Aitē PARTNER. ADVISOR. CATALYST.

Cómo aprovechar la administración de fraude para hacer crecer tu negocio de eCommerce

ABRIL DE 2021

Preparado para:

cybersource
A Visa Solution

ÍNDICE DE CONTENIDOS

LISTA DE FIGURAS

RESUMEN EJECUTIVO

El informe *Cómo aprovechar la administración de fraude para hacer crecer tu negocio de eCommerce*, encomendado por Cybersource —una solución Visa— y desarrollado por Aite Group, analiza los cambios que se están produciendo en las actitudes respecto de la prevención de fraudes. En lugar de limitarse a minimizar las pérdidas por fraude, las empresas más modernas están aprovechando para expandir su negocio y maximizar sus ventas.

Estas son algunas de las principales conclusiones del estudio:

- El fraude en transacciones con tarjeta no presente (CNP) sigue siendo un riesgo comercial y financiero para los comercios.
- El uso de contraseñas débiles y la repetición de contraseñas en distintos sitios facilitan el acceso de los estafadores a las cuentas online.
- Un método emergente para abordar el fraude en CNP consiste en conformar hubs de orquestación que reúnan soluciones tanto a nivel de cuenta como de transacción en un solo sistema cohesivo.
- La prevención de fraude ya no tiene que ver con elegir entre reducir los índices de fraude o aumentar las tasas de aprobación de órdenes. Los comercios están buscando un equilibrio entre ambas cosas.
- Los departamentos de prevención de fraude se están reinventando y dejando de ser una función dentro del área de operaciones. Cada vez más trabajan en conjunto con los departamentos de finanzas, ventas y marketing para reducir el abandono de carritos de compra e impulsar los ingresos.

INTRODUCCIÓN

El eCommerce experimentó una explosión mundial cuando empresas de todos los tamaños comenzaron a vender productos físicos y digitales online. La pandemia de COVID-19 aceleró bastante el auge del comercio digital, y los estafadores no demoraron en aprovechar las debilidades existentes y buscar métodos nuevos y creativos para cometer sus delitos. Los comercios se enfrentan constantemente al desafío de hallar el equilibrio correcto entre brindar al cliente una experiencia inmejorable y minimizar las pérdidas por fraude. Tradicionalmente, durante el recorrido del cliente, hay dos instancias en las que se evalúa el riesgo: al iniciar sesión y al hacer la compra. Los departamentos de prevención de fraudes, que suelen estar vinculados con operaciones, generalmente se enfocan en detener a los estafadores —y así se han ganado la fama de ser el equipo de "prevención de ventas"—. Sin embargo, las empresas más visionarias han transformado la prevención de fraude en un área crítica, y la han aprovechado para aumentar los ingresos mediante la aprobación de más órdenes legítimas y una continua gestión de riesgo en todo el recorrido del cliente. Este documento analiza una nueva manera de encarar la prevención de fraude y el modo en que los comercios, sea cual fuere su envergadura, pueden posicionarse para crecer en eCommerce.

METODOLOGÍA

Este informe se basa en investigaciones primarias y secundarias que llevó a cabo el Aite Group, así como sesiones informativas con una cantidad de comercios y proveedores de soluciones.

LA EXPLOSIÓN DEL ECOMMERCE

Si bien el eCommerce lleva ya varios años de crecimiento constante, esa tendencia se aceleró con la pandemia cuando el mundo pasó, casi del día a la noche, a ser una economía digital-first. Durante la última década, los porcentajes de crecimiento de las ventas online oscilaron en torno al 16%, mientras que los de las ventas presenciales fueron menores del 10%. En 2020, las ventas por eCommerce en todo el mundo tuvieron un crecimiento asombroso del 27.6% (Figura 1).

Figura 1: Crecimiento de las ventas minoristas regionales por eCommerce en 2020

Fuente: eMarketer e InsiderIntelligence.com

América Latina, EUA y Canadá, y Europa Central y del Este van a la cabeza con un crecimiento del eCommerce que supera el promedio mundial. En EUA, las ventas por eCommerce crecieron casi un 32%, y un supermercado llegó a figurar entre los primeros diez minoristas digitales gracias a su servicio de compra online y retiro sin contacto. En el lapso de tres meses, la pandemia impulsó en EUA un crecimiento de las ventas online que de otro modo habría demorado diez años.

Los dispositivos móviles y los servicios de fulfillment son un factor que ha dado un gran impulso a las ventas online, especialmente en áreas del mundo que no cuentan con telecomunicaciones tradicionales con línea fija. A diciembre de 2020, 5.240 millones de personas tienen un smartphone; esto representa el 67% de la población mundial.[1] Gracias a los dispositivos móviles y los servicios de entregas a domicilio, las personas de América Latina, Medio Oriente y África, así como aquellas que viven en zonas apartadas, no urbanas del mundo, pudieron acceder a

1. "*How Many Smartphones Are in the World?*" BankMyCell, acceso del 12 de enero de 2021, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.

mercados y comercios que anteriormente estaban fuera de su alcance. Se prevé que, para 2023, el 22% de todas las ventas minoristas se realizará online.[2]

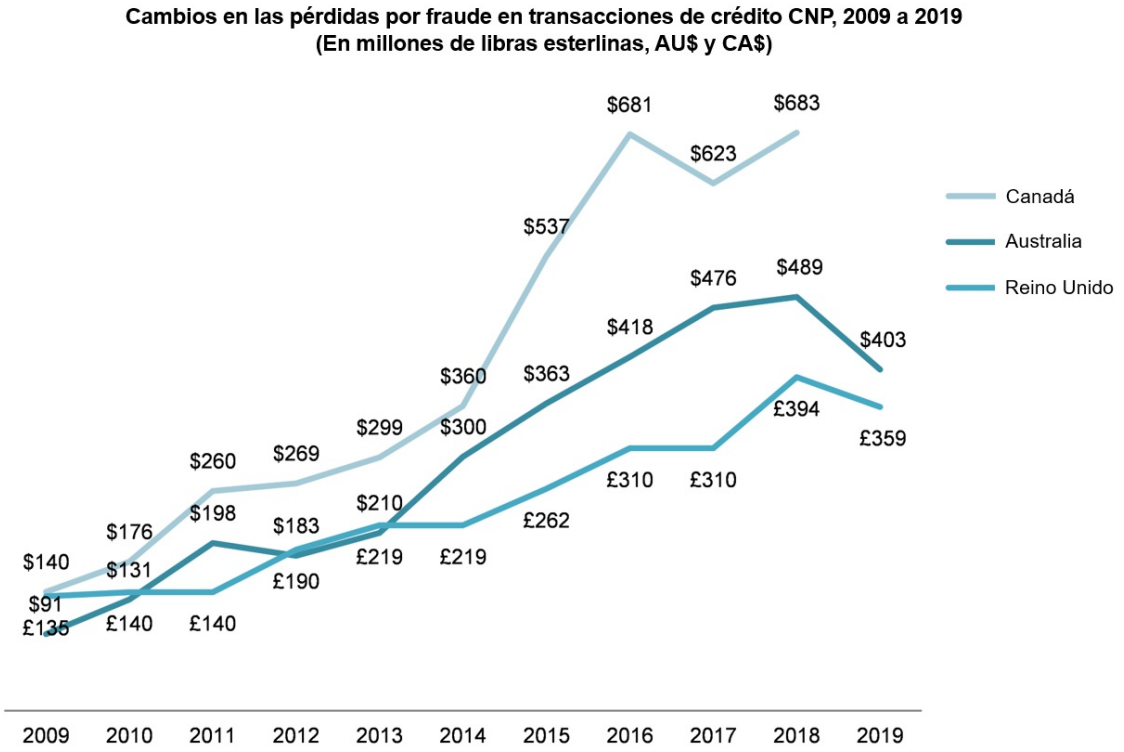
ADÓNDE VA EL DINERO

Así como las empresas tienen plena conciencia del aumento en las ventas online, también la tienen los estafadores. Los pagos con tarjeta, que son el principal método de pago en el caso de las compras online, no están protegidos por la tecnología EMV y, por ende, son un blanco fácil. Las marcas de tarjetas protegen a los tarjetahabientes contra las transacciones fraudulentas mediante una política de responsabilidad cero. Las marcas han definido una serie de reglas que asignan la responsabilidad pecuniaria a la institución financiera o bien al comercio. En términos generales, el fraude en eCommerce constituye un pasivo financiero, y con el crecimiento de este tipo de fraude, los comercios están en busca de soluciones para protegerse. Esto no resulta sorprendente si se tiene en cuenta que las pérdidas por fraude en eCommerce oscilan entre US$20.000 millones y US$30.000 millones cada año.

Algunos países son mejores que otros a la hora de mitigar el fraude en eCommerce. El Reino Unido, Australia y Canadá tuvieron aumentos anuales en fraude en transacciones de crédito CNP desde 2009 hasta mediados a fines de la década de 2010. En los últimos años, estas pérdidas disminuyeron gracias a iniciativas del sector, a disposiciones gubernamentales, o a una combinación de ambas cosas (Figura 2).

2. Daniela Coppola, "*E-Commerce Share of Total Retail Sales Worldwide From 2015 to 2023*," Statista, 26 de noviembre de 2020, acceso del 12 de enero de 2021, https://www.statista.com/statistics/534123/eCommerce-share-of-retail-sales-worldwide/.

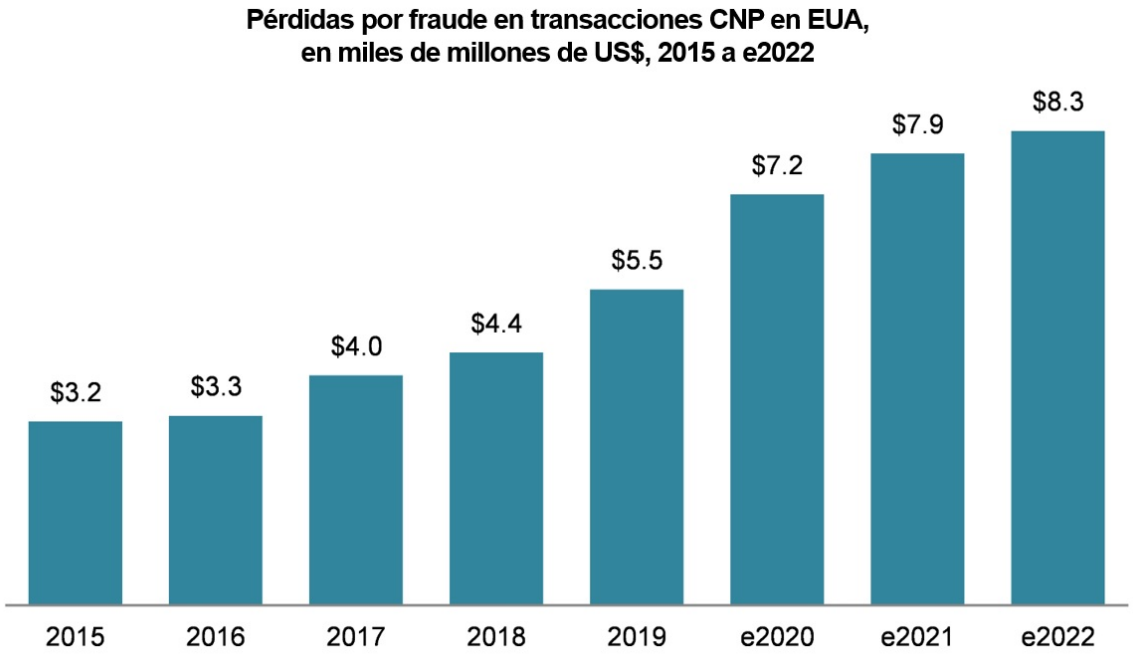
Figura 2: Cambios en las pérdidas por fraude en transacciones de crédito CNP



Fuente: UK Finance, AusPay, Canadian Banking Association

En EUA, las pérdidas por fraude en transacciones de crédito CNP han ido aumentando de forma anual durante una cantidad de años, y se prevé que seguirán en aumento hasta 2022. Esto se debe, en parte, a que a los comercios les preocupa que las medidas de seguridad puedan tener un impacto negativo en la experiencia del consumidor al sumar fricción al proceso de compra y checkout. (Figura 3).

Figura 3: Pérdidas por fraude en transacciones CNP en EUA

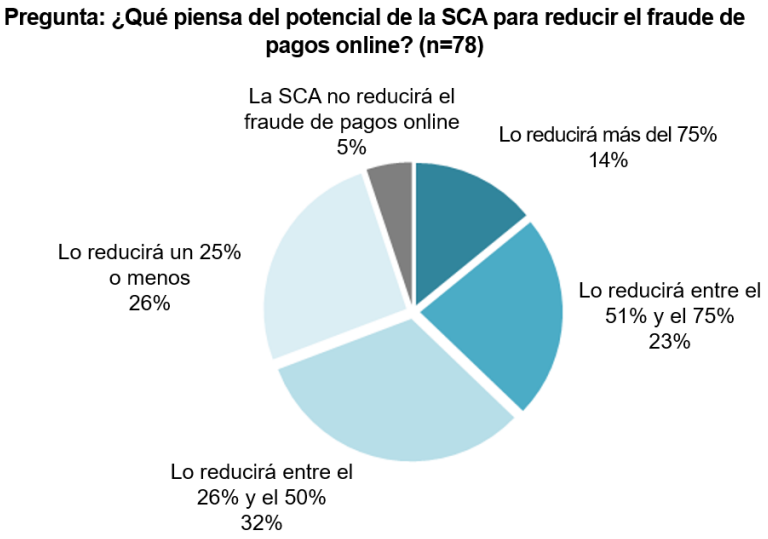


Fuente: Aite Group

La Unión Europea (UE) adoptó nuevos requisitos para reducir el fraude en eCommerce. En la mayoría de los países de la UE, el componente de autenticación reforzada de clientes (*strong customer authentication*, SCA) de la versión revisada de la Directiva sobre servicios de pago (PSD2) entró en vigencia el 1.º de enero de 2021. Algunas excepciones destacables, con sus respectivas fechas de entrada en vigencia, son Alemania (15 de marzo de 2021), Francia e Italia (1.º de abril de 2021) y el Reino Unido (14 de septiembre de 2021). Las empresas que operen en la UE deben implementar la SCA en esas fechas. Esta forma superior de autenticación del consumidor brinda protección adicional a las transacciones por eCommerce para reducir las pérdidas por fraude en transacciones CNP. Tras una encuesta a 88 ejecutivos europeos del área de pagos realizada en noviembre de 2019, Aite Group y la conferencia *Merchant Payment Ecosystem* (MPE) hallaron una amplia variedad de opiniones sobre los beneficios que aportará la SCA (Figura 4).[3] El resto del mundo observa con atención para ver cómo se desempeña la SCA y cuál será, en última instancia, su impacto en las pérdidas por fraude.

3. Véase el reporte de Aite Group *Strong Customer Authentication: Friend or Foe?*, enero de 2020.

Figura 4: Opiniones sobre el impacto de la SCA en el fraude en transacciones CNP



Fuente: Encuesta de Aite Group a 88 ejecutivos europeos del área de pagos en colaboración con la MPE, noviembre de 2019

MÉTODOS PARA MITIGAR EL FRAUDE

Al implementar soluciones para mitigar el fraude, los comercios pueden concentrarse principalmente en dos cosas: proteger la cuenta o proteger la transacción financiera.

SOLUCIONES DE PREVENCIÓN DE FRAUDE A NIVEL DE CUENTA

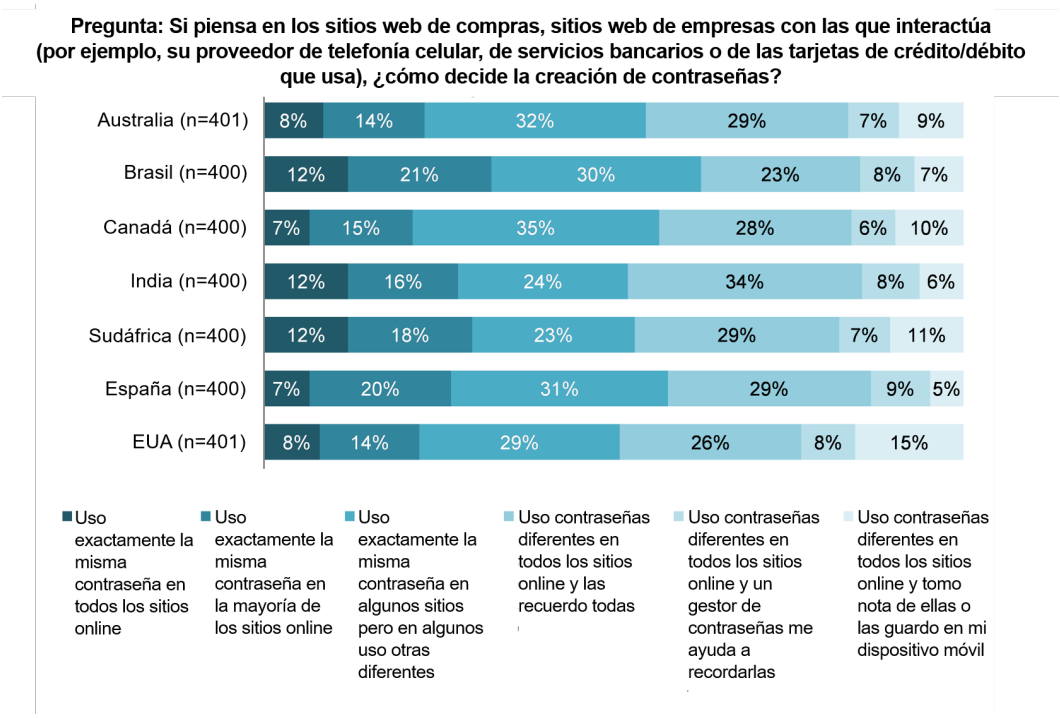
Los ataques fraudulentos relacionados con cuentas apuntan a la cuenta digital que el cliente tiene en un comercio. Los estafadores aprovechan la gran cantidad de información personal identificable que obtienen por filtración de datos para crear una nueva cuenta online o bien apoderarse de una cuenta ya existente. Desde 2013, se ha filtrado información de más de 30.000 millones de registros que contienen nombres de usuario, contraseñas, domicilios, números telefónicos y otros datos, y esa cifra sigue en aumento cada año.

Es sabido que los usuarios, además de tener contraseñas débiles, las reutilizan en distintos sitios. Según una encuesta de Aite Group, más de la mitad de los consumidores usa exactamente la misma contraseña en varios o todos los sitios online (Figura 5).[4] A los estafadores les resulta muy fácil hacer una prueba a gran escala para comprobar qué combinaciones de nombre de usuario y contraseña son válidas. Una vez identificadas, es muy probable que esas credenciales les sirvan también en otros sitios. En un estudio de NordPass sobre más de 275 millones de contraseñas afectadas, había tres contraseñas comunes que representaban casi el 13% del total ("123456",

4. Véase el reporte de Aite Group *Second Annual Global Security Engagement Scorecard™*, octubre de 2017.

"123456789" y "contraseña"). Y las contraseñas únicas eran apenas el 44%.[5] No sorprende, entonces, que las cuentas resulten atacadas cuando quienes compran online usan contraseñas tan simples y repetidas.

Figura 5: Cómo crea contraseñas el consumidor global



Fuente: Encuesta de Aite Group a 2.802 consumidores, septiembre de 2016

El fraude a nivel de cuenta es difícil de detectar por muchas razones. Si un estafador tiene acceso al nombre de usuario y la contraseña de un cliente y los utiliza para entrar a su cuenta online, puede ser difícil saber si en verdad se trata del cliente o si es un estafador. Esto puede resultar problemático por dos motivos. El primero es que, si el comercio online guarda los datos de la tarjeta de crédito o débito del cliente para compras futuras, para el estafador será muy fácil hacer una compra y dar una dirección de entrega que le convenga. En segundo lugar, los estafadores pueden acceder al programa de fidelización del cliente en una aerolínea, un hotel u otra empresa preferida y robarle los puntos ganados. Resulta cada vez más imperativo, entonces, proteger ambos tipos de cuentas online.

Hay muchas clases de soluciones de prevención de fraude a nivel de cuenta; por ejemplo, los servicios de verificación (identidad, dirección de e-mail, documento oficial), relleno de credenciales mediante bots, huellas digitales del dispositivo, datos biométricos (físicos, conductuales) y autenticación de dispositivo móvil, entre otros. Algunas de estas soluciones son pasivas en el sentido de que son transparentes para el usuario y brindan una sólida experiencia

5. "*Top 200 Most Common Passwords of the Year 2020*," NordPass, acceso del 12 de enero de 2021, https://nordpass.com/most-common-passwords-list/.

del consumidor. Otras soluciones son activas porque requieren cierta participación del usuario. Últimamente se usó una combinación de huella digital del dispositivo y datos biométricos conductuales que demostró ser eficaz para detectar el fraude.

SOLUCIONES DE PREVENCIÓN DE FRAUDE A NIVEL DE TRANSACCIÓN

El fraude a nivel de transacción apunta a aquellas compras online en las cuales se usan credenciales de pago robadas (por lo general, una tarjeta de crédito o débito) para adquirir productos físicos o digitales que los estafadores pueden convertir fácilmente en efectivo. Cuando una persona hace clic en el botón de "Comprar ahora" de la página de checkout, se evalúa la transacción en busca de un posible fraude y se toma la decisión de aprobarla o rechazarla. Los comercios tienen la opción de recurrir a estas herramientas antes de que se active la red (es decir, antes de enviar la autorización a las redes y la institución financiera de la tarjeta) o después (después de recibir una respuesta de las redes y de la institución financiera). Estas herramientas de prevención de fraude usan una combinación de machine learning (ML) y un motor de reglas para determinar la acción adecuada. En algunos casos, la transacción sospechosa se puede enviar a un equipo de revisión manual, donde el análisis está a cargo de una persona quien toma la decisión de autorizar o no.

Por lo general, el esfuerzo de los comercios por mitigar el fraude comienza a nivel de la transacción. Las herramientas de prevención de fraude en transacciones han evolucionado con los años y ahora incluyen la detección de fraude a nivel de cuenta. La ventaja de contar con una solución que actúa en dos instancias es que, antes de que se genere una transacción, los datos a nivel de cuenta pueden brindar información a un modelo ML a nivel de transacción a fin de mejorar la detección de fraudes y aumentar los índices de aprobación de órdenes. Estas soluciones combinadas suelen denominarse hubs de orquestación, donde un sistema central hace las veces de director y las soluciones individuales de prevención de fraude son los músicos que componen la orquesta. Para los comercios, los hubs proporcionan una única API que les permite acceder a una solución holística que protege a la vez la cuenta y la transacción; de esta manera, se simplifican en gran medida la implementación y la gestión operacional continua.

CÓMO LOGRAR EL EQUILIBRIO EN LA EXPERIENCIA DEL CONSUMIDOR

Ya sea que un comercio utilice una solución a nivel de cuenta o de transacción, o una combinación de ambas, es necesario tomar en cuenta la experiencia del consumidor. Hay dos palabras que a los comercios no les agradan: "fricción" y "abandono". Fricción es la cantidad de acciones que un cliente debe realizar en el proceso de hacer una compra online. Estas acciones podrían ser, entre otras, crear una cuenta online, proporcionar identificación en el momento de la compra, o ingresar un código de un solo uso (OTP) en un sitio web. El abandono de carritos de compra se produce cuando los consumidores agregan artículos a su carrito pero no completan el proceso de compra. La fricción puede ocasionar el abandono de carritos y la pérdida de ventas.

Una encuesta realizada por Aite Group a 1.400 consumidores del Reino Unido, Singapur y EUA sobre el impacto de la fricción en el abandono de carritos reveló algunos datos interesantes. Los usuarios veían de manera muy similar la creación de una cuenta online y la comprobación de identidad en el momento del pago. En promedio, entre el 30% y el 40% de los usuarios respondió que era muy probable que estos dos tipos de fricción lo llevaran a abandonar la transacción eCommerce. Entre el 15% y el 29% admitió que era muy probable que abandonara una

transacción si se le pedía que ingresara un OTP. El rango se basa en usuarios que dijeron hacer compras por eCommerce con poca, media o mucha frecuencia. Examinados desde una perspectiva etaria, los consumidores de 55 años o más se mostraron ligeramente más dispuestos a aceptar la fricción.[6] Las mejores soluciones contra el fraude optimizan la experiencia del cliente aplicando la fricción adecuada al riesgo y solo cuando resulta necesario para proteger tanto al cliente como al comercio.

ADMINISTRACIÓN DE FRAUDE: PREVENCIÓN DE PÉRDIDAS O ACTIVO DE NEGOCIO

Tradicionalmente, el objeto de una solución de prevención de fraudes es controlar y reducir las pérdidas por fraude. Por lo común, el departamento que se ocupa del fraude está ligado a un área de operaciones, y su rendimiento se mide por la cantidad de pérdidas irrecuperables. En muchos casos, esto ha despertado cierta preocupación en los protagonistas internos, como los departamentos de ventas por eCommerce, finanzas y marketing, que se concentran en maximizar las ventas. Es algo común que la gente piense que, para minimizar el fraude, es inevitable que se vean afectados los clientes en el sentido de que se rechazarán algunas transacciones legítimas. Es una cuestión sin términos medios. Una empresa puede limitar sus pérdidas por fraude o maximizar sus índices de aprobación, pero no puede hacer ambas cosas. En este entorno conflictivo, el departamento de prevención de fraudes a veces tiene la reputación de ser el equipo de "prevención de ventas".

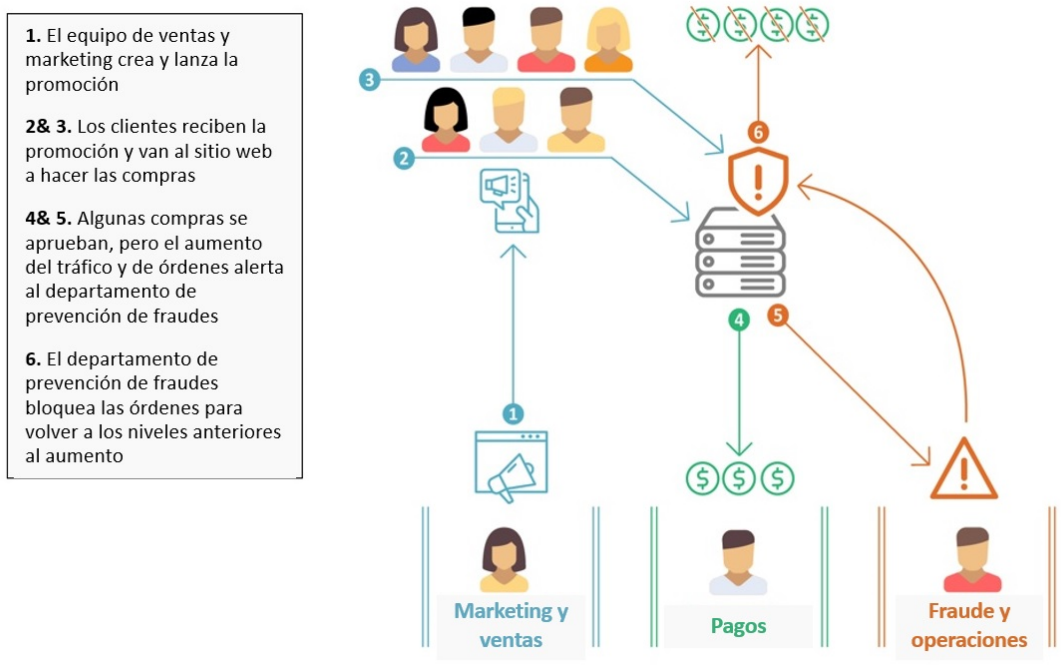
Pero ¿es necesario que sea así?

En lugar de tener que optar entre reducir el fraude y aumentar los índices de aprobación, algunos comercios están trabajando para lograr reducir el fraude y a la vez aumentar sus índices de aprobación, es decir, lograr un equilibrio entre estas métricas para aumentar la cantidad de órdenes legítimas que se aceptan. El departamento de prevención de fraudes está ganando espacio y ahora trabaja en conjunto con otros actores internos para impulsar el crecimiento. La prevención de fraude se considera un activo de negocio y parte del proceso de planeamiento, junto con ventas y marketing.

En un caso de uso, los departamentos de ventas y marketing de un comercio planificaron una promoción en la cual se ofrecían descuentos en diversos productos para impulsar el tráfico a su sitio web y aumentar las ventas. Esto no se informó al departamento de prevención de fraudes. Cuando se lanzó la promoción, el departamento de prevención de fraudes detectó un notable aumento del tráfico a su sitio web, como también en la cantidad de compras y el importe del ticket promedio. Esto hizo que el sistema activo de prevención generara alertas que advertían sobre aquel comportamiento anormal. Se pusieron en marcha controles de riesgo para limitar la actividad y volver a los niveles normales. Se perdieron ventas, se desperdició el dinero invertido en marketing, y los clientes se fastidiaron (Figura 6).

6. Véase el reporte de Aite Group *Global Consumers' Authentication Preferences: Have Your Cake and Eat It Too*, septiembre de 2018.

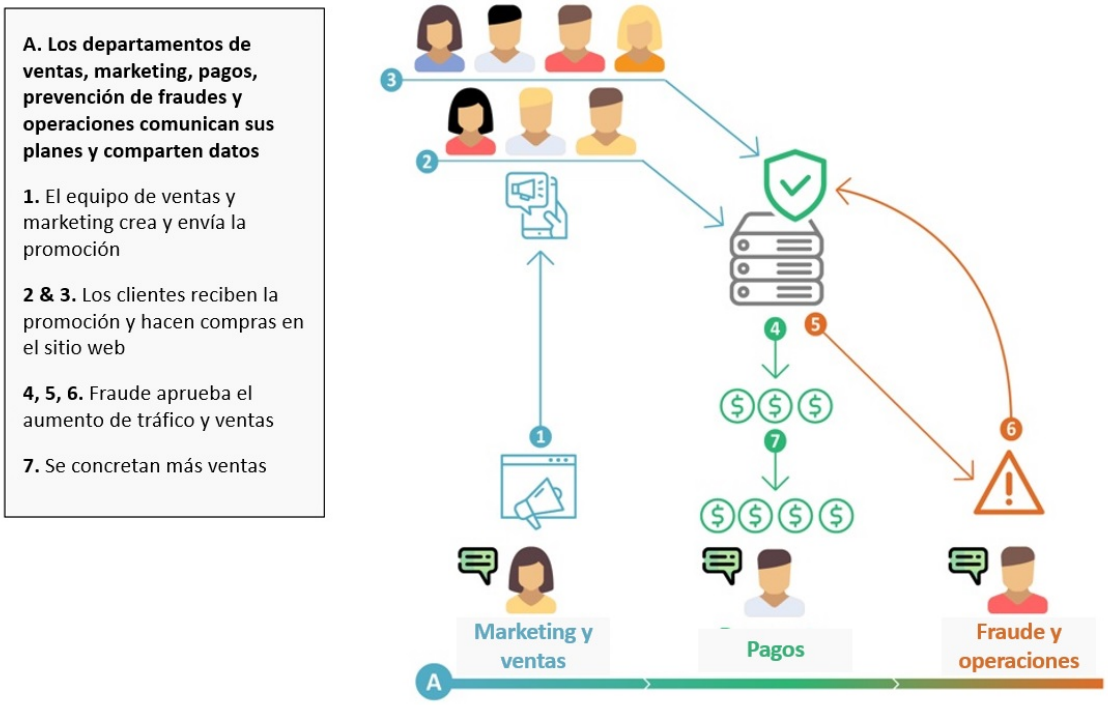
Figura 6: Entorno empresarial aislado



Fuente: Aite Group

Los comercios proactivos están derribando los "muros" organizacionales y poniendo a los departamentos de ventas, marketing, pagos, fraude y operaciones a trabajar de forma colaborativa, comunicando sus planes y compartiendo datos para optimizar las estrategias de prevención de fraude y gestión de riesgo. Por ejemplo, se pueden modificar las herramientas de prevención de fraudes a fin de prever esos aumentos en las órdenes y los niveles de riesgo relativos a las promociones. El equipo de pagos puede compartir información sobre los índices de aprobación y trabajar en conjunto con el equipo de prevención de fraudes en los planes para mejorarlos. Operaciones puede permitir el acceso al sistema de gestión de órdenes para informar cuáles son los clientes fieles y que el sistema de prevención de fraudes no los rechace. El departamento de prevención de fraudes puede aprovechar los contracargos que ingresen para informar a los departamentos de ventas/marketing sobre reclamos de los consumidores, con el fin de mejorar la claridad en los sitios web o aumentar la visibilidad de los términos y condiciones en el proceso de checkout. Mediante este trabajo colectivo, el departamento de prevención de fraudes puede llegar a ser un activo estratégico para el crecimiento del negocio (Figura 7).

Figura 7: Entorno empresarial colaborativo



Fuente: Aite Group

CAMINO A LA PERFECCIÓN

En un mundo perfecto, una herramienta de prevención de fraude identifica y aprueba todas las transacciones legítimas y rechaza todas las fraudulentas. Un sistema de fraude tiene dos métricas operativas que el comercio puede controlar: los falsos positivos y los falsos negativos. Con una administración adecuada de estas métricas, es posible aumentar tanto las ventas como la satisfacción de los clientes.

Los falsos positivos son aquellos casos en los que se rechaza una transacción legítima, lo cual provoca insatisfacción en el cliente e ineficiencias internas. En el caso de los falsos negativos, se aprueba una transacción fraudulenta, lo que ocasiona un contracargo y un perjuicio económico al comercio. Con la mitigación de los falsos positivos, se maximizan los ingresos del comercio, y al optimizar los falsos negativos, se minimizan los costos para el comercio: un doble beneficio comercial.

Los falsos positivos y negativos son medidas de la eficacia de las estrategias de prevención de fraude que implementa el comercio dentro de la herramienta o del sistema de prevención de fraudes. De los dos, los más fáciles de manejar son los falsos negativos. Visa y Mastercard informan periódicamente a los comercios sobre falsos negativos en forma de contracargos marcados con un código de motivo del fraude. Visa proporciona estos datos en su archivo TC40, y Mastercard lo hace en su archivo SAFE. Los falsos negativos se pueden mitigar si se analizan con detenimiento los contracargos y se efectúan los ajustes necesarios al sistema de prevención de fraudes. Además, es recomendable incorporar un ciclo de retroalimentación al modelo ML del

sistema de prevención de fraudes, para lo cual se ingresan los datos de las transacciones fraudulentas para que el modelo ML los aprenda.

Los falsos positivos son más difíciles de manejar porque no hay una fuente definitiva de esa información. En un mundo ideal, un comercio llamaría al tarjetahabiente de cada transacción rechazada y le preguntaría si realizó esa transacción. Esto no es realista, debido a limitaciones de recursos y a la falta de certeza respecto del número telefónico, que podría ser del tarjetahabiente o del estafador. En este caso, una fuente de información es el call center. Los clientes legítimos cuyas transacciones se rechazaron inadvertidamente pueden llamar para preguntar el motivo. El departamento de prevención de fraudes debe trabajar en conjunto con el área de operaciones para establecer un mecanismo que capte esa información valiosa. Otra opción consiste en adoptar una práctica que es común en el mundo de la emisión. Por lo general, las instituciones financieras contactan a sus tarjetahabientes cuando hay una transacción sospechosa, ya sea por mensaje de texto, e-mail o por una llamada con respuesta interactiva de voz (IVR), a fin de determinar si la reconocen. Según las encuestas, los tarjetahabientes aprecian y valoran esta práctica, ya que demuestra que la institución financiera está cuidándolos. Los comercios pueden hacer lo mismo; así, crearían buena disposición con sus clientes y, a la vez, recabarían datos valiosos sobre los falsos positivos para refinar el rendimiento de su sistema de prevención de fraudes. Para ello, necesitarían una herramienta de verificación de identidad que comprobara que el número de teléfono y la dirección de e-mail pertenecen al tarjetahabiente y no al estafador. Un reporte global sobre fraude en eCommerce elaborado por Cybersource descubrió que los comercios que operan en eCommerce rechazan el 2.5% de todas las órdenes por sospecha de fraude.[7] Toda reducción de ese porcentaje implica un aumento inmediato en las ventas sin costos agregados: una propuesta muy atractiva para cualquier comercio que opere en eCommerce.

7. "*2019 Global eCommerce Fraud Management Report*," Cybersource, 2019, acceso del 3 de marzo de 2021, https://www.cybersource.com/content/dam/cybs2019/documents/en/global-fraud-report-2019.pdf.

CONCLUSIÓN

Los estafadores continúan modernizando sus vectores de ataque y usando técnicas cada vez más sofisticadas. Para contar con las defensas apropiadas, el comercio debe ser muy diligente. Sin embargo, no se trata solo de impedir las transacciones ilegítimas. El fraude también puede constituir una ventaja estratégica para el crecimiento de tu negocio online. Las compañías eficientes adjudican a la prevención del fraude la misma importancia que al marketing, al producto y a las ventas. Cuando todos los engranajes están bien lubricados y se trabaja de forma colaborativa, mejora el rendimiento general. No hay diferencia con el departamento de prevención de fraudes en un contexto empresarial.

Veamos algunas conclusiones específicas para los comercios:

- El comercio online llegó para quedarse. Aquellos que lo incorporen y optimicen la experiencia para sus clientes serán los futuros ganadores.
- Los estafadores están plenamente conscientes del cambio en las preferencias de los consumidores y su adopción de las compras online. Esto plantea a los comercios un riesgo comercial y financiero que es necesario gestionar con cuidado.
- Hay una gran cantidad de soluciones para mitigar el fraude comercial a nivel de cuenta y de transacción. Las soluciones más recientes ofrecen funciones de hub de orquestación que combinan ambos tipos de solución.
- Independientemente de las soluciones de mitigación de fraude que se implementen, los comercios deben seguir de cerca la experiencia del consumidor para no añadir demasiada fricción, ya que esta puede provocar el abandono de carritos de compra.
- La prevención del fraude ya no es una función operativa que se ocupe solamente de minimizar las pérdidas. A medida que la venta online gana en competitividad, los comercios proactivos están apostando más a la administración y prevención del fraude para impulsar el crecimiento.

ACERCA DE AITE GROUP

Aite Group es una empresa global de investigación y consultoría que ofrece asesoramiento integral y práctico sobre negocios, tecnología y cuestiones normativas y su impacto en la industria de los servicios financieros. Con nuestro conocimiento y experiencia en servicios bancarios, pagos, seguros, administración patrimonial y mercados de capitales, asesoramos a instituciones financieras, proveedores de tecnología y empresas de consultoría de todo el mundo. Establecemos alianzas con nuestros clientes, revelamos sus puntos ciegos y les compartimos insights para que su negocio sea más inteligente y fuerte. Visítanos en la web y conéctate con nosotros en Twitter y LinkedIn.

ACERCA DEL AUTOR

David Mattei
+1.617.398.0908
dmattei@aitegroup.com

CONTACTO

Para más información sobre nuestros servicios de investigación y consultoría, contáctanos:

Aite Group Ventas
+1.617.338.6050
sales@aitegroup.com

Para consultas de prensa y conferencias:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

Para otras consultas:

info@aitegroup.com