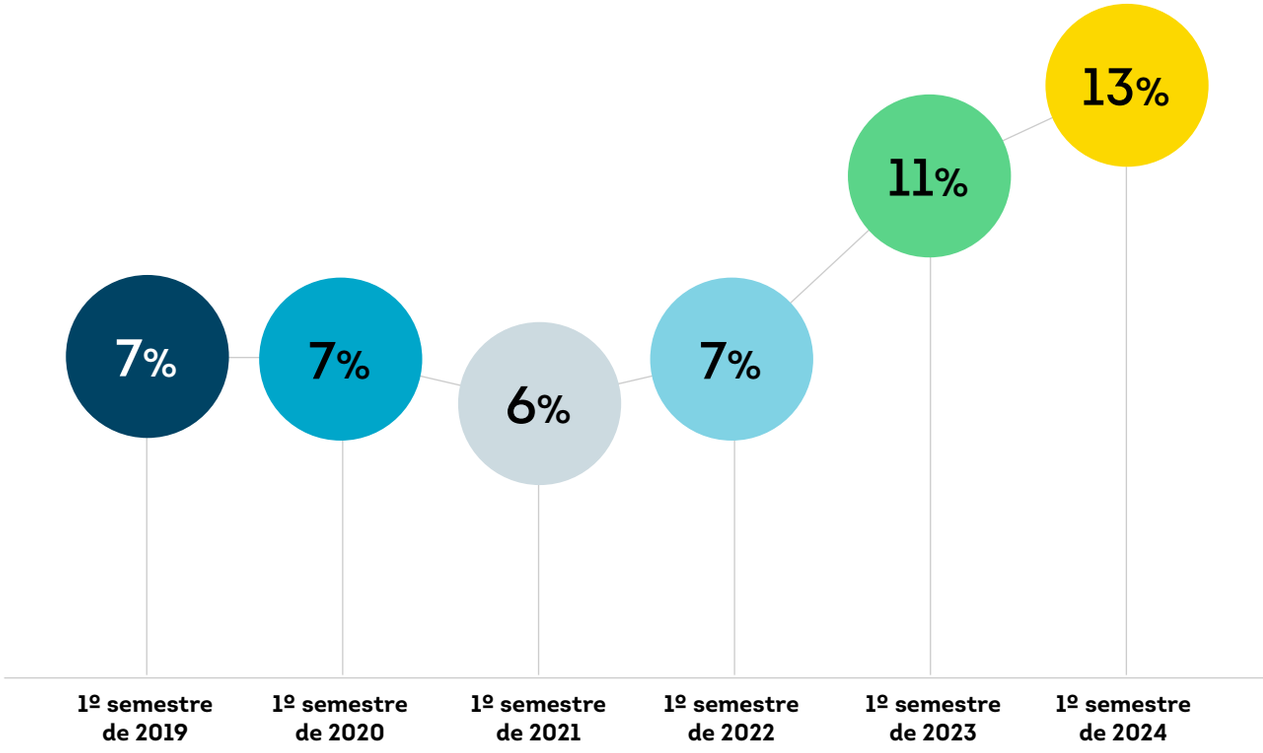
TransUnion

## Credit Washing amplia o risco de fraude na abertura de novas contas no mercado americano

À medida que a fraude de identidade aumenta, os criminosos que cometem fraude em benefício próprio com identidades roubadas ou sintéticas podem tentar reciclar uma identidade através da do credit washing. Trata-se de um esquema de manipulação de crédito recorrente nos Estados Unidos que consiste em eliminar informações negativas do histórico de crédito de uma identidade, fazendo uma falsa alegação de fraude de identidade. Ou seja, ao contestar informações negativas num relatório de crédito, esta pessoa pode induzir a agência a "limpar" ou eliminar temporariamente as informações negativas do relatório e, em última análise, aumentar a pontuação de crédito do mutuário, a partir de uma identidade roubada ou sintética. Estas disputas de relatórios de crédito falsos podem ser feitas contra contas abertas usando uma identidade de consumidor roubada ou uma identidade sintética, ou transações não autorizadas na conta de crédito legítima.

Consumidores nos EUA (ou seus representantes autorizados) têm o direito legal de contestar registros em seus relatórios de crédito, e a TransUnion segue um processo de resolução de disputas altamente regulamentado. No 1º semestre de 2024, os litígios nos EUA devido à reclamação de fraude representaram 13% de todos os litígios, o valor mais elevado no período de cinco anos analisado pela TransUnion.

**Disputas no relatório de crédito ao consumidor nos EUA devido a reclamações de fraude como percentual do total de disputas**




Fonte: TransUnion Consumer Credit

# Conclusão

A fraude digital tem altos e baixos, mas as tendências em vazamentos de dados e golpes ao consumidor são claras. Agora e no futuro, as organizações enfrentam pessoas que cometem crimes cibernéticos mais sofisticados que usam dados de identidade como arma em escala para executar esquemas de fraude em benefício próprio e de terceiros. Não apenas as organizações terão de lidar com a invasão persistente de contas, como os fraudadores continuarão a construir identidades falsas, mas consistentes, possibilitadas pela tecnologia para operar com escala e velocidade sem precedentes.

Quanto à liderança empresarial, eles querem proteger igualmente os clientes e as organizações. As fraudes custam para as organizações uma parte significativa da receita e causa perdas de lucro todos os anos. À medida que a liderança percebe o aumento do risco de fraude em todos os canais, a prevenção a fraude se torna um custo necessário que precisa ser o mais eficiente possível. Os líderes de fraude devem adotar uma abordagem empresarial para prevenir fraudes e construir a confiança do cliente. Empregue uma estratégia de inovação contínua por meio de melhores dados e alertas de risco, análises avançadas e tecnologia integrada para detectar possíveis fraudes de forma mais eficaz, sem aumentar a perda de negócios e despesas adicionais com falsos positivos.

# 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 entrevistados), na Índia (200 entrevistados), no Reino Unido (201 entrevistados) e nos EUA (200 entrevistados) de 14 a 29 de maio de 2024 pela TransUnion em parceria com o provedor de pesquisa terceirizado Dynata. A pesquisa foi direcionada a cargos gerenciais com responsabilidade por risco e/ou fraude em empresas cujas principais bases de clientes eram consumidores e cujas receitas eram maiores que CA$ 300 milhões no Canadá, ₹1 bilhão na Índia, £ 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. Os resultados desta pesquisa não são ponderados e são estatisticamente significativos em um nível nacional individual dentro de ± 6,9 pontos percentuais a um nível de confiança de 95% com base em uma margem de erro calculada. Tenha em mente que alguns percentuais dos gráficos podem não somar 100% devido a arredondamentos ou aceitação de diversas respostas.

## Call center

As conclusões da central de atendimento da TransUnion foram baseadas 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 pessoas consumidoras

As conclusões da disputa do relatório de crédito de pessoas consumidoras 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.

## Pesquisa Consumer Pulse

Esta pesquisa on-line com 15.372 pessoas adultas foi realizada de 29 de abril e 20 de maio de 2024 pela TransUnion em parceria com o provedor de pesquisa terceirizado Dynata. Pessoas adultas de 18 anos ou mais residentes de 18 mercados globais (Botsuana, Brasil, Canadá, Chile, Colômbia, República Dominicana, Guatemala, Hong Kong, Índia, Quênia, Namíbia, Filipinas, Ruanda, África do Sul, Espanha, Reino Unido, Estados Unidos e Zâmbia) foram entrevistadas usando um método de pesquisa painel on-line em uma combinação de computadores, celulares e tablets. As perguntas da pesquisa foram administradas em chinês (Hong Kong), inglês, francês (Canadá), português (Brasil) e espanhol (Chile, Colômbia, República Dominicana, Guatemala e Espanha). Para garantir a representatividade entre os dados demográficos dos residentes, a pesquisa incluiu cotas para equilibrar as respostas entre as principais demografias, como de 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.

## Vazamento de dados

A TruEmpower da TransUnion obtém seus próprios dados sobre violações físicas e digitais 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 para produzir um padrão e uma pontuação de risco e ações prescritas às pessoas consumidoras. O 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 as pessoas 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 do cliente; ou 4) violação da política corporativa após investigação do cliente, em comparação com todas as transações avaliadas. As análises nacionais e regionais examinaram transações em que a pessoa consumidora ou o fraudador suspeito estavam em determinado país e 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 30 de junho de 2024. As medidas de exposição do credor se baseiam na fórmula proprietária da TransUnion para capturar uma possível perda total em risco para os credores.

## Sobre o TransUnion TruValidate

O TruValidate coordena dados de identidade, reputação de dispositivos e insights para ajudar as organizações a se conectarem com as pessoas consumidoras de forma confiável e segura em diferentes canais, em cada etapa da jornada do cliente, ajudando a melhorar as conversões, reduzir as perdas por fraude e proporcionar experiências de usuário melhores e sem atritos.

**transunion.com/truvalidate**



TransUnion