O Real Custo das Fraudes na America Latina - 2019

Panorama no Brasil

LexisNexis®
RISK SOLUTIONS

A pesquisa “O Real Custo das Fraudes 2019 LATAM” da LexisNexis® Risk Solutions ajuda comerciantes e empresas de serviços financeiros a aumentar os seus negócios de maneira segura e administrar o custo das fraudes, ao mesmo tempo em que fortalecem a confiança e fidelidade dos clientes.

Brasil

A pesquisa oferece uma síntese das:

Atuais tendências de fraude para as empresas de varejo, comércio eletrônico e serviços financeiros do Brasil.

As principais questões relacionadas à inclusão de novos mecanismos de pagamento, realizando operações em canais online e móveis, e à expansão internacional.

Definições de fraude

Fraude é definida como:

- Operações fraudulentas e/ou não autorizadas;
- Solicitações fraudulentas de reembolso/estorno; cheques devolvidos;
- Mercadorias perdidas ou roubadas, assim como custos de redistribuição associados ao reenvio de itens comprados;
- Processos fraudulentos (ex.: envio proposital de informações incorretas sobre si mesmo, como renda, vínculo empregatício, etc.);
- Invasão a contas por pessoas não autorizadas; e
- Uso de contas para lavagem de dinheiro.

Essa pesquisa cobre métodos de fraudes voltadas ao consumidor.

- Não engloba fraudes com uso de informações privilegiadas e nem fraudes realizadas por funcionários.

O LexisNexis Fraud Multiplier℠

- Estima o prejuízo total que comerciante/empresa sofre com base no valor real da operação fraudulenta.

LexisNexis® RISK SOLUTIONS

Os dados da pesquisa foram coletados online e por telefone, de junho a agosto de 2019, com um total de 450 entrevistas realizadas com tomadores de decisões sobre fraudes, distribuídos em cinco mercados da América Latina. *O relatório a seguir reflete os resultados do Brasil.*


Brasil

	México	Brasil	Colômbia	Argentina	Chile
Varejo	30	30	30	30	**30**
Comércio eletrônico	30	30	30	30	**30**
Serviços Financeiros	30	30	30	30	**30**
TOTAL	**90**	**90**	**90**	**90**	**90**

As categorias de varejo e comércio eletrônico incluem:

- Vestuário/Roupas
- Autopeças
- Livros/Música
- Computadores/Software
- Medicamentos/Saúde e Beleza
- Alimentos e Bebidas
- Mercadorias no geral
- Hardware/Materiais de construção
- Hotel/Viagem
- Utensílios domésticos/mobiliário
- Material para escritório
- Artigos esportivos

As categorias de serviços financeiros incluem:

- Bancos de varejo/comerciais
- Cooperativas de crédito
- Investimentos
- Fideicomisso
- Gestão de Fortunas

Definições de segmento:

Comércio móvel
Permite operações através de navegadores para dispositivos móveis, aplicativos para dispositivos móveis ou pagamentos via telefone celular.

Digital
Empresas de varejo ou comércio eletrônico que vendem somente produtos digitais ou produtos digitais e físicos; empresas de serviços financeiros com 50% ou mais da receita anual proveniente dos canais online e/ou móveis.

LexisNexis® RISK SOLUTIONS

Principais achados

Brasil

1 O custo das fraudes apresenta tendência de alta para as empresas de varejo, de comércio eletrônico e de serviços financeiros no Brasil.

O custo de cada operação fraudulenta cresceu 3,61 vezes o valor das operações perdidas (comparado a 3,44 em 2018) para os comerciantes e as empresas de serviços financeiros brasileiros e aparenta tendência de alta por conta do último.

2 Os canais móveis continuam contribuindo para o risco de fraudes.

Isso inclui os navegadores para dispositivos móveis e, cada vez mais, os aplicativos para dispositivos móveis, conforme o seu uso é propagado para alcançar a população não bancarizada.

3 A verificação da identidade do cliente é chave tanto para os canais móveis quanto para os online.

Ataques de botnets e a velocidade de equilíbrio contra o atrito com o cliente são fatores que contribuem.

4 O custo das fraudes continua mais alto para quem oferece comércio móvel. Mas as empresas de serviços financeiros digitais sofrem ainda mais (regionalmente).

O custo de cada operação fraudulenta cresceu 3,77 vezes o valor das operações perdidas (comparado a 3,58 em 2018) para as empresas de comércio móvel brasileiras, totalizando custos de fraudes que representam, agora, 2,88% das receitas anuais. E esse custo é ainda maior para as organizações de serviços financeiros digitais nos países, chegando a até 4,10 vezes o valor da operação perdida.

5 As empresas ainda não combatem fraudes da melhor maneira.

Uma parte significativa ainda não identifica operações fraudulentas bem-sucedidas por canal e forma de pagamento. Além disso, cerca de 1/3 das operações marcadas continuam sendo enviadas para revisões manuais caras e demoradas.

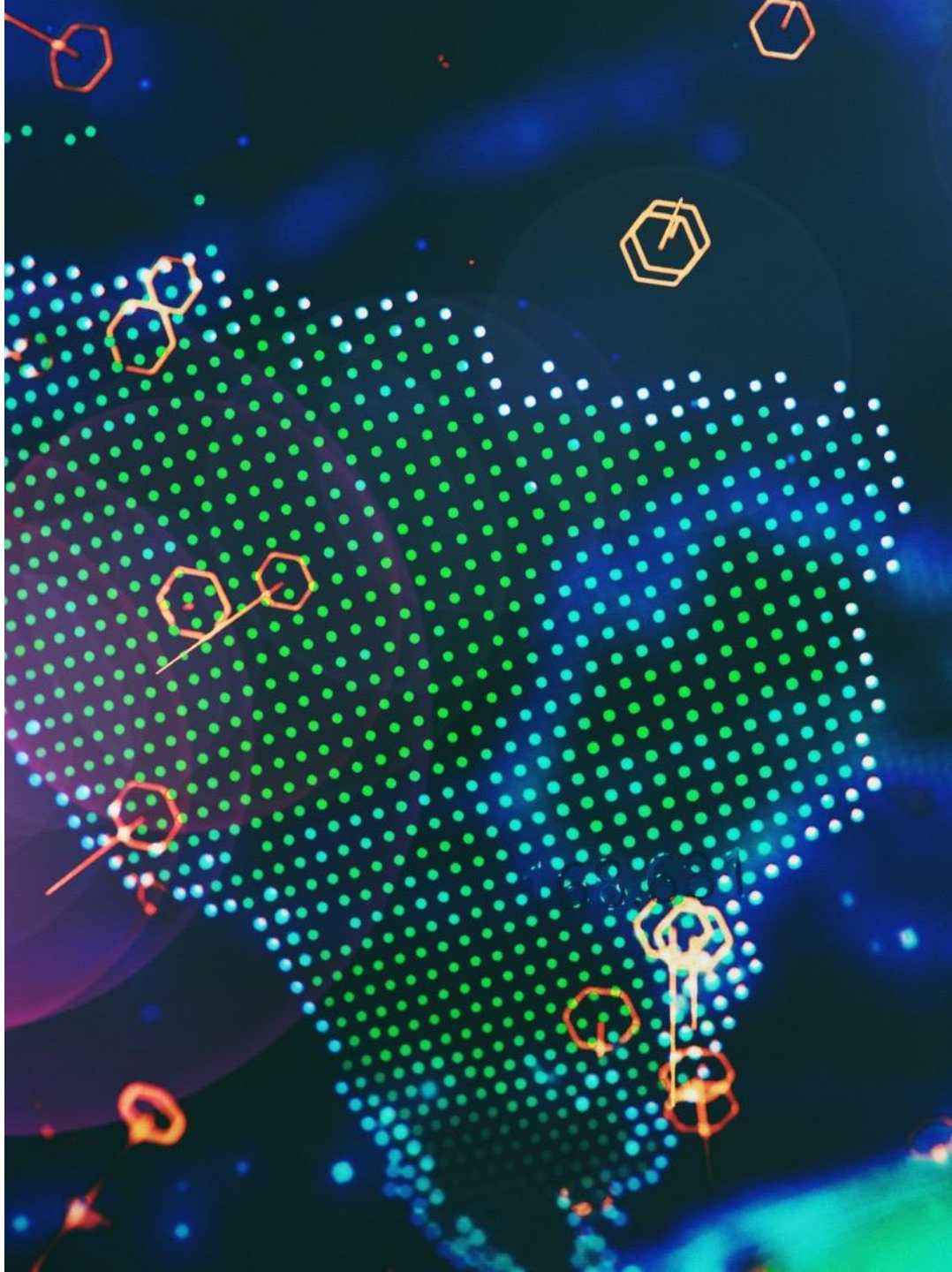
6 E, à medida que as fraudes se tornam mais sofisticadas, o uso de soluções mais refinadas continua limitado.

O uso de soluções mais avançadas e direcionadas para a detecção de fraudes móveis, como identidade/ impressão digital de dispositivos, localização geográfica e classificação de operações em tempo real são mais limitadas do que outras.

LexisNexis® RISK SOLUTIONS

1

O custo das fraudes apresenta tendência crescente para as empresas de varejo, de comércio eletrônico e de serviços financeiros no Brasil.

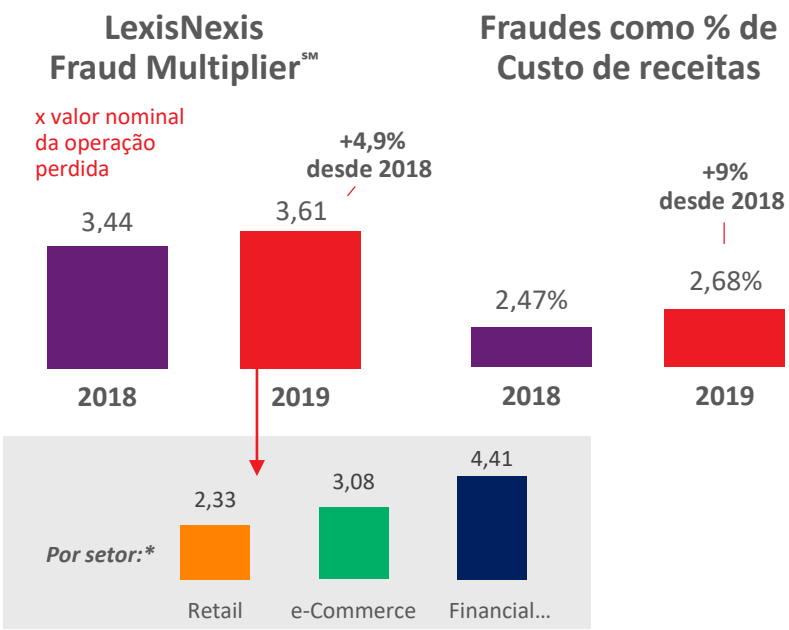


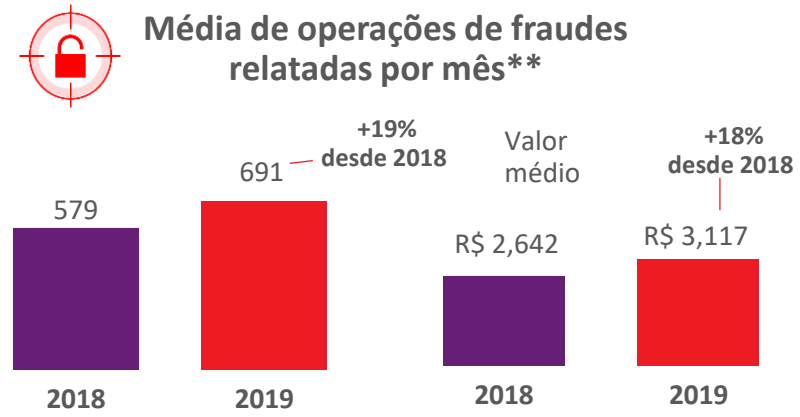
LexisNexis®
RISK SOLUTIONS

O LexisNexis Fraud Multiplier℠ apresenta tendência de alta de 3,61% desde o ano passado para as empresas de varejo, de comércio eletrônico e de serviços financeiros.

Brasil

- Isso quer dizer que para as empresas brasileiras atualmente, o custo de cada operação fraudulenta é 3,61 vezes o valor da operação perdida, o que resulta em custos de fraudes que somam, aproximadamente, 2,68% da receita anual geral.
- Os volumes e os custos de fraudes em nível de país continuam subindo, em parte, por causa do setor de serviços financeiros, onde os volumes e os custos são mais altos.* E, embora sem comprovação (devido ao tamanho pequeno da base), o custo das fraudes para os serviços financeiros permanece direcionalmente mais alto no Brasil (4,41 vezes o valor nominal da operação perdida) do que nos Estados Unidos (3,25 vezes). *As operações de serviços financeiros na América do Sul são **as mais prováveis** de serem atacadas na região.* Isso mostra ainda a vulnerabilidade da região às fraudes, à medida que as ofertas online e móveis continuam evoluindo.[1]





*As empresas de serviços financeiros sofrem operações bem-sucedidas de fraude com 4x o volume e 6x o valor monetário das empresas de varejo e de comércio eletrônico**

[1] Relatório sobre crimes cibernéticos H2 2018 da ThreatMetrix (ThreatMetrix H2 2018 Cybercrime Report)

* ATENÇÃO: pequeno número de casos, os dados devem ser somente usados direcionalmente

** Baseado em números autodeclarados e provável recall; sem pretensão de ser exato; pode aumentar ou diminuir dependendo da sazonalidade

P16a: Considerando o prejuízo total por fraudes sofrido pela sua empresa, indique a distribuição de vários custos diretos de fraudes nos últimos 12 meses.
P10: Qual o valor aproximado do total de prejuízo por fraudes da sua empresa nos últimos 12 meses, como % da receita total?
P22/24: Em um mês normal, quantas operações fraudulentas, aproximadamente, são impedidas/concluídas com sucesso pela sua empresa?
P22/25: Qual o valor médio de tais operações?

LexisNexis® RISK SOLUTIONS

Fatores que contribuem para as fraudes no Brasil.


Brasil

Condições do mercado

- **O Brasil tem o maior e mais crescente mercado de comércio eletrônico na América Latina e altos níveis de fraudes continuam afetando esse setor:**
  - Espera-se que esse mercado continue aumentando consideravelmente, passado de 55 milhões a estimados 75 milhões de clientes em 2022. Um fator que complica essa evolução é que o Brasil apresenta uma das maiores taxas de atividades fraudulentas no comércio eletrônico no mundo.[2]
  - O número de operações do comércio móvel está em ascensão. Durante o 1T 2019, os dispositivos móveis foram responsáveis por 35% de todas as operações.
  - O prejuízo nacional total de quase R$ 70 bilhões (US$ 18.6 bilhões) é atribuído a fraudes e golpes online.[4]
- **Barreiras para proteger formas de pagamento;** população não bancarizada considerável, o que exige que os comerciantes atraiam esses consumidores com formas alternativas de pagamento e dispositivos móveis que nem sempre são seguros.
- **Entre os 5 principais mercados de onde ataques cibernéticos são originados.[5]**

Riscos de operações

- À medida em que as operações de comércio eletrônico e comércio móvel aumentam, **os canais onde essas compras online/móveis acontecem são**, cada vez mais, alvos de fraudadores e mais arriscados/menos seguros.
- O **uso intenso de navegadores e aplicativos para dispositivos móveis também aumenta o risco** para quem vende produtos e serviços digitais.
- Entre as empresas de comércio eletrônico, de varejo e de serviços financeiros, **existe a necessidade de identificação de fraudes e verificação de identidade em tempo real** nas compras via navegadores e aplicativos para dispositivos móveis, devido à velocidade e à natureza das operações (ex.: downloads rápidos, sem endereço de entrega para dar suporte à verificação).
- **O uso de soluções de mitigação de risco** que tratam especificamente de **riscos de produtos/serviços móveis está aumentando, mas ainda é limitado**.

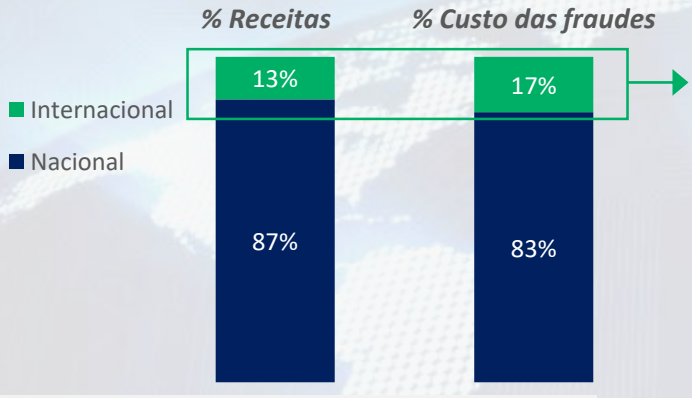
LexisNexis® RISK SOLUTIONS

[2]https://www.digitalriver.com/5-things-know-selling-brazil/
[3]https://www.pagbrasil.com/news/brazilian-e-commerce-grows/
[4] https://securityintelligence.com/easy-does-it-a-timely-look-into-fraud-ttps-in-the-brazilian-financial-cybercrime-landscape/
[5] Relatório sobre crimes cibernéticos H2 2018 da ThreatMetrix (ThreatMetrix H2 2018 Cybercrime Report)

Grandes prejuízos de receitas e por fraudes são provenientes de operações baseadas no Brasil.

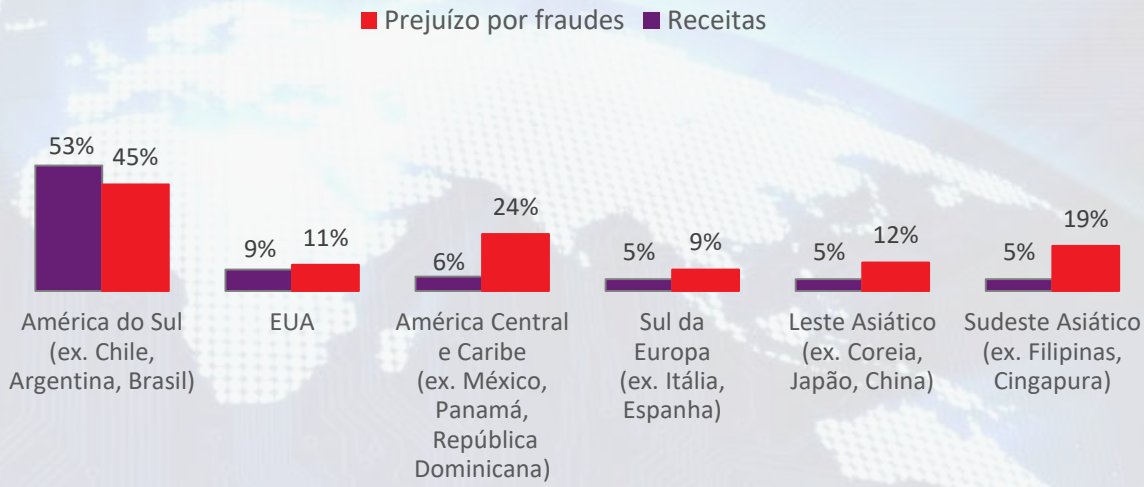
- Quando as fraudes não são brasileiras, quase metade origina-se em outros mercados sul-americanos. Outros prejuízos por fraudes estão bem espalhados pelas regiões.
- Há um grau desproporcional de fraudes vindas da América Central e do Caribe em comparação às receitas geradas nessas regiões. Isso vai em linha com uma tendência crescente de dispersão de ataques, onde os atacantes estão começando a ter como alvo mercados fora de sua região.[6]

Nacional vs. Internacional...



		% Receitas	% Custo das fraudes
2018	Internacional	12%	10%
	Nacional	88%	90%

% Distribuição internacional por localização



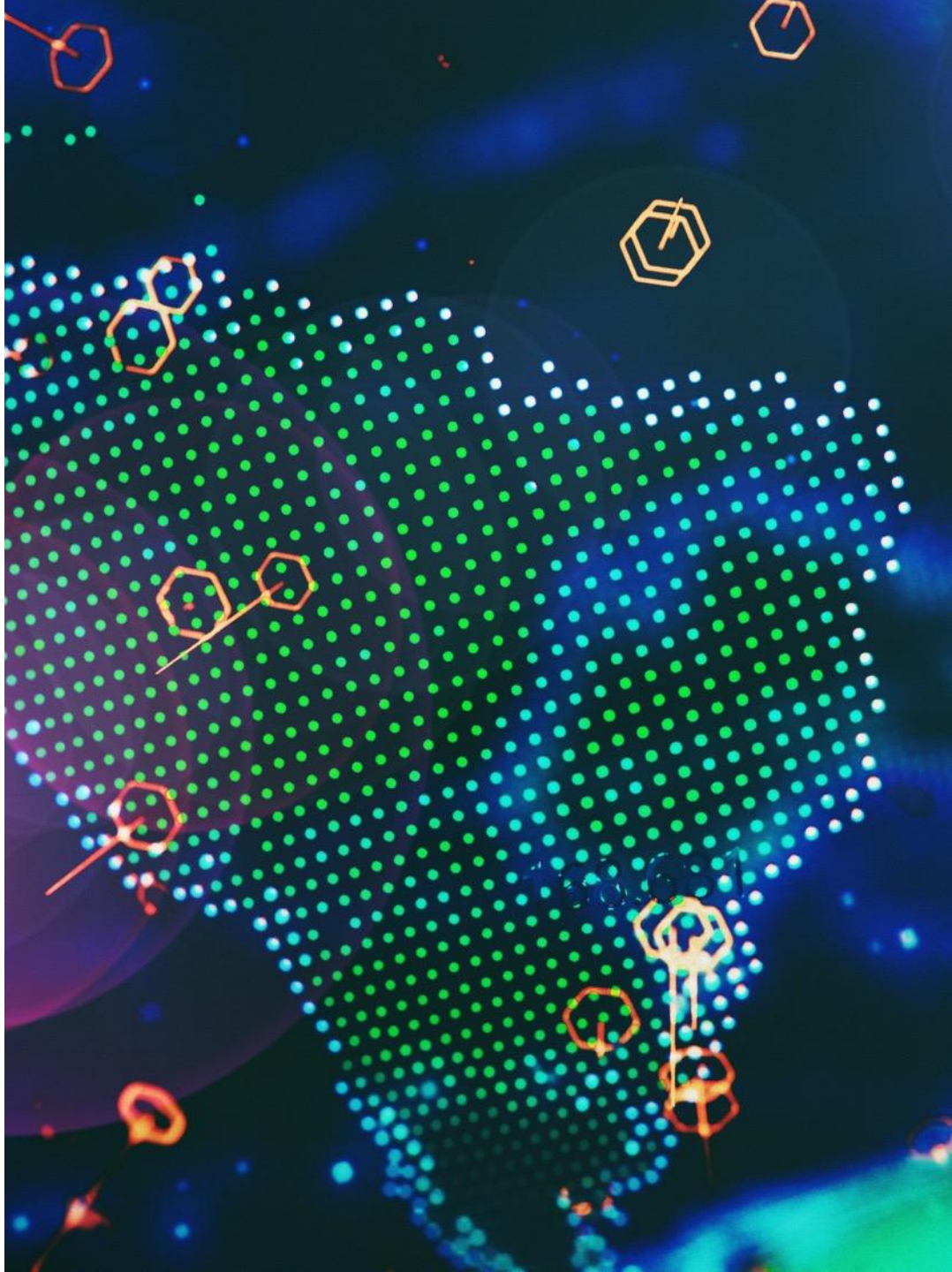
LexisNexis® RISK SOLUTIONS

[6] Ibid.

P9/13: Indique a taxa da receita/custo anual das fraudes gerada/o em operações nacionais em comparação às internacionais nos últimos 12 meses.
P9b/14c: Distribua 100 pontos entre os itens a seguir indicando a parcela que cada região representa das suas receitas de operações internacionais/custo das fraudes internacionais.

2

Os canais móveis continuam contribuindo com o risco de fraudes.

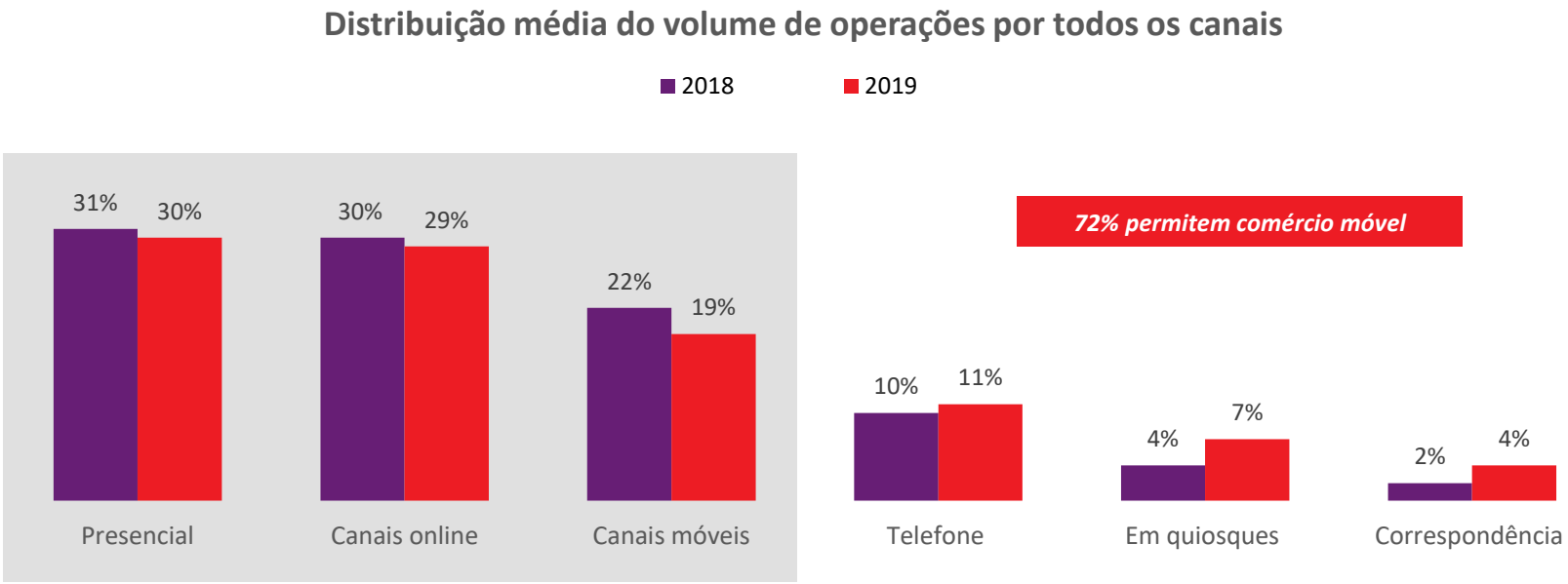


LexisNexis®
RISK SOLUTIONS

A maior parte das operações de varejo, comércio eletrônico e serviços financeiros continua passando pelos canais presenciais e online, seguidos pelos canais móveis.

Brasil

Apesar do volume de operações nos canais móveis ser menor do que o nos canais online e presenciais, compras realizadas em dispositivos móveis apresentaram crescimento de 43% no primeiro semestre de 2019, alcançando R$ 9.6 bilhões. E, em junho, mais de 43% de todas as compras online foram realizadas em dispositivos móveis, principalmente smartphones.[7]



LexisNexis® RISK SOLUTIONS

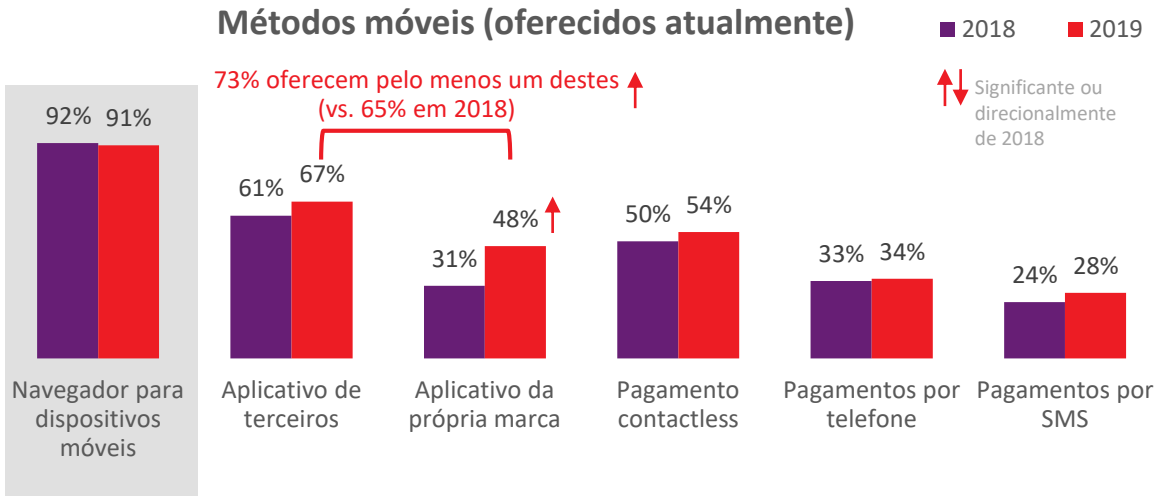
[7] https://www.bnamericas.com/en/features/bit-by-bit-the-outlook-for-e-commerce-in-brazil

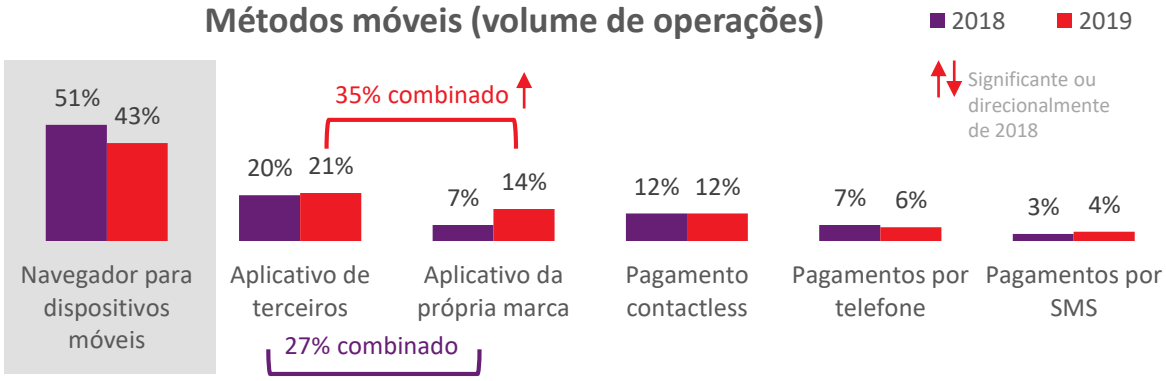
P2: Indique a taxa de operações concluídas (nos últimos 12 meses) para cada um dos seguintes canais usados pela sua empresa.

Embora a maioria das operações em canais móveis continuam sendo realizadas em navegadores de internet e aplicativos para dispositivos móveis de terceiros, o volume através de aplicativos da marca tem aumentado, à medida que mais empresas oferecem os seus próprios apps em comparação a 2018.

Brasil

- Isso continua aumentando o risco de fraude. Os navegadores para dispositivos móveis nem sempre são seguros, caso não tenham certos recursos de segurança geralmente encontrados em navegadores de desktop.
- Cada vez mais, os fraudadores focam nos aplicativos para dispositivos móveis no mundo todo, impulsionados, em parte, pela inundação de cliques e ataques de botnets, sendo compras, jogos e aplicativos financeiros os mais atingidos. Botnets atacam os dispositivos através de malwares, possibilitando que imitem operações legítimas originadas em um aplicativo para dispositivos móveis. É possível que os donos dos dispositivos nem estejam cientes do ocorrido.
- Além disso, a taxa de ataques a dispositivos móveis na América do Sul é uma das mais altas de todas as regiões.[9]





LexisNexis® RISK SOLUTIONS

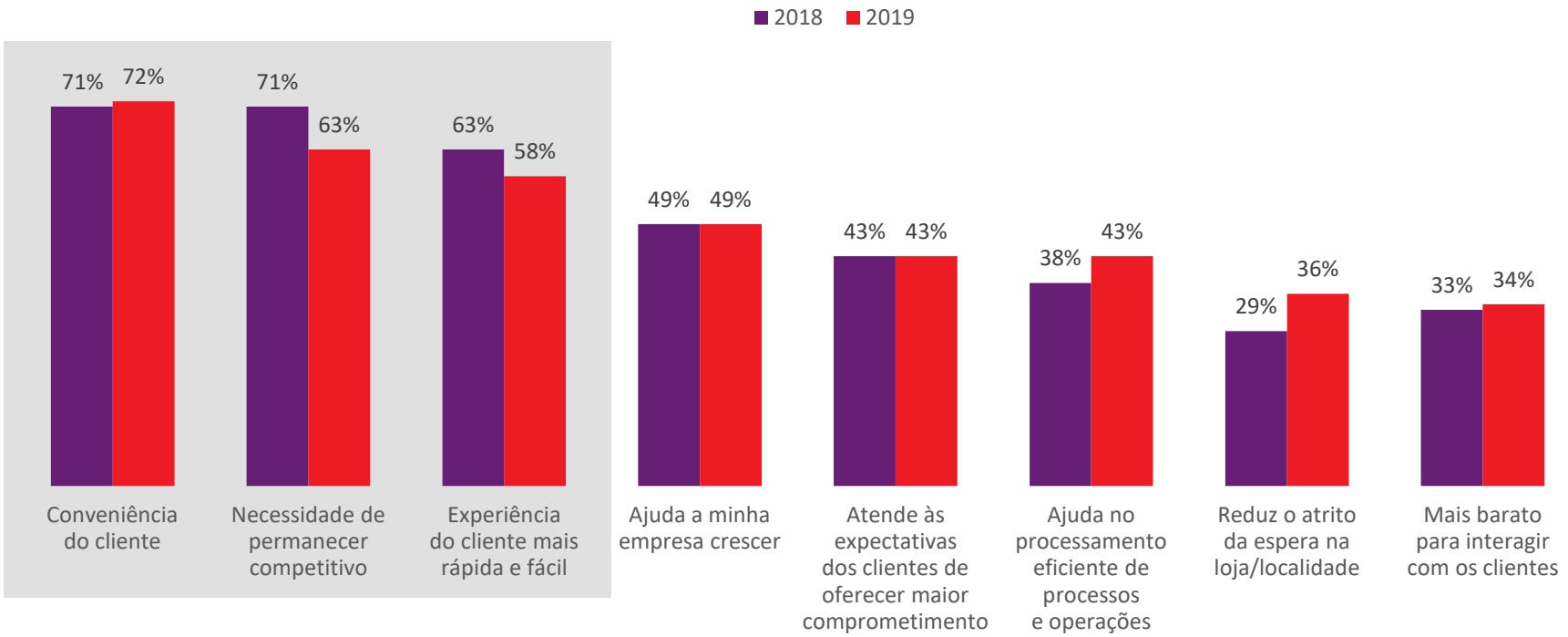
[8] https://www.appsflyer.com/resources/the-state-of-mobile-fraud-q1-2018/
[9] Relatório sobree crimes cibernéticos H2 2018 da ThreatMetrix (ThreatMetrix H2 2018 Cybercrime Report)
P4: Como é a distribuição das operações em cada um dos canais móveis que a sua empresa utiliza/aceita?

O risco dos canais móveis continua sendo uma contrapartida aceita em nome da conveniência/experiência otimizada do cliente e para permanecer competitivo.

Brasil

Razões para aceitar operações móveis

(Entre os que realizam operações em canais móveis)



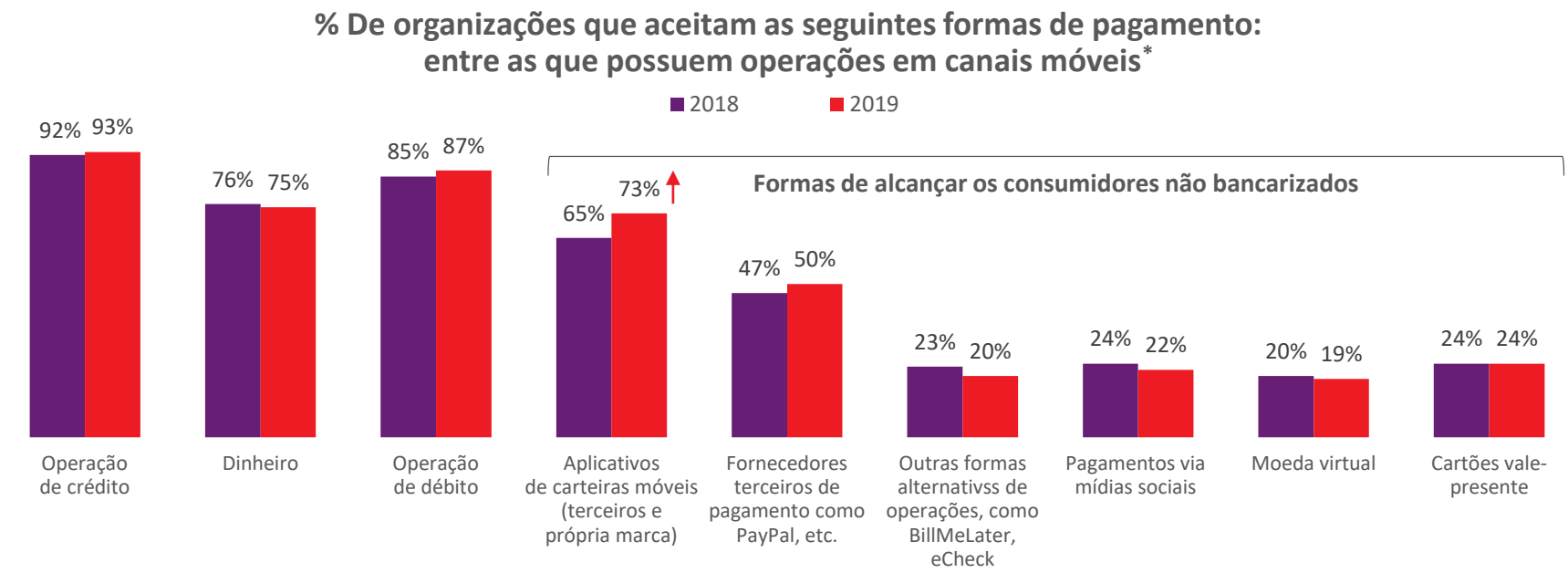
LexisNexis® RISK SOLUTIONS

P5: Quais os motivos que levaram a sue empresa a começar a aceitar abertura de contas e operações em dispositivos móveis?

Formas de pagamento tradicionais continuam bem aceitas (cartão de crédito, de débito, dinheiro), mas como mencionado, os aplicativos para dispositivos móveis estão em ascensão. Essas e outras formas alternativas de pagamento continuam acrescentando risco à medida que as empresas se esforçam para alcançar clientes não bancarizados.

Brasil

Estima-se que 55 milhões de pessoas ainda não possuem conta bancária no Brasil, mas muitas delas têm telefone celular. Por esse motivo, pagamentos móveis são a principal alternativa para os não bancarizados. Soluções como cartões pré-pagos, o PagBrasil e o PEC Flash® da PagBrasil contribuem para a inclusão desses consumidores no país. Optar por não usar o sistema bancário tradicional não é apenas viável, mas tornou-se uma tendência. A população não bancarizada está impulsionando a criação de novas soluções e os fornecedores de serviços financeiros estão focados em abolir as barreiras da inclusão financeira. Atualmente, há 377 fintechs no país e até 25% delas se dedicam a fornecer soluções inovadoras de pagamento.



Significante ou direcionalmente de 2018

* Não é necessariamente usado em operações em canais móveis, já que comerciantes e empresas são multicanais.

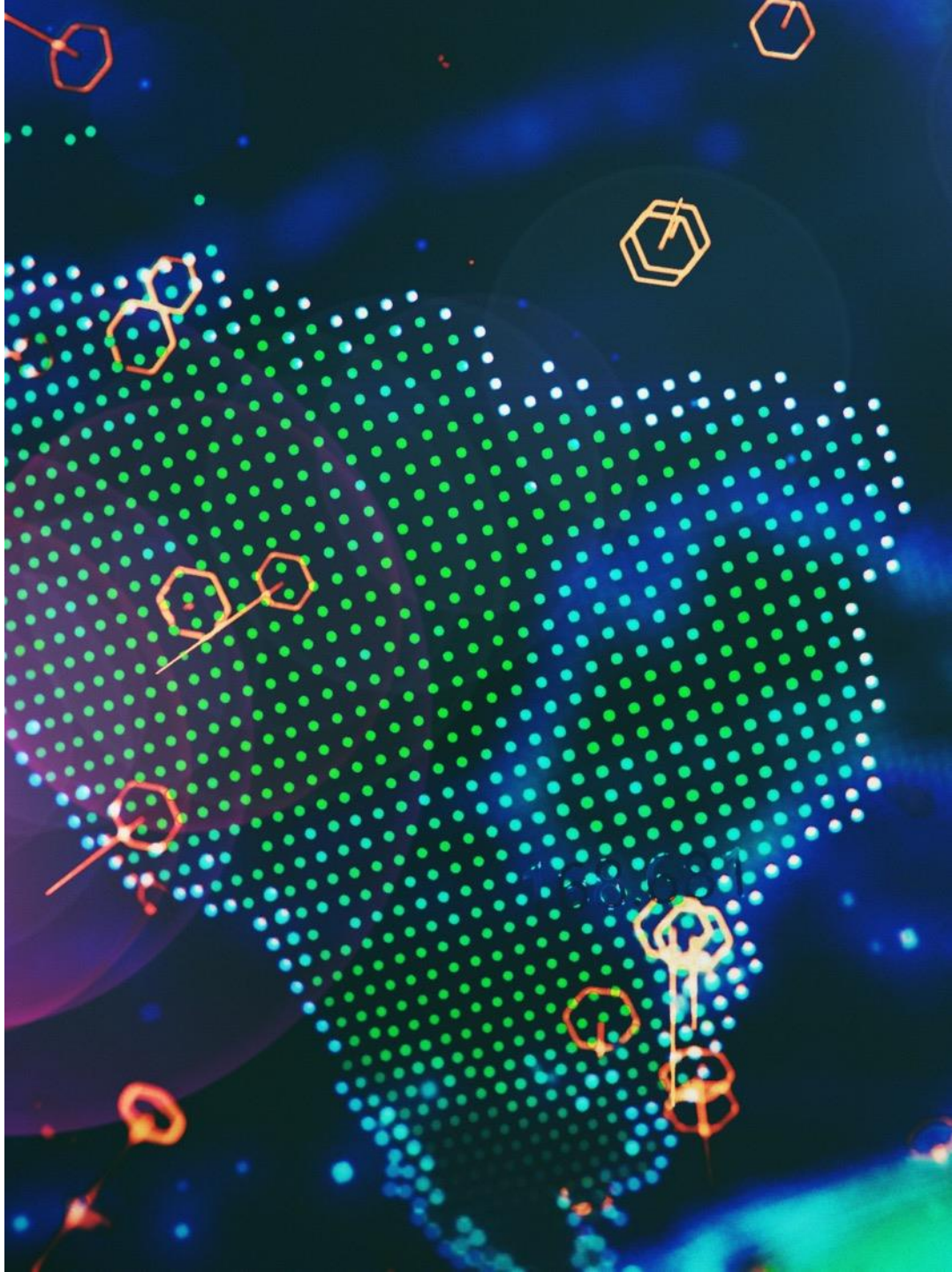
[10] https://www.pagbrasil.com/insights/unbanked-become-trendsetters

P3: Indique a taxa de cada forma aceita pela sua empresa/usada para financiar operações ou desembolsar fundos (nos últimos 12 meses).

LexisNexis® RISK SOLUTIONS

3

A verificação da identidade do cliente é uma questão fundamental tanto para canais online como móveis.

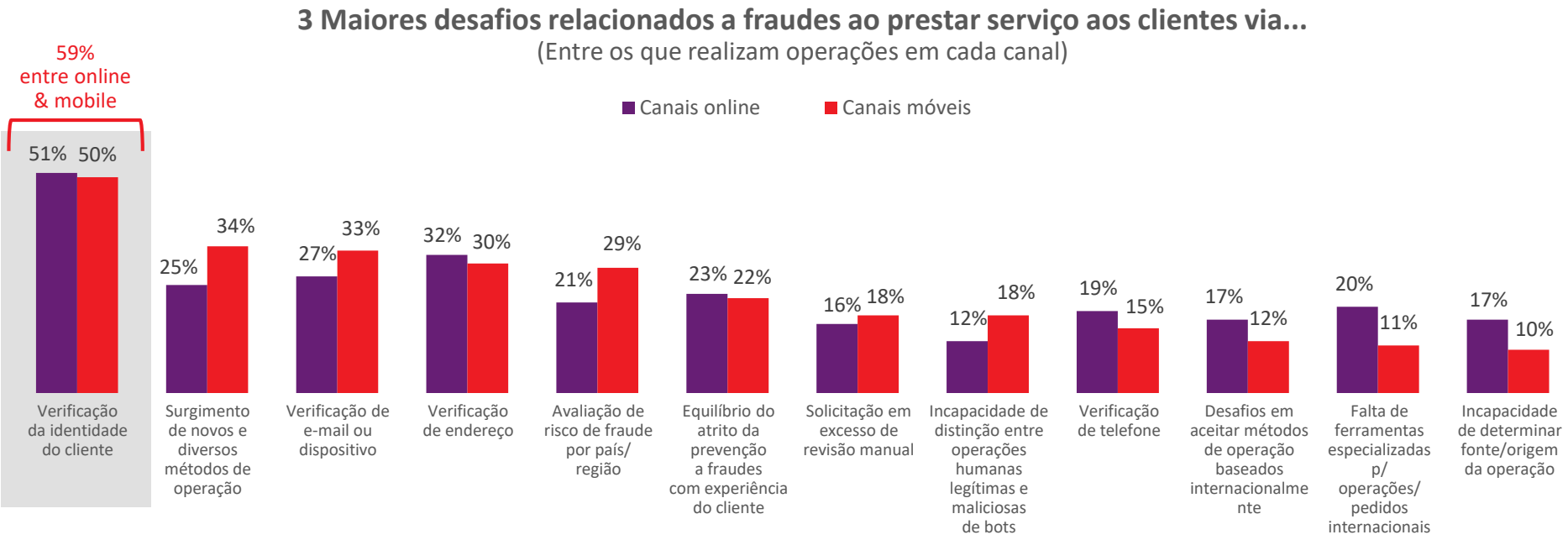


LexisNexis®
RISK SOLUTIONS

A verificação de identidade do cliente é o principal desafio quando serviços são oferecidos por meio de canais online e móveis aos clientes.

Brasil

- Spoofing de identidade continua sendo o vetor de ataque de maior prevalência na região da América Latina, especialmente para o setor de serviços financeiros.[11]
- O surgimento de novos e variados métodos de operações, a análise de risco por país/região e a incapacidade de distinguir entre operações humanas legítimas e maliciosas de bots são um pouco mais desafiantes para os canais móveis.



LexisNexis® RISK SOLUTIONS

[11] Relatório sobre crimes cibernéticos Q2 2018 da ThreatMetrix (ThreatMetrix H2 2018 Cybercrime Report)

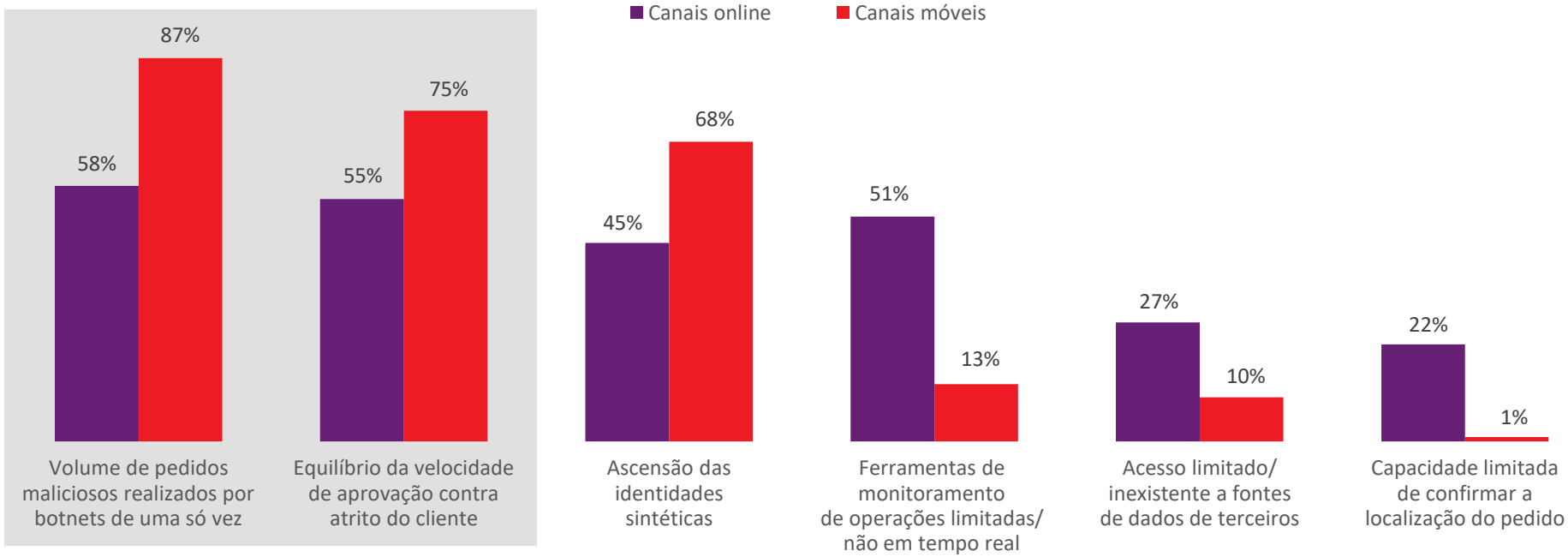
P20: Classifique os 3 principais desafios relacionados a fraudes ao fornecer serviço a clientes em canais móveis/online:

O volume de pedidos maliciosos de botnets realizados de uma só vez, combinado ao equilíbrio da velocidade de aprovação contra atrito no cliente causa estragos nos processos de verificação de identidade, especialmente em operações realizadas por dispositivos móveis.

Brasil

A ascensão de identidades sintéticas também é problemática para os canais móveis. Ferramentas de monitoramento de operações limitadas/não em tempo real é uma questão mais para os canais online.

3 Principais fatores que fazem com que a verificação de identidade do cliente seja um desafio via...
(Entre os que realizam operações em cada canal)



LexisNexis® RISK SOLUTIONS

P20c/d: Classifique os 3 principais fatores que fazem com que a verificação de identidade do cliente seja um desafio ao fornecer serviço a clientes em canais móveis/online:

As identidades sintéticas representam uma séria ameaça. A sua própria natureza faz com que seja muito difícil identificá-las antes que causem danos.

Brasil

As identidades sintéticas são formadas por informações pessoais reais e/ou falsas. Elas são criadas usando informações de:

Diversas pessoas reais compiladas em uma única identidade falsa, com um endereço de entrega válido, número de CPF/seguro/identidade, data de nascimento, nome, etc. – sendo que nenhuma dessas informações corresponde a uma única pessoa. Esse método pode ser usado para ganhos no curto prazo, como itens mais caros.

Uma pessoa real utilizando algumas de suas informações combinadas a dados falsos. Neste caso, é provável que o fraudador esteja alimentando essa identidade, usando-a para estabelecer um bom histórico de crédito, antes de “ir para o mal caminho”.

Nenhuma pessoa conhecida quando as informações de identificação pessoal não pertencem a nenhum consumidor, são totalmente inventadas e podem ser alimentadas para ganhos a longo prazo, além de úteis para se passarem por consumidor com acesso limitado aos serviços bancários, com uma pegada de consumo menos estabelecida (ex.: milenials mais jovens).

Riscos e desafios

Distinção extremamente difícil de clientes legítimos

Foco em nutrir a identidade para imitar um bom cliente: estabelece bom crédito, paga em dia, etc. antes de "ir para o mal caminho".

Difícil identificação com as soluções tradicionais de verificação/autenticação de identidade

Fraudadores profissionais que costumam conhecer os tipos de informações necessárias para conseguir aprovação e passar por certos pontos de verificação. O uso de dados verdadeiros de identidade os ajuda a fazer isso.

Os clientes reais não ajudam, pois o seu comportamento dificulta a detecção de anomalias com as atuais soluções de identidade

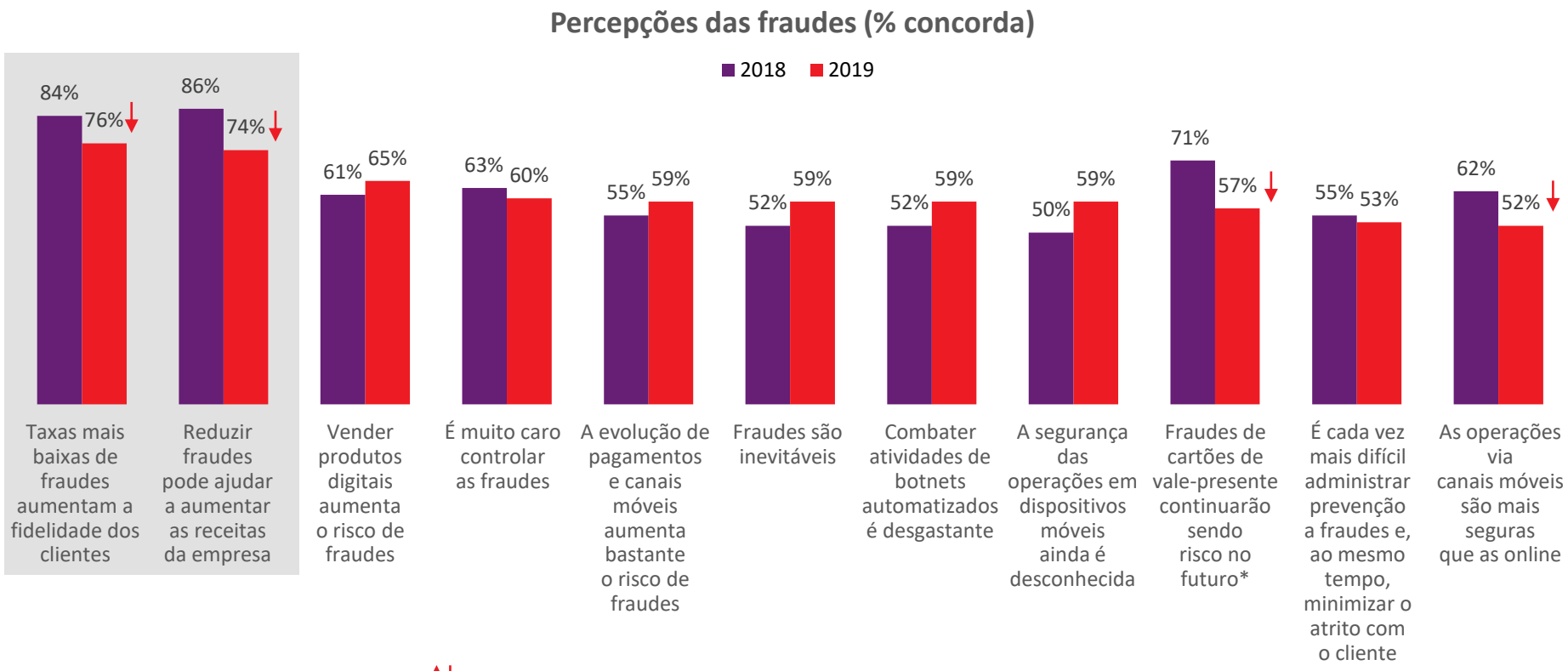
Os clientes têm várias formas de consumir, de diferentes localidades, a qualquer hora e em qualquer lugar, podendo compartilhar senhas e utilizar dispositivos diferentes em momentos distintos. É mais difícil realizar conexões físicas e digitais que distingam padrões fraudulentos de legítimos.

LexisNexis® RISK SOLUTIONS

A maioria dos comerciantes e das empresas de serviços financeiros brasileiros continuam acreditando que baixar as taxas de fraudes pode aumentar a fidelidade dos clientes e as receitas.

Brasil

Mas para que isso aconteça, as empresas ainda precisam adotar soluções eficazes de mitigação de fraude. Isso é especialmente importante dado o reconhecimento constante de que produtos e canais digitais aumentam o risco de fraudes e que o seu gerenciamento é desgastante.



Significante ou direcionalmente de 2018

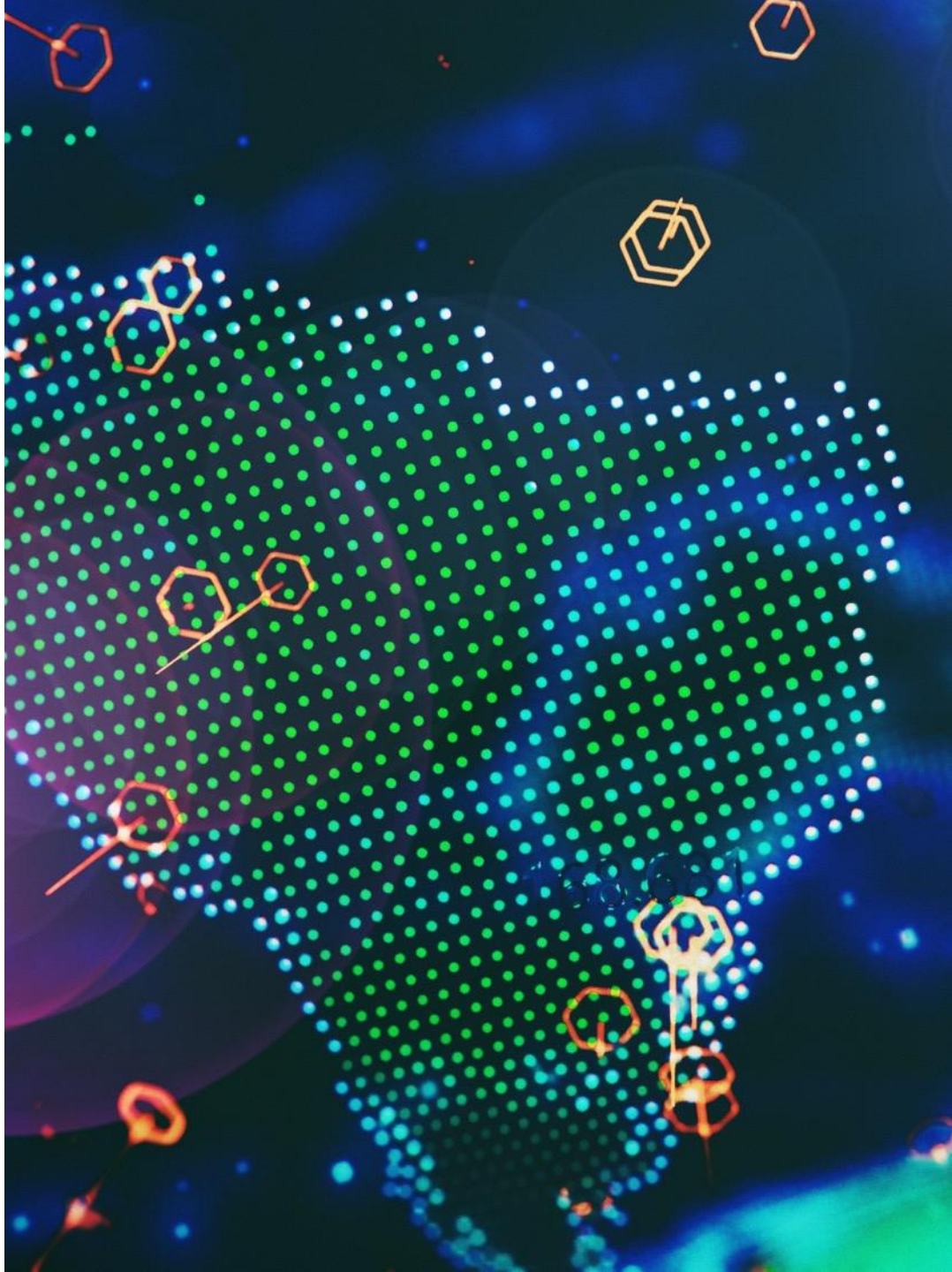
*Pergunta feita somente para varejo/comércio eletrônico que vende produtos digitais.

P33: Em uma escada de 1 a 5, onde "5" é "concordo completamente" e "1" é "não concordo nada", classifique o quanto você concorda ou discorda com as afirmações abaixo.

LexisNexis® RISK SOLUTIONS

4

O custo das fraudes continua mais alto para quem oferece comércio móvel.



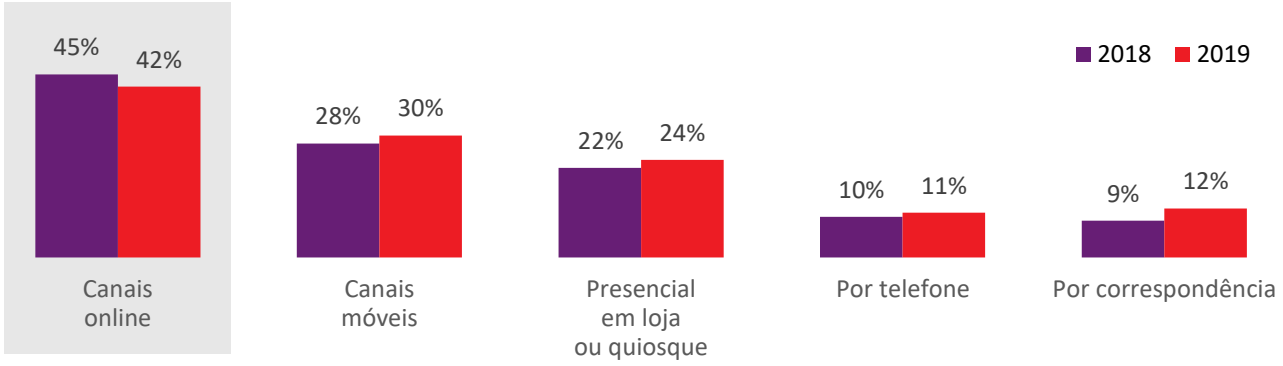
LexisNexis®
RISK SOLUTIONS

As fraudes permanecem mais prevalentes nos canais online, seguidos dos canais móveis.

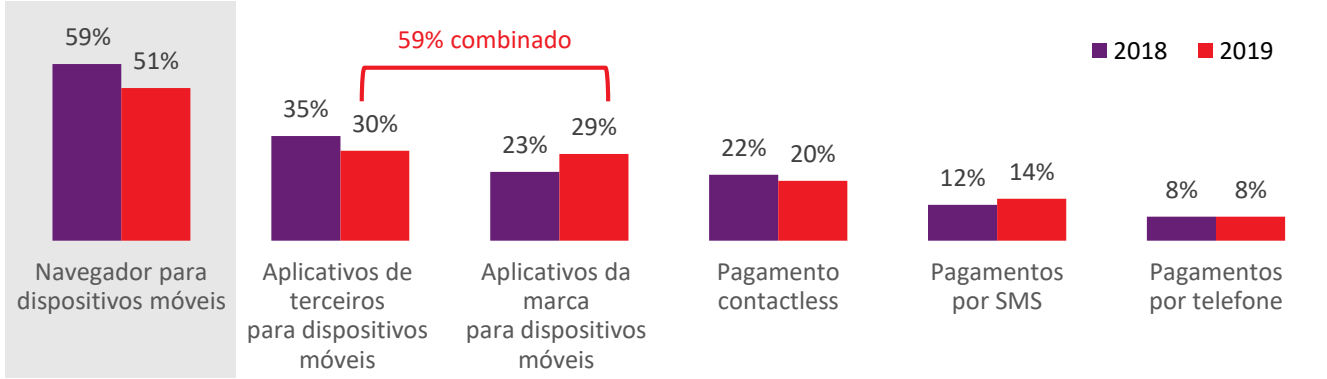
Brasil

- Os aplicativos para dispositivos móveis (da marca e de terceiros) continuam contribuindo para os prejuízos por fraudes tanto quanto os navegadores para dispositivos móveis.
- Os ataques aos apps podem ser de botnets móveis e de inundação de cliques atacando através de malwares e obtendo acesso/controle das operações em dispositivos móveis.

% De fraudes por canal de operação ***(Como % do prejuízo anual total por fraudes)****



Fraudes em dispositivos móveis por canal ***(Como % do prejuízo por fraudes em dispositivos móveis)****



LexisNexis® RISK SOLUTIONS

*% Pode somar mais de 100% já que as respostas são baseadas em uso do canal.
P15: Indique a taxa de custo das fraudes gerada por meio de cada uma das seguintes canais de operação atualmente usados pela sua empresa (como porcentagem do prejuízo anual total por fraudes).
P17: Indique a distribuição das fraudes pelos diversos canais móveis que você utiliza/aceita.

Fraudes de identidades (roubo de identidade de terceiros/fraudes de identidade sintética) somam quase 1/3 dos prejuízos por fraudes.

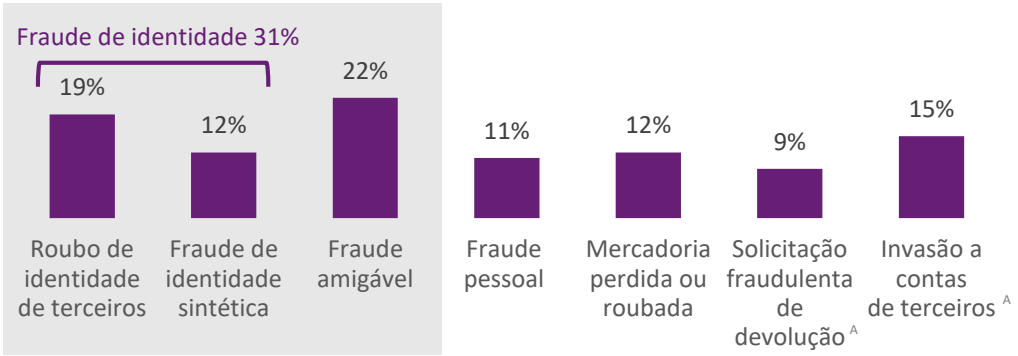
- Fraudes por invasão a contas e por criações de contas fraudulentas representam muito mais fraudes baseadas em identidade do que as provenientes de compras ou operações.
- Operações de criação de novas contas na América do Sul, principalmente relacionadas às de comércio eletrônico, são atacadas à altíssima taxa de 33%.

[A]Pergunta feita somente para varejo/comércio eletrônico.
[B]Pergunta feita somente para serviços financeiros.

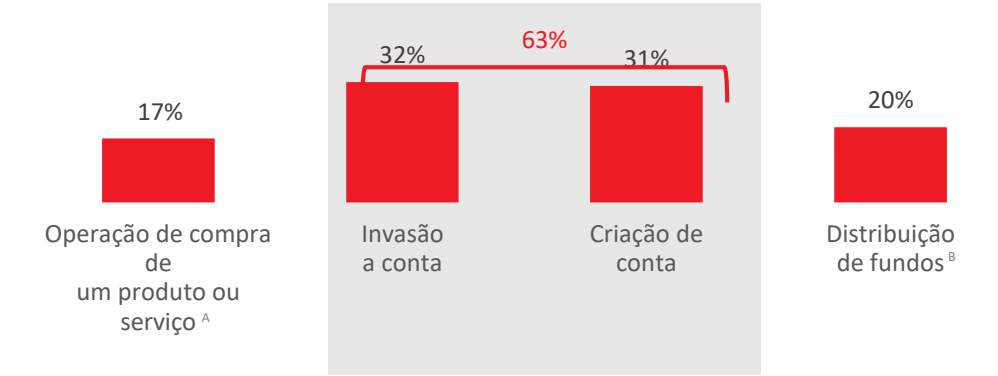
[12] Ibid.

Brasil

% Distribuição do prejuízo por fraudes por método



Tipos de fraudes relacionadas a identidades



P12: De acordo com o seu conhecimento, indique a taxa de distribuição dos métodos de fraude abaixo, já que são atribuídas ao prejuízo anual total por fraudes nos últimos 12 meses.
- Fraudes amigáveis (indivíduo associado a/que tem acesso a uma conta e que realiza operações sem o conhecimento ou permissão do titular desta conta).
- Fraude pessoal (titular ou usuário autorizado da conta cometem a fraude).
- Fraudes de identidade de terceiros (operações não autorizadas usando informações reais/existentes de outras pessoas).
- Fraudes de identidade sintética (criação de uma nova identidade combinando informações reais e fabricadas, às vezes completamente fictícias).

P12b: Qual a distribuição de fraudes relacionadas a identidades de acordo com as seguintes atividades:

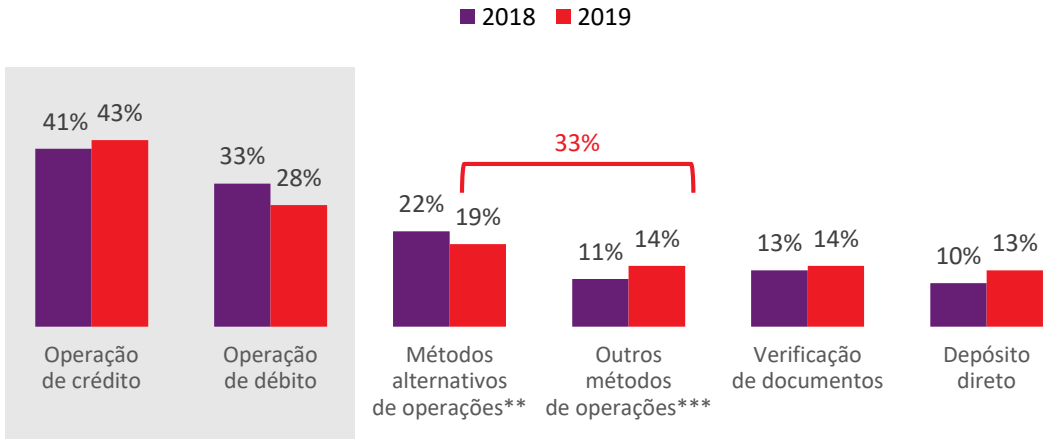
LexisNexis® RISK SOLUTIONS

Enquanto crédito e débito permanecem os principais métodos de operações fraudulentas, prejuízos atribuídos a métodos alternativos/outros (inclusive opções de pagamento online/móveis) representam quase o mesmo volume.

O Brasil tem a maior economia da América Latina, mas enfrenta uma grande desigualdade social. Por conta disso, é muito comum que as pessoas sejam criativas para tentar cobrir suas despesas. Além disso, o país apresenta altos índices de criminalidade, o que é diretamente refletido no setor de comércio eletrônico. Parte disso se da porque os cartões de crédito e de débito são sempre emitidos com a tecnologia EMV. Graças às exigências de inserção da senha para completar a operação de pagamento, as chances de fraudes físicas foram reduzidas. Como resultado, os fraudadores migraram para o ambiente de comércio eletrônico e fraudes de CNP (cartão não presente).

Brasil

Fraudes por método de operação
*(Como % do prejuízo anual total por fraudes)**

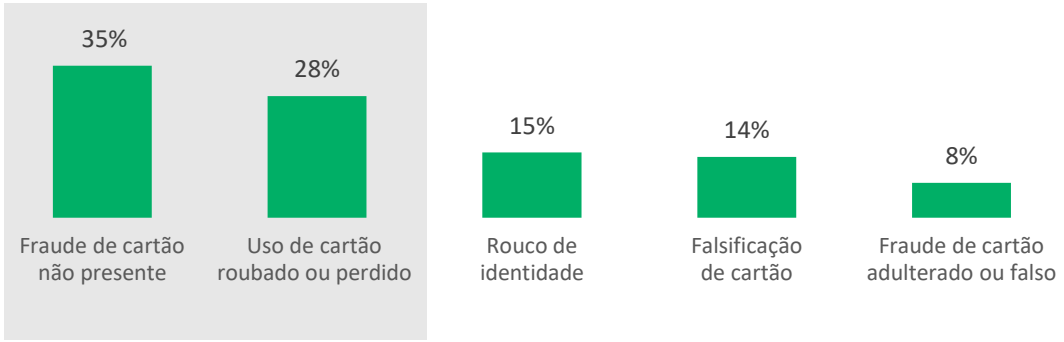


*% Pode somar mais de 100% já que as respostas são baseadas em uso do canal.

***Métodos alternativos de operações incluem PayPal, BillMeLater, eCheck*

****Outros métodos de operações incluem dinheiro, carteiras para dispositivos móveis, vale-presentes*

Prejuízo por fraudes relacionados a cartão



[13] https://www.pagbrasil.com/news/brazilian-e-commerce-grows/

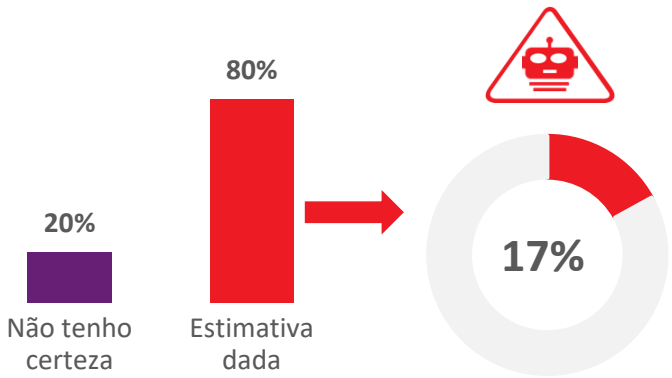
P18: Indique a taxa de distribuição dos métodos de pagamento usados para cometer fraudes contra a sua empresa.
P18e: com relação ao prejuízo por fraudes relacionado a cartão de crédito e de débito, indique a distribuição nos seguintes tipos de fraude de cartão.

Quase metade das empresas relataram crescimento na atividade de botnets automatizados no último ano, estimado em 16%.

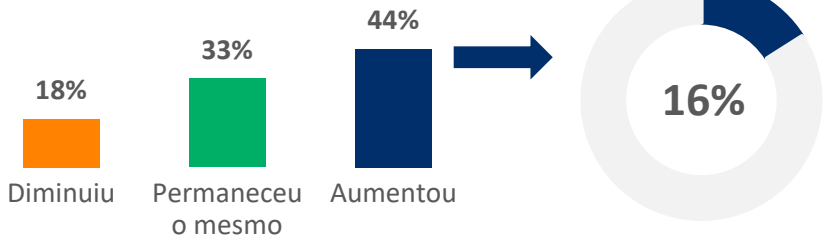
Brasil

Atualmente, o Brasil ocupa a 6ª posição entre os 10 piores países no mundo quando o assunto é botnet.[14] No começo deste ano, observou-se malwares roubando informações de máquina e credenciais de usuários, procurando por cadeias relacionadas a três bancos brasileiros específicos (Banco Bradesco, Banco do Brasil e Sicredi) e outras possíveis conexões de rede através de contatos salvos no Outlook. Além de acessar as contas bancárias dos usuários, as informações pessoalmente identificáveis (PII) coletadas dos sites visitados e as credenciais registradas de máquinas podem ser mais usadas ou vendidas. Além disso, considerando a ampla base de serviços financeiros e clientes desses três bancos, existe a possibilidade de poderem ser usados como alvo de ataques maiores de botnets ou de envio de correspondência em massa.

Atividade de botnet como % de operações por mês



Mudança em volume das atividades de botnet no último ano



[14] https://www.spamhaus.org/statistics/botnet-cc/
[15] https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/

B1a: Em um mês normal, qual a taxa das suas operações que é identificada como ataques de bots automatizados e maliciosos?
B1b/c: Como fica quando comparado ao mesmo período do ano passado? Você diria que a taxa de ataques de bots automatizados e maliciosos mensal tem:

LexisNexis® RISK SOLUTIONS

A combinação desses fatores contribui para aumentar o risco.

Brasil

Dispositivos Móveis

- **Ascensão da ataques de botnets a dispositivos móveis:** malware infecta dispositivos sem o conhecimento do consumidor; rouba a identidade, invade contas, realiza compras fraudulentas.[16]
- **Comportamentos de risco do consumidor:** o uso de redes de WiFi abertas aumenta o risco de smishing (phishing baseado em SMS) e man-in-the-middle interceptarem senhas usadas para autenticação multifator[17]; hábitos como "mantenha-me conectado" tornam-se um ponto de entrada desbloqueado para contas.
- **Maior conjunto de oportunidades para fraudadores** à medida em que mais pessoas realizam operações em dispositivos móveis.

Além de fronteiras

- **Incertezas, pontos cegos e novas formas de pagamento:** torna-se difícil determinar a origem das operações; falta da dados verificáveis sobre clientes (principalmente com o Regulamento Geral sobre a Proteção de Dados).

Digital

- **Operações rápidas:** produtos/serviços digitais, como downloads e assinaturas, tendem a acontecer com rapidez; a não necessidade de endereço físico para entrega elimina o período de segurança para verificação contra fraudes antes do envio; temendo o abandono, os comerciantes lutam para equilibrar a prevenção a fraudes e minimizar o atrito com o cliente.
- **Alvos fáceis:** identidades sintéticas e dados roubados dificultam a distinção entre ataques maliciosos e clientes legítimos no canal anônimo.
- **Alvo favorito para testes de cartão fraudado:** uso de bots para testar informações de cartão de crédito roubado com produtos/serviços de baixo valor (típico de produtos/serviços digitais) costumam levantar menos suspeitas.

LexisNexis® RISK SOLUTIONS

[21] Threat Metrix Q2 2018 Cybercrime Report
[22] 4 tendencias de fraude móvil para buscar en 2019; https://threatmetrix.com/digital-identity-blog/fraud-prevention/4-mobile-fraud-trends-look-out-for-2019

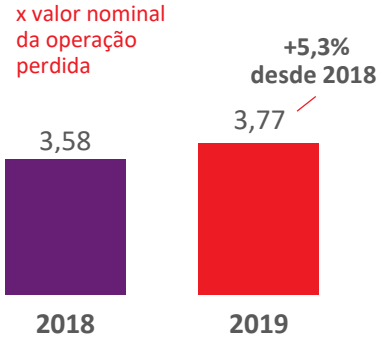
Isso continua resultando em maiores volumes e custo de fraudes para empresas que oferecem comércio móvel.

Brasil

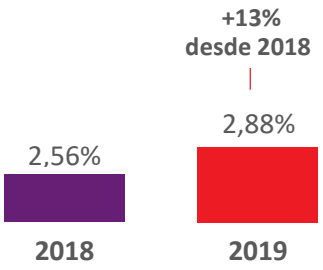
- Cada **operação fraudulenta** *custa, na verdade,* **3,77 vezes o valor da operação perdida** para as empresas de comércio móvel comparado à média (3,61) para empresas no geral. Os custos das fraudes como porcentagem das receitas também é mais alto entre os que possibilitam comércio móvel do que para as empresas no geral (2,88%).
- Além disso, o número de operações de fraudes bem-sucedidas e respectivos valores monetários associados apresentaram crescimento e continuam mais altos do que para as empresas no geral.

Entre as empresas que oferecem comércio móvel

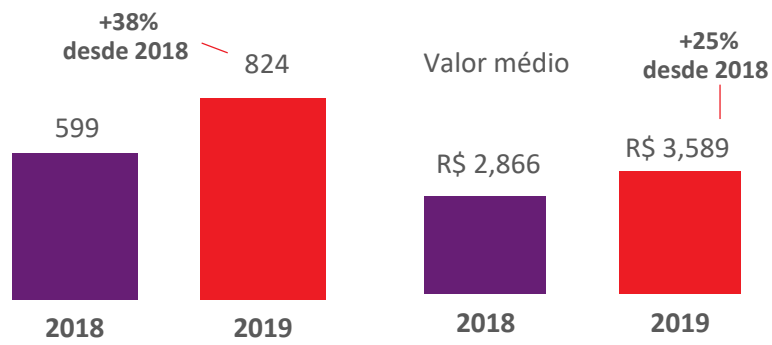
LexisNexis Fraud Multiplier℠



Fraudes como % de Custo de receitas



Média de operações fraudulentas relatas por mês*



LexisNexis® RISK SOLUTIONS

* Baseado em números autodeclarados e provável recall; sem pretensão de ser exato; pode aumentar ou diminuir dependendo da sazonalidade

P16a: Pensando no total de perdas por fraude sofridas pela sua empresa, mostre a distribuição de vários custos diretos de fraude nos últimos 12 meses.
P10: Qual o valor aproximado do total de perdas por fraude da sua empresa nos últimos 12 meses, como % da receita total?
P22/24: Em um mês normal, quantas operações fraudulentas, aproximadamente, são impedidas/concluídas com sucesso pela sua empresa?
P22/25: Qual o valor médio de tais operações?

Regionalmente, as empresas que são “digitais” continuam tendo maior risco e custos associados a fraudes, o que tende a se sobrepor ao comércio móvel.

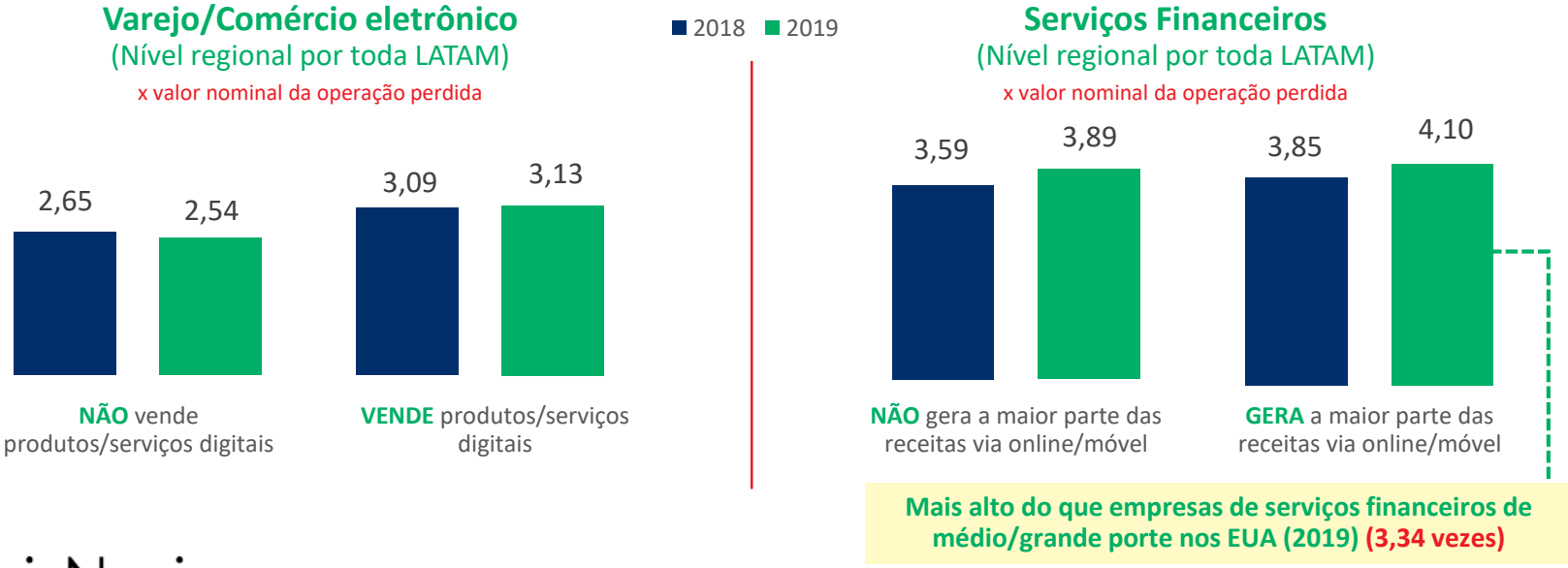
Achados Regionais

Para as empresas de varejo, comércio eletrônico e serviços financeiros, verificação de identidade é um desafio e um risco.

- Para o varejo e o comércio eletrônico, a questão é a velocidade e o tipo de operação. Produtos/serviços digitais envolvem mais imediatismo de distribuição/downloads. Enquanto os comerciantes que vendem mercadorias físicas contam com um endereço de entrega e um período de segurança entre a operação e o envio para confirmar a identidade e a legitimidade da venda, o mesmo não é válido para os que comercializam bens digitais. Existe uma necessidade em tempo real maior para os esforços de identificação de fraudes.
- Para as empresas de serviços financeiros, o anonimato do próprio canal dificulta muito mais a verificação de identidade.
- E, em todos os segmentos, dispositivos (computadores, tablets, telefones celulares) podem confundir coisas com spoofing e malwares.

Em todos os setores, os que são digital continuam sendo afetados com um custo maior de fraudes.

LexisNexis Fraud Multiplier℠



LexisNexis® RISK SOLUTIONS

P16a: Pensando no total do prejuízo por fraudes sofrido pela sua empresa, mostre a distribuição de vários custos diretos de fraude nos últimos 12 meses.

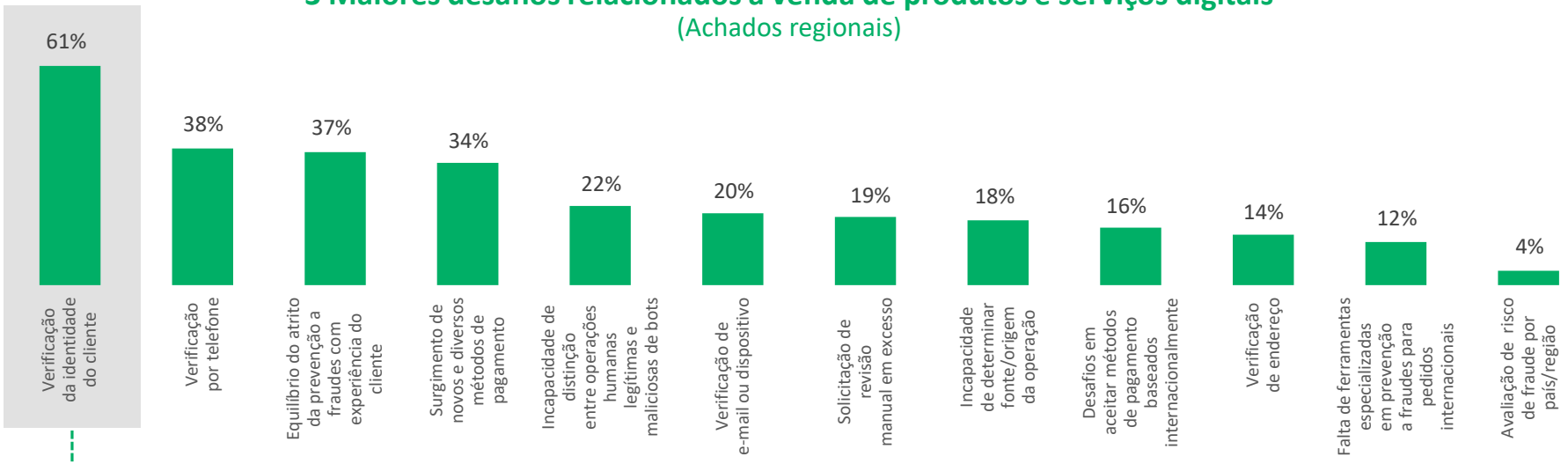
Regionalmente, administrar a verificação do risco levando em conta o atrito com o cliente é desafiador para o varejo/comércio eletrônico que vende produtos digitais, especialmente entre os que não possuem ferramentas de monitoramento de operações em tempo real e a capacidade de confirmar a origem da operação.

Achados Regionais

Isso é ainda agravado pela necessidade de realizar verificação por telefone, equilibrar os esforços de identificação de fraudes com o mínimo de atrito com o cliente e lidar com novos e diferentes métodos de pagamento. Para mais da metade, a ascensão das identidades sintéticas complica esse esforço.

3 Maiores desafios relacionados à venda de produtos e serviços digitais

(Achados regionais)



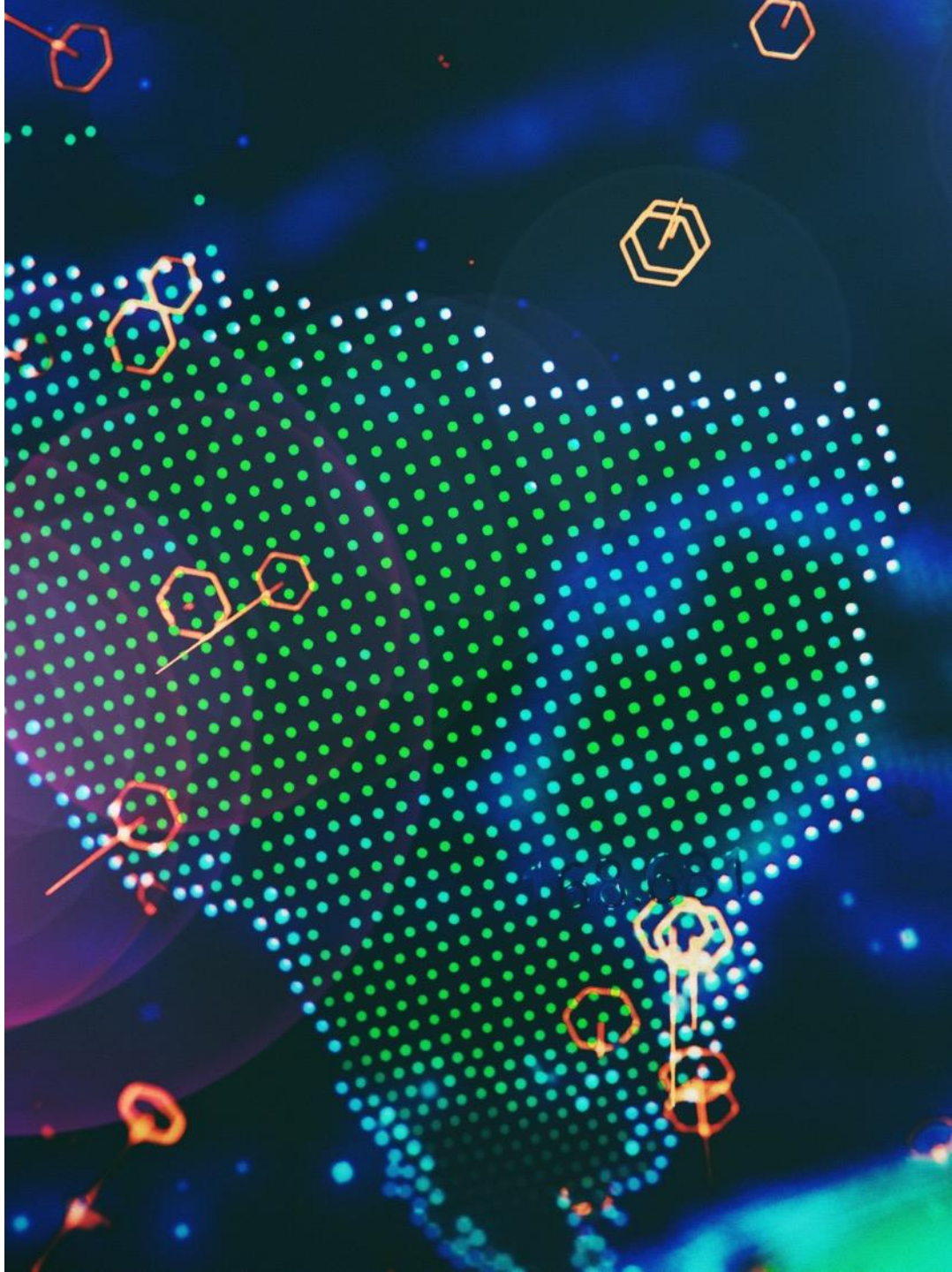
59% dos que classificaram verificação de identidade como um desafio a atribuem **à ascensão das identidades sintéticas**. Outros **46%** a atribuem às **ferramentas de monitoramento de operações limitadas/não em tempo real** e à **capacidade limitada para confirmar a localização do pedido (geográfica ou por dispositivo).**

LexisNexis® RISK SOLUTIONS

P19: Classifique os três principais desafios relacionados à fraude enfrentados pela sua empresa ao vender produtos digitais aos clientes.
P19_2: Classifique os 3 principais fatores que fazem com que a verificação de identidade do cliente seja um desafio quando se vende produtos digitais aos clientes.

5

As empresas ainda não combatem fraudes da melhor maneira.



LexisNexis®
RISK SOLUTIONS

Uma maioria declarou ainda monitorar os custo das fraudes por canal e forma de pagamento.

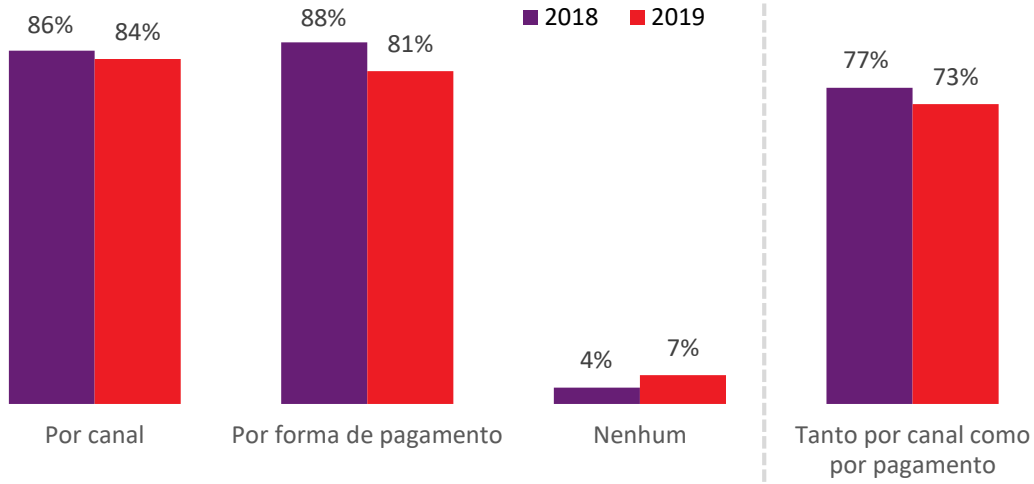
- Entretanto, poucas parecem monitorar operações de fraudes *bem-sucedidas* tanto por canal como por forma de pagamento.
- É importante monitorar fraudes bem sucedidas e prevenidas tanto por canal como por forma de pagamento para entender os pontos fracos. Os fraudadores continuarão testando esses métodos.

↑↓ Significante ou direcionalmente de 2018

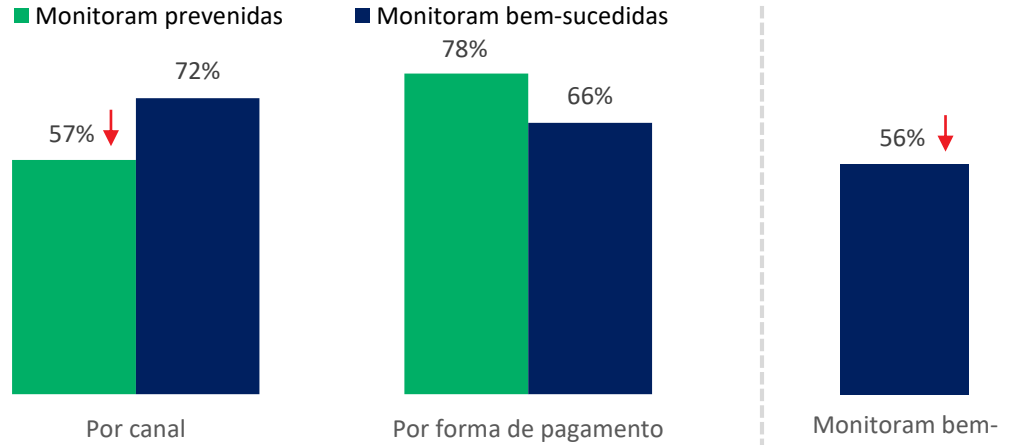
P14: A sua empresa monitora o custo de operações fraudulentas por canais e formas de pagamento?
P26: A sua empresa monitora fraudes bem-sucedidas por canais e formas de pagamento?

% Empresas monitorando custo das fraudes por canal e/ou forma de pagamento

Brasil



% Monitoram operações de fraudes BEM-SUCEDIDAS e/ou PREVENIDAS



2018	69%	78%	81%	74%

69%

LexisNexis® RISK SOLUTIONS

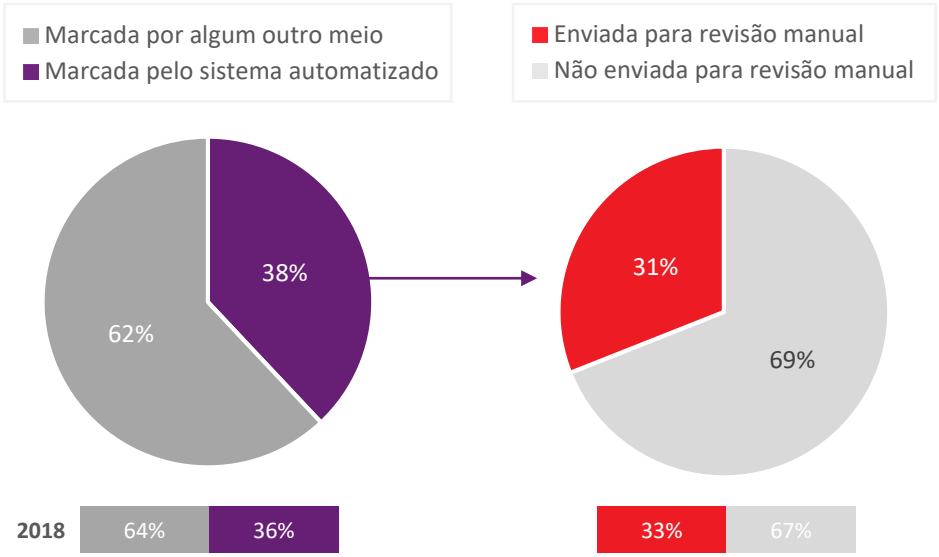
E, mesmo assim, menos de 4 em cada 10 operações são marcadas pelo sistema automatizado.

- E, entre as que são, quase ***1/3*** continua sendo enviada para revisão manual.
- Mesmo assim, o número de falsos positivos não tem diminuído, com **1/5** das operações rejeitadas ainda resultando de falsos positivos.

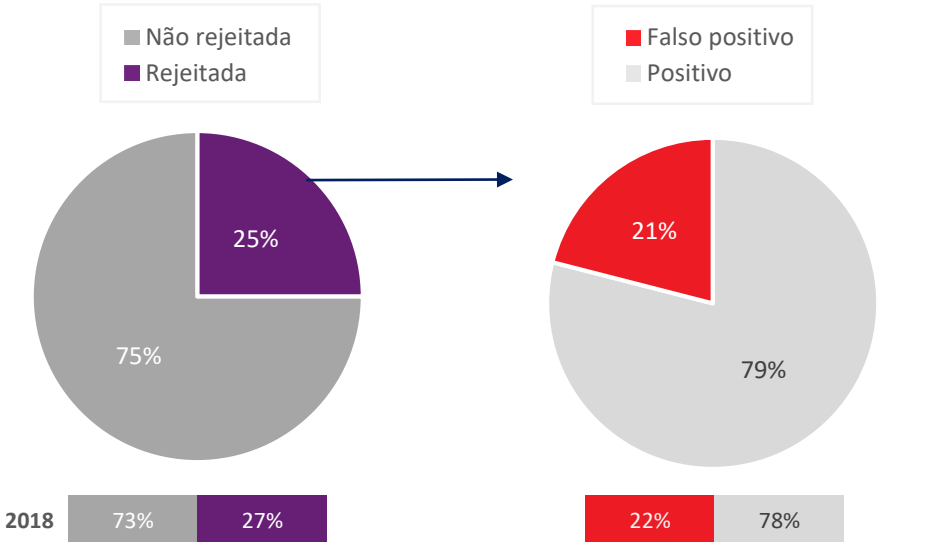
P36: De todas as operações que a sua empresa marcou como potencialmente fraudulentas nos últimos 12 meses, qual taxa foi feita pelo seu sistema automatizado?
P37: Deste (...), qual proporção é enviada para revisão manual?
P38: Qual a taxa das operações que a sua empresa inicialmente marca como potencialmente fraudulenta, mas que é rejeitada no final?
P39: Qual a taxa das operações rejeitadas acabou sendo falso positivo?

Brasil

% Operações marcadas pelo sistema automatizado e enviadas para revisão manual



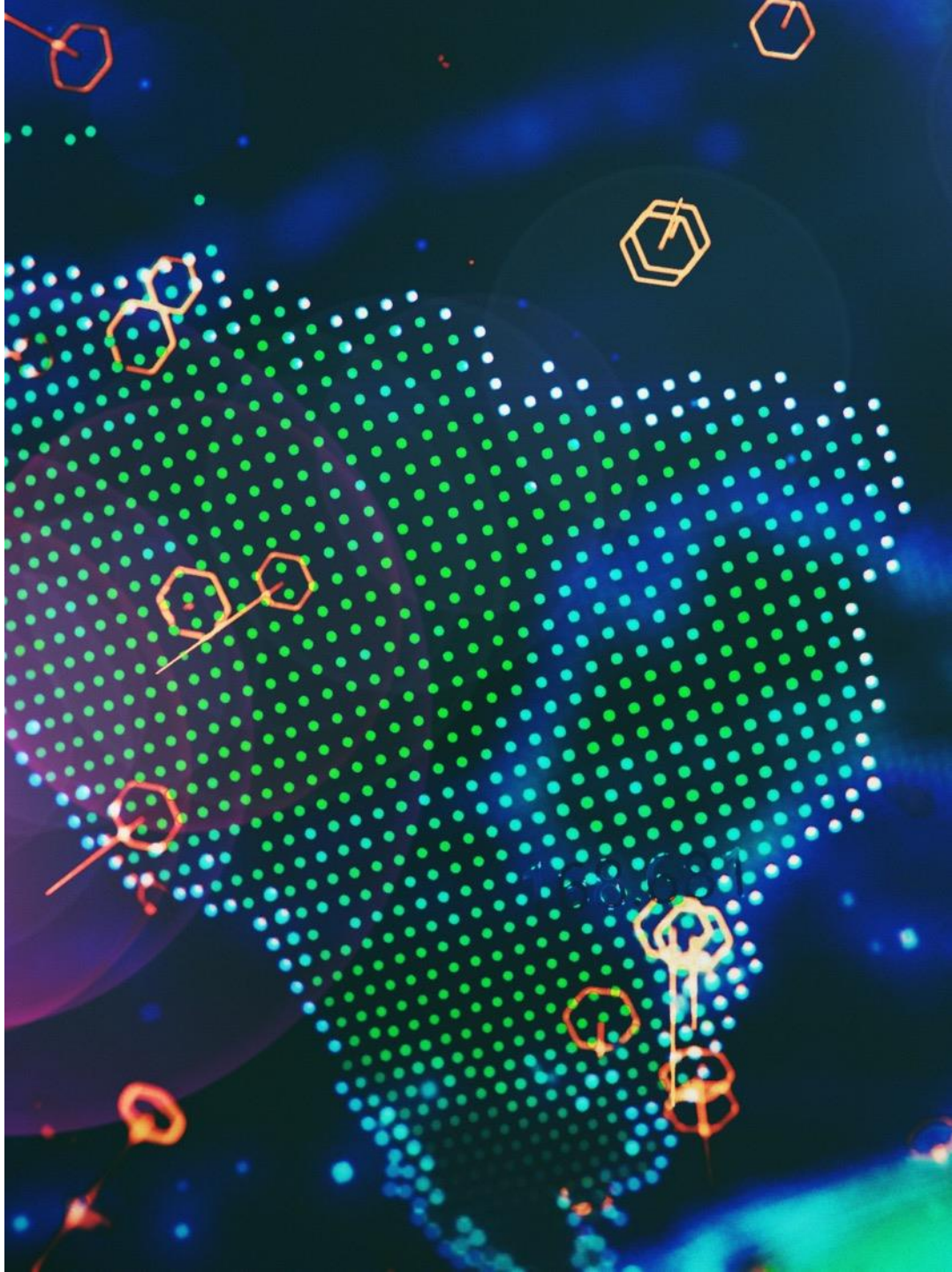
% Operações marcadas que são rejeitadas, falsos positivos



LexisNexis® RISK SOLUTIONS

6

E, mesmo com as fraudes se tornando mais sofisticadas, o uso de soluções mais refinadas continua limitado.



LexisNexis®
RISK SOLUTIONS

As fraudes se tornaram mais complexas e vários riscos podem existir ao mesmo tempo, sem nenhuma solução. As ferramentas de fraudes precisam autenticar os critérios digitais e os físicos, além do risco da identidade e da operação.

QUESTÕES DAS FRAUDES

- **Produtos e serviços digitais**: operações rápidas, alvos fáceis de identidades sintéticas e botnet; ***necessidade de verificação de velocidade*** para determinar o ***risco da operação*** junto a ***dados e análises para autenticação do*** indivíduo.
- **Fraudes relacionadas a contas**: dados violados ***exigem mais níveis de segurança, além de autenticação da pessoa de um bot ou de uma identidade sintética.***
- **Identidades sintéticas**: ***necessidade de autenticação completa do indivíduo*** por trás da operação para poder distinguir as identidades falsas com base em dados reais parciais.
- **Ataques de botnets**: ataques em massa automatizados ou realizados por humanos para testar cartões, senhas/credenciais ou dispositivos infectados.
- **Canais móveis**: origem da fonte e dispositivos infectados acrescentam risco; *bots* móveis e malwares maliciosos dificultam a autenticação; ***necessidade de avaliação do dispositivo e o indivíduo.***

OPÇÕES DE SOLUÇÕES

AVALIAÇÃO DO RISCO DA OPERAÇÃO

Verificação de velocidade/classificação de operação: monitoramento dos padrões históricos de compra de um indivíduo e faz a comparação com as compras atuais para identificar se o número de pedidos realizados pelo titular do cartão corresponde ou se indica irregularidades ***(Exemplos de soluções: classificação de operação em tempo real; classificação de operação automatizada).***

AUTENTICAÇÃO DA PESSOA FÍSICA

Verificação básica verificação de nome, endereço, data de nascimento ou fornecimento do código CVV associado a um cartão ***(Exemplos de soluções: serviços de verificação de cheques; autenticação do instrumento de pagamento; verificação de nome/endereço/data de nascimento).***

Ativação de autenticação de identidade uso dos dados pessoais conhecidos pelo cliente para autenticação; ou quando o usuário fornecer dois fatores diferentes de autenticação para a sua verificação ***(Exemplos de soluções: autenticação por desafio ou perguntas; autenticação com senha de uso único/de dois fatores)***.

AUTENTICAÇÃO DA PESSOA DIGITAL

Identidade digital/biometria comportamental: análise das interações humano-dispositivo e padrões de comportamento, como cliques no mouse e toques de tecla, para distinguir entre usuários reais e um impostor, ao reconhecer comportamento normal e fraudulento ***(Exemplos de soluções: autenticação por biometria; avaliação de riscos por e-mail/telefone; monitoramento do navegador/malware ; identidade/impressão digital do dispositivo).***

Avaliação do dispositivo: identificação exclusiva de um dispositivo de computação remota ou usuário ***(Exemplos de soluções: identidade/ impressão digital do dispositivo; localização geográfica)***

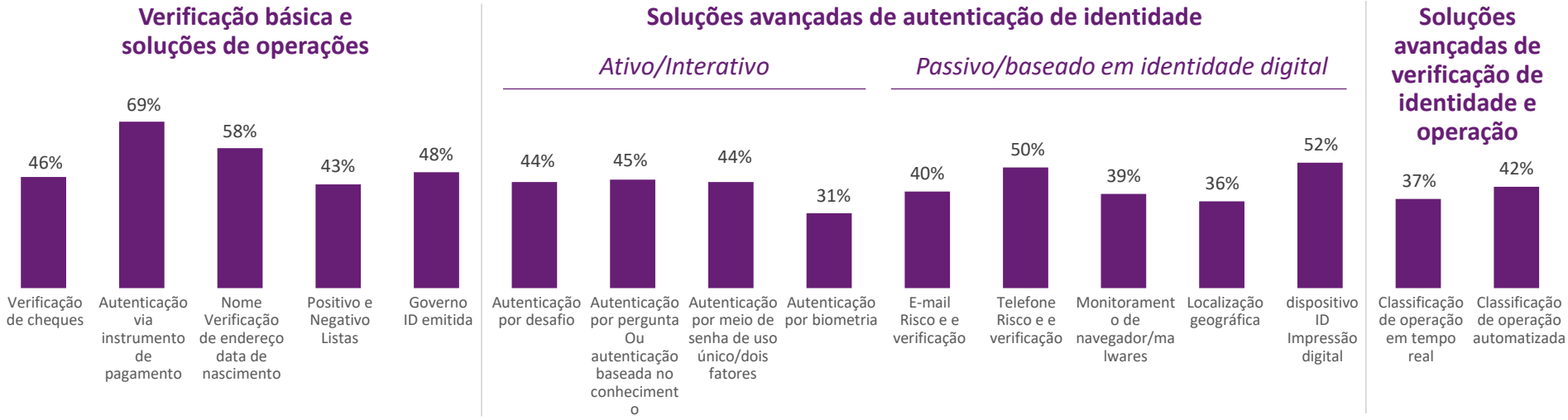
LexisNexis® RISK SOLUTIONS

Um média de 5,8 soluções de mitigação de fraudes é usada pelas empresas de varejo, comércio eletrônico e serviços financeiros.

- No entanto, o uso de soluções mais sofisticadas para lidar com a natureza complicada das fraudes é limitado, especialmente com relação à biometria comportamental e outras soluções de identidade digital que podem combater fraudes de identidades sintéticas e ataques de botnets. A taxa semelhante de incidência entre algumas das soluções físicas (verificação de cheques, identidades emitidas por governos) e digitais (classificação automatizada de operações) sugere que sobrepor soluções colabora para uma detecção mais eficiente de fraudes. Porém, ainda há uma parcela significativa de empresas que não o faz.
- Além disso, o uso de soluções para lidar com ameaças móveis (localização geográfica, senha de uso único/dois fatores) e o desafio da rapidez de operações digitais/anônimas (classificação de operações em tempo real) é mais limitado. E embora as soluções representem uma parte considerável do orçamento de mitigação de fraudes, as revisões manuais são metade disso, sugerindo ainda que faltam tentativas atuais de prevenção a fraudes.

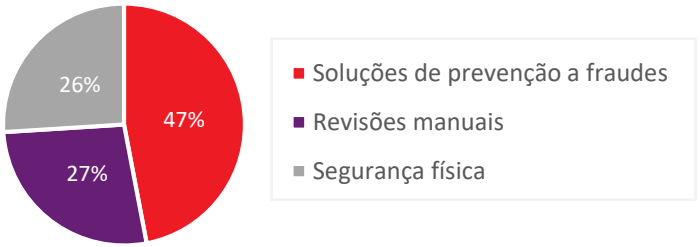
Uso de soluções de mitigação de fraudes

Média 5,8 soluções usadas



P27: Quais das afirmações a seguir melhor descreve a sua consciência e uso das soluções de fraudes mencionadas?
P41b: Qual é a taxa de distribuição de custos de mitigação nas seguintes áreas no últimos 12 meses?

Distribuição dos custos de mitigação de fraudes por percentual gasto



LexisNexis® RISK SOLUTIONS

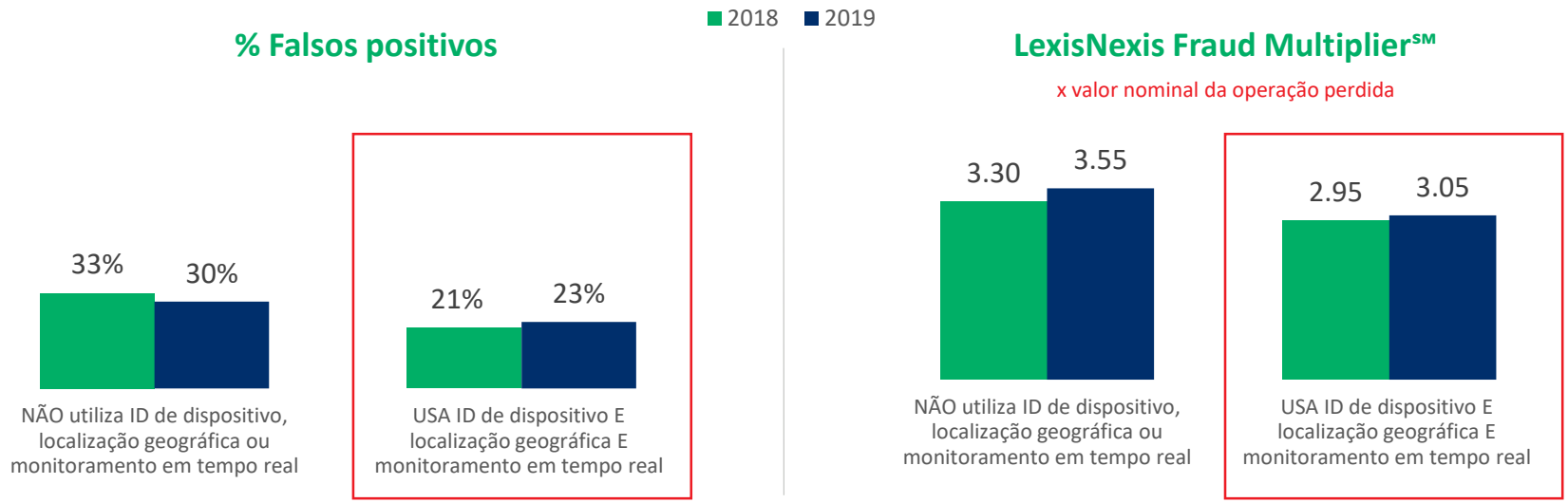
Mas não se trata do número de soluções, o importante é compor a combinação correta para combater as fraudes por tipos específicos de canais e operações.

Achados Regionais

Os achados continuam mostrando que empresas digitais de varejo/comércio eletrônico/serviços financeiros na LATAM que agrupam soluções para lidar com as ameaças móveis (ID/impressão digital de dispositivo, localização geográfica) e a rapidez das operações digitais/anônimas (classificação de operação em tempo real) podem sofrer menos falsos positivos e apresentar custos mais baixos de fraudes no geral.

Comerciantes/empresas de serviços financeiros da LATAM que são digitais* e permitem operações em canais móveis

(Achados regionais por toda LATAM)

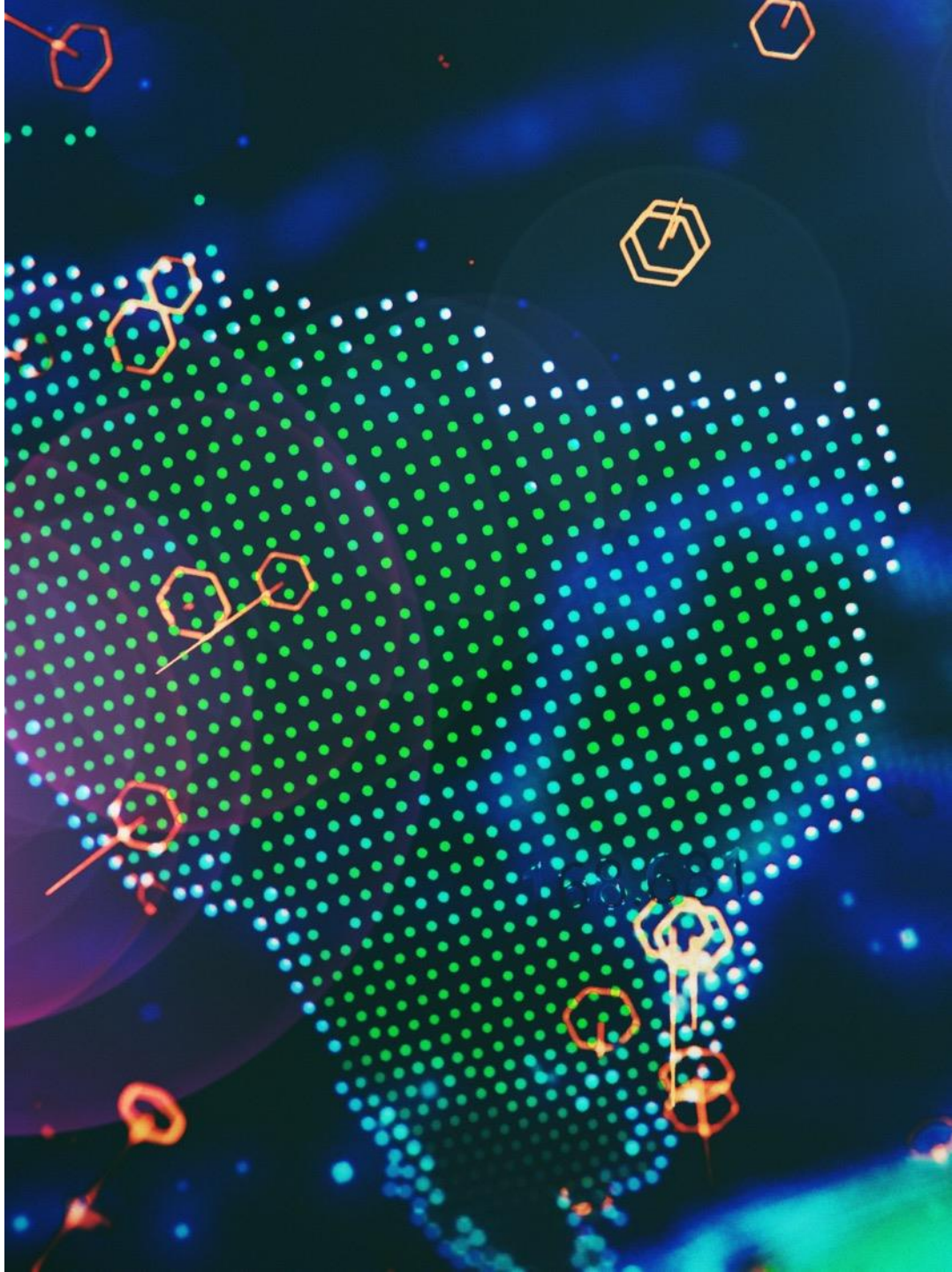


LexisNexis® RISK SOLUTIONS

* Para empresas de varejo/comércio eletrônico, digital se refere à venda de produtos e serviços digitais. Para empresas de serviços financeiros, digital se refere à geração de 50% ou mais da receita por meio de canais remotos (online ou móvel).

P27: Quais das afirmações a seguir melhor descreve a sua consciência e uso das soluções de fraudes mencionadas?
P39: Qual a taxa das operações rejeitadas acabou sendo falso positivo?

Recomendações



LexisNexis®
RISK SOLUTIONS

Recomendação 1

Brasil

As empresas devem implementar diferentes soluções de mitigação de risco para lidar com os riscos exclusivos aos diferentes canais e modelos de venda.

As soluções usadas para mitigar os riscos de operações de produtos físicos não mitigará completamente os de produtos digitais porque a natureza da mercadoria muda o risco (ex.: mais operações rápidas e em tempo real com bens digitais).

Dada a natureza da mobilidade, os canais móveis e os online representam riscos e desafios diferentes. Combinados aos produtos digitais e ao maior volume de fraudes em aplicativos para dispositivos móveis, isso aumenta a complexidade.

Soluções específicas ao dispositivo e verificações em tempo real/velocidade são exemplos de tecnologias únicas que oferecem suporte a esses ambientes de operações específicas.

LexisNexis® RISK SOLUTIONS

Recomendação 2

Brasil

Uma abordagem de solução multicamadas é essencial para combater fraudes e, ao mesmo tempo, mitigar o atrito com o cliente, especialmente para quem vende produtos digitais e usam canais móveis.

É fundamental lidar tanto com as fraudes relacionadas a identidades quanto a operações. São duas perspectivas diferentes.

Verificação/autenticação de identidade é importante para permitir que seu clientes “entrem” com o mínimo de atrito e risco.

Fraudes relacionadas a operações se trata de manter os "bandidos do lado de fora”.

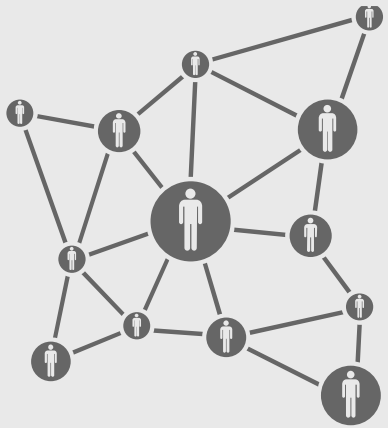
Uma abordagem em camadas pode reduzir os custos associados a revisões manuais, tentativas bem-sucedidas de fraudes e menos falsos positivos.

LexisNexis® RISK SOLUTIONS

Recomendação 3

Brasil

As empresas devem buscar fornecedores externos com dados profundos e recursos de análises para lidar com os desafios de fraudes de identidade com mais eficiência, especialmente para os tipos de ataques mais novos e sofisticados.



As fraudes de identidade podem ser complicadas, com várias camadas de máscaras e conexões no pano de fundo.

O investimento em uma abordagem de solução em camadas será muito mais eficiente se fornecida por um parceiro que oferece capacidades únicas de vinculação que identificam e fazem a correspondência de relacionamentos ocultos, esclarecem atividades ou operações suspeitas e identificam conluios.

Esses padrões não são descobertos facilmente por diversas soluções de risco no mercado atual.

LexisNexis® RISK SOLUTIONS

Recomendação 4

Brasil

Comerciantes e empresas de serviços financeiros que realizam comércio móvel precisam focar, principalmente, nas soluções de avaliação de dispositivo para combater o crescente volume de fraudes em aplicativos para dispositivos móveis.

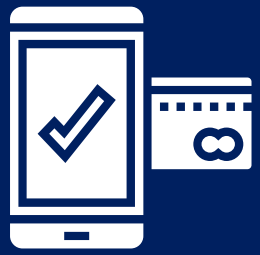
Porque bonets e malwares podem comprometer dispositivos, os aplicativos para dispositivos móveis usados para operações também ficam vulneráveis. Portanto, a verificação e a autenticação não tem a ver somente com o usuário, mas também com o dispositivo e se o aplicativo foi adulterado.

Para minimizar o atrito com os clientes e evitar abandono de operação, a avaliação do dispositivo se torna importante para verificar, imediatamente, a identidade do dispositivo e os atributos de localização, VPN e proxies, malwares e bots.

LexisNexis® RISK SOLUTIONS

Recomendação 5

Brasil



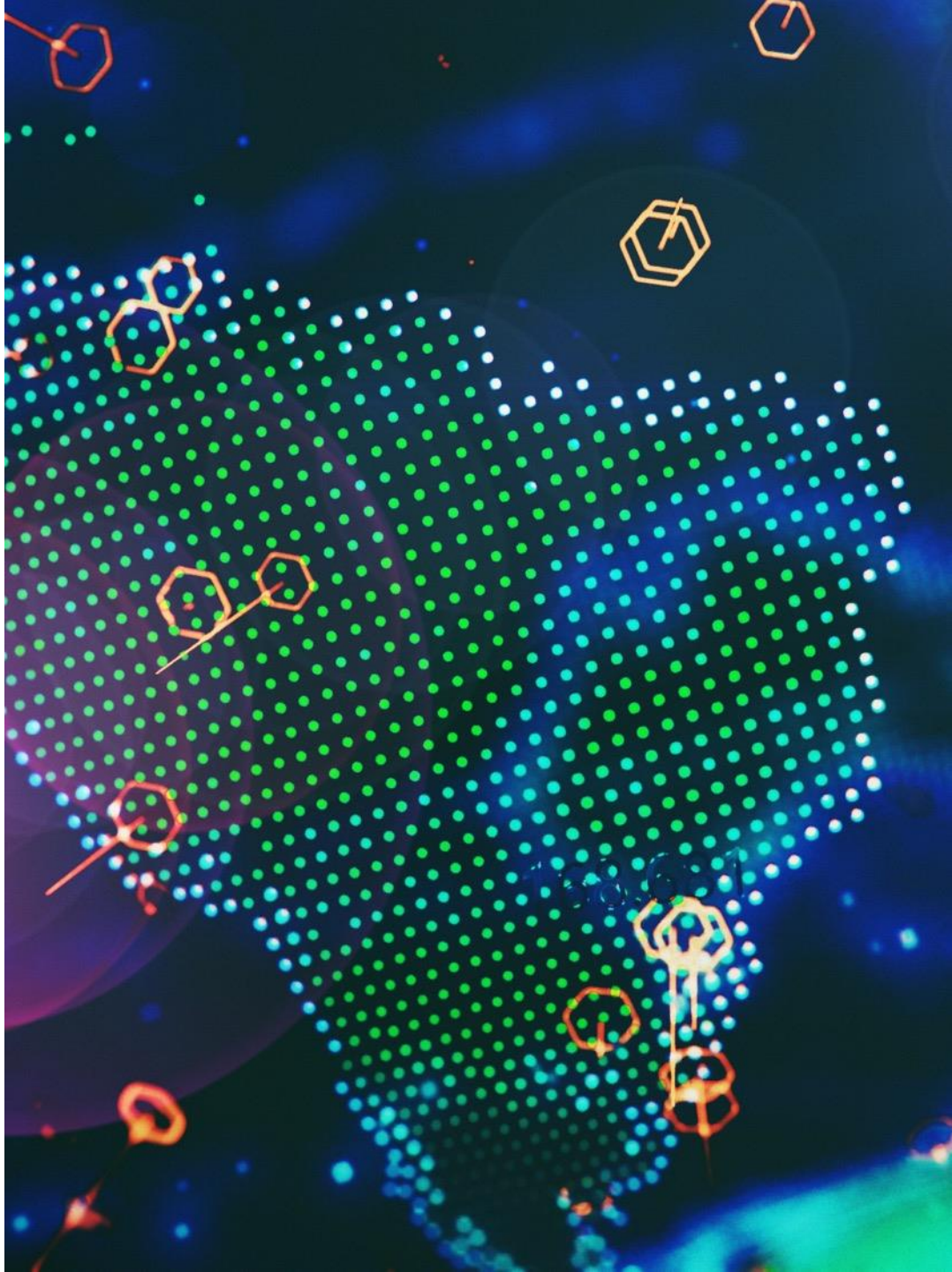
As empresas precisam monitorar as fraudes de pagamentos e de canal, em termos de custos e de tentativas bem-sucedidas. Mas isso precisa fazer parte de uma abordagem mais ampla, envolvendo soluções de identificação de fraudes projetadas para lidar com riscos únicos.

Como as fraudes ocorrem de formas diferentes dependendo se a venda é de produto físico ou digital e se feita por um canal móvel, isso cria diversos endpoints e oportunidades para os fraudadores atacarem. Eles continuam realizando testes para encontrar os pontos mais fracos onde podem operar sem serem detectados. Saber onde eles são bem-sucedidos é importante para "preencher os espaços vazios", mas também conhecer onde tentaram e falharam é igualmente relevante para manter a vigilância.

Dito isso, a ascensão das identidades sintéticas facilita que as fraudes passem despercebidas. Sem a ajuda de soluções de mitigação de risco projetadas para reconhecer características de identidades fraudulentas, abordagens de monitoramento não perceberão certas pistas, enfraquecendo os esforços de monitoramento.

LexisNexis® RISK SOLUTIONS

A LexisNexis® Risk Solutions pode ajudar



LexisNexis®
RISK SOLUTIONS

A LexisNexis® Risk Solutions oferece potente verificação de identidade, autenticação de identidade e ferramentas de classificação de operações para combater as fraudes.

LexisNexis® Risk Solutions:

- Vastos recursos de dados
- \+
- Tecnologia de megadados
- \+
- Vinculação & Análises
- \+
- Conhecimento e entrega específicos ao setor

= Soluções com foco no cliente

Verificação de identidade

- Validação de nome, endereço e telefone;
- Reconciliação de variações e duplicidade de nomes, diversos endereços e inúmeras outras inconsistências e vinculações;
- Execução de verificações globais de identidade com integração perfeita e funcionalidades para geração de relatórios.

Classificação de risco da operação

- Identificação dos riscos associados a identidades para cobrança e envio com uma pontuação única de risco numérico;
- Identificação rápida de padrões de fraudes e isolamento de operações de alto risco;
- Resolução de falsos positivos e falhas nos sistemas de verificação de endereço.

Suporte à pesquisa manual

- Acesso a bilhões de registros de dados sobre clientes e empresas;
- Identificação de vínculos entre pessoas, empresas e ativos;
- Aproveitamento de ferramentas especializadas para due diligence, gestão de conta e compliance.

Autenticação de identidade

- Autenticação de identidades imediatamente usando questionários baseados em conhecimento.
- Ajuste dinâmico do nível de segurança para se adequar ao cenário de risco.
- Recebimento de resultados de aprovado/reprovado em tempo real.

LexisNexis® RISK SOLUTIONS

Resumo Regional de 2019

LexisNexis®
RISK SOLUTIONS

As fraudes permanecem consideráveis para as empresas na LATAM, mas continuam mais evidentes no setor de serviços financeiros, assim como negócios de todos os tipos que conduzem operações através de canais móveis.

Achados Regionais

- Essas empresas continuam sofrendo altos volumes de fraudes bem-sucedidas e quantias de operações, mesmo que acabem utilizando um pouco mais de soluções de mitigação de fraudes que outras.
- Elas também continuam contribuindo com mais prejuízo por fraudes para a fraudes de identidade do que outros negócios.

↑↓ Significante ou direcionalmente de 2018

2019

	Região Geral	Setor			Oferece comércio móvel	
		Varejo	Comércio eletrônico	Serviços financeiros	Sim	Não
LexisNexis Fraud Multiplier℠	**3,46** ↑	**2,61**	**2,96** ↑	**3,96** ↑	**3,65** ↑	**2,52**
Custos das fraudes como % das receitas	2,16%	2,38%	2,23%	2,03%	**2,35%** ↑	1,72% ↑
Média de soluções de mitigação de fraudes	5,6	4,6	5,3	**6,1**	5,0	4,7
Média de operações de fraudes BEM-SUCEDIDAS mensalmente	598 ↑	288 ↑	303 ↑	**815** ↑	**742** ↑	232
Média do valor das operações de fraudes BEM-SUCEDIDAS mensalmente	R$ 2.237	R$ 917	R$ 811 ↑	R$ 3.210	R$ 2.684	R$ 1.558 ↑
% de comércio móvel que oferece aplicativos para dispositivos móveis	77% ↑	**79%**	58% ↑	**79%** ↑	77% ↑	
% das distribuição de prejuízo relacionado a fraudes de identidade	34% (12% sintética)	23% (7% sintética)	31% (10% sintética)	**40% (15% sintética)**	**37% (3% sintética)**	28% (11% sintética)
% Ranking de verificação de identidade como grande desafio online/móvel	56%	56%	57%	56%	**62%**	40%

LexisNexis® RISK SOLUTIONS

E, ao analisar os setores, **empresas de produtos digitais e serviços financeiros** continuam sendo os mais atingidos por fraudes.

Achados Regionais

- Produtos digitais representam mais da metade dos prejuízo por fraudes para o varejo/comércio eletrônico, enquanto que os canais online/móveis somam 3/4 para os serviços financeiros.
- Essas empresas continuam apresentando maiores volume e valores de fraudes bem-sucedidas do que outras, o que contribui para custos mais altos de fraudes.
- Negócios de natureza digital (por tipo de produto vendido ou canal de operação) permanecem mais prováveis a possibilitar operações por meio de aplicativos para dispositivos móveis de alto risco, o que acrescenta aos desafios relacionados a verificação de identidade, inclusive identidades sintéticas.

↑↓ Significante ou direcionalmente de 2018

*Os produtos digitais mais vendidos incluem software para download, jogos online/jogos, aplicativos para dispositivos móveis e assinaturas digitais.
** Ganha mais de 50% da receita através dos canais online/móveis

LexisNexis® RISK SOLUTIONS

2019

	Varejo/ Comércio eletrônico		Serviços financeiros	
	Vende produtos digitais*	Vende somente produtos físicos	Digital**	Não digital
LexisNexis Fraud Multiplier℠	**3,13**	2,54	**4,10** ↑	3,89 ↑
Custos das fraudes como % das receitas	**2,76%**	2,01%	**2,42%** ↑	1,83%
% Prejuízo por fraudes de...	Produtos digitais = 53%		**Canais online/móveis = 74%**	Canais online/móveis = 55%
Média de soluções de mitigação de fraudes	5,0	4,7	6,5	5,9
Média de operações de fraudes BEM-SUCEDIDAS mensalmente	395	191 ↑	**1.200** ↑	621 ↑
Média do valor das operações de fraudes BEM-SUCEDIDAS mensalmente	R$ 1.229	R$ 626	**R$ 5.681** ↑	R$ 2.787
% de comércio móvel que oferece aplicativos para dispositivos móveis	79%	67% ↑	77%	81% ↑
% Distribuição do prejuízo relacionado a fraudes de identidade	28% (9% sintética)	23% (8% sintética)	42% (13% sintética)	39% (16% sintética)
% Ranking de verificação de identidade como grande desafio online/móvel	44%	43%	**83%**	43%
% Ranking de identidades sintéticas como grande desafio para verificação de identidade	60%			

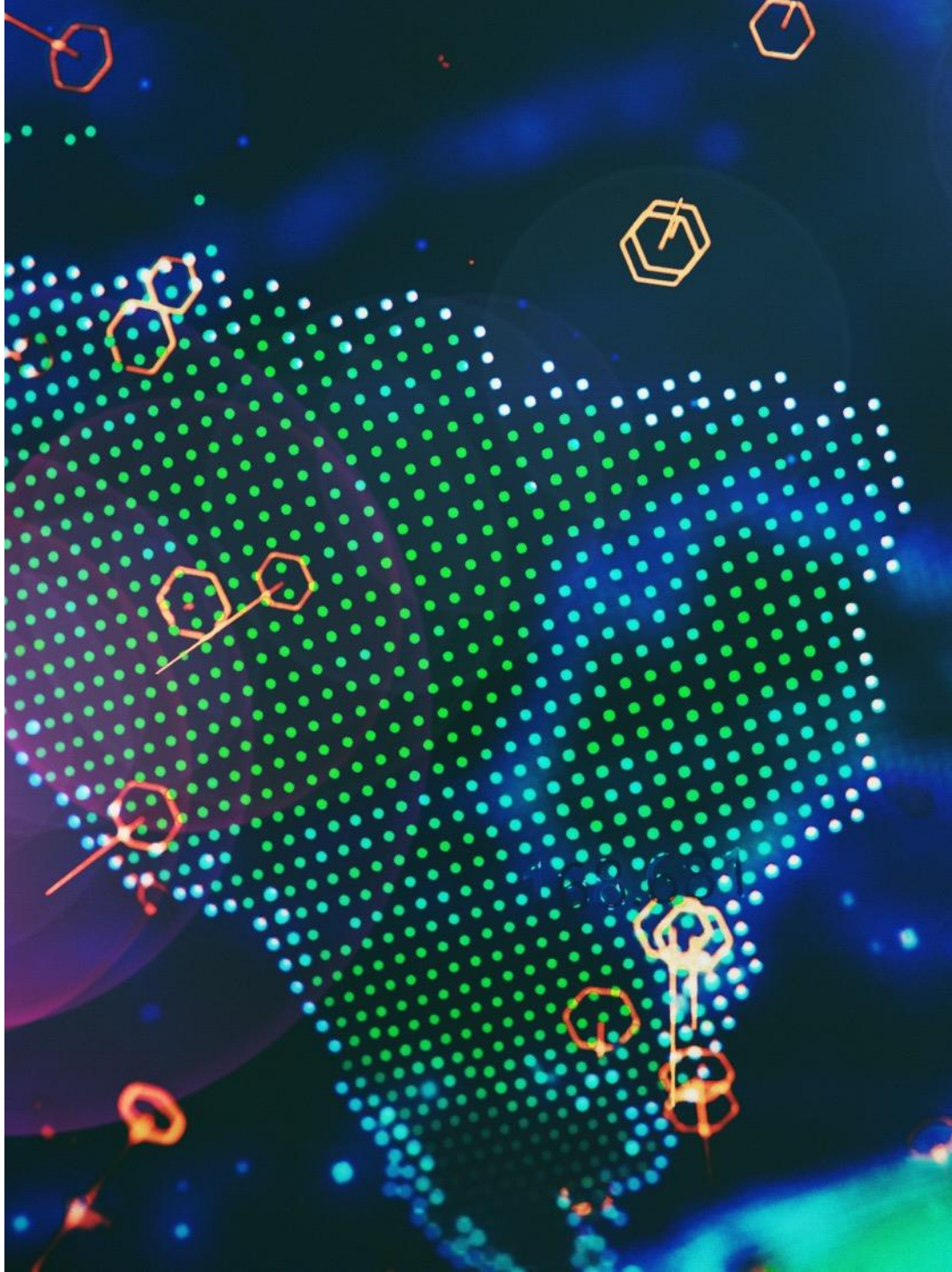
As fraudes permanecem numerosas nos países da LATAM, mas continuam mais altas no Brasil, onde os volumes e as quantias de fraudes são os mais elevados.

Achados Regionais

2019	Região Geral	País				
		México	Brasil	Colômbia	Argentina	Chile
LexisNexis Fraud Multiplier℠	3,46	3,55	**3,61 (+4.9% desde 2018)**	3,29	3,35	3,52
Custos das fraudes como % das receitas	2,16%	1,96%	**2,68%**	1,56%	1,73%	2,02%
Média de soluções de mitigação de fraudes	5,6	5,5	5,8	5,7	4,9	5,7
Média de operações de fraudes BEM-SUCEDIDAS mensalmente	598	562	**691**	491	536	564
Média do valor das operações de fraudes BEM-SUCEDIDAS mensalmente	R$ 2.237	R$ 2.278	**R$ 3.117**	R$ 1.331	R$ 1.342	R$ 1.865
% do comércio móvel que oferece aplicativos para dispositivos móveis	77%	**83%**	73%	**87%**	74%	70%
% das distribuição de prejuízo relacionado a fraudes de identidade	34% (12% sintética)	37% (12% sintética)	31% (12% sintética)	33% (13% sintética)	31% (12% sintética)	35% (12% sintética)
% Ranking de verificação de identidade como grande desafio online/móvel	56%	54%	59%	**64%**	51%	52%

LexisNexis® RISK SOLUTIONS

Apêndice



LexisNexis®
RISK SOLUTIONS

Achados Regionais

	Região Geral	Setor			Oferece comércio móvel	
		Varejo	Comércio eletrônico	Serviços financeiros	Sim	Não
LexisNexis Fraud Multiplier℠	3,27	2,59	2,71	3,78	3,42	2,54
Custos das fraudes como % das receitas	2,0%	2,06%	2,29%	1,92%	2,18%	1,17%
Média de soluções de mitigação de fraudes	4,6	3,8	4,1	5,2	4,8	3,7
Média de operações de fraudes BEM-SUCEDIDAS mensalmente	491	249	244	673	551	235
Média do valor das operações de fraudes BEM-SUCEDIDAS mensalmente	R$ 2.109	R$ 801	R$ 383	R$ 3.094	R$ 2.375	R$ 458
% de comércio móvel que oferece aplicativos para dispositivos móveis	66%	78%	32%	65%	66%	

LexisNexis® RISK SOLUTIONS

Achados Regionais

	Varejo/ Comércio eletrônico		Serviços financeiros	
	Vende produtos digitais*	Vende somente produtos físicos	Digital**	Não digital
LexisNexis Fraud Multiplier℠	3,09	2,65	3,84	3,59
Custos das fraudes como % das receitas	2,44%	1,88%	2,24%	1,79%
% Prejuízo por fraudes de...	Produtos digitais = 45%		Canais online/móveis = 71%	Canais online/móveis = 52%
Média de soluções de mitigação de fraudes	3,6	4,1	5,4	5,1
Média de operações de fraudes BEM-SUCEDIDAS mensalmente	382	81	917	331
Média do valor das operações de fraudes BEM-SUCEDIDAS mensalmente	R$ 1.174	R$ 480	R$ 3.380	R$ 2.415
% do comércio móvel que Oferece aplicativos para dispositivos móveis	84%	52%	71%	59%
% Distribuição do prejuízo Relacionada a fraudes de identidade	40% (15% sintética)	32% (12% sintética)	54% (25% sintética)	56% (26% sintética)

LexisNexis® RISK SOLUTIONS

*Os produtos digitais mais vendidos incluem software para download, jogos online/jogos, aplicativos para dispositivos móveis e assinaturas digitais.
** Ganha mais de 50% da receita através dos canais online/móveis

Achados Regionais

	Região Geral	País				
		México	Brasil	Colômbia	Argentina	Chile
LexisNexis Fraud Multiplier℠	3,27	3,39	3,44	3,21	3,27	3,34
Custos das fraudes como % das receitas	2,0%	1,75%	2,47%	1,41%	1,59%	1,97%
Média de soluções de mitigação de fraudes	4,6	4,6	4,7	5,0	4,0	5,0
Média de operações de fraudes BEM-SUCEDIDAS mensalmente	491	468	579	453	448	495
Média do valor das operações de fraudes BEM-SUCEDIDAS mensalmente	R$ 2.109	R$ 1.960	R$ 2.642	R$ 1.326	R$ 1.569	R$ 1.852
% de comércio móvel que oferece aplicativos para dispositivos móveis	66%	76%	65%	83%	48%	53%

LexisNexis® RISK SOLUTIONS

Para mais informações visite: risk.lexisnexis.com/fraudes