

Resultados da Pesquisa Global de Fraude 2021



Conteúdos do relatório

03	Panorama
04	Sumário executivo
05	Firmografia da pesquisa
06	Impacto das fraudes no negócio: Principais conclusões
10	Impacto das fraudes no negócio: insights aprofundados sobre a revisão manual e a PSD2
15	Variedade dos ataques de fraude: Principais conclusões
20	Estratégias de prevenção de fraude: Principais conclusões
24	Conclusão
25	Sobre os autores
26	Apêndice (perguntas da pesquisa)

Panorama

Cybersource e o Merchant Risk Council (MRC) têm o prazer de apresentar os resultados da Pesquisa Global de Fraude 2021, relatório educativo elaborado a partir de uma pesquisa transparente e imparcial. O relatório se baseia em uma pesquisa realizada com empresários do mundo todo, com perguntas sobre sua experiência com fraude de eCommerce e as práticas adotadas para mitigá-las.

Os resultados da pesquisa possibilitam que a comunidade de estabelecimentos comerciais conheça os dados de fraude mais recentes do setor, os métodos de gestão de fraude adotados por seus pares e um conjunto substancial de parâmetros de desempenho que podem ajudar a otimizar seu negócio. A pesquisa foi realizada entre março e abril de 2021.

A Cybersource gostaria de agradecer aos participantes por terem respondido à pesquisa on-line, ao MRC por sua contínua parceria e à B2B International por dirigir o programa e fornecer a análise.

Sumário executivo

Os principais resultados e conclusões da pesquisa deste ano foram organizados em três áreas de foco. Cada área aborda uma questão central, essencial para entendermos o estado e a gestão das fraudes de eCommerce.

Primeiro, o relatório examina o impacto das fraudes no negócio para entender seus efeitos nos estabelecimentos comerciais e suas variações nas diferentes regiões e segmentos de porte. A seguir, o relatório investiga a variedade dos ataques de fraude que atingem os estabelecimentos comerciais para entender os tipos de ameaça enfrentados e onde eles estão mais vulneráveis. Por fim, o relatório explora as estratégias de prevenção de fraude para entender como os empresários estão lidando com as fraudes de pagamento em nível estratégico e tático.

A seguir, os principais insights de cada uma dessas áreas:



Impacto das fraudes no negócio: Quais os efeitos das fraudes?

- Segundo cerca de três em quatro empresários globalmente, a Covid elevou as tentativas de fraude e o percentual de fraude em relação ao faturamento, afetando especialmente os estabelecimentos medianos e os localizados na região Ásia-Pacífico
- As tentativas de fraude, os custos e outros KPIs de gestão de fraude aumentaram, atingindo mais fortemente os estabelecimentos comerciais da APAC e da América Latina, e os de porte mediano
- Os empresários estão alocando mais de um terço da verba destinada à prevenção de fraudes no eCommerce para cobrir custos ligados à revisão de pedidos: a maioria quer reduzir – ou eliminar – sua dependência de revisões manuais no futuro



Variedade dos ataques de fraude: Onde os estabelecimentos comerciais estão mais vulneráveis?

- Os ataques sofridos pelos estabelecimentos comerciais ficaram menos variados (embora o volume tenha aumentado)
- As fraudes amigáveis e os testes de cartão desbancaram os ataques de phishing/pharming e roubo de identidade, e são hoje os tipos de fraude mais comuns no mundo
- Felizmente, a maioria dos empresários tem uma estratégia formal para combater as fraudes amigáveis, enviando vários avisos aos clientes, adotando políticas claras e visíveis e verificando e analisando seu histórico de compra



Estratégias de prevenção de fraude: Como os empresários estão tratando a questão?

- Proteger e melhorar a experiência do cliente/de compra passou a ser o principal imperativo estratégico para os empresários no que diz respeito a práticas de prevenção de fraude
- Em nível tático, os empresários estão racionalizando seu arsenal de prevenção de fraude, apostando mais fortemente em um número menor de ferramentas amplamente usadas (principalmente a verificação do CVN e do e-mail)
- Muitas das ferramentas mais eficazes não são as mais amplamente adotadas pelos empresários, nem são consideradas adoções prioritárias no futuro

Firmografia da pesquisa

A pesquisa foi realizada em março e abril de 2021 com 650 empresários envolvidos nas decisões de gestão de fraude de eCommerce em suas empresas. A amostragem incluiu empresas das quatro regiões geográficas, com ampla representação em todos os segmentos de porte, canais de vendas e categorias de estabelecimento comercial. O gráfico abaixo mostra a composição geral da amostra nas principais firmografias.

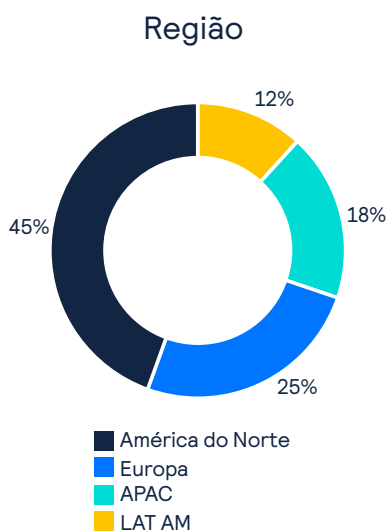


Figura 1

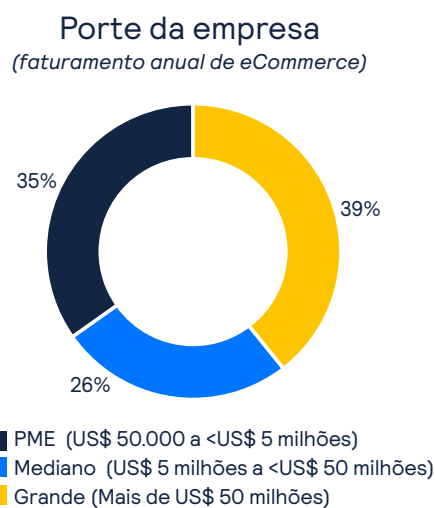


Figura 2

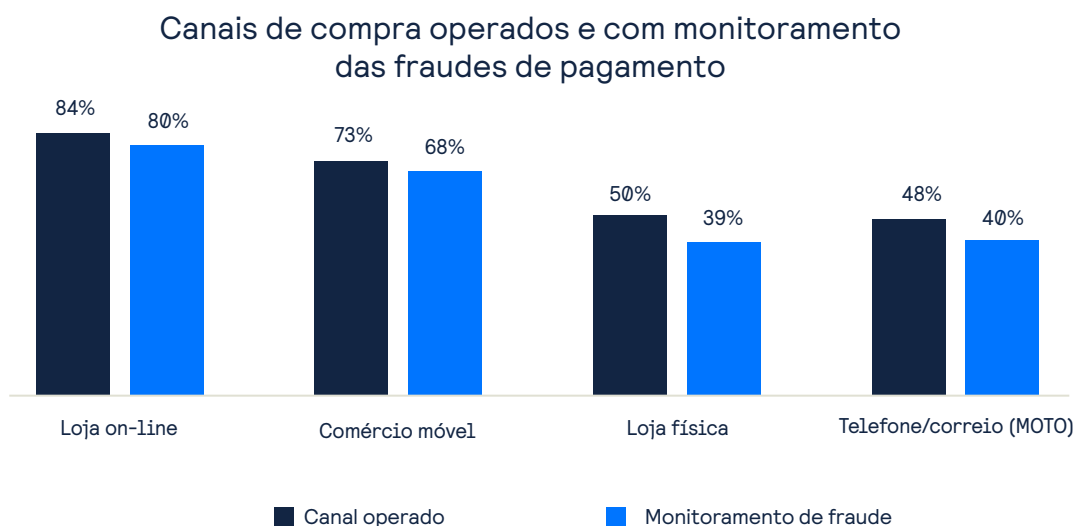


Figura 3

Na comparação com o estudo anterior, realizado em 2019, o percentual de estabelecimentos comerciais da amostra que operam os canais móvel e MOTO aumentou significativamente este ano – alta de 65% para 73% no canal móvel e de 34% para 48% no MOTO. Sem dúvida, os dois canais se tornaram mais atraentes e importantes para o negócio nos últimos dois anos, dadas as restrições impostas pela Covid-19 às compras em lojas físicas e a popularização dos smartphones no mundo todo.

Impacto das fraudes no negócio: Principais conclusões



A primeira área de insight ilustra o impacto das fraudes de eCommerce no negócio dos estabelecimentos comerciais, as mudanças e evoluções desses impactos desde 2019, e onde os empresários têm tido mais sucesso reprimindo as tentativas de fraude e reduzindo seus danos à organização.

Além de discutirmos as quatro conclusões a seguir, oferecemos insights mais profundos sobre dois tópicos relevantes para o entendimento de como as fraudes estão afetando o negócio dos estabelecimentos comerciais: o estado atual da revisão manual de pedidos e a preparação e as expectativas dos empresários com relação à recente alteração na Diretriz de Serviços de Pagamento da União Europeia, conhecida como PSD2.

01

A Covid provocou um aumento nos ataques de fraude e no percentual de fraude em relação ao faturamento em três quartos dos estabelecimentos comerciais: todos os KPIs de gestão de fraude aumentaram desde 2019.

02

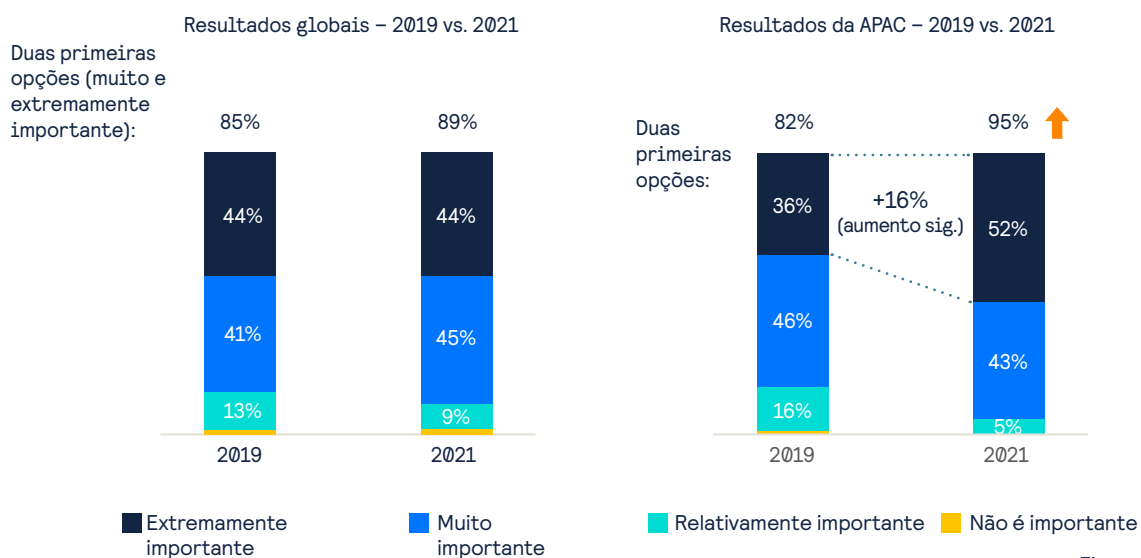
Considerando o percentual que eles representam do faturamento de eCommerce, os gastos com a gestão de fraude foram multiplicados por cinco desde 2019. Os estabelecimentos comerciais de porte mediano são os que mais gastam com isso.

03

As organizações situadas fora da América do Norte sentiram mais os impactos das fraudes impulsionadas pela Covid. As estabelecidas na APAC foram as mais atingidas, o que exigiu que os empresários da região se dedicassem mais à gestão de fraude e aumentassem os gastos com isso.

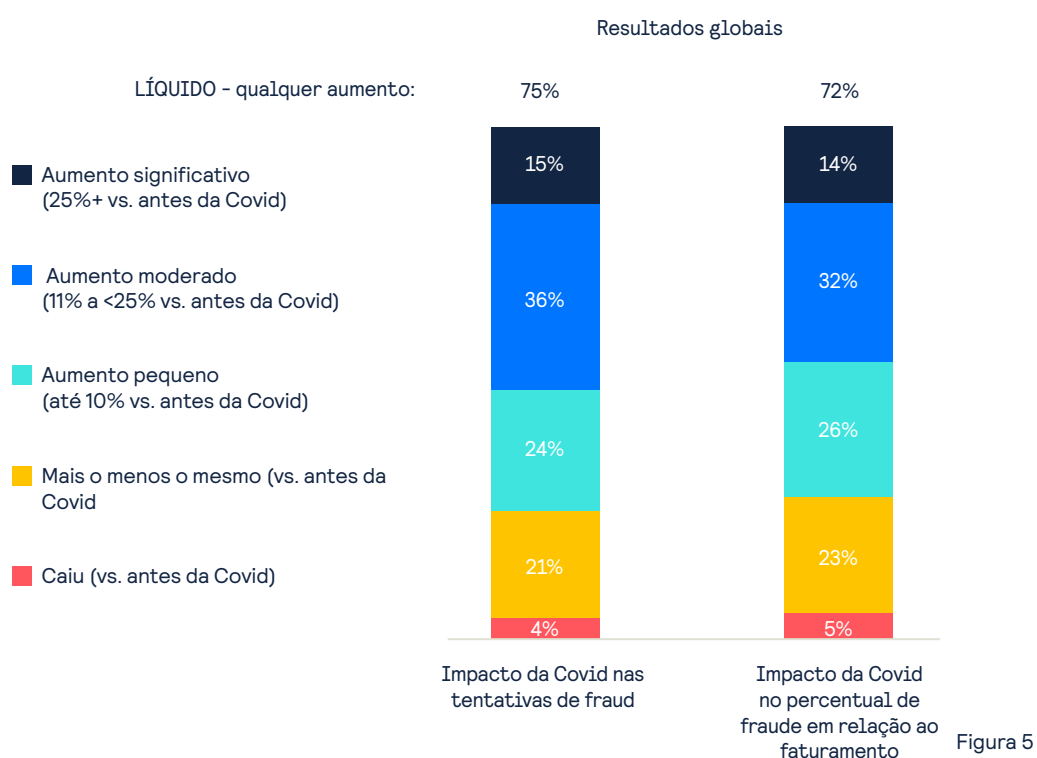
Mundialmente, a emergência da Covid-19 e as consequentes restrições ao comércio físico tradicional nos últimos dois anos catalisaram as vendas on-line e catapultaram o eCommerce como um canal de vendas crítico para muitos empresários. Portanto, não é de se surpreender que 9 em cada 10 empresários considerem a gestão das fraudes no eCommerce "muito ou extremamente importante" para sua estratégia empresarial geral (vide Figura 4). Além disso, a gestão das fraudes de eCommerce se tornou pertinente para os estabelecimentos comerciais localizados na região Ásia-Pacífico (APAC), onde se observa o maior aumento no percentual de empresários que consideram a questão muito importante para sua estratégia empresarial geral – 82% em 2019 ante 95% este ano.

Importância da gestão das fraudes de eCommerce para a estratégia empresarial geral



A gestão das fraudes de eCommerce se tornou relevante devido à alta nas vendas de eCommerce e ao aumento mundial nas tentativas de fraude e nos ataques sofridos pelos estabelecimentos comerciais. Na comparação com os dias anteriores à Covid, cerca de três quartos dos empresários relataram que tanto as tentativas de fraude quanto o percentual de fraude em relação ao faturamento aumentaram (Figura 5).

Proporção de organizações que disseram que as tentativas de fraude e o percentual de fraude em relação ao faturamento aumentaram



COVID estimulou um aumento nas tentativas de fraude e nas taxas de fraude por receita. Isso teve um impacto especial sobre os comerciantes localizados fora da América do Norte, empresas de porte mediano e grande. Esses grupos apresentam as maiores receitas online (Figura 6).

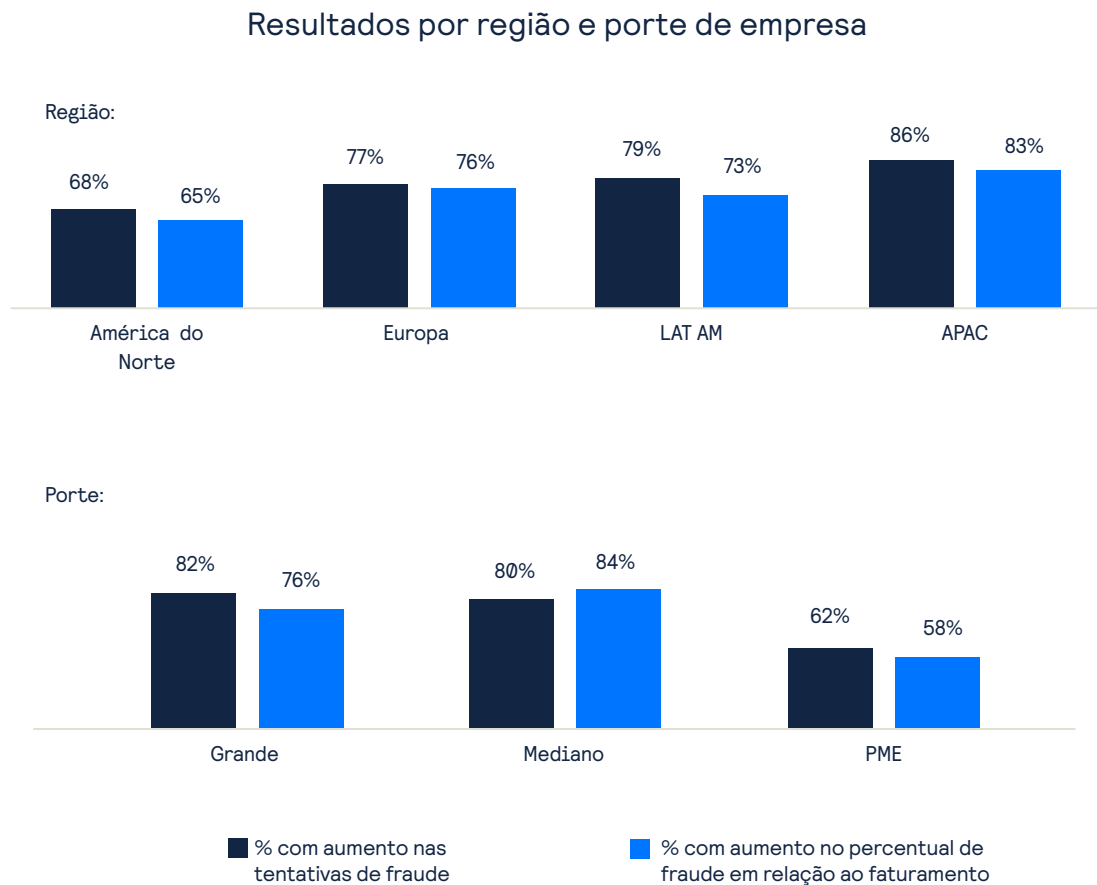
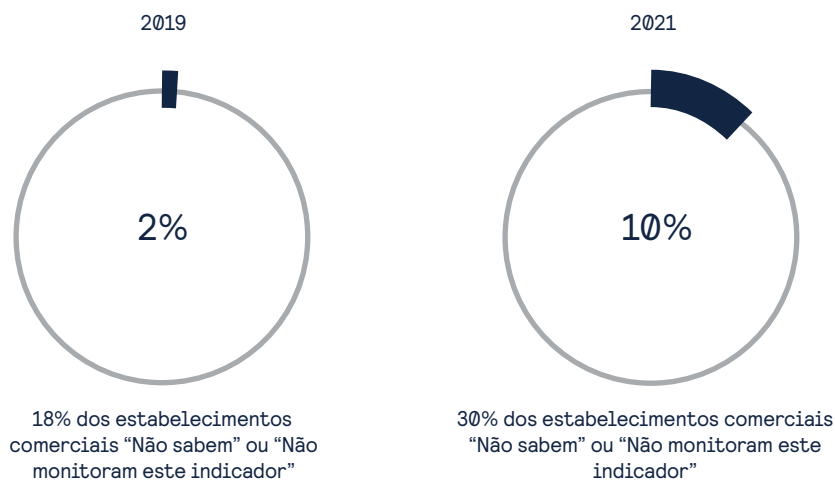


Figura 6

Com o aumento das tentativas de fraude e do percentual de fraude em relação ao faturamento, os gastos com gestão de fraude subiram em média cinco vezes se comparados aos níveis antes da Covid, aumentando de uma média de 2% do faturamento anual de eCommerce em 2019, para cerca de 10% este ano (Figura 7).

% do faturamento anual de eCommerce gasto com a gestão das fraudes de pagamento

Resultados globais

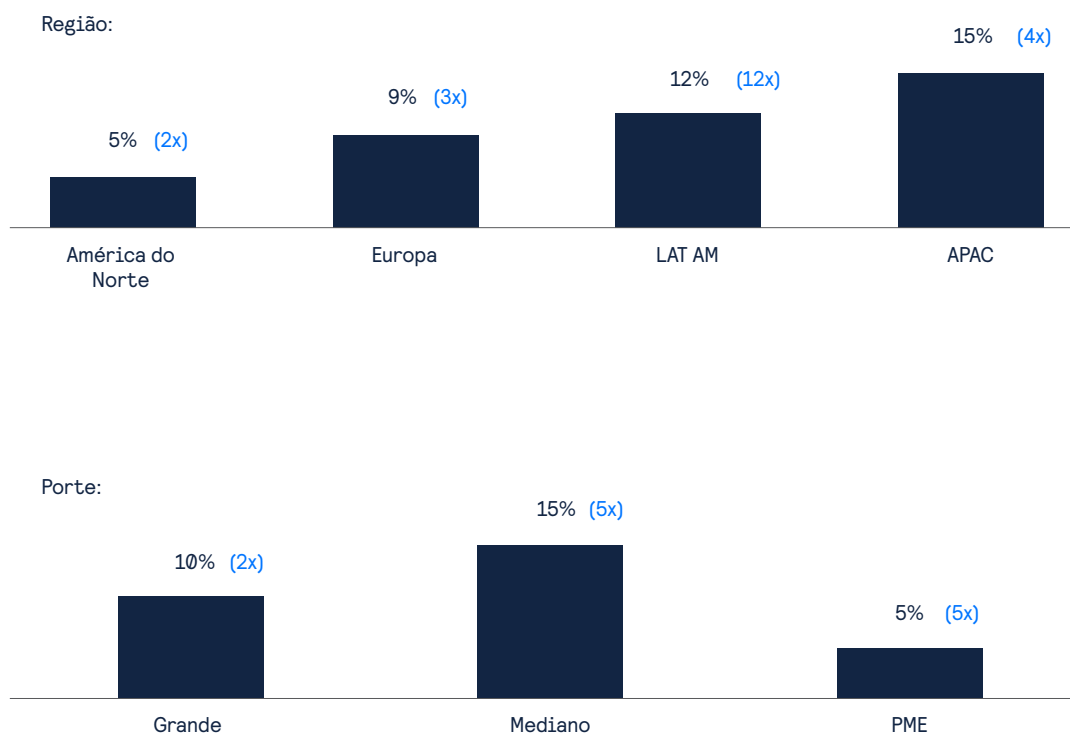


Nota: Usamos as médias truncadas de todas as estimativas de custos.

Figura 7

Na comparação com seus pares de outras regiões e outros segmentos de porte, as empresas da América Latina e da Ásia e os estabelecimentos comerciais de porte mediano despendem uma parcela maior de seu faturamento anual gerenciando fraudes de pagamento (Figura 8).

% do faturamento anual de eCommerce gasto para gerenciar fraudes de pagamento – por região e segmento de porte



(Percentual de **aumento** comparado a 2019)

Figura 8

O padrão de aumento nos ataques de fraude, custos e impactos nos estabelecimentos comerciais fica claro e inequívoco quando examinamos os outros indicadores de gestão de fraude e KPIs monitorados por este estudo nos últimos dois anos. Do percentual de receita perdida com fraudes de pagamento, passando pelo número de pedidos de eCommerce rejeitados até o número de pedidos de eCommerce que resultam em estornos, todos os indicadores usados para avaliar os efeitos das fraudes de pagamento aumentaram desde 2019 (vide Figura 9).

Embora esse aumento nas fraudes afete os estabelecimentos comerciais do mundo todo, os estabelecimentos da Europa, Ásia e América Latina e os de porte mediano – negócios que faturam de US\$ 5 milhões a US\$ 50 milhões – são os mais atingidos. As crescentes altas nos KPIs de gestão de fraude em todo mundo estão mais diretamente ligadas a um aumento nos indicadores dos estabelecimentos europeus, asiáticos, latino-americanos e de porte mediano, do que em qualquer outro segmento de estabelecimento comercial.

Tabela de KPIs de gestão de fraude

(Todos os KPIs são mostrados com médias truncadas)

% do faturamento de eCommerce perdido com fraudes de pagamento globalmente

% do faturamento de eCommerce perdido com fraudes de pagamento nos pedidos domésticos

Índice de rejeição de pedidos domésticos (%)

Índice de rejeição de pedidos internacionais (%)

% dos pedidos de eCommerce que se revelaram fraudulentos

% de pedidos de eCommerce que resultaram em estornos

			Por região – 2021				Por porte – 2021		
	2019	2021	América do Norte	Europa	LATAM	APAC	Grande	Mediano	PME
% do faturamento de eCommerce perdido com fraudes de pagamento globalmente	2.4	3.1	2.6	3.2	3.7	4.0	3.0	3.4	3.0
% do faturamento de eCommerce perdido com fraudes de pagamento nos pedidos domésticos	2.1	3.0	2.5	2.9	3.9	3.9	3.1	3.4	2.7
Índice de rejeição de pedidos domésticos (%)	2.5	3.0	2.8	2.8	4.0	3.8	3.3	3.7	2.4
Índice de rejeição de pedidos internacionais (%)	5.1	5.6	5.0	5.6	6.9	5.7	5.5	6.2	5.1
% dos pedidos de eCommerce que se revelaram fraudulentos	2.3	2.6	2.2	2.5	3.5	3.6	2.7	3.0	2.3
% de pedidos de eCommerce que resultaram em estornos	1.3	2.7	2.2	2.6	3.8	3.6	2.9	3.0	2.4

Figura 9

Principais conclusões derivadas dos insights e tendências acima: primeiro, as fraudes de pagamento no eCommerce estão aumentando e abocanhando uma parcela maior das vendas on-line e do faturamento dos estabelecimentos comerciais. Segundo, a pressão para que os estabelecimentos gastem mais e façam mais para gerenciar e mitigar eficazmente essa crescente ameaça ao seu negócio e aos clientes nunca foi tão forte.

Impacto das fraudes no negócio: Insights aprofundados sobre duas tendências importantes – Revisão manual e PSD2

O estudo deste ano revelou conclusões notáveis relacionadas à revisão manual e à recente implementação da alteração na Diretriz de Serviços de Pagamento, conhecida como PSD2.

Análise aprofundada da revisão manual:

- Embora menos pedidos estejam sendo revisados manualmente em 2021, o número de pedidos rejeitados aumentou, especialmente na APAC
- Muitas organizações acreditam que há lugar para revisão manual em sua estratégia de gestão de fraude, mas a grande maioria quer reduzir o uso desse processo

A revisão manual dos pedidos de eCommerce ainda é um elemento básico, mas essencial, da estratégia de prevenção de fraude de praticamente todos os empresários. Os dados mostram que, embora a proporção de pedidos revisados manualmente tenha caído de cerca de um quarto para um quinto de todos os pedidos de eCommerce, um percentual ligeiramente maior dos pedidos revisados tem sido rejeitado. Este ano, foram rejeitados 17% dos pedidos revisados, contra 12% em 2019 (vide Figura 10).

% de pedidos revisados manualmente & rejeitados posteriormente

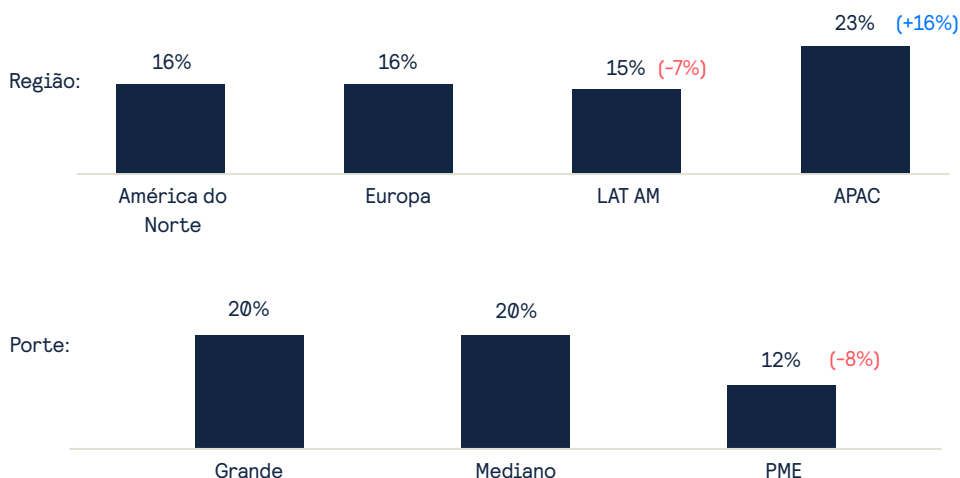


Figura 10

Além disso, embora o número de pedidos analisados manualmente em todos os estabelecimentos comerciais no mundo fique em torno de 20%, o estudo mostra que, na região APAC, o percentual de pedidos rejeitados após a análise supera, de longe, o de todas as regiões. Essa diferença só se estabeleceu nos últimos dois anos, quando o percentual de pedidos revisados e rejeitados pelos estabelecimentos comerciais da região aumentou 16%. Esse número contrasta fortemente com os índices de rejeição estáveis ou decrescentes registrados nas demais regiões, podendo até sinalizar que a maioria dos empresários da Ásia está rejeitando pedidos sistemática e automaticamente por se sentirem inseguros, uma vez que foram os mais atingidos pelo aumento das tentativas de fraude e dos gastos com gestão de fraude (como vimos na seção anterior).

Além disso, os dados revelam uma recente divergência no número de pedidos rejeitados pelos estabelecimentos comerciais de diferentes portes após a revisão: os estabelecimentos médios e grandes, por serem alvos maiores e relativamente mais atraentes para os fraudadores, continuam rejeitando um quinto dos pedidos revisados, como em 2019. As PMEs (faturamento inferior a US\$ 5 milhões/ano) reduziram em 8% seu percentual de pedidos rejeitados nos últimos dois anos e seu índice de rejeição médio é 12% (vide Figura 11). É provável que a relativa falta de medidas de prevenção de fraude sofisticadas (inclusive o uso de um menor número de ferramentas de detecção de fraude) esteja levando as PMEs a submeter uma parcela maior de pedidos legítimos à revisão manual.

% de pedidos revisados manualmente e rejeitados em 2021 – por região e segmento de porte



(Os parênteses mostram tendência dignas de nota comparadas a 2019: o texto em azul indica aumento, enquanto o texto em vermelho indica queda)

Figura 11

Estrategicamente, a revisão manual de pedidos ainda é um elemento crucial nas estratégias de gestão de fraude dos estabelecimentos comerciais, o que é evidenciado pelo fato de que, mundialmente, os empresários reservam 36% do total gasto com a gestão de fraudes de eCommerce para custos relacionados à revisão manual (Figura 12). Esse número é relativamente consistente com o de 2019, quando 42% do total gasto era reservado para custos relacionados à revisão, mundialmente.

Alocação dos gastos de gestão de fraudes de eCommerce

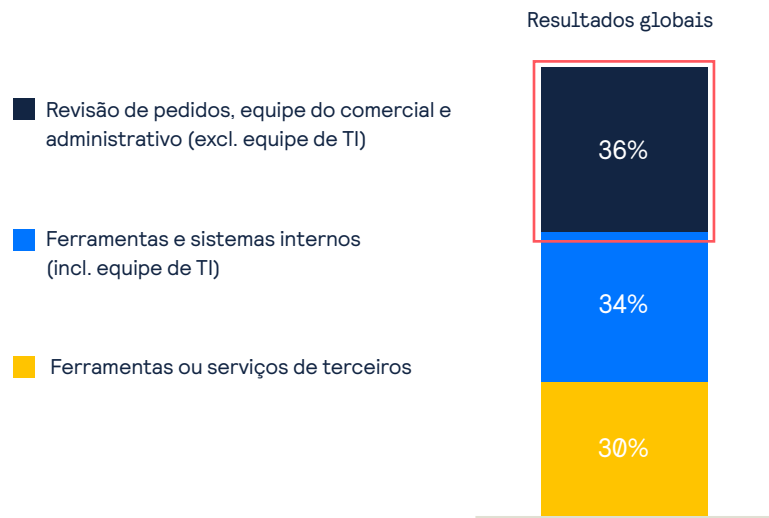
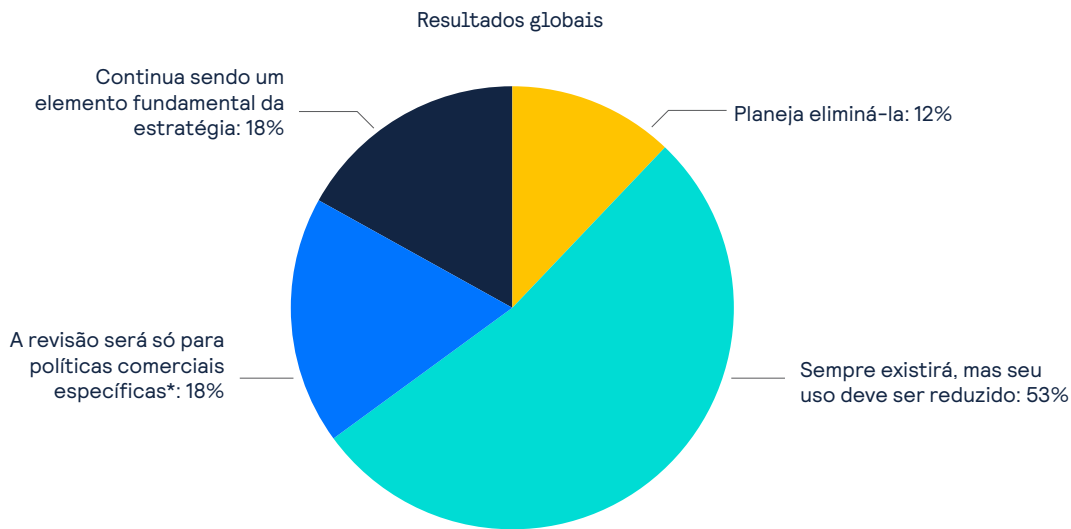


Figura 12

Os dados coletados com a pesquisa deste ano indicam que, para a maioria dos empresários, a revisão manual continuará sendo um elemento fundamental de suas estratégias de gestão de fraude. Porém, a maior parte deles planeja reduzir o tempo, a mão de obra e o dinheiro dedicado a esse processo. Mais de metade (53%) acredita que sempre realizará algum tipo de revisão, mas deseja reduzir seu uso, enquanto 18% dizem que só farão essas revisões quando políticas comerciais específicas o exigirem. Outros 12% relatam planos de eliminar a revisão manual de pedidos. Menos de um quinto (18%) dos empresários planeja manter a revisão manual como um elemento fundamental de sua estratégia de prevenção e mitigação de fraude num futuro próximo (Figura 13).

Papel da revisão manual nas estratégias de prevenção de fraude planejadas para o futuro



(*Exemplos de política: somente 1 PS5 por cliente, só enviar para certos países, etc.)

Figura 13

Análise aprofundada da PSD2:

- Os empresários se sentem cada mais preparados para a alteração da Diretriz de Serviços de Pagamento da União Europeia. A maioria acredita que a PSD2, especialmente a autenticação forte do cliente (SCA), tornará a gestão dos pagamentos e das fraudes de pagamento mais complexa.

Sobre a PSD2 e a SCA, os dados mostram que os empresários se sentem cada vez mais preparados, mundialmente. Embora a proporção de empresários que se sentem pelo menos “relativamente preparados” não tenha variado (cerca de 9 em 10 em 2019 e 2021), dois terços dizem estar “muito ou extremamente preparados” para a alteração da PSD2 e os requisitos da SCA. Isso representa um aumento significativo de 50% em relação a 2019 (vide Figura 14).

Preparação dos empresários para a PSD2 – Resultados globais

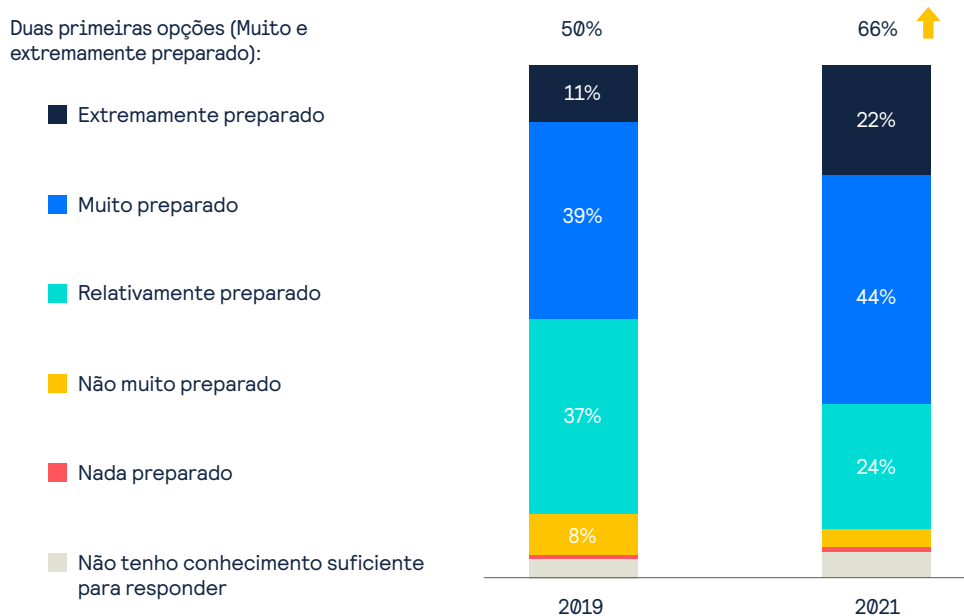


Figura 14

Embora mais empresários se sintam pelo menos muito preparados para a PSD2 e a SCA hoje, a parcela que acredita que elas terão um grande impacto na organização não variou muito em relação a 2019 – 56% este ano, contra 53% dois anos atrás. Especificamente, mais de metade (56%) dos empresários espera que a PSD2 vá “complicar a gestão dos pagamentos” e “complicar a gestão de fraude”, enquanto pouco menos de um quarto (23%) acha que ela “complicará a gestão do cumprimento de normas”.

Entretanto, tanto a preparação dos empresários para a PSD2 e SCA quanto suas expectativas em relação ao impacto da PSD2 e a SCA variam nas diferentes regiões e segmentos de porte. Os empresários da Europa, América Latina e APAC são mais propensos do que os da América do Norte a se sentir preparados e a esperar que a PSD2 tenha um grande impacto em sua organização. Mas é preciso observar que um em dez pesquisados da América do Norte não estão familiarizados com a PSD2, contra somente 1% dos pesquisados de outras regiões – provavelmente porque esses empresários norte-americanos não operam na União Europeia ou no Espaço Econômico Europeu. Da mesma forma, empresários à frente de organizações grandes e medianas têm números mais altos nesses dois indicadores atitudinais se comparados às suas contrapartes do segmento de PMEs (vide Figura 15).

Resultados por região e porte de empresa – 2021

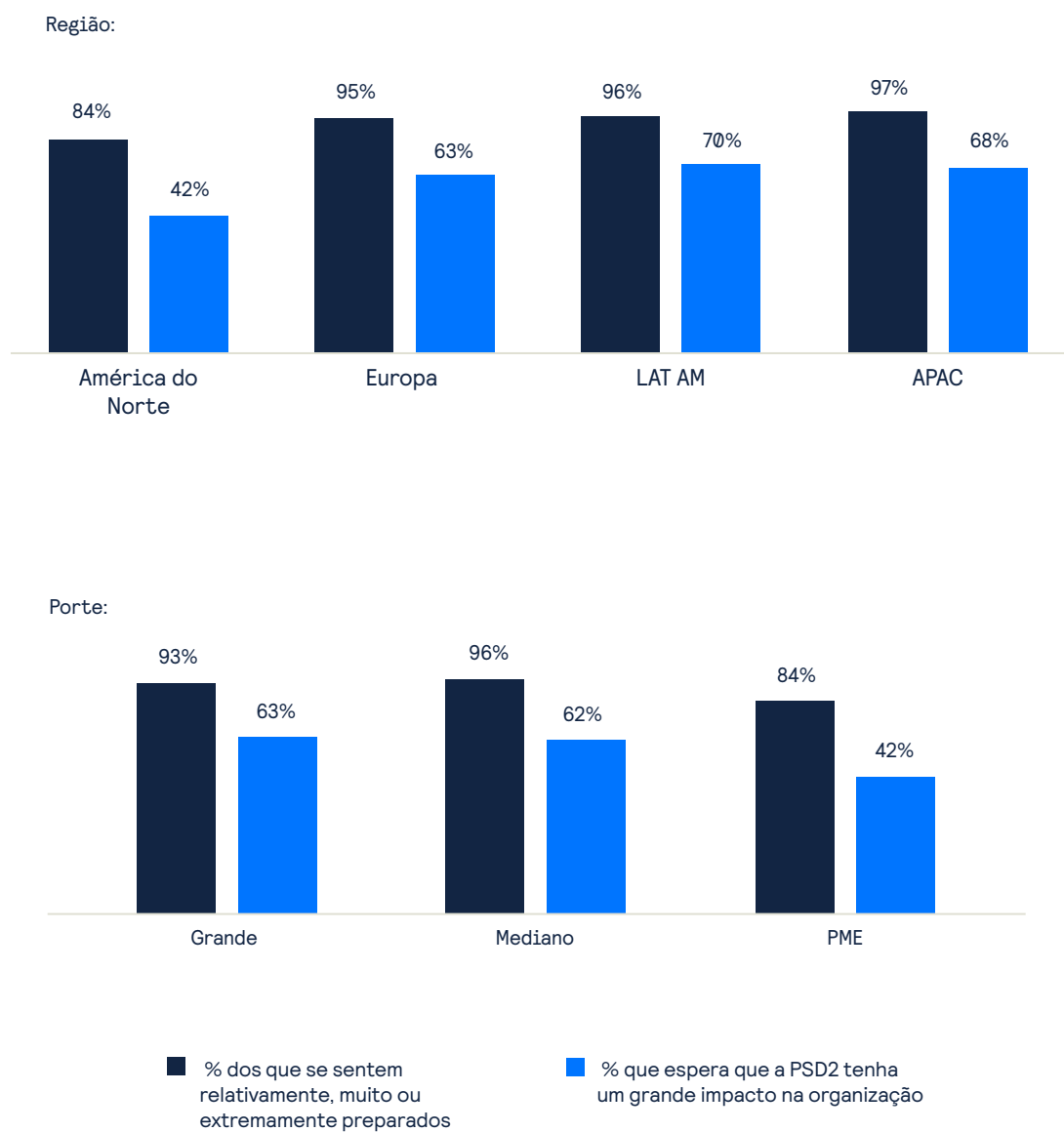


Figura 15

Variedade dos ataques de fraude: Principais conclusões



A próxima área de insight enfoca o volume e a variedade dos ataques de fraude sofridos pelos estabelecimentos comerciais, suas mudanças nos últimos anos, o que os empresários estão fazendo hoje para tentar ficar menos vulneráveis às formas de fraude mais comuns e nefastas que afetam suas organizações, e como enfrentam vários outros desafios relacionados à fraude.

01

Embora o volume de ataques de fraude tenha aumentado, eles estão menos variados (ou seja, há mais ataques, mas de menos tipos).

02

Fraude amigável, teste de cartão, phishing e roubo de identidade são hoje os tipos mais comuns de ataque, afetando percentuais maiores de estabelecimentos comerciais mundo afora.

- A maioria dos empresários tem uma estratégia formal para combater as fraudes amigáveis, enviando vários avisos aos clientes, adotando políticas claras e visíveis e verificando e analisando seu histórico de compra.
- A prevalência dos ataques de invasão de conta caiu desde 2019, em parte porque os empresários implementaram mais ferramentas para monitorar e mitigar esse tipo de fraude.

03

Os empresários precisam enfrentar outros desafios relacionados à fraude além da detecção e prevenção de fraudes e do aumento dos custos de gestão de fraude – e cada desafio tem dificuldades consideráveis a serem superadas.

Como vimos na primeira parte do relatório, em três quartos dos estabelecimentos comerciais, o volume dos ataques de fraude aumentou desde o início da pandemia de Covid. Entretanto, a variedade dos ataques diminuiu nesse mesmo período. Em 2019, os estabelecimentos comerciais foram atingidos por quatro tipos diferentes de ataque de fraude, em média. Este ano, essa média caiu para três. Em resumo, os estabelecimentos comerciais estão sendo atingidos com mais frequência, mas os tipos de ataque variam menos.

Os tipos de fraude de pagamento mais comuns também mudaram significativamente desde 2019. Hoje, a fraude amigável – que ocorre quando um cliente recebe o produto ou serviço e, na sequência, solicita o estorno da compra ao banco – e os testes de cartão desbancaram o phishing/pharming e o roubo de identidade como os dois ataques mais comuns. A fraude amigável é especialmente problemática para os estabelecimentos comerciais da América do Norte e da APAC, onde os índices relatados subiram respectivamente 9% e 16% na comparação com 2019. A Figura 16 traz dados detalhados dos tipos de ataque mais comuns.

	Posição em 2019	Posição em 2021	% global das ocorrências (2021)
Fraude amigável	5	1	39%
Teste de cartão	4	2	37%
Phishing / pharming / whaling	1	3	34%
Roubo de identidade	2	4	28%
Cupom / desconto / abuso nos reembolsos	7	5	27%
Fraude de fidelidade	10	6	27%
Invasão de conta	3	7	23%
Fraude no marketing de afiliados	6	8	21%
Golpes de triangulação	11	9	20%
Botnets	8	10	19%
Lavagem de dinheiro	12	11	16%
Reenvio	9	12	15%

= Caiu de posição = Subiu de posição

Figura 16

Há algumas variações nos tipos de fraude mais comuns sofridos pelos estabelecimentos comerciais de diferentes regiões e portes, como mostram os rankings da Figura 17. Mas embora seja importante notar as diferenças e nuances específicas de cada segmento, os dados também ressaltam a predominância universal e a relevância da fraude amigável, do phishing / pharming e do teste de cartão como os três tipos de fraude de pagamento que praticamente todo estabelecimento comercial está propenso a vivenciar, independentemente de sua localização geográfica e do seu faturamento on-line.

	Principais tipos de fraude por região				Principais tipos de fraude por porte de empresa		
	América do Norte	Europa	LATAM	APAC	PME	Mediano	Grande
1	Teste de cartão	Phishing / pharming / whaling	Fraude amigável	Phishing / pharming / whaling	Fraude amigável	Fraude amigável	Fraude amigável
2	Fraude amigável	Fraude amigável	Teste de cartão	Fraude amigável	Teste de cartão	Teste de cartão	Teste de cartão
3	Phishing / pharming / whaling	Invasão de conta	Cupom / desconto / abuso nos reembolsos	Fraude de fidelidade	Phishing / pharming / whaling	Roubo de identidade	Phishing / pharming / whaling
4	Roubo de identidade	Fraude de fidelidade	Phishing / pharming / whaling	Roubo de identidade	Roubo de identidade	Phishing / pharming / whaling	Fraude de fidelidade
5	Cupom / desconto / abuso nos reembolsos	Teste de cartão	Fraude no marketing de afiliados	Teste de cartão	Cupom / desconto / abuso nos reembolsos	Cupom / desconto / abuso nos reembolsos	Cupom / desconto / abuso nos reembolsos
				Cupom / desconto / abuso nos reembolsos			

Figura 17

A fraude amigável já é o tipo de ataque mais comum entre os estabelecimentos comerciais do mundo todo e estima-se que cerca de 1.2% dos pedidos de eCommerce aceitos se revelarão uma fraude amigável. A fraude amigável é a maior preocupação dos empresários da América Latina e da Ásia, tendo em vista o percentual de pedidos aceitos que acabam sendo estornados (Figura 18).

	Região - 2021				Porte - 2021		
	América do Norte	Europa	LATAM	APAC	Grande	Mediano	PME
	% de pedidos aceitos que se revelaram uma fraude amigável	1.0	1.3	1.6	1.5	1.3	1.4

Figura 18

Como os empresários estão respondendo ao aumento da fraude amigável em suas organizações nos últimos dois anos?

Globalmente, 80% dos empresários têm uma estratégia formal para combater a fraude amigável (contra somente 71% dos empresários da América do Norte e 68% dos empresários à frente de PMEs). Dos 4 em 5 empresários que dispõem de estratégias formais, a maioria optou por uma abordagem de várias frentes, utilizando uma série de táticas específicas — como enviar vários avisos ao cliente, adotar políticas de pagamento e devolução claras e medidas para verificar e confirmar a identidade do cliente (Figura 19).

Abordagens usadas para combater a fraude amigável – 2021

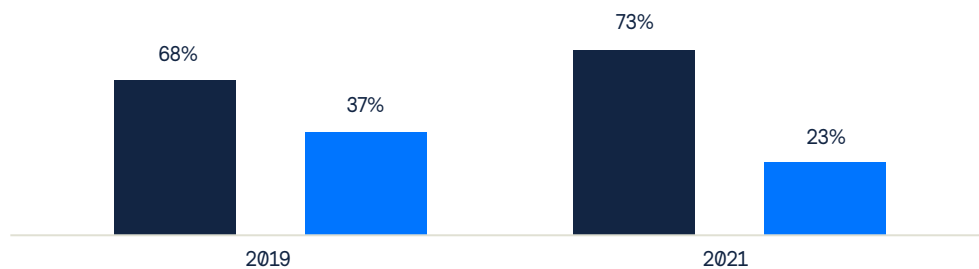


Figura 19

Embora os empresários estejam enfrentando mais fraudes amigáveis, as invasões de conta – tipo de ataque em que os fraudadores acessam ou manipulam ilegalmente os dados da conta do cliente – estão caindo. Em 2019, as invasões de conta eram o terceiro tipo de ataque de fraude mais comum, atingindo 37% dos estabelecimentos comerciais. Este ano, as invasões de conta caíram para a sétima posição e afetaram menos de um quarto (23%) dos estabelecimentos comerciais do mundo (Figura 20).

Parte da diminuição nas invasões de conta pode ser atribuída à adoção de ferramentas especializadas para monitorar e prevenir esse tipo de ataque, visto que o percentual de organizações que as usam subiu significativamente. Os estabelecimentos comerciais da América do Norte e as PMEs parecem estar atrasados em relação aos de outras regiões e segmentos de porte na implementação dessas ferramentas especializadas (vide Figura 20).

% global de organizações com ferramentas para monitorar a fraude de invasão de conta e % de organizações atingidas por fraudes de invasão de conta



% que têm ferramentas implementadas em 2021 - Por região e segmento de porte

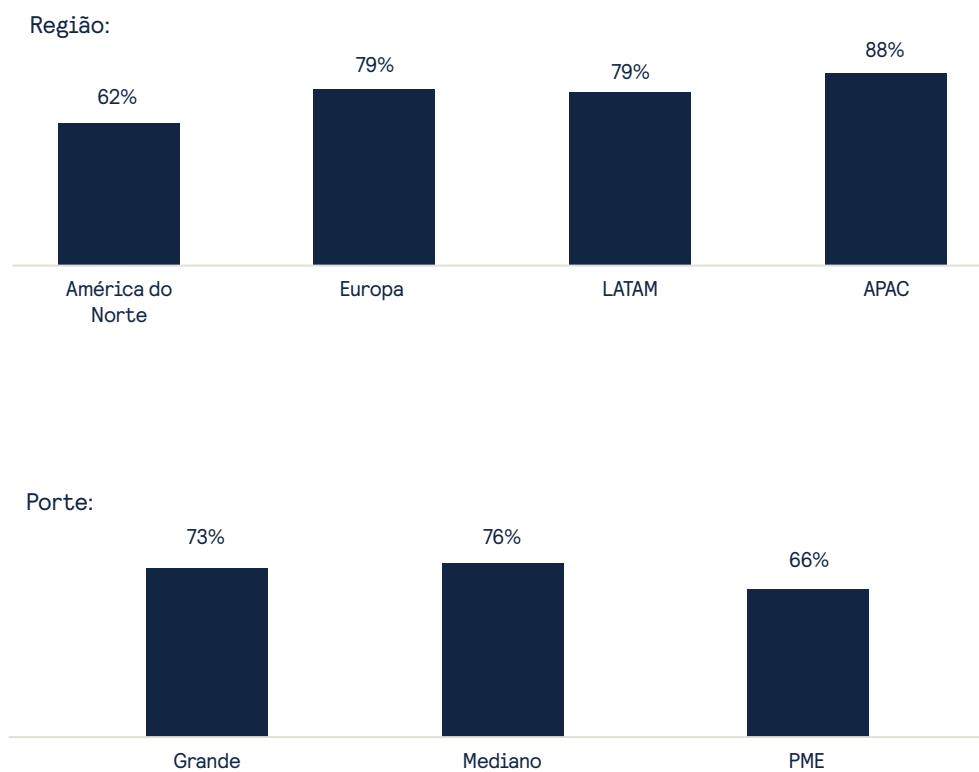


Figura 20

Um dos motivos pelo qual é tão difícil e complexo para os empresários gerenciarem as fraudes é que eles precisam lidar com uma série de outros desafios além de monitorar e prevenir as fraudes de pagamento. A Figura 21 ilustra a variedade, a incidência relativa e a gravidade desses desafios de gestão de fraude. Esses desafios atingem 92% dos estabelecimentos comerciais mundialmente.

Incidência e gravidade dos desafios de gestão de fraude enfrentados pelas organizações nos últimos 12 meses



Figura 21

Em 2021, o empresário médio enfrentou pelo menos três dos desafios acima nos últimos 12 meses e muitos estão se desdobrando para superar vários ao mesmo tempo. Os grandes estabelecimentos comerciais, por exemplo, são bem mais propensos a enfrentar a maioria dos desafios listados na Figura 21, se comparados aos medianos e às PMEs: mais de um quarto (26%) dos estabelecimentos de grande porte observou cinco ou mais dos desafios acima no último ano, contra 12% dos medianos e 9% das PMEs.

Cada desafio de gestão de fraude apresenta diferentes níveis de gravidade e/ou dificuldade para as organizações comerciais. Embora três dos cinco desafios mais comuns também sejam considerados os mais graves, há um segundo conjunto de problemas altamente nefastos – indicado pelas barras amarelas na Figura 21 – afetando um percentual menor de estabelecimentos comerciais no mundo. É importante reconhecer que, para os estabelecimentos comerciais que os enfrentam, esses desafios podem ser tão problemáticos quanto os que encabeçam a lista.

Os resultados sugerem que combater as fraudes de eCommerce com eficácia significa reduzir o volume de ataques direcionados às organizações comerciais, entender e combater diferentes tipos de ataque à medida que eles evoluem e vão surgindo, e superar vários outros desafios relacionados à fraude que prejudicam e restringem as capacidades de prevenção de fraude, em diferentes níveis.

Estratégias de prevenção de fraude: Principais conclusões



A área final deste relatório analisa as estratégias de prevenção de fraude dos empresários. Como eles estão abordando e combatendo as fraudes de pagamento no eCommerce, agora e no futuro?

01

Apesar do aumento nos ataques e na perda de receita, as práticas de gestão de fraude dos empresários têm priorizado a melhoria da experiência de compra/do cliente (em vez de minimizar os custos operacionais relacionados à fraude, por exemplo).

02

Do ponto de vista tático, os empresários estão racionalizando seus arsenais de gestão de fraude, apostando mais fortemente em um número menor de ferramentas amplamente usadas, se compararmos com 2019.

03

Com exceção da solicitação do CVN, da autenticação de dois fatores pelo telefone e da autenticação 3DS, muitas das ferramentas de detecção de fraude mais eficazes não são amplamente usadas e têm baixa probabilidade de serem adotadas no futuro.

Um ponto fundamental para entendermos as estratégias de prevenção de fraude dos empresários é conhecermos as metas ou objetivos priorizados por eles em suas estratégias de gestão de fraude. Em 2019, os dados mostravam que eles eram muito mais propensos a eleger a redução das fraudes e dos estornos como a meta estratégica primária de sua gestão de fraude.

Este ano, metade dos empresários tem como prioridade melhorar a experiência do cliente, contra 40% que continuam priorizando a redução das fraudes e meros 11% que se preocupam mais em minimizar os custos (vide Figura 22).

A Figura 22 também ilustra algumas diferenças dignas de nota nas metas estratégicas preteridas pelos empresários nas diferentes regiões, segmentos de porte e setores. Enquanto um grupo priorizou a melhoria da experiência do cliente ao traçar suas estratégias de gestão de fraude, os empresários da América Latina e os de grande porte tenderam a dar menos ênfase à redução de fraudes e estornos. Os empresários europeus, os de porte mediano, as PMEs, e os que se dedicam à venda de produtos digitais e produtos e serviços de viagem e turismo, se mostraram mais propensos a dar menos foco à redução dos custos operacionais relacionados a fraude. Os empresários da América do Norte e da APAC, bem como os que vendem produtos físicos no varejo são igualmente propensos a preterir a redução das fraudes e dos custos, pois sua prioridade é melhorar a experiência do cliente.

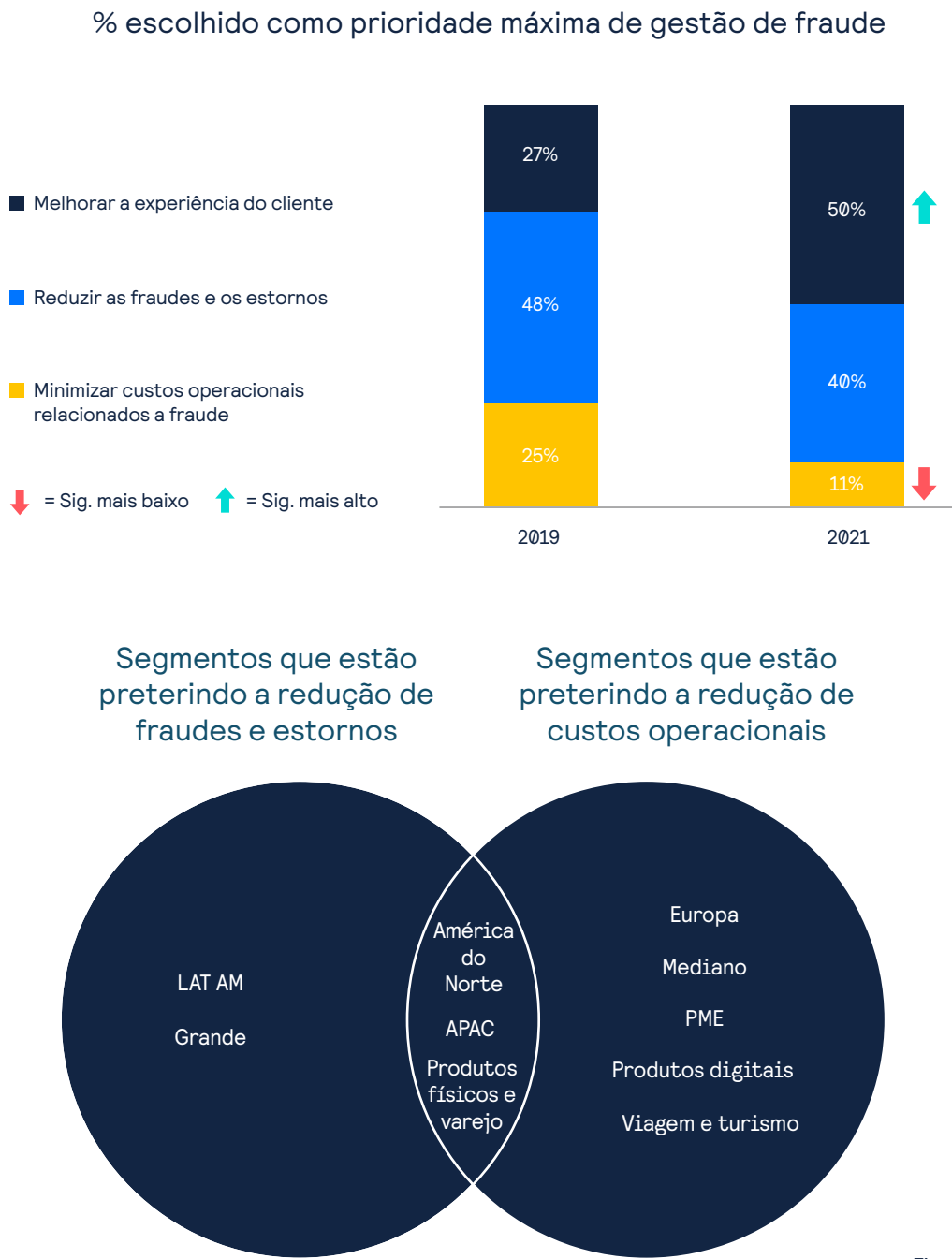


Figura 22

Essa mudança estratégica na gestão de fraude dos estabelecimentos comerciais tem por objetivo encontrar um equilíbrio entre a proteção dos ativos e das operações da empresa e oferecer uma experiência de compra e pagamento de alta qualidade aos clientes.

Nos dois últimos anos, as estratégias de prevenção de fraude dos empresários evoluíram em nível organizacional, enquanto a qualidade dos seus arsenais de gestão de fraude evoluiu taticamente. Em vez de continuarem implementando uma série de novas ferramentas e tecnologias antifraude, os empresários optaram por racionalizar as soluções de prevenção de fraude. O número médio de ferramentas em uso em cada estabelecimento comercial caiu pela metade, baixando de 10 em 2019, para 5 este ano.

As 15 ferramentas de detecção de fraude mais usadas	Posição em 2019*	Posição em 2021* % global que usam a ferramenta (2021)	% global que usam a ferramenta (2021)
CVN (número de verificação do cartão)	2	1	54%
Verificação do e-mail	3	2	43%
Histórico de pedidos do cliente	1	3	38%
Address verification service (AVS)	4	4	37%
Autenticação 3-D Secure	5	5	36%
Verificação do número do telefone / pesquisa reversa	13	6	31%
Serviços de validação do endereço postal	8	7	27%
Lista de negativados / excluídos (listas internas)	6	8	24%
Análise do comportamento do site do cliente / de padrões	10	9	23%
Listas de positivados / autorizados	9	10	21%
Monitoramento da velocidade do pedido	19	11	21%
Indicadores geográficos / mapas	17	12	18%
Geolocalização do país / cidade, etc.	7	13	18%
Autenticação de dois fatores pelo telefone (no app, via SMS, etc.)	11	14	18%
Sites de redes sociais	18	15	18%

*Somente América do Norte e Europa (para monitoramento)

■ = Caiu de posição ■ = Subiu de posição

Figura 23

As ferramentas de detecção de fraude mais comuns também não variam muito entre as regiões e segmentos de porte, como mostra a Figura 24. Mas há algumas diferenças notáveis nos tipos e na quantidade de ferramentas em que os empresários de cada grupo mais apostam: por exemplo, é mais provável que os empresários da Europa e da APAC tenham adotado a Autenticação 3DS do que os da América do Norte (na Europa, a maior adoção se deve à necessidade de cumprir as normas de SCA e a PSD2 e, na APAC, ao maior volume de ataques de fraude, como já comentado neste relatório). Além disso, na média, os grandes estabelecimentos comerciais investem em uma gama maior de ferramentas de detecção de fraude do que os medianos e as PMEs, o que é compreensível.

Ferramentas de detecção de fraude mais usadas por região

	América do Norte	Europa	LATAM	APAC
1	CVN	CVN	Verificação do e-mail	Aut. 3DS / SafeKey
2	Verificação do e-mail	Aut. 3DS / SafeKey	CVN	CVN
3	Histórico de pedidos do cliente	Verificação do e-mail	Histórico de pedidos do cliente	Verificação do e-mail
4	AVS	AVS	AVS	Verificação do nº telefone
5	Verificação do nº telefone	Histórico de pedidos do cliente	Verificação do histórico de crédito	AVS
Nº médio de ferramentas detecção usadas	5	4	6	6

Ferramentas de detecção de fraude mais usadas por segmento de porte

	PME	Mediano	Grande
1	CVN	CVN	CVN
2	Verificação do e-mail	Aut. 3DS / SafeKey	Verificação do e-mail
3	Histórico de pedidos do cliente	Verificação do e-mail	AVS
4	AVS	Histórico de pedidos do cliente	Aut. 3DS / SafeKey
5	Validação do endereço postal	AVS	Histórico de pedidos do cliente
		Verificação do nº telefone	
Nº médio de ferramentas detecção usadas	4	4	6

Figura 24

À medida que os empresários forem avaliando e implementando novas ferramentas antifraude no futuro, será importante lembrar dos dois últimos números desta seção (abaixo), que segmenta 25 ferramentas de prevenção de fraude com base no quão amplamente usadas elas são e, o mais importante, no quão eficazes os empresários afirmam que elas são para prevenir e detectar fraudes. A Figura 25 mostra o uso atual e os índices de adoção planejados das ferramentas apontadas pelos empresários como as mais eficazes para impedir fraudes, enquanto a Figura 26 mostra as mesmas estatísticas para as ferramentas que, na média, são consideradas menos eficazes.

% que usa ou planeja adotar as ferramentas de detecção de fraude “mais eficazes”

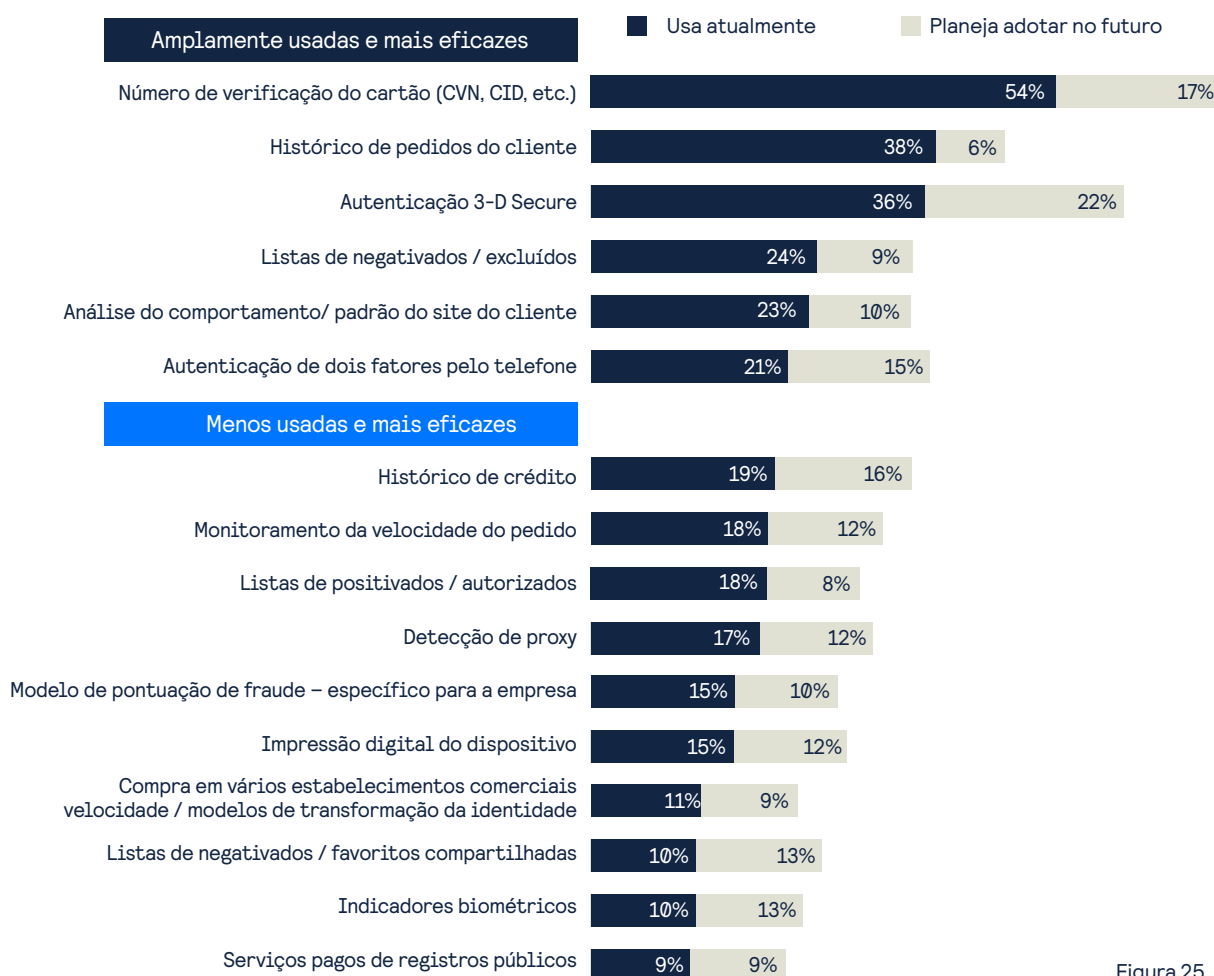


Figura 25

% que usa ou planeja adotar as ferramentas de detecção de fraude “menos eficazes”

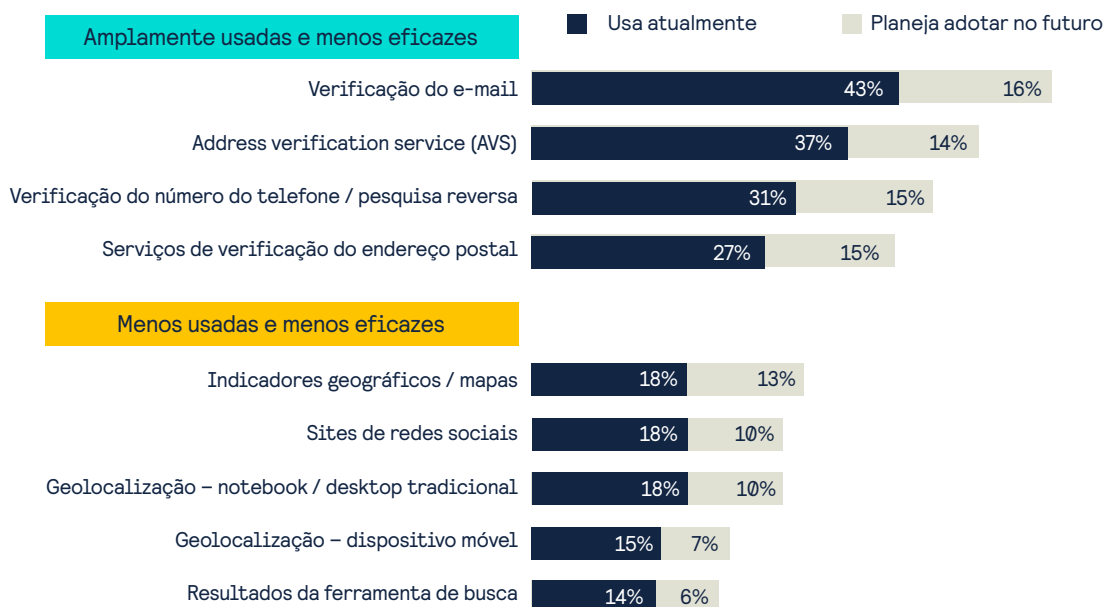


Figura 26

As Figuras 25 e 26 devem ajudar a alertar e orientar taticamente o empresário na escolha das soluções antifraude em que investirá no futuro. Os dados acima mostram que muitas das ferramentas de detecção de fraude mais eficazes não são as mais amplamente usadas hoje nem são as que os empresários mais tendem a adotar no futuro. Para evoluírem suas capacidades antifraude e atingirem os melhores resultados táticos, eles devem considerar investir em ferramentas que, embora não sejam tão amplamente usadas, são apontadas como as mais eficazes, como a verificação do histórico de crédito, o monitoramento da velocidade dos pedidos, as listas de positivados / aprovados, a detecção de proxy, a impressão digital de dispositivos e modelos de pontuação de fraude específicos da empresa.

Conclusão

Os principais resultados e conclusões discutidos neste relatório destacam como as fraudes de pagamento no eCommerce global se tornaram uma questão crítica, complexa e desafiadora para os empresários. O relatório ilustra várias tendências e indicadores positivos que, juntos, enviam um sinal positivo e animador para as capacidades coletivas dos empresários de aprimorar e evoluir, com sucesso, suas estratégias e táticas de gestão de fraude a fim de melhor protegerem suas organizações e seus clientes de ameaças e danos relacionadas às fraudes no futuro. A Cybersource está comprometida a apoiar os esforços de gestão e prevenção de fraude dos empresários e a continuar patrocinando e publicando novas pesquisas e análises sobre esses importantes tópicos nos próximos anos.

Sobre os autores



A CyberSource é uma plataforma de gestão de pagamentos global e modular alicerçada na infraestrutura da Visa com os benefícios e insights proporcionados por uma vasta rede global de processamento de US\$ 427 bilhões. Esta solução agrega agilidade às operações das empresas e as ajuda a alcançar suas metas de comércio digital, melhorando a experiência do cliente, aumentando o faturamento e reduzindo os riscos. Para os parceiros credenciadores, a CyberSource oferece uma plataforma de tecnologia, expertise de pagamento e serviços de suporte, ajudando-os a expandir e a gerenciar seu portfólio de estabelecimentos comerciais para cumprir sua promessa de marca.

Para mais informações, visite: cybersource.com



Como associação comercial independente e sem fins lucrativos, o Merchant Risk Council tem por missão facilitar a colaboração entre os profissionais das áreas de risco e pagamento de eCommerce. O MRC disponibiliza recursos valiosos o ano todo aos seus membros, como conteúdos educativos exclusivos, webinários, melhores práticas, tendências do setor, relatórios comparativos e documentos técnicos. Além disso, o MRC promove quatro conferências anuais nos EUA e na Europa, bem como vários eventos regionais de networking que permitem que os profissionais da área desenvolvam conexões mais fortes com os stakeholders do setor.

Para mais informações, visite: merchantriskcouncil.org



A B2B International é uma empresa global de pesquisa de mercado full-service, especializada em pesquisas de mercados B2B. Ajudamos nosso cliente a atingir suas metas comerciais tomando decisões mais inteligentes, orientadas por insights.

A B2B International é parte de um consórcio de agências B2B de classe mundial que se uniram para formar a Merkle B2B. O fato de sermos uma empresa da Merkle B2B nos permite oferecer a primeira solução B2B de ponta a ponta e totalmente integrada do mundo. Nossa promessa? Arquitetar as melhores experiências para clientes B2B.

Para mais informações, visite: b2binternational.com

Apêndice – Perguntas da pesquisa

Esta seção mostra as perguntas realizadas aos participantes da pesquisa a fim de coletar os dados mostrados neste relatório.

Figura 1: Em que país você está?

Figura 2: Por favor, estime o faturamento anual de eCommerce de sua organização. Entenda 'eCommerce' como qualquer canal usado pelo cliente para fazer um pedido fora da loja. Pode ser seu site ou um dispositivo móvel.

Figura 3 – “Canal operado”: Quais dos seguintes canais de compra sua organização opera?

Figura 3 – “Monitoramento de fraude: Sua organização monitora as fraudes de pagamento em quais dos canais a seguir?

Figura 4: Qual a importância da gestão das fraudes de eCommerce para a estratégia empresarial geral de sua organização?

Figuras 5 e 6:

- Impacto da Covid nas tentativas de fraude: Qual foi o impacto da pandemia de Covid no volume de tentativas de fraude sofridas por sua organização?
- Impacto da Covid no percentual de fraude em relação ao faturamento: Qual foi o impacto da pandemia de Covid no percentual do faturamento anual de eCommerce perdido com fraudes de pagamento de forma global, ou seja, o percentual de fraude em relação ao faturamento?

Figuras 7 e 8: Indique o percentual do faturamento anual de eCommerce que sua organização gasta para gerenciar as fraudes de pagamento – sem incluir as perdas efetivas com fraude.

Figura 9:

- % do faturamento de eCommerce perdido com fraudes de pagamento globalmente: Indique o percentual do seu faturamento anual de eCommerce perdido com fraudes de pagamento globalmente, ou seja, o percentual de fraude em relação ao faturamento.
- % do faturamento de eCommerce perdido com fraudes de pagamento nos pedidos domésticos: Indique o percentual do seu faturamento anual de eCommerce perdido com fraudes de pagamento nos pedidos domésticos.
- Índice de rejeição de pedidos domésticos: Indique seu índice de rejeição de pedidos domésticos, ou seja, o percentual de pedidos rejeitados por suspeita de fraude.
- Índice de rejeição de pedidos internacionais: Indique seu índice de rejeição de pedidos internacionais, ou seja, o percentual de pedidos rejeitados por suspeita de fraude.
- % dos pedidos de eCommerce que se revelaram fraudulentos: Indique o percentual de pedidos de eCommerce aceitos em um ano que se revelaram fraudulentos.
- % de pedidos de eCommerce que resultaram em estornos: Informe o percentual de pedidos de eCommerce para os quais o cliente solicitou estorno alegando fraude nos últimos 12 meses.

Figura 10:

- % de pedidos revisados manualmente: Indique o percentual de pedidos de eCommerce analisados manualmente por suspeita de fraude.
- % de pedidos rejeitados posteriormente: Considerando os pedidos de eCommerce revisados manualmente por sua organização, indique o percentual de pedidos rejeitados (cancelados) por suspeita de fraude.

Figura 11: % de pedidos revisados manualmente que são rejeitados: Considerando os pedidos de eCommerce revisados manualmente por sua organização, indique o percentual de pedidos rejeitados (cancelados) por suspeita de fraude

Figura 12: Alocação dos gastos de gestão de fraudes de eCommerce: Indique o percentual dos seus gastos anuais com a gestão de fraudes de eCommerce alocado em cada uma destas áreas:

Figura 13: Papel da revisão manual nas estratégias de prevenção de fraude planejadas para o futuro: Como sua organização planeja incorporar a revisão manual na estratégia de prevenção de fraude planejada para o futuro?

Figura 14: O quanto a sua organização está preparada para a PSD2?

Figura 15:

- Preparação para a PSD2: O quanto a sua organização está preparada para a PSD2?
- % que espera que a PSD2 tenha um grande impacto na organização: Que tipo de impacto você espera que a PSD2 tenha em sua organização? [Opção de resposta: Grande impacto]

Figuras 16 e 17: Quais dos seguintes ataques de fraude atingiram sua organização, se aplicável?

Figura 18: Indique o percentual de pedidos de eCommerce aceitos nos últimos 12 meses que se revelaram uma fraude amigável / fraude de estorno, ou seja, compras que o cliente pediu para o banco estornar após receber o produto/serviço.

Figura 19: Quais dos seguintes descrevem a atual estratégia da sua organização para combater a fraude amigável / fraude de estorno, ou seja, para evitar que o cliente receba o produto ou serviço e, na sequência, peça para o banco estornar a compra?

Figura 20:

- % de organizações que dispõem de ferramentas para monitorar fraudes de invasão de conta: Você dispõe de ferramentas para monitorar a fraude de invasão de conta durante o processo de criação da conta e login do cliente? [Opção de resposta: Sim]
- % de organizações atingidas por fraudes de invasão de conta: Quais dos seguintes tipos de ataque de fraude atingiram sua organização, se aplicável?

Figura 21:

- Incidência dos desafios de gestão de fraude: Quais dos seguintes desafios relacionados à gestão de fraude de eCommerce, se aplicável, sua organização enfrentou nos últimos 12 meses?
- Gravidade dos desafios de gestão de fraude: E quão desafiador foi para a sua organização gerenciar cada item a seguir? [A escala variou de “extremamente desafiador” a “nem um pouco desafiador”]

Figura 22: Qual prática de gestão de fraude você elegeria como a mais importante para sua organização, considerando suas práticas de gestão de fraude?

Figuras 23 e 24: Indique as ferramentas de detecção de fraude usadas atualmente por sua organização.

Figuras 25 e 26:

- Ferramentas usadas atualmente: Indique as ferramentas de detecção de fraude usadas atualmente por sua organização.
- Ferramentas que as organizações planejam adotar no futuro: Você indicou que sua organização não usa nenhuma das ferramentas de detecção de fraude a seguir atualmente. Quais ferramentas sua organização planeja começar a usar no futuro, se aplicável?
- Eficácia das ferramentas: Qual a eficácia de cada uma das seguintes ferramentas na detecção das fraudes de pagamento de eCommerce? [A escala variou de “extremamente eficaz” a “nada eficaz”]

Para mais informações,
visite: cybersource.com

