Antifraude Omnichannel

Como impedir que a fraude atravesse seus canais

A digitalização trouxe consigo mudanças que transformaram substancialmente a maneira como clientes e empresas se relacionam. **A integração entre canais físicos e digitais diversificou os pontos de relacionamento, tornando a jornada do consumidor muito mais fluida e conectada.**

No entanto, essa conexão entre canais, que deveria ser explorada de forma positiva e gerar mais conveniência, passou a representar uma oportunidade para os fraudadores. Atualmente, os ataques fraudulentos ocorrem de maneira coordenada e transversal à jornada do cliente, iniciando em um ponto supostamente legítimo e se concretizando em outro, aproveitando as vulnerabilidades existentes entre os diversos canais de relacionamento com o cliente.

Nesse cenário, adotar estratégias antifraude segmentadas não só é insuficiente, como pode representar um risco suplementar para o negócio, ampliando custos operacionais, falsos positivos e as barreiras na experiência do cliente, fatores estes que se opõem ao que o ambiente omnichannel exige.

Neste ebook, apresentamos os principais desafios da prevenção à fraude em contextos omnichannel e como uma abordagem unificada, baseada em indicadores de risco cruzados, comportamento do usuário e decisões em tempo real, é fundamental para um combate eficaz a essas ameaças.

Boa leitura!

O desafio da fraude no ambiente omnichannel

À medida que o conceito de omnicalidade avança entre as organizações, crescem também os ataques disponíveis para fraudadores, tornando a segurança digital ainda mais complexa e desafiadora.

O Relatório Global de Tendências de Fraude Omnichannel da TransUnion revela que o Brasil está entre os países que mais sofrem com fraudes digitais. Os dados da pesquisa apontam que:

40% dos brasileiros entrevistados afirmaram já ter sido alvo de fraudes digitais.

R$ 6.331,00 a perda financeira média associada a essas ameaças.

equivalente a 4 salários mínimos

Entre os principais desafios da fraude no ambiente omnichannel está a **fragmentação operacional dos canais de relacionamento com os clientes.** Cada canal, seja ele físico, mobile, web ou por integração via API, possui seu próprio fluxo operacional e sistema antifraude. Ao operar de forma isolada, **esses canais abrem lacunas dificilmente perceptíveis em análises pontuais,** resultando em falhas no monitoramento que podem ser exploradas pelos fraudadores, elevando a exposição a fraudes digitais sofisticadas.

Outro ponto crítico para as empresas envolve a natureza progressiva dos ataques fraudulentos nesse cenário. **Em grande parte dos casos, as fraudes evoluem ao longo da jornada, com início em um canal mais vulnerável, e seguem até se concretizar em outro ponto de contato mais robusto.** A ausência de um compartilhamento unificado de informações de risco entre os canais forma silos de dados isolados, que dificultam a obtenção de um panorama geral das ações fraudulentas, tornando a detecção e prevenção das fraudes ainda mais desafiadora.

Consequentemente, as fraudes digitais acabam afetando diretamente as instituições, gerando prejuízos complexos que vão além de perdas financeiras. Seus impactos também são sentidos:

Operacional

Com o aumento de falsos positivos, maiores custos de logística reversa e complexidade na verificação de dados.

Financeiro

Com maior índice de chargebacks e disputas, além de altas despesas com novas tecnologias antifraude.

Operacional

Com o aumento de falsos positivos, maiores custos de logística reversa e complexidade na verificação de dados.

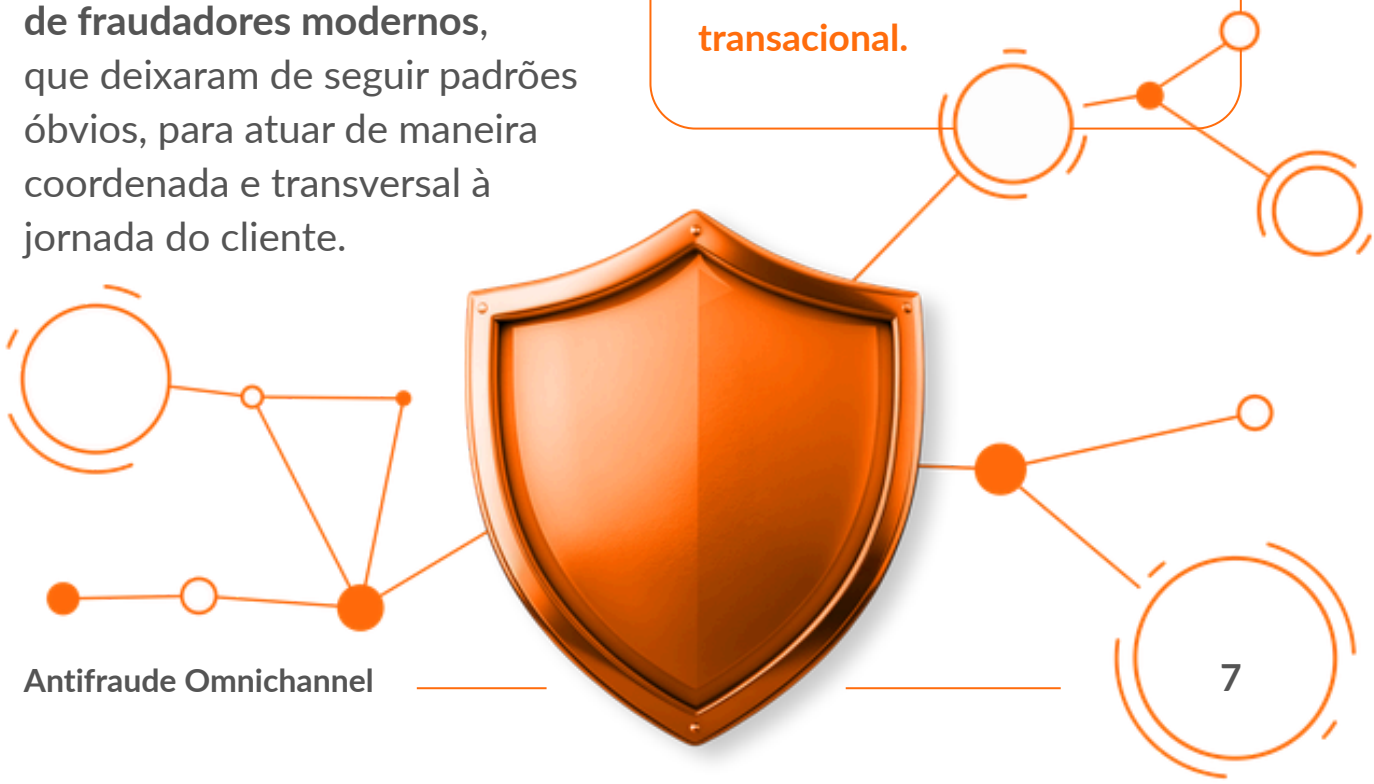
Além disso, fraudes digitais também podem ocasionar penalidades regulatórias e danos reputacionais irreparáveis, tornando a necessidade de equilibrar segurança e fluidez em uma jornada sem fronteiras entre os canais algo desafiador, porém essencial para as empresas.

Por que estratégias antifraude por canal falham

No ambiente omnichannel, as estratégias de segurança que focam em um único canal se mostram ineficientes por várias razões.

Os sistemas antifraude tradicionais normalmente operam com base em regras específicas para cada canal. Desse modo, ainda que funcionem de maneira isolada, **essa arquitetura de segurança possui dificuldade para detectar e combater ataques de fraudadores modernos**, que deixaram de seguir padrões óbvios, para atuar de maneira coordenada e transversal à jornada do cliente.

As estratégias antifraude por canal também são falhas porque não conseguem ter uma visão unificada do comportamento dos clientes. Sistemas que analisam riscos de modo isolado ignoram o fato de que o comportamento do cliente ao longo da jornada é contínuo, e não segmentado. Eles não analisam suas interações, padrões de uso e nem seu contexto transacional.



Consequentemente, **a falta dessa visão integrada impede que as estratégias antifraude por canal consigam diferenciar um usuário legítimo de fraudadores que simulam normalidade em etapas isoladas**, tornando os modelos tradicionais ultrapassados e pressionando as empresas a adotar uma arquitetura de segurança mais robusta.

dos alertas de sistemas antifraude tradicionais se revelam falsos positivos.

Fonte: Anti-Money Laundering Trends and Challenges

Esses bloqueios indevidos geram fricções desnecessárias que não só comprometem a experiência do cliente, como resultam **em perdas significativas de receita e escalabilidade operacional.** No contexto omnichannel, isso se torna tão prejudicial, quanto o risco de fraude em si.

Indicadores de risco omnichannel que realmente importam

Para prevenir ataques fraudulentos modernos com agilidade, é preciso ir além da análise de eventos isolados. Nesse caso, é necessário correlacionar de forma inteligente os sinais sutis de risco no decorrer da jornada do cliente, que incluem:

1

Mudança de canal + comportamento atípico

Comportamentos inconsistentes e mudanças de canal, como alterações cadastrais, tentativas de redefinições de credenciais de acesso ou transações que normalmente eram feitas em um canal, mudam abruptamente para outro, podem ser sinais de evasão de controles. Reconhecê-los permite que a empresa reforce sua camada de segurança contra roubos de contas e outras ameaças.

2

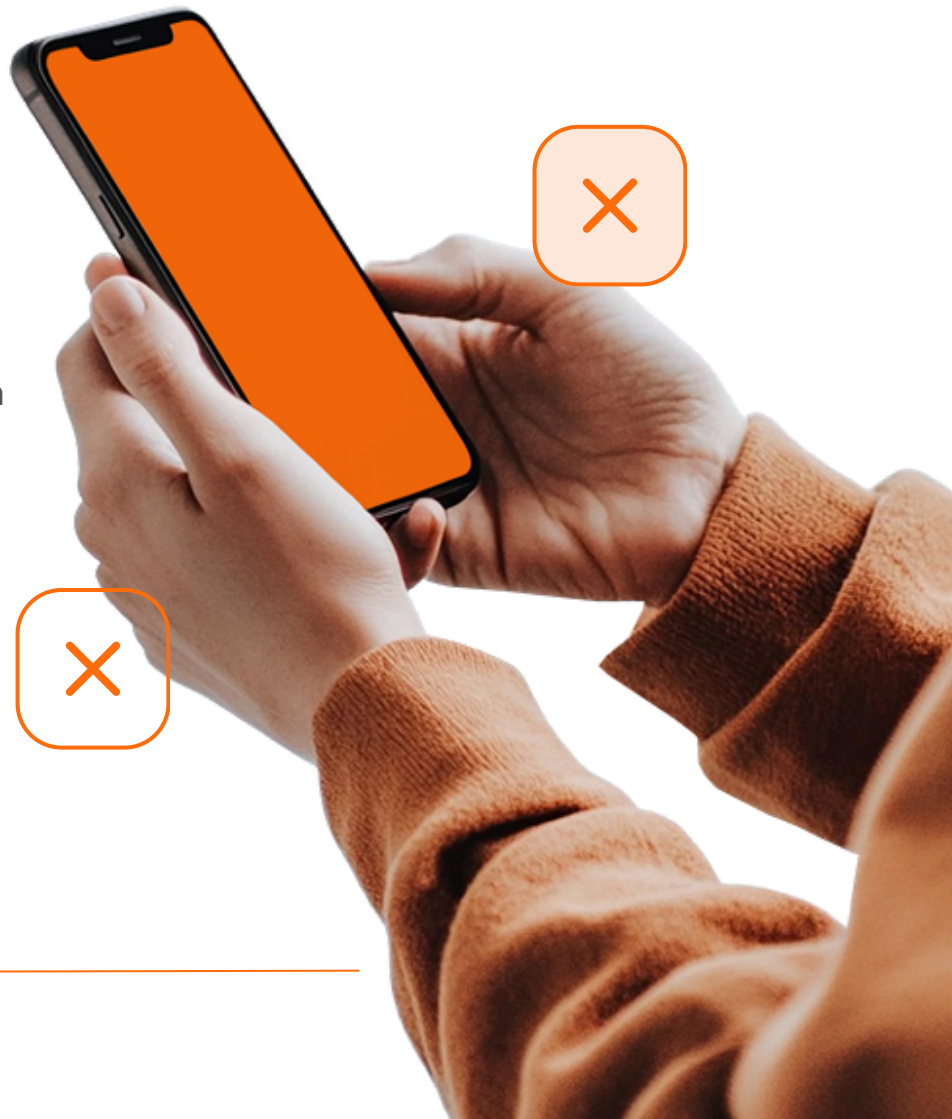
Reuso de dispositivos em canais diferentes

Fraudadores normalmente reutilizam um mesmo dispositivo para testar múltiplas identidades ou credenciais roubadas em canais diferentes. É o que acontece quando, por exemplo, um usuário que acessa sua conta pelo celular, aparece tentando acessar suas credenciais por um computador de um local distante. Este é um sinal de risco relevante, que se identificado de modo precoce, ajuda a prevenir fraudes omnichannel.

3

Tentativas de autenticação inconsistentes

Erros simultâneos de autenticação seguido por um acesso repentino na credencial de acesso, podem sugerir tentativa de fraude. Do mesmo modo, variações no método de acesso e alterações no padrão de navegação da conta, como preenchimentos rápidos de formulários e acessos a seções incomuns, também sinalizam anomalias de comportamento que podem auxiliar na detecção de golpes em estágio inicial.



4

Padrões transacionais cruzados

Transações que parecem legítimas quando feitas isoladamente, podem se tornar suspeitas quando realizadas múltiplas vezes em um curto espaço de tempo e envolvendo altos valores. Esse padrão geralmente é adotado pelos fraudadores como forma de aplicar golpes nas contas, antes que o sistema detecte a ação fraudulenta, mas podem ser detectadas ao comparar o histórico de transações do usuário em outros canais ou momentos da jornada.

Abordagens modernas de antifraude omnichannel se apoiam nesses indicadores para fazer uma análise integrada de múltiplas dimensões de risco, correlacionando transações financeiras, comportamentos do usuário e dispositivos com foco na identificação de padrões que modelos isolados não conseguem detectar.

Esse é um fundamento central de plataformas como o Risk Center 360, que foi desenvolvido para avaliar sinais dispersos simultaneamente, em tempo real, e prevenir fraudes equilibrando segurança e inovação, com uma experiência positiva na jornada dos clientes.

Framework Evertec de Antifraude Omnichannel

Ser eficaz em uma abordagem de antifraude omnichannel exige bem mais do que implementar múltiplas ferramentas de segurança. É preciso contar com um framework integrado, que seja capaz de acompanhar as complexidades e sustentar decisões ao longo de toda a jornada do cliente.

Modelos flexíveis, que permitem a integração com múltiplos canais e ambientes também são necessários. Isso elimina silos operacionais, além de ampliar a consistência nas decisões, sendo um fator crucial para escalar operações com segurança e sem prejudicar a experiência do cliente.

Soluções completas de antifraude, como o Framework Evertec, também devem ser capazes de oferecer:

- Uma visão 360° de risco, baseada em uma análise consolidada de dados em tempo real. Isso permite a detecção de padrões anômalos de forma precisa, independentemente do canal de origem.
- Monitoramento contínuo, com capacidade de resposta em tempo real e que permita identificar tentativas de fraude a partir do reconhecimento de dispositivos e mudanças em padrões de uso para interrupção de ataques antes que se concretizem.
- Tokenização para proteger informações sensíveis e atender critérios regulatórios, mitigando potenciais riscos de conformidade

Checklist final: sua operação está preparada?

Em um cenário omnichannel, os ataques fraudulentos ultrapassam fronteiras, atravessando canais, explorando vulnerabilidades e se adaptando com rapidez a controles fragmentados. Nesse contexto, é de suma importância avaliar se sua empresa está protegida contra essas ameaças. **Para isso, considere as questões ao lado.**

Se a resposta for não para a maioria dessas perguntas, isso significa que sua empresa necessita de uma mudança clara de estratégia, que avance rumo a uma abordagem mais integrada e voltada para experiências mais coerentes e seguras.

- Você possui uma visão unificada do cliente, independentemente do canal onde a interação aconteça?
- Os sistemas antifraude da sua empresa correlacionam transações, comportamento e dispositivos de forma integrada?
- As decisões sobre análise de risco são consistentes entre os canais, ou sofrem variações de acordo com o ponto de contato?
- O monitoramento de ameaças ocorre em tempo real ou de forma reativa?
- Sua estratégia antifraude é escalável com o crescimento digital, sem elevar falsos positivos e fricções ao longo da jornada do cliente?

evertecinc.com