ESTUDIO SOBRE EL IMPACTO FINANCIERO DEL FRAUDE EN 2017:

EXPLORANDO EL IMPACTO DEL FRAUDE EN UN MUNDO DIGITAL

Septiembre, 2017

Patrocinado por:

VESTA

Americas | Europe | Asia

Elaborado independientemente por:

JAVELIN

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

PRÓLOGO

El presente informe de investigación original, patrocinado por Vesta, examina los desafíos a los que se enfrentan los comerciantes que utilizan el comercio electrónico para equilibrar la experiencia del cliente con las realidades financieras del combate al fraude en un mundo digital. Los costos relacionados con éste van mucho más allá de las pérdidas directas y abarcan las herramientas, así como el personal utilizado junto con la pérdida de ingresos de clientes legítimos que se rechazan. Este informe fue elaborado independientemente por Javelin Strategy & Research, que conserva la independencia absoluta de los hallazgos y análisis de su conjunto de datos.

PANORAMA GENERAL

Los consumidores invierten cada vez más su poder adquisitivo en el espacio digital, al comprar bienes y servicios a través de los canales *online* y móviles, que han comprado históricamente en establecimientos físicos. Como los patrones de gasto han cambiado, los defraudadores también lo han hecho, al aumentar su enfoque en los comerciantes digitales, así como al desarrollar nuevas técnicas y tecnologías para explotar los canales en línea y móviles. Los comerciantes se enfrentan al aumento en pérdidas, a los crecientes costos de gestión de fraudes, así como a la necesidad de evaluar y experimentar constantemente para encontrar las mejores herramientas y personal para combatir las cambiantes modalidades de fraudes; al tiempo que conservan y maximizan la experiencia del cliente.

RESUMEN EJECUTIVO

Hallazgos clave

El fraude les cuesta a los comerciantes el 8% de los ingresos anuales en promedio. Los costos del fraude para los comerciantes están aumentando a medida que las operaciones continúan migrando a los canales digitales como consecuencia de la conversión a la norma de la tarjeta con chip. La gestión de fraudes, las pérdidas por contracargos y los falsos positivos son un costo cada vez mayor para todos los comerciantes. El impacto más grande ha sido sobre los comerciantes de bienes digitales, que han perdido 9.7% de ingresos en promedio debido al fraude, un aumento del 13% a partir de 2016. La mayoría de los gastos relacionados con el fraude son para la gestión de éste, que corresponde al 75% de los costos, el triple de las pérdidas por fraude reales en sí.

Los comerciantes gastan en prevención de fraudes hasta 10 veces lo que pierden en contracargos. Del 8.0% de ingresos que el comerciante promedio perdió en fraudes en 2017, 5.9 puntos porcentuales representan los costos de la gestión de fraudes, que incluye inversiones en áreas tales como la tecnología y el personal, mientras que 0.6 puntos porcentuales representan el ingreso perdido por contracargos relacionados con fraudes.

Los contracargos y falsos positivos son una parte cada vez mayor de los costos por fraude. Los contracargos aumentaron 60% para los comerciantes de bienes digitales y 75% para los comerciantes de bienes físicos, resultado del incremento en la sofisticación de los defraudadores y la exposición al cambio de responsabilidad por fraude con tarjeta con chip para algunos comerciantes de bienes físicos. Los falsos positivos continúan creciendo también, no obstante que sea ligeramente más lento, con un aumento del 25% para los comerciantes de bienes digitales y del 27% para los comerciantes de bienes físicos.

El fraude de tarjeta no presente es una creciente preocupación para los comerciantes, ya que los defraudadores se vuelven más sofisticados. El fraude de tarjeta no presente sigue siendo una gran preocupación para más del 85% de los comerciantes, de los cuales, la tercera parte muestra un aumento en su preocupación en 2017. Ésta se debe en gran medida al surgimiento de nuevas tácticas de fraude, tales como ataques de botnet y nuevas técnicas de entrega, como lo es comprar en línea o recoger en tienda. De igual preocupación es el impacto que tiene la conversión de tarjetas con chip al pasar más fraudes a los canales digitales y menos a los establecimientos físicos. Finalmente, el crecimiento en las operaciones de TNP significa más clientes de diferentes países, aumentando las preocupaciones por el fraude internacional, donde las herramientas existentes para la mitigación del fraude pueden ser menos eficaces.

Los comerciantes continúan dependiendo enormemente de los nombres de usuario y contraseñas vulnerables. La principal herramienta de autenticación, utilizada por el 75% de los comerciantes con TNP es el par débil del nombre de usuario y contraseña, explotado ampliamente por filtraciones de datos y software malicioso. La dependencia de los comerciantes sobre este método es comprensible, debido a la familiaridad y comodidad del cliente con ésta; sin embargo, con el fin de combatir el fraude con eficacia, necesitarán aumentar su enfoque en los segundos factores de autenticación, tales como la obtención de la huella de identificación del dispositivo, autenticación fuera de banda y geolocalización.

Las operaciones no autorizadas aumentaron 33% en 2017 y representaron casi la mitad de las pérdidas por fraude promedio de los comerciantes. Los criminales continúan beneficiándose de los datos obtenidos de las filtraciones y el *software* malicioso, mientras que, al mismo tiempo, se sofistican más, aprovechándose de tecnologías tales como redes privadas virtuales (RPV) y máquinas

virtuales para disfrazar sus ubicaciones y dispositivos.

El gasto de los comerciantes en gestión de fraudes creció más del 15%, llegando a 17% en 2017, más notablemente para los comerciantes de bienes digitales, cuyo gasto aumentó 42% en relación con el año anterior. La mitad de todas las pérdidas por contracargos ocurre en tiendas en línea y, a medida que el fraude continúe migrando hacia los canales digitales después de la transición a tarjetas con chip, las presiones sobre los comerciantes en línea para combatir el fraude solamente aumentarán. Aun cuando la necesidad de invertir en la prevención de fraudes y las herramientas de gestión sean cruciales para todos los tipos de comerciantes, la necesidad será mucho mayor para los comerciantes de bienes digitales.

Las personas, la tecnología y la subcontratación externa atraerán mayor inversión en 2018 al ser el área principal que verá el mayor aumento en inversión para todos los tipos de comerciantes, donde casi dos tercios de estos en bienes digitales e híbridos, asignarán más gasto en ese rubro, junto con la mitad de los comerciantes de bienes físicos. Esto será seguido de cerca por el aumento en el gasto en personal de gestión de fraudes, que es de suma importancia para los comerciantes híbridos, debido a las complejidades de navegar la mitigación del fraude para los distintos tipos de productos.

La subcontratación externa es una opción atractiva para muchos comerciantes al estar convirtiéndose en un método más popular para gestionar el fraude, donde el 24% de los comerciantes actualmente subcontratan todos o algunos de sus esfuerzos de mitigación del fraude y casi la mitad de los de bienes digitales y comerciantes híbridos esperan hacerlo en un futuro cercano. Con el 21% de los gastos operativos asignados a la gestión de fraudes en 2017, los comerciantes están revisando de manera integral los costos internos del combate al fraude y evaluando los beneficios de contratar un tercer experto para gestionar el fraude a su favor.

Las medidas antifraude más nuevas son muy atractivas para los comerciantes. Mientras que los comerciantes continúan dependiendo de soluciones correctivas para la mitigación del fraude, tales como verificación de la identidad del cliente y código de seguridad de la tarjeta (CVC2 o CVV2), se prevé que el análisis del comportamiento y la obtención de la huella de identificación del dispositivo logren los mayores avances en la adopción en los años por venir. Estas soluciones más nuevas y menos invasivas prometen ayudar a los comerciantes a combatir de mejor manera los intentos de fraude, sin degradar la experiencia del cliente o sin alejarlo.

Es probable que aumente la adopción de 3-D Secure el año entrante. La introducción de la versión 2.0 de 3-D Secure, con su promesa de ofrecer una mayor prevención del fraude con menos interrupciones a la experiencia del cliente, está convenciendo a un número creciente de comerciantes a darle una segunda oportunidad a la solución. Cerca del 63% de los comerciantes —algunos de los cuales tienen una presencia internacional— esperan contar con la solución el año entrante, con interés particular en las implementaciones para el canal móvil, con la expectativa de que se ha hecho bastante para mejorar la experiencia del usuario, así como para integrar las carteras móviles y las operaciones dentro de las aplicaciones.

Recomendaciones

Evaluar enfoques adicionales de autenticación más allá de los que utilizan elementos de datos estáticos. La mayoría de los comerciantes continúa dependiendo del nombre de usuario y contraseña, códigos de seguridad de la tarjeta y verificación del domicilio para mitigar el fraude. Los comerciantes necesitan invertir en herramientas más dinámicas como factores alternativos o segundos factores para autenticar a los clientes, particularmente aquellas que interrumpan al mínimo la experiencia del cliente. Las herramientas que evalúan el comportamiento del cliente, monitorean la información de dispositivos, o proporcionan comparaciones contra actividades previas de compra de los clientes son muy adecuadas para combatir intentos de fraude en operaciones digitales.

Invertir en la capacitación integral y continua del personal encargado de la gestión de fraudes. Con la evolución constante de las herramientas y técnicas contra el fraude, resulta fundamental que el personal especializado para combatirlo esté informado y actualizado en cuanto a las últimas amenazas de fraude, así como los enfoques más nuevos para su mitigación, los cuales se requieren para salvaguardar la rentabilidad de sus negocios.

Implementar herramientas "invisibles" de gestión de fraudes para maximizar su prevención al tiempo que se reduce al mínimo el impacto a la experiencia del cliente. Los comerciantes deben recurrir a la implementación de algunas de las herramientas más nuevas para la mitigación del fraude, tales como la métrica del comportamiento (*behaviometrics*), aprendizaje de máquina, obtención de la huella de identificación del dispositivo, y la versión más nueva de 3-D Secure. Estas herramientas prometen ofrecer más éxito en la mitigación de intentos defraude con poco impacto sobre la experiencia del cliente durante el proceso de compra y venta.

Considerar la subcontratación externa de todas o algunas de las funciones de gestión de fraudes. Las herramientas y técnicas del fraude están evolucionando a la velocidad de la luz, lo que constituye un desafío aun para aquellos que se dedican por completo a la gestión de fraudes para mantenerse al día con los nuevos métodos que los defraudadores están utilizando. Los comerciantes, especialmente aquellos con un alto volumen de operaciones digitales, deben evaluar sus opciones para la subcontratación externa de todas o algunas de las actividades de gestión de fraudes. Esto requerirá de un análisis integral de los costos internos de su combate al compararlo con los costos y beneficios de la subcontratación externa.

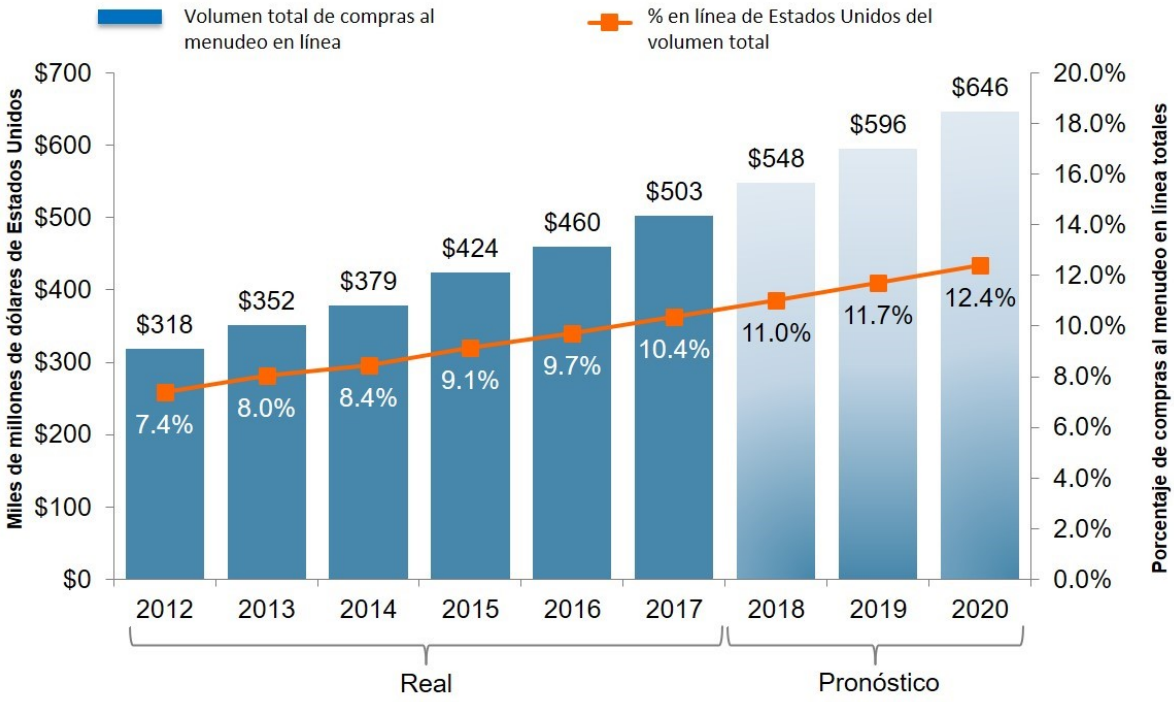
INTRODUCCIÓN

Tendencias del comercio electrónico

El comercio minorista está pasando por una revolución al orientar a los consumidores cada vez más hacia los medios digitales. Las tiendas físicas tradicionales están experimentando un bajo rendimiento, dejando los centros comerciales vacíos, ya que los consumidores recurren más a menudo a sus dispositivos en línea y móviles para conseguir una gama cada vez más amplia de productos y servicios. Se espera que el volumen de compras en línea al menudeo, sobrepase los $500 mil millones en 2017, representando más de una décima parte (10.4%) del volumen total del comercio al menudeo en Estados Unidos. Javelin pronostica que lo anterior crecerá a casi $650 mil millones y 12.4% del volumen del comercio al menudeo en Estados Unidos para 2020 (véase la Figura 1).

El comercio al menudeo total en línea aumentará a $646 mil millones antes de 2020

Figura 1: Volumen en dólares de operaciones de comercio electrónico al menudeo en Estados Unidos y proporción de compras hechas en línea (Incluyendo aplicaciones móviles (2012-2020).



	2015	2015–2020	2020
Métrica	Compras al menudeo en línea	Crecimiento en términos de dólares en el volumen total de pagos en línea	Volumen total de pagos en línea
Compras al menudeo en línea	$424MM	$222MM	$646MM

Fuente: Javelin Strategy & Research, 2017

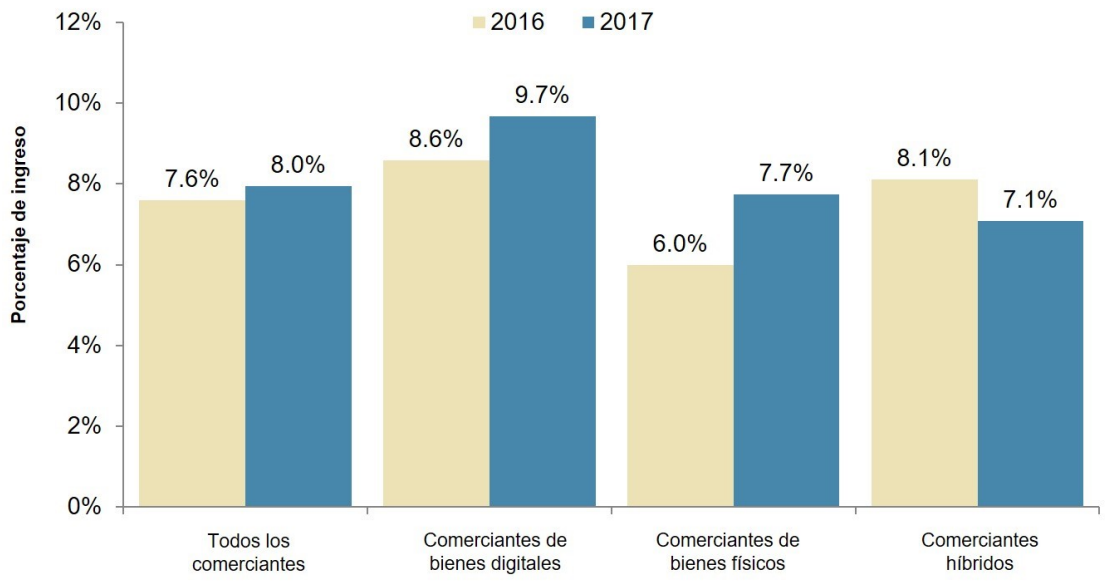
Tendencias del fraude

Este constante cambio al comercio electrónico, a través de los canales tanto en línea como móviles, está haciendo que la gestión de fraudes sea un desafío cada vez más crítico para los comerciantes. En comparación con las operaciones físicas del punto de ventas (PDV), las del comercio electrónico pueden involucrar productos únicos, junto con enfoques de mercadotecnia y métodos de entrega distintos. A medida que el volumen continúe migrando a los canales digitales, los defraudadores concentrarán más de sus esfuerzos en identificar y explotar las cualidades únicas del comercio electrónico, y los comerciantes tendrán que permanecer ágiles y alertas con el fin de mantener sus ingresos y márgenes de utilidades. La vigilancia requiere de inversiones continuas y crecientes, y los costos totales del fraude promedio para el comerciante en 2017 crecieron en consecuencia, sumando $15.5 millones, 6% más que el año pasado ($14.6 millones) (véase el Apéndice). Esto representa una mayor proporción de ingresos que en 2016 se utilizaron para enfrentar los desafíos de intentos de fraude (8.0% en 2017 contra 7.6% en 2016) (véase la Figura 2). Esto después de un año de inversión significativa para muchos comerciantes de bienes físicos e híbridos que evolucionaron al uso de tarjetas con chip en puntos de venta.

> *"En este momento nos encontramos en un proceso donde estamos intentando modernizarnos y hacer lo mejor con lo que tenemos. Hemos invertido mucho en infraestructura pero todavía no alcanzamos el objetivo. No logramos tener toda la sofisticación todavía. Nos encantaría llegar a una situación donde sea un cliente conocido, que tengamos toda su información y que pueda hacer su compra con un solo clic, pero todavía no hemos llegado a ese punto".* - Ejecutivo de fraude, comerciante híbrido.

El fraude consumió más del ingreso promedio de los comerciantes en 2017

Figura 2: Costos totales del fraude como porcentaje del ingreso (2016-17).

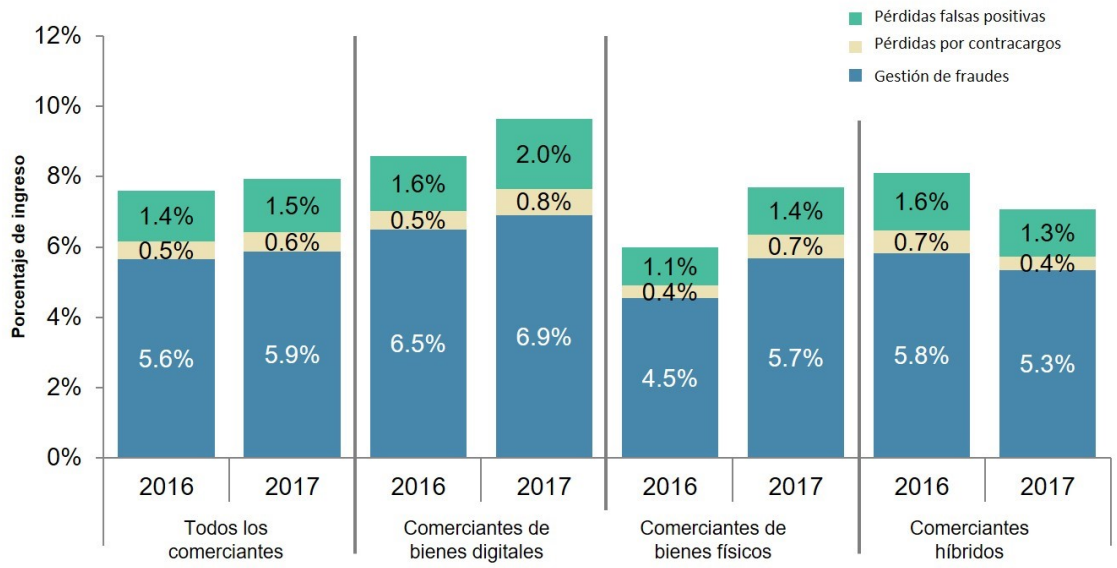


Fuente: Javelin Strategy & Research, 2017

Específicamente, los comerciantes de bienes digitales y los de bienes físicos están gastando más, lidiando con mayores pérdidas por contracargos (60% y 75% más como porcentaje del ingreso en comparación con 2016, respectivamente) y mayores falsos positivos (25% y 27% más como porcentaje del ingreso, respectivamente). Estas pérdidas han forzado a dichos comerciantes a gastar más tiempo y dinero en buscar las mejores maneras de limitar el riesgo de fraude al tiempo que reducen al mínimo el impacto a la experiencia del cliente y a las operaciones rechazadas que resultan de los falsos positivos. Por otro lado, los comerciantes híbridos, y más específicamente los de viajes, se beneficiaron de los cambios en las reglas de los contracargos que les brindan más ventajas al impugnar controversias. En combinación con el sólido aumento de los ingresos entre comerciantes de viajes al recuperarse la economía, estos cambios a las reglas contribuyeron a menores pérdidas por contracargos como porcentaje del ingreso, junto con costos de gestión de fraudes más bajos.

Las pérdidas más altas por fraude se están combatiendo con inversiones para la mitigación de éste

Figura 3: Desglose de costos relacionados con fraudes como porcentaje del ingreso (2016-17).



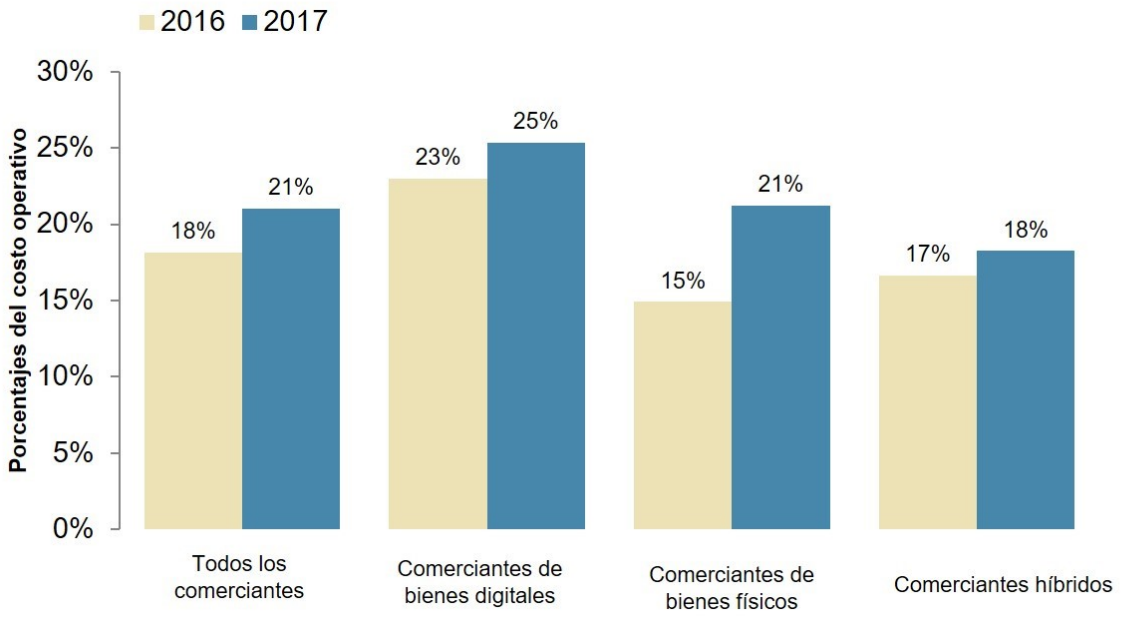
Fuente: Javelin Strategy & Research, 2017

[1] http://www.iata.org/pressroom/pr/Pages/2016-12-08-01.aspx, accessed Sept. 14, 2017.

Este gasto reduce aún más su capacidad para invertir en otras áreas de sus negocios, ya que los costos por fraude están consumiendo una mayor porción, no sólo de los ingresos de los comerciantes, sino también de sus costos operativos. En promedio, el 21% de los costos operativos de un comerciante fue consumido por los relacionados con el fraude en 2017, en comparación con el 18% en 2016. Este aumento fue mayor entre los comerciantes de bienes físicos, probablemente debido a los costos asociados con la reciente implementación de tarjetas con chip en los puntos de venta. No obstante, la adopción demorada de terminales capaces de utilizar tarjetas con chip por parte de algunos comerciantes también les ha representado un aumento en los contracargos, que se manifiesta en las tasas más altas de estos, experimentadas por los comerciantes de bienes físicos, muchos de los cuales cuentan con establecimientos físicos. Por lo tanto, aun cuando los contracargos pueden disminuir en un futuro cercano cuando las tarjetas con chip en PDV se vuelven omnipresentes, los costos asociados del despliegue mantendrán a los gastos más altos hasta que se complete la transición a tarjetas con chip. Los comerciantes de bienes digitales continuaron disponiendo de la proporción más alta de sus gastos operativos en la gestión de fraudes (el 25% en 2017). Debido a las complejidades de las operaciones digitales, incluyendo tiempos de entrega casi inmediatos y números potencialmente mayores de clientes internacionales, mitigar el fraude en forma exitosa requiere de inversiones en una gama más amplia de herramientas, procesos y personal de gestión de fraudes altamente capacitado.

Los comerciantes asignan una mayor proporción de gastos operativos en la gestión de fraudes en 2017

Figura 4: Promedio de gastos por gestión de fraudes como porcentaje de los costos operativos (2016-17)).



Fuente: Javelin Strategy & Research, 2017

CAMBIANTES TÁCTICAS DE LOS ESTAFADORES

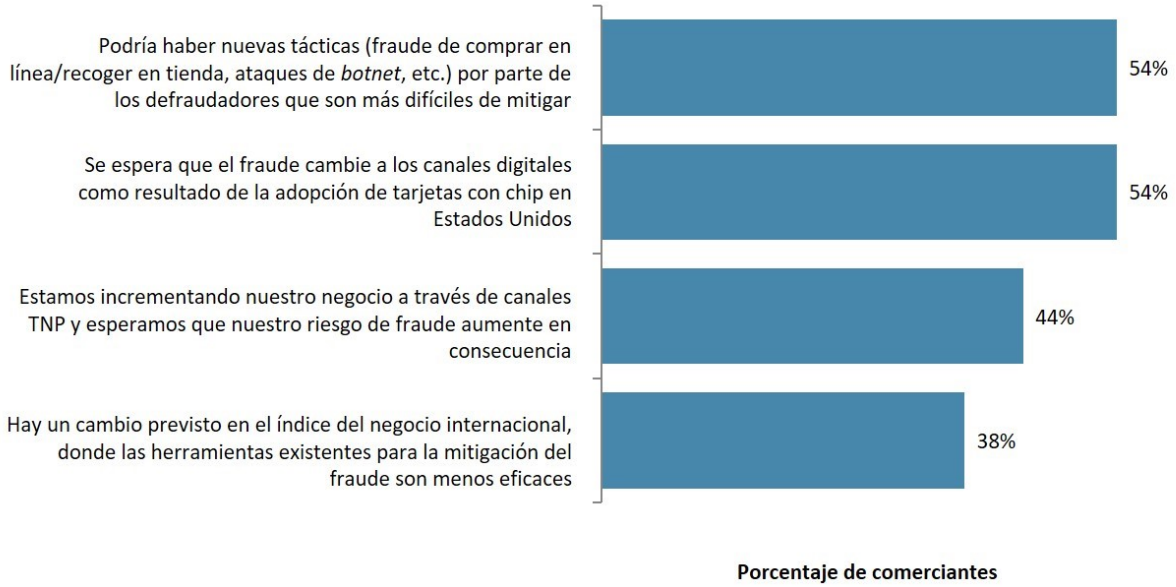
Amenazas de fraude

Aunque las operaciones de tarjeta no presente (TNP) brindan una oportunidad de impulsar el negocio —y aumentar los ingresos— del comerciante, lo cual no sería posible únicamente con operaciones con tarjeta presente; 1 de cada 3 comerciantes está preocupándose cada vez más por la posibilidad de que el fraude de TNP aumente en los siguientes 12 meses (véase el Apéndice). Estos comerciantes están equilibrando el aumento en los ingresos, la gestión de riesgos de fraude asociados, y el aumento en los costos y pérdidas administrativas asociadas con las operaciones de TNP. Entre aquellos comerciantes preocupados por un incremento en el fraude de TNP, más de la mitad citan nuevas tácticas y el lanzamiento de la tarjeta con chip como los factores principales (véase la Figura 5). Estas últimas continúan aumentando la presión sobre las redes de defraudadores en PDV para que encuentren alternativas, aumentando la inquietud entre los comerciantes de que el cambio al fraude de TNP seguirá creciendo conforme los criminales pongan a prueba a los comerciantes del canal digital para hallar vulnerabilidades.

A pesar de las amenazas a las que se enfrentan los comerciantes por el incremento del fraude nacional de TNP después de la conversión de tarjetas con chip, el fraude internacional se sitúa a la cabeza de las preocupaciones de los comerciantes, relacionadas con amenazas de fraude (véase la Figura 6). Esto se debe en gran medida a que la mitigación del fraude internacional obliga a los comerciantes a adaptarse a reglas de fraude más diversas al tiempo que deben ajustarse a las limitaciones de algunos controles. Un ejemplo clave es el servicio de verificación del domicilio (AVS, por sus siglas en inglés) que, aunque es bastante útil y eficaz para ciertos tipos de operaciones en Estados Unidos, tiene una utilidad insignificante internacionalmente. La complejidad de la gestión

Las nuevas tácticas de fraude y el cambio a tarjetas con chip aumentan la preocupación sobre el fraude de TNP

Figura 5: Motivos para creer que el fraude de TNP aumentará durante los siguientes 12 meses.



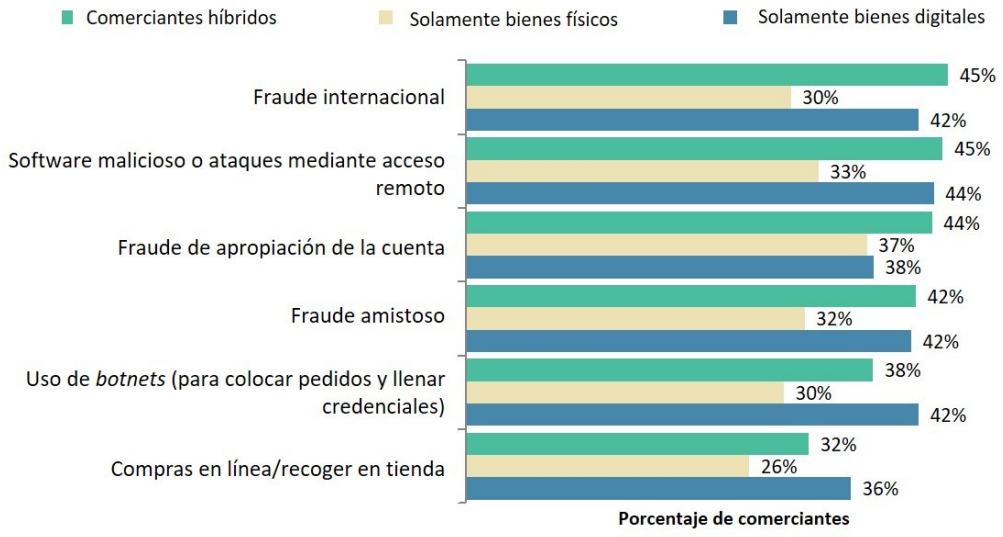
Fuente: Javelin Strategy & Research, 2017

de fraudes para operaciones internacionales lleva a algunos comerciantes a utilizar a un tercero para que administre esas ventas y para que actúe en última instancia como el comerciante responsable registrado. Los ataques ofuscados comparten el primer sitio en la lista de las preocupaciones relacionadas con los fraudes de los comerciantes. El software malicioso, las máquinas virtuales, y el acceso remoto deterioran la capacidad de los comerciantes para comprobar si están tratando con un cliente conocido y legítimo, en un dispositivo conocido, en un sitio de confianza o, en cambio, si están tratando con un criminal. Por su mismo diseño, estos tipos de ataques disfrazan la huella digital o la ubicación del dispositivo del cliente, afectando las herramientas de las que los comerciantes dependen para mitigar el fraude. Resulta interesante que la preocupación principal de los comerciantes de bienes físicos es el fraude por apropiación de la cuenta, mientras que los comerciantes híbridos y comerciantes de bienes digitales están más preocupados por el fraude internacional, los ataques ofuscados y el fraude amistoso. La preocupación de la apropiación de cuentas entre comerciantes de bienes físicos es intrigante, debido a que dichos comerciantes cuentan con el punto adicional de validación de un domicilio físico para protegerse contra intentos de fraude. Su preocupación podría deberse a la creciente sofisticación entre defraudadores al introducir domicilios físicos fraudulentos, pero es más probable que se deba al incremento en las técnicas de entrega innovadoras, como comprar en línea y recoger en la tienda.

> *"No son personas que trabajan solas sino organizaciones delictivas. Hay preocupaciones más importantes fuera de eso, se han vuelto realmente buenos, y odiaríamos ver que se utilice para otros propósitos tales como el terrorismo u otros riesgos de seguridad".*
>
> - Ejecutivo de fraude, bienes digitales

Controlar el fraude internacional y el de dispositivos ofuscados le está quitando el sueño a los comerciantes

Figura 6: Porcentaje de amenazas catalogadas de "muy" a "extremadamente difíciles" por tipo de comerciante.



Fuente: Javelin Strategy & Research, 2017

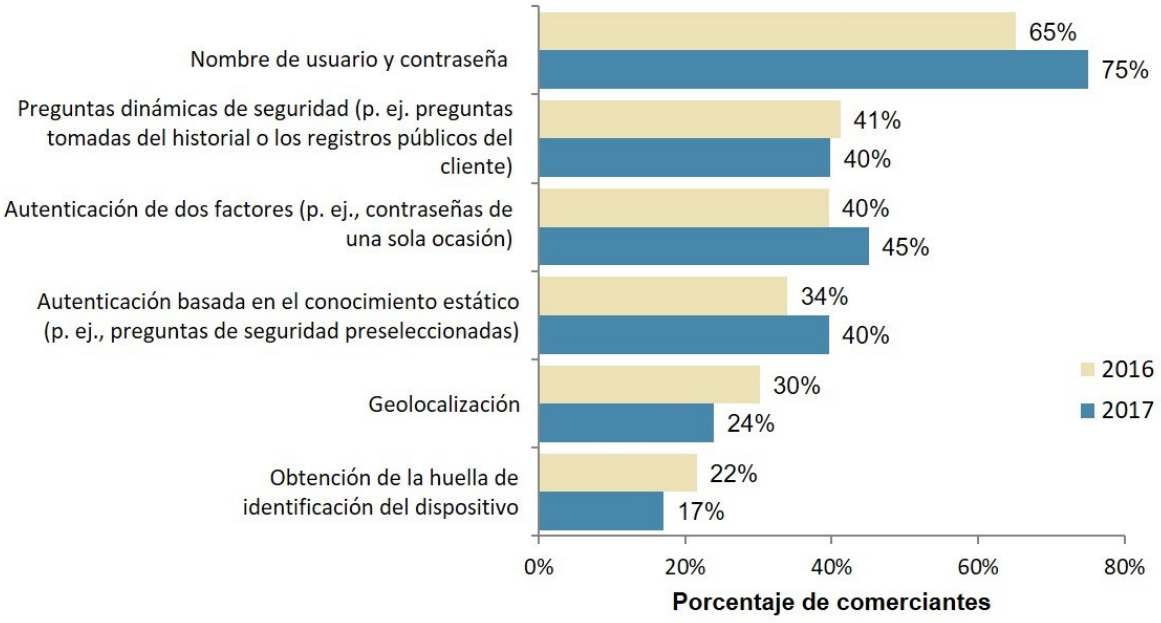
Un área clave de preocupación, particularmente para los comerciantes de bienes digitales, son los ataques automatizados (también conocidos como llenado de credenciales (*credential stuffing).* Este tipo de fraude está dirigido a cuentas existentes de comerciantes, eliminando la necesidad de que los criminales pongan en peligro directamente la información de la tarjeta. Los ataques automatizados se aprovechan de filtraciones de contraseñas en gran escala, y existe una gran probabilidad de la reutilización de contraseñas en las cuentas, incluso con filtraciones de varios años atrás. Los defraudadores introducen credenciales a los scripts que automáticamente se dirigen a las instituciones financieras y a los comerciantes más grandes.

La creciente popularidad entre consumidores de comprar en línea, recoger en la tienda (BOPIS, por sus siglas en inglés), que ofrecen los grandes minoristas tales como Wal-Mart, Target y Home Depot, también tiene preocupados a los comerciantes. A los consumidores les gusta BOPIS, ya que les permite evitar cargos de envío y brinda la conveniencia del tener el artículo listo para su recolección sin espera de la entrega. Sin embargo, los defraudadores siguen dependiendo y se aprovechan de BOPIS como un paso

> *"Nuestra identificación de la cuenta es la dirección de correo electrónico, así que es obvio que la gente utiliza las mismas contraseñas, eso lo vemos. Contamos con reglas contra el fraude específicamente en torno a ciertos atributos que se cambian para un pedido, tal como agregar una nueva dirección a la cuenta, al titular de ésta, etc.".*
>
> - Ejecutivo de fraude, bienes digitales

Los comerciantes aumentan el uso de 2FA, pero al mismo tiempo aumentan su dependencia sobre nombres de usuario y contraseñas quebrantadas

Figura 7: Autenticación utilizada para acceso a la cuenta del cliente (2016-17.



Fuente: Javelin Strategy & Research, 2017

intermedio entre el PDV y el fraude de TNP, confiando en una red establecida de mensajeros para recoger bienes adquiridos en línea en vez de tener que navegar por el proceso de entrega de los productos y potencialmente detonar los controles de fraude de un comerciante.

Las inquietudes acerca del fraude de TNP se complican por el hecho de que los nuevos —y a menudo menos sofisticados— comerciantes continúan inundando el canal digital y ofrecen a los clientes la capacidad de crear cuentas en línea. Su primera herramienta de autenticación es el débil par del nombre de usuario y contraseña, que utilizó el 75% de los comerciantes en 2017, por encima del 65% en 2016. La opción de nombre de usuario y contraseña es comprensible, a pesar de sus limitaciones, debido a la familiaridad del consumidor y el nivel de comodidad con este método de autenticación.

Ya que los comerciantes no están en condiciones de eliminar contraseñas, para defenderse contra ataques automatizados requieren invertir en una variedad de controles complementarios, como por ejemplo:

- Reconocimiento del dispositivo e identificación de los que están asociados con botnets y bloqueo de intentos de acceso sospechosos.
- Ofrecer soluciones de autenticación que no puedan violarse o reproducirse fácilmente (p. ej., contraseñas no basadas en texto de una sola ocasión y biométrica).
- Reducir al mínimo la información proporcionada a los defraudadores en intentos fallidos — si los criminales conocen que el nombre de usuario es correcto pero la contraseña no, pueden iniciar ataques adicionales, posiblemente mediante el uso de rutas de restablecimiento de contraseñas.

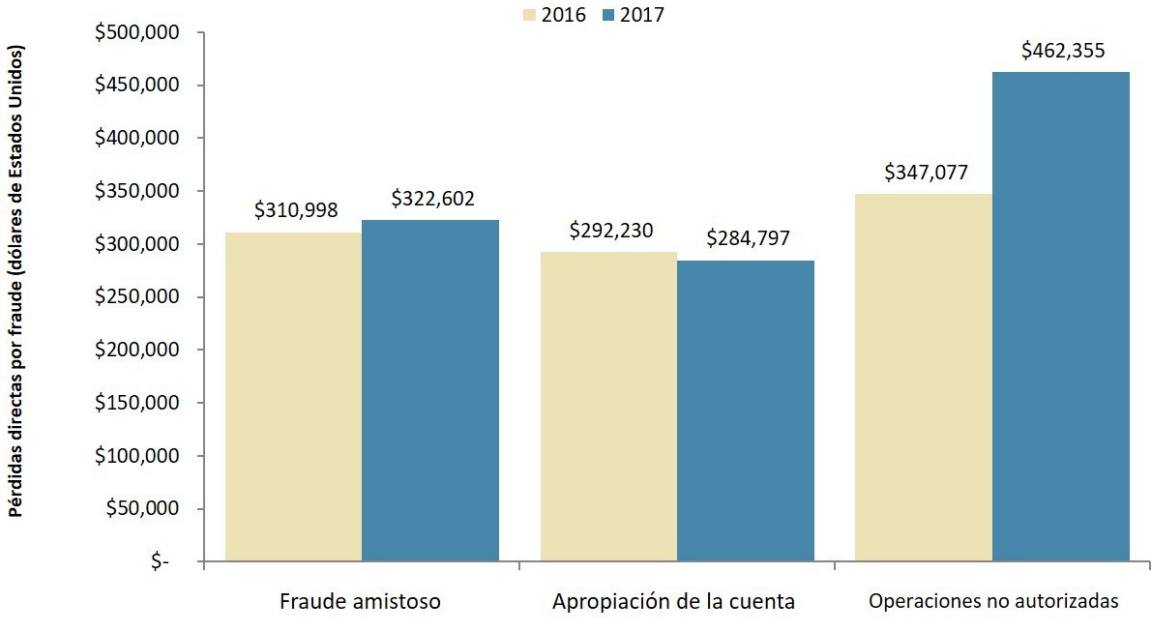
TIPO DE FRAUDES

Los comerciantes experimentaron pérdidas por fraude 13% más altas en 2017 que en 2016, alcanzando un promedio de más de $1 millón en pérdidas por fraude (véase la Figura 8). Queda claro que, a pesar del lanzamiento de la tarjeta con chip en un esfuerzo por combatir el fraude en el PDV, los defraudadores no han reducido sus esfuerzos, sino que los han cambiado a los canales digitales y han empleado nuevas capacidades tecnológicas con el fin de explotar las debilidades en los sistemas de los comerciantes. Son tres los tipos clave de fraude: operaciones no autorizadas, apropiación de la cuenta y fraude amistoso. Si los observamos, el cambio más notable es el aumento dramático en las operaciones no autorizadas, 33% desde 2016 y que representan casi la mitad de las pérdidas por fraude promedio de los comerciantes en 2017 ($462K). El fraude amistoso y la apropiación de la cuenta continuaron en niveles casi iguales, indicando que al parecer, mientras los defraudadores explotan nuevas oportunidades en operaciones no autorizadas, siguen atacando en todos los frentes de la guerra del fraude.

> *"Definitivamente, la apropiación de cuentas es una manera en la que pueden conseguir los bienes y eludir nuestras reglas más rápida y fácilmente, en comparación con crear una nueva cuenta o usar la verificación del huésped".* - Ejecutivo de fraude, bienes físicos.

Los comerciantes tuvieron las mayores pérdidas en operaciones no autorizadas en 2017

Figura 8: Pérdidas promedio por tipo de fraude.



Fuente: Javelin Strategy & Research, 2017

Operaciones no autorizadas

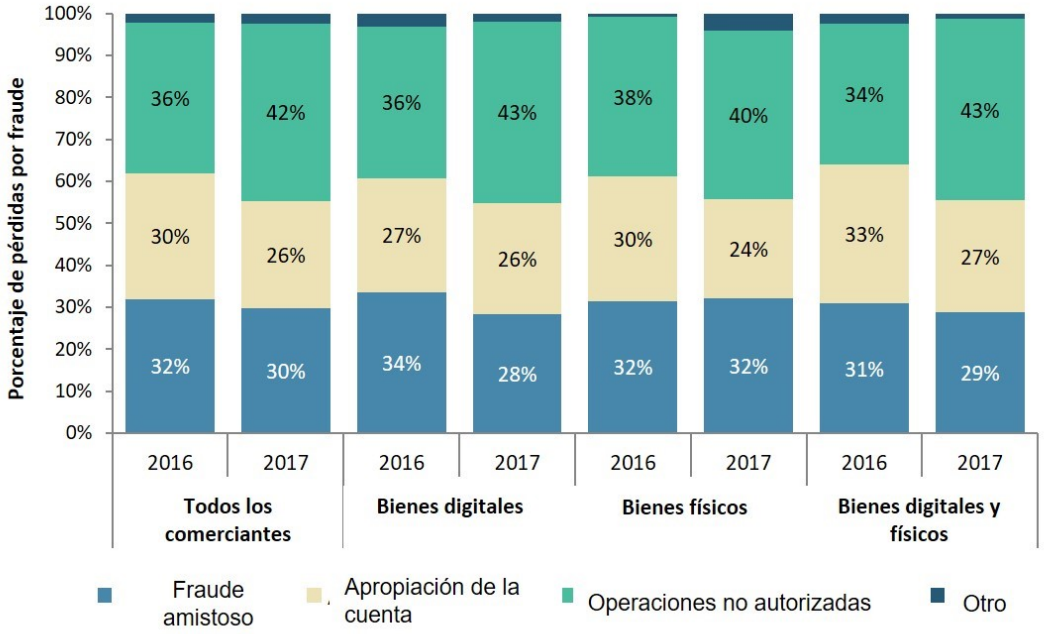
Las operaciones no autorizadas son posibles a través del uso de la tarjeta o las credenciales de pago robadas, lo que permite que los defraudadores se hagan pasar por el cliente para comprar bienes con cargo a la tarjeta o la cuenta de pago robadas. Mientras que los criminales migran del PDV como resultado del lanzamiento de la tarjeta con chip, se dirigen cada vez más a los comerciantes que utilizan el comercio electrónico, dando como resultado una oleada de operaciones no autorizadas durante los últimos 12 meses. Las operaciones no autorizadas se han convertido en una proporción más grande de las pérdidas que en 2016, representando el 40% o más de las pérdidas a través de todos los segmentos de comerciantes (véase la Figura 9).

Los criminales que ya estaban en el canal están agravando el desafío al volverse más sofisticados. Están aprovechándose de tecnologías tales como RPVs y máquinas virtuales para disfrazar sus ubicaciones y dispositivos. Estas nuevas tecnologías se han combinado con resultados obtenidos de esfuerzos de filtraciones y *software* malicioso dirigido a datos de TNP, que ocasionaron que los números de tarjetas de crédito y de débito ahora son el tipo de datos más comprometido, afectando el 70% de las víctimas de filtración de los mismos.

Además, la actual transición a tarjetas con chip ha dejado expuestos a algunos comerciantes de bienes físicos a las pérdidas por fraude en el punto de venta de las que no habían sido responsables previamente. Estos establecimientos son blancos atractivos para los criminales que buscan realizar operaciones fraudulentas con tarjetas de pago con tiras magnéticas. Esto ha aumentado el índice de operaciones no autorizadas para dichos comerciantes, aunque se espera que se reduzca en los siguientes años.

Las operaciones no autorizadas se han convertido en un problema mayor

Figura 9: Porcentaje de pérdidas por tipo de fraude.



Fuente: Javelin Strategy & Research, 2017

Apropiación de la cuenta (ATO, por sus siglas en inglés)

La apropiación de la cuenta ocurre cuando un defraudador utiliza la información de la cuenta de otra persona (p. ej., nombre de usuario y contraseña) para obtener productos y servicios utilizando las cuentas existentes de esa persona. Esto difiere de las operaciones no autorizadas ya que el criminal utiliza los datos robados de la cuenta para tomar el control de ésta mediante el restablecimiento del nombre de usuario y contraseña, a menudo cambiando el domicilio físico o el número de teléfono registrado para evitar que el titular legítimo descubra el robo. La ingeniería social desempeña un gran papel en la apropiación de la cuenta, ya sea que se enfoque en la recopilación de datos personales del titular legítimo o pasando por encima de los controles del emisor o del comerciante. Mientras que ATO puede representar una proporción más pequeña de las pérdidas por fraude totales que en 2016, éste aun representa un promedio de $285K de las pérdidas por fraude anuales para los comerciantes (véase la Figura 8).

Otro factor que impacta la capacidad de los comerciantes de combatir la ATO es el auge de la apropiación secundaria de cuentas, en la cual los criminales ponen en riesgo las no financieras para facilitar la apropiación de cuentas comerciales o financieras. Un blanco popular de este tipo de apropiación se refiere a las cuentas móviles, que pueden ser interceptadas por criminales, tales como alertas, restablecimiento de contraseñas, o captar las que son enviadas por mensajes SMS. En ese momento, pueden utilizar dicha información para descifrar nombres de usuario y contraseñas, con el fin de responder con éxito preguntas de autenticación basadas en el conocimiento, o iniciar el restablecimiento de contraseñas, que les da acceso total a las cuentas objetivo. La apropiación de cuentas móviles ha crecido estos últimos años, donde el doble de los consumidores fue objeto de apropiación de sus cuentas del teléfono móvil en 2016, en comparación con 2015.

La apropiación de cuentas a menudo toma más tiempo para detectarse que otros tipos de fraude, ya que puede ser más difícil confirmar que realmente existió una actividad fraudulenta Tarda un promedio de 53 días detectar fraude de apropiación de la cuenta contra un promedio de 30 días en todos los tipos de fraude. A menudo, los consumidores no se dan cuenta de que ha ocurrido la ATO hasta que vacían su cuenta o su tarjeta de crédito sobrepasa el límite de crédito. Puede ser que las preguntas de la autenticación basada en el conocimiento no distingan por completo entre el cliente verdadero y el defraudador si este último ha obtenido suficientes datos sobre el cliente verdadero para contestar las preguntas con éxito.

Las tecnologías de reconocimiento del dispositivo, el análisis de la sesión, y la métrica del comportamiento pueden ser métodos eficaces en el combate al fraude de apropiación de la cuenta. Una ventaja principal de estos métodos es que pueden seguir siendo invisibles en gran parte para el cliente, de modo que contribuyen a la prevención del fraude con interrupción mínima a la experiencia de compras del cliente. Sin embargo, para aprovechar estas técnicas de gestión de fraudes más nuevas requiere que los comerciantes —con mayor frecuencia los comerciantes de bienes digitales— aumenten su gasto en tecnología contra el fraude para facilitar la integración en tiempo real en sus sistemas de autorización

Fraude amistoso

El fraude amistoso ocurre cuando los defraudadores son los titulares reales de las tarjetas. Este tipo de fraude se presenta a través de una combinación de factores. El primero y más

> *"El cambio real que observamos yace en el fraude amistoso. Estos individuos acumulan beneficios o simplemente perdieron y lo están disputando. Siento que las empresas de tarjetas no están haciendo lo suficiente, pero nosotros cargamos con la pérdida".*
> - Ejecutivo de fraude, bienes digitales

notorio es el abuso intencional y premeditado del sistema de contracargo, ascendiendo a una clase de robo en tiendas cibernético. El menos notorio pero no menos impactante es una respuesta al remordimiento del comprador en el cual los clientes legítimos cambian de opinión acerca de una compra y en vez de devolver el artículo comprado al comerciante por un reembolso, decide entrar en contacto con su emisor para refutar la operación. Este enfoque puede ser más fácil para el cliente, ya que a menudo involucra hacer un simple clic en el botón de "rechazar" en el sitio web del emisor, mientras que al mismo tiempo pasa por alto las políticas de devolución y reembolso del comerciante.

Las compras no intencionales y las no reconocidas también contribuyen en gran medida al fraude amistoso. Con frecuencia los consumidores verán un cargo en su estado de cuenta y no reconocerán al comerciante o el monto del cargo. Las compras pueden ser no reconocibles debido a nombres confusos de los comerciantes en los registros de las operaciones o a las diferencias en las fechas de operación contra las fechas de envío. Las compras no intencionales pueden resultar de errores en los carros de compras, hacer clic accidentalmente en el botón de "comprar", o por el uso de aplicaciones por parte de los niños.

Los contracargos iniciados después de compras legítimas suponen un problema constante para los comerciantes, quienes reportaron pérdidas promedio de $323K en 2017,un aumento de 4% a partir de 2016. La prevención del fraude amistoso plantea un desafío notable debido a que, como el comprador es el titular legítimo de la cuenta, la persona pasará todas las pruebas de prevención de fraudes/verificación de identidad. Puede resultar costoso y suponer pérdida de tiempo el disputar un contracargo, de manera que, a veces, el comerciante simplemente tomará la decisión de absorber la pérdida, al ser la opción menos costosa. Más allá de consideraciones puras del costo, estos casos deben manejarse con pinzas para evitar que se alejen buenos clientes, lo que obliga indudablemente a los comerciantes a absorber pérdidas por fraude amistoso.

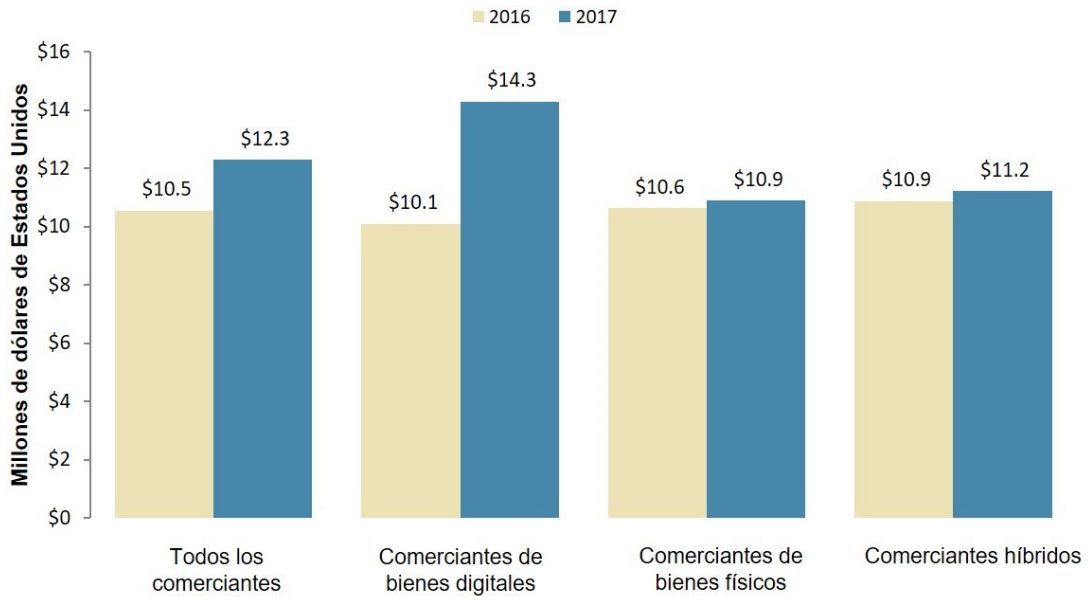
RESPUESTA DE LOS COMERCIANTES AL FRAUDE

Inversión en gestión de fraudes

Motivados por un aumento en los intentos de fraude y la creciente sofisticación en el canal digital (véase el Apéndice), junto con un deseo de mejorar la experiencia del cliente, los comerciantes continúan invirtiendo mucho en la prevención del fraude. Se espera que el gasto por la gestión de éste aumente en todos los segmentos de comerciantes invirtiendo en más gente, tecnología y subcontratación externa para combatir el problema que cada vez es mayor. La gestión de fraudes promedio aumentó el 17%, a $12.3 millones por comerciante en 2017, de $10.5 millones de 2016 (véase la Figura 10). Lo más destacado es el incremento en el gasto de los comerciantes de bienes digitales, un aumento de 42% interanual; ya que son los que reciben el mayor impacto de las pérdidas por contracargos, la mitad de las cuales ocurre en las tiendas en línea (véase el Apéndice). A medida que el fraude continúa migrando hacia el canal digital después de la conversión a tarjetas con chip, las presiones sobre los comerciantes en línea para combatir el fraude solamente aumentarán. En consecuencia, dichos comerciantes tienen una necesidad continua de invertir en herramientas para la prevención y gestión de fraudes más que sus contrapartes de las tiendas físicas. Los comerciantes de bienes físicos experimentaron solamente un aumento del 3% en el gasto de gestión de fraudes, y ya habían aumentado sus inversiones en años recientes para concluir la conversión a tarjetas con chip. En un momento en el que el gasto del consumidor cambia a los canales digitales, los comerciantes físicos probablemente tendrán que negarse a que las inversiones en gestión de fraudes sigan adelante, debido a que su gasto está restringido, tanto por el tráfico en sus tiendas como sus costos de operación más altos en relación con los comerciantes digitales.

El gasto de los comerciantes en gestión de fraudes creció más del 15% por año

Figura 10. Costos promedio de gestión de fraudes (2016-17).

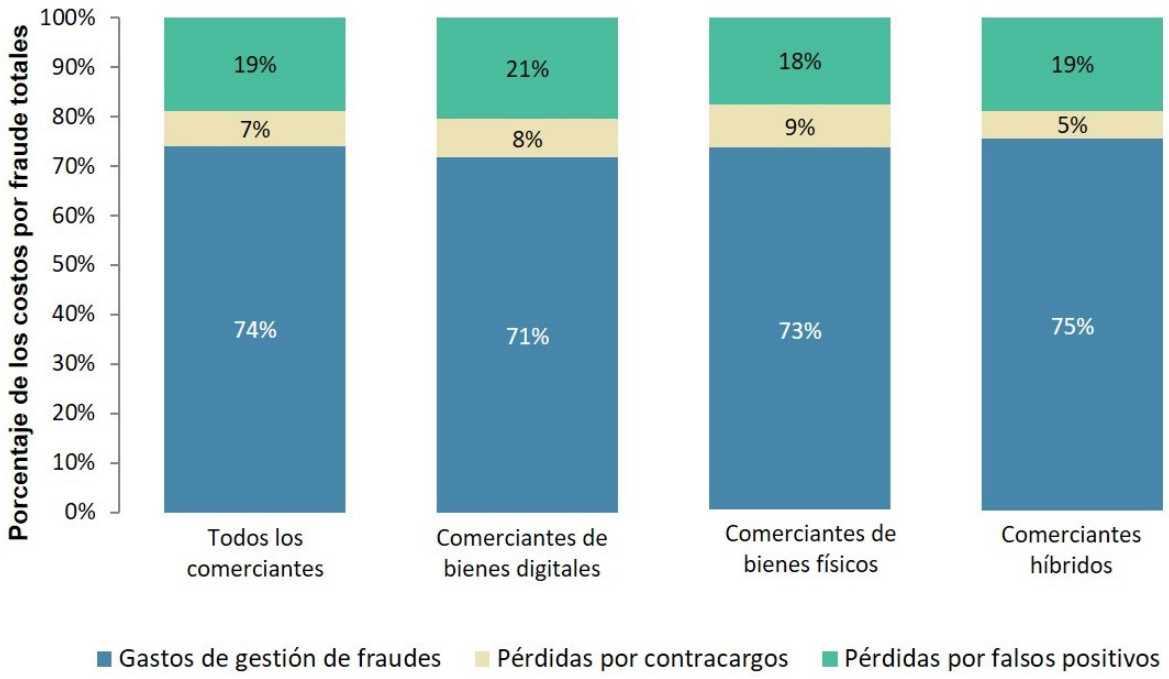


Fuente: Javelin Strategy & Research, 2017

El gasto de la gestión de fraudes es por mucho un componente que supone un alto costo para los comerciantes, representando casi el 75% en promedio (véase la Figura 11). El gasto de los comerciantes en la prevención de la pérdida por fraude es superior a las pérdidas reales en sí, lo que indica claramente la dimensión de la amenaza. También habla de la eficacia de los sistemas con los que se cuenta actualmente, pues cada día se evitan pérdidas por fraude significativas a través de la inversión activa y continua en las medidas de detección y prevención de fraudes. Las áreas principales de la inversión en gestión de fraudes para los comerciantes son administración y servicios y personal de tecnología, donde la subcontratación externa es una prioridad pero está rezagada de las otras dos categorías. La tecnología para la gestión y automatización de procesos de fraude es el área principal del aumento de la inversión para todos los tipos de comerciantes, donde casi dos tercios de los comerciantes de bienes digitales y comerciantes híbridos planean gastar más, junto con la mitad de los comerciantes de bienes físicos. Con la evolución constante de las tácticas de fraude y las capacidades tecnológicas de los defraudadores, mantener y mejorar los sistemas de tecnología de gestión de fraudes pueden verse en forma comprensible como un costo inevitable y crucial para hacer negocios.

La gestión de fraudes representa gran parte de los costos por fraude

Figura 11: Desglose de costos relacionados con fraudes como proporción de los costos por fraude totales.



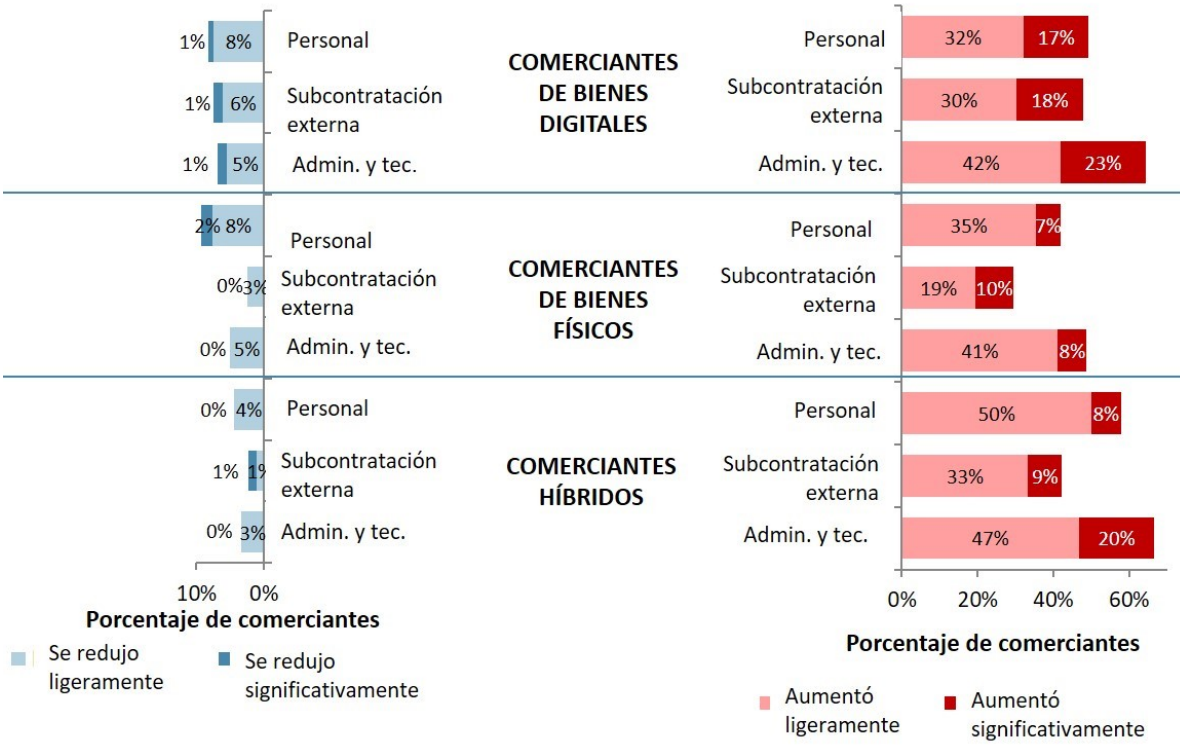
Fuente: Javelin Strategy & Research, 2017

Aproximadamente la mitad de todos los comerciantes se proponen aumentar su gasto en personal de gestión de fraudes, mientras que casi el 60% de los comerciantes híbridos se proponen hacerlo. Dado que estos últimos deben manejar el fraude tanto en los canales físicos como digitales, con sus muy diversas características y tácticas, la necesidad de contar con personal que se centre en cada canal aumenta la inversión que requieren estos comerciantes. Por otra parte, la inversión en personal es una prioridad menor para los comerciantes de bienes físicos, donde el 42% planea aumentar la inversión, pero el 10% reporta planes para reducir el gasto en esa área. Es muy probable que dichos comerciantes hayan incrementado el personal para concluir la conversión a tarjetas con chip y ahora estén volviendo a niveles sustentables. La subcontratación externa es más importante para los comerciantes de bienes digitales que para los demás segmentos, seguidos de cerca por los comerciantes híbridos. Mientras que estos lidian con una mayor complejidad en torno a las operaciones de tarjeta no presente y las transfronterizas, subcontratar la gestión de fraudes a terceros especialistas a menudo resulta ser el enfoque más rentable.

> *"Estamos en un negocio sensible a la conversión, así que nunca ponemos controles sólidos para bloquear a la gente. Esto es todo muy manual, y no estamos intentando bloquear muchas cosas… Nuestro proceso es muy a posteriori. Revisamos cada día para efectos de comprobación después de que se hacen los depósitos. No hay un rechazo automatizado".* - Ejecutivo de fraude, bienes digitales

Las personas, la tecnología y la subcontratación externa atraerán más inversión en 2018

Figura 12: Cambio anticipado en los gastos por gestión de fraudes.

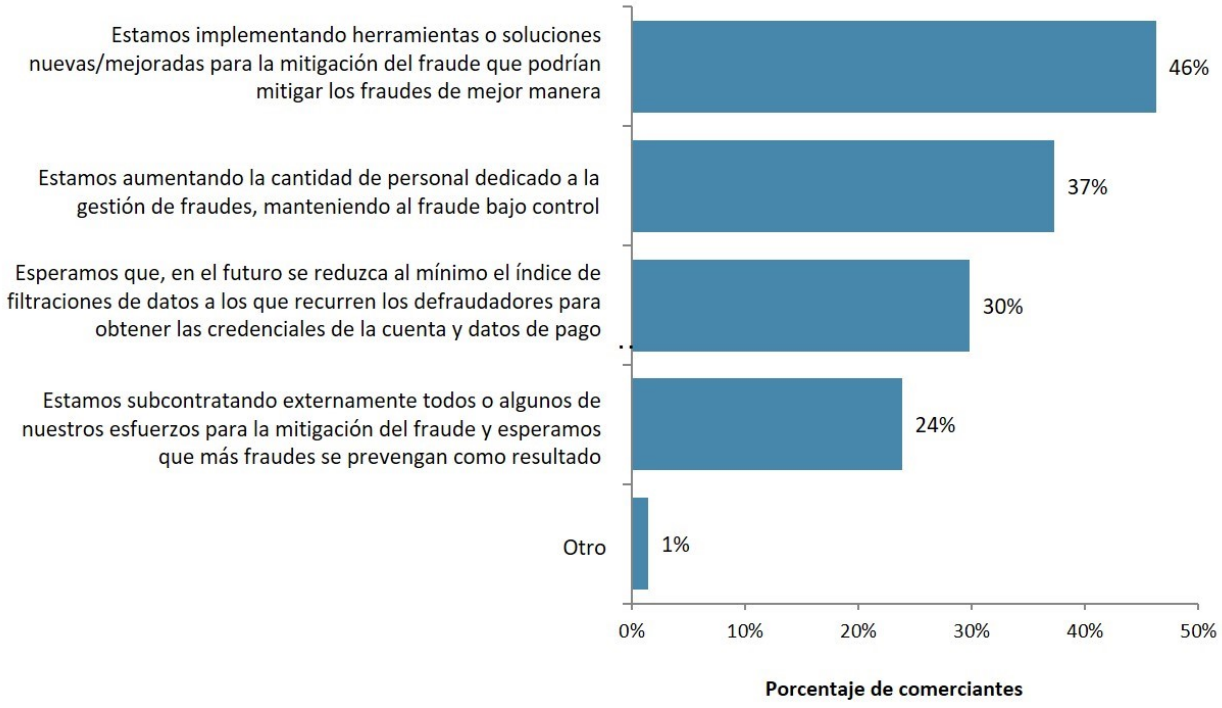


Fuente: Javelin Strategy & Research, 2017

Los comerciantes encuentran motivos para ser optimistas acerca de su capacidad para reducir sus pérdidas por fraude. Casi la mitad de los que esperan una reducción del fraude de TNP espera que las inversiones en herramientas nuevas/ mejoradas contra el fraude (véase la Figura 13) mitigarán las preocupaciones de éste, y más de un tercio espera beneficios de los incrementos en el personal dedicado al fraude. La subcontratación externa es una fuente de esperanza para casi un cuarto de los comerciantes. Asignar actividades para la mitigación del fraude a un tercero dedicado y experto ayuda a asegurarse de que las últimas herramientas y tecnologías están utilizándose para combatir el fraude de un comerciante. También es más probable que una firma de gestión de fraudes de terceros esté actualizada en una amplia gama de los últimos métodos, tácticas y esquemas contra el fraude que el equipo interno de fraudes de un comerciante.

La nueva tecnología y el creciente personal son los principales elementos para mitigar las preocupaciones del fraude

Figura 13: Actitudes en torno a la gestión de fraudes y la experiencia del cliente.



Fuente: Javelin Strategy & Research, 2017

Herramientas para la gestión de fraudes

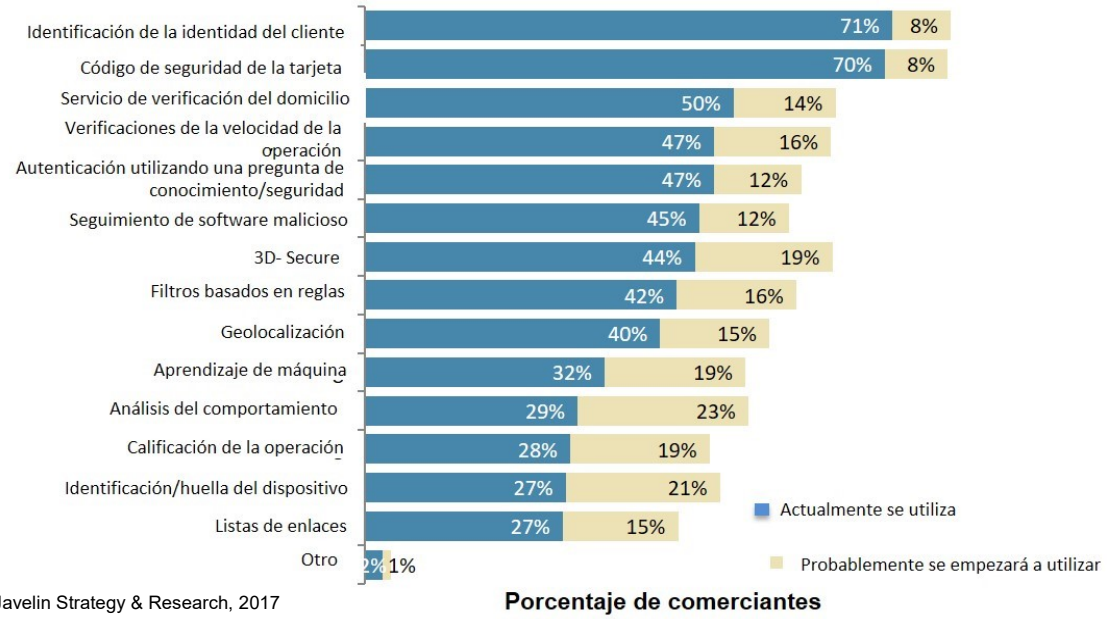
La mayoría de los comerciantes espera aumentar el gasto en tecnología y las medidas antifraude más nuevas son muy atractivas para ellos. Sin embargo, las soluciones correctivas para la mitigación del fraude, tales como la verificación de la identidad del cliente y el código de seguridad de la tarjeta (CVC2 o CVV2) continúan encabezando la lista de las tecnologías en uso para la prevención del fraude (véase la Figura 14).

Las soluciones más populares todavía se basan en validar elementos de datos estáticos y los defraudadores las conocen bien y las abordan fácilmente. La verificación de la identidad del cliente es el proceso de comprobar que la información de identificación personal (PII, por sus siglas en inglés) proporcionada por el cliente es precisa; al tratarse de bienes digitales, esta solución puede ser menos eficaz ya que los domicilios físicos no son un factor. El código de seguridad de la tarjeta es el valor de tres o cuatro dígitos impreso en una tarjeta que se captura durante las operaciones de TNP y es uno de los elementos de los datos que pueden interceptarse en línea u obtenerse por medio de una filtración de datos.

Sin embargo, a pesar de la gran dependencia en los elementos de datos estáticos para la gestión de fraudes, el crecimiento más alto previsto entre los no usuarios consiste en el análisis del comportamiento, la identificación del dispositivo, el aprendizaje de máquina y la calificación de la operación. Con el crecimiento de los volúmenes de operaciones digitales, acompañado del aumento en las maquinaciones de fraudes más sofisticados, las soluciones "invisibles", tales como el análisis del comportamiento, la obtención de la huella de identificación del dispositivo y el aprendizaje de máquina han prometido ayudar a que los comerciantes se enfrenten al desafío sin degradar la experiencia del cliente y con ello alejarlos. La ventaja adicional proviene de tener la capacidad de identificar mejor los ataques de bots, así como en los cuales se ocultan los dispositivos.

Se prevé que el análisis del comportamiento y la obtención de la huella de identificación del dispositivo logren los mayores avances para su adopción entre los comerciantes

Figura 14: Adopción actual y anticipada de herramientas contra el fraude.



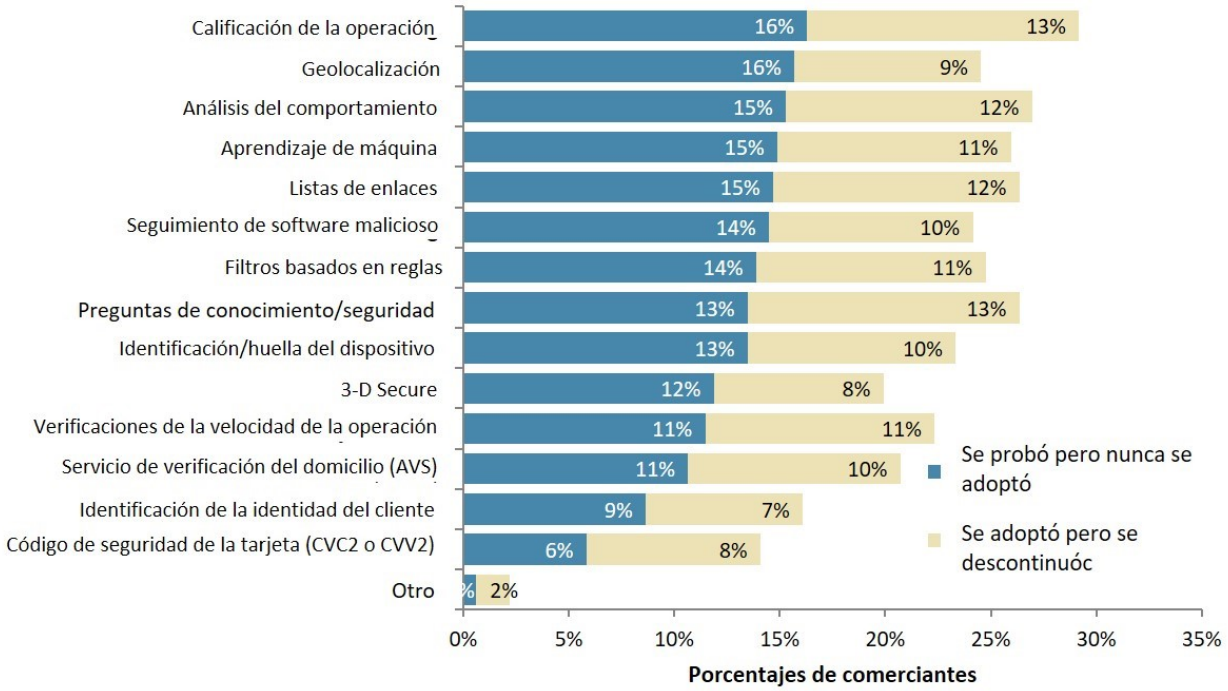
Fuente: Javelin Strategy & Research, 2017

Al mismo tiempo, el análisis del comportamiento y el aprendizaje de máquina se encuentran entre las soluciones que era más probable que los comerciantes probaran pero que no adoptaron o que lo hicieron, pero la descontinuaron (véase la Figura 15). Esto implica que, a pesar de la promesa de la reducción del fraude en combinación con disminuir al mínimo la inconveniencia para el cliente, el rendimiento de la inversión todavía puede ser insuficiente en relación con soluciones más tradicionales.

De manera similar, la calificación de la operación es el producto menos atractivo entre los comerciantes, donde casi un tercio de los comerciantes han probado o adoptado la solución pero ya no la usan más. Considerando que la calificación de la operación tradicionalmente implica o aún requiere la participación de parte del comerciante para establecer reglas, la falta de experiencia interna también puede perjudicar realmente el retorno de la inversión (ROI, por sus siglas en inglés) en esta solución. A pesar de las inversiones en personal previstas que arriba se mencionan, es poco probable que esa dinámica cambie, ya que seis de cada 10 comerciantes consideran que la capacitación contra el fraude es demasiado costosa (véase el Apéndice).

Casi un tercio de los comerciantes prueba o adopta soluciones avanzadas pero no continúa utilizándolas

Figura 15: Descontinuación o falta de adopción de soluciones contra fraudes.



Fuente: Javelin Strategy & Research, 2017

3D Secure (3DS)

3-D Secure, que ostenta la marca de MasterCard SecureCode, Verificado por Visa y Amex SafeKey, es una de las soluciones de prevención de fraudes utilizada más ampliamente en el mundo, en gran parte debido a los mandatos que requieren su uso para las operaciones en línea. En muchos mercados, 3-D Secure ofrece sólidos beneficios a los comerciantes en términos de menores tarifas de intercambio, transferencia de la responsabilidad del fraude al emisor y, por lo tanto, pocos contracargos. Sin embargo, existe el riesgo de mayores rechazos por parte del emisor, así como un abandono más alto del carro de compras debido al paso adicional de autenticación que la solución introduce en el proceso de verificación. Los comerciantes deben equilibrar los beneficios de la prevención del fraude contra la posible pérdida de ventas.

Esta solución ha sido impactada por un componente pesado al que se enfrentan los clientes, por lo que uno de cada cinco comerciantes evita la solución por el miedo al efecto que podría tener sobre la experiencia del cliente. Además de las inquietudes acerca de la experiencia del cliente, un tercio de los comerciantes considera que la solución no tendrá un impacto lo suficientemente grande sobre el fraude para que sea rentable. Desde la perspectiva del cliente, los consumidores en los Estados Unidos se inclinan menos a adoptar el 3-D Secure, debido a la política de cero responsabilidad del fraude para la mayoría de los titulares de tarjetas de dicho país. No existe un incentivo para que los consumidores agreguen fricción a su experiencia de compras cuando el uso de la solución no les proporciona ningún beneficio directo. De acuerdo con los comentarios de los consumidores y sin los mandatos que son comunes en otras partes del mundo, la solución solamente ha sido adoptada por el 44% de los comerciantes en los Estados Unidos (véase la Figura 16). Sin embargo, el hecho de que dichos comerciantes han adoptado la solución no necesariamente significa que la estén utilizando; es sabido que los comerciantes utilizan el 3-D Secure en forma selectiva, de hecho, buscando la manera de aprovecharse del sistema.

Contar con mejores herramientas desalienta a los comerciantes a impulsar el 3D Secure, así como la preocupación persistente sobre la experiencia del cliente

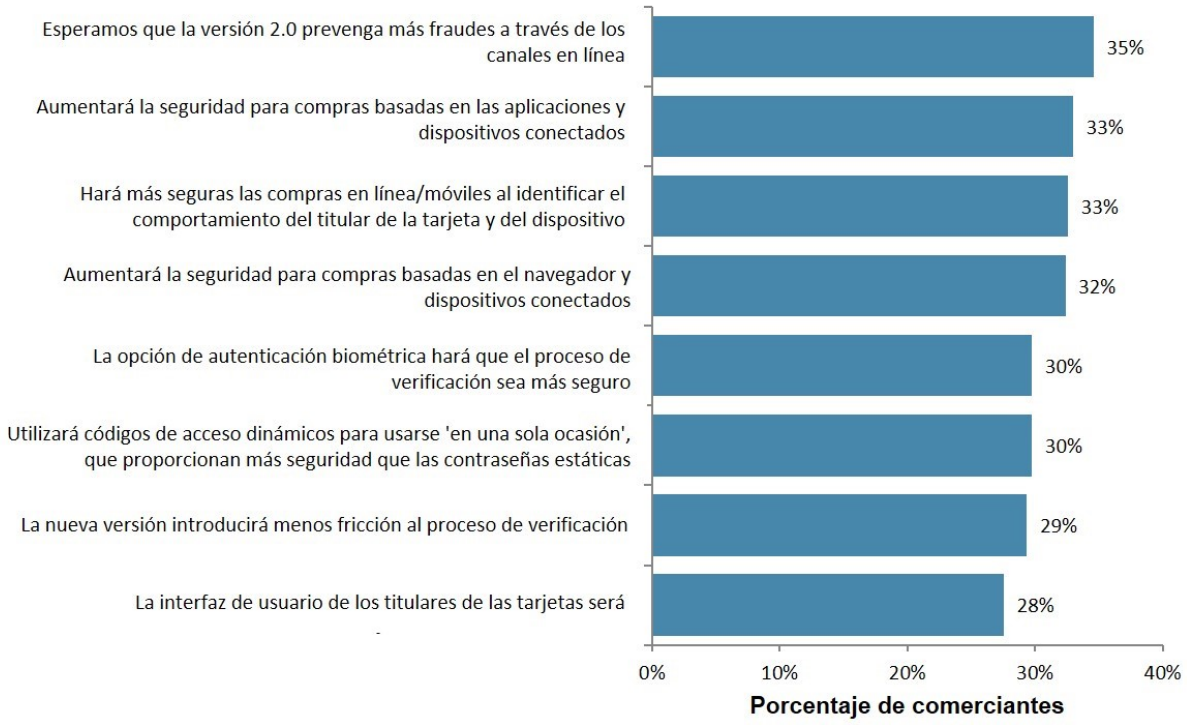
Figura 16: Motivos por los cuales los comerciantes evitan 3D Secure .

Fuente: Javelin Strategy & Research, 2017

El 3D Secure versión 2.0 ha evolucionado la tecnología 3D Secure para permitir un método de autenticación en tiempo real basado en el riesgo que los comerciantes pueden utilizar para enviar atributos de la operación que el emisor puede usar para autenticar a los clientes de manera más precisa, sin pedir una contraseña estática ni demorar la operación, a menos que el análisis del riesgo muestre la necesidad de hacerlo. De acuerdo con algunos informes, estas mejoras en el proceso 3-D Secure han ayudado a disminuir el dolor en el punto de venta (virtual), reduciendo el número de operaciones sujetas a autenticación adicional y disminuyendo el abandono en relación con la versión anterior de 3D Secure. Incluso con este nuevo enfoque de evaluación del riesgo de fraude en la operación, los comerciantes siguen sin estar convencidos de la manera en que el 3-D Secure puede afectar al cliente. Sin embargo, muestran entusiasmo respecto del prospecto de reducir el fraude al utilizar la versión 2.0, en comparación con la experiencia mejorada del cliente (35% y 29%, respectivamente) (véase la Figura 17).

Al enfrentarse al considerable aumento del fraude de TNP, los comerciantes esperan que la capacidad de prevención de fraudes del 3-D Secure sea el beneficio principal

Figura 17: Beneficios previstos de la 3-D Secure versión 2.0 .

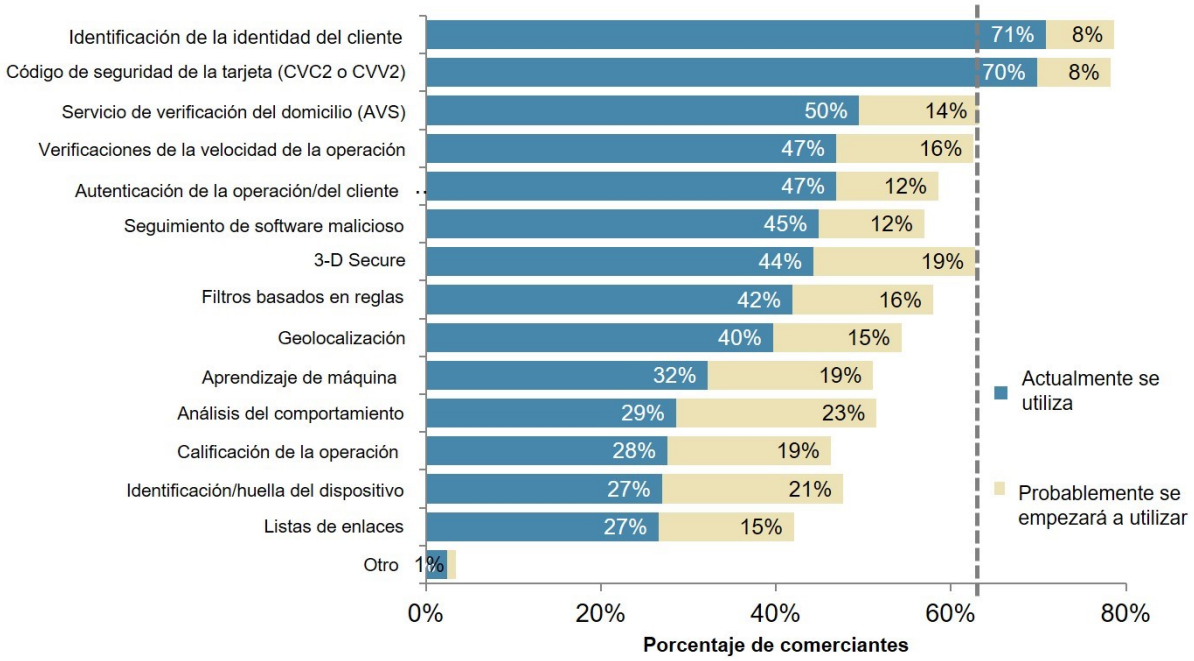


Fuente: Javelin Strategy & Research, 2017

Y, a pesar de las preocupaciones persistentes de la experiencia del cliente en torno al 3-D Secure versión 2.0, hasta el 63% de los comerciantes pueden contar con la solución el año entrante, haciéndola tan generalizada como la verificación del domicilio y a niveles cercanos a las soluciones utilizadas más ampliamente, la verificación de la identidad del cliente y el valor de verificación de la tarjeta (véase la Figura 18).

El 3-D Secure podría ser tan generalizado como la verificación del domicilio en los próximos 12 meses

Figura 18: Uso de soluciones de seguridad, que se espera se adopten en siguientes 12 meses.

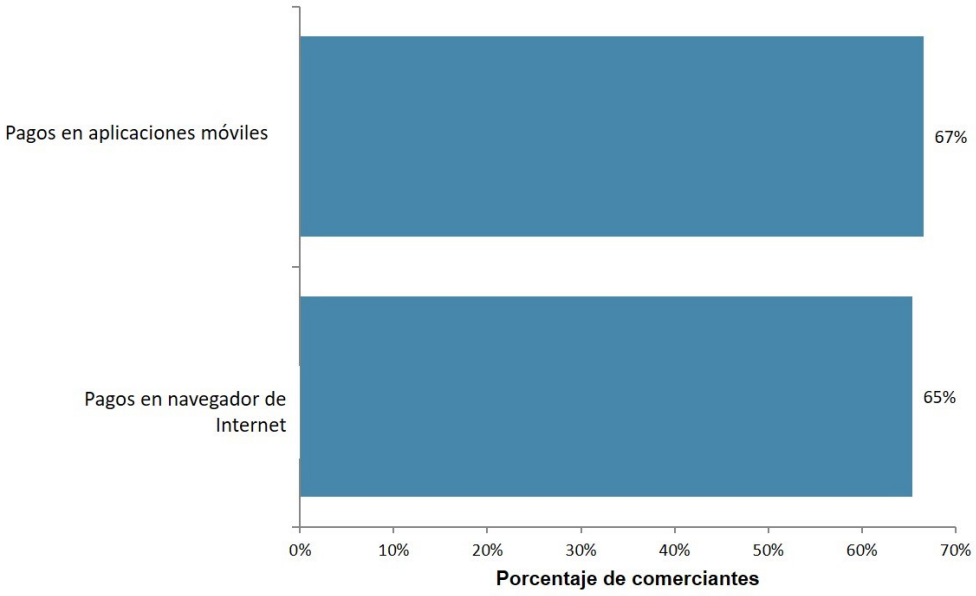


Fuente: Javelin Strategy & Research, 2017

Si bien existe un gran interés en el 3-D Secure versión 2.0 en todos los canales, es especialmente fuerte para las aplicaciones móviles, ya que los comerciantes luchan con el fraude en este canal que cobra importancia (véase la Figura 19). El 3-D Secure se diseñó originalmente en 2001, mucho antes de la era del smartphone, por lo que la interfaz móvil en la versión anterior a la 2.0 fue una idea de último momento mal diseñada. Con el 3-D Secure versión 2.0, mucho se ha hecho para resolver la experiencia deficiente en dispositivos móviles, así como para integrar las carteras móviles y las operaciones dentro de las aplicaciones.

Las aplicaciones móviles son un caso de uso más atractivo para el 3-D Secure que el navegador

Figura 19: Canales donde los comerciantes planean sacar provecho del 3-D Secure .



Fuente: Javelin Strategy & Research, 2017

CONCLUSIÓN

Ya que los consumidores compran bienes y servicios cada vez más por medio de los canales en línea y móviles, los comerciantes están ofreciendo una gama más amplia de productos, métodos de compra y opciones de entrega para atraer a consumidores a sus sitios web y aplicaciones. Si bien esto presenta una enorme oportunidad para que los ingresos de los comerciantes crezcan, y atraigan nuevos segmentos de clientes, también se combina con el impacto de la conversión a tarjetas con chip en el punto de venta que promueve más actividad de fraudes en línea.

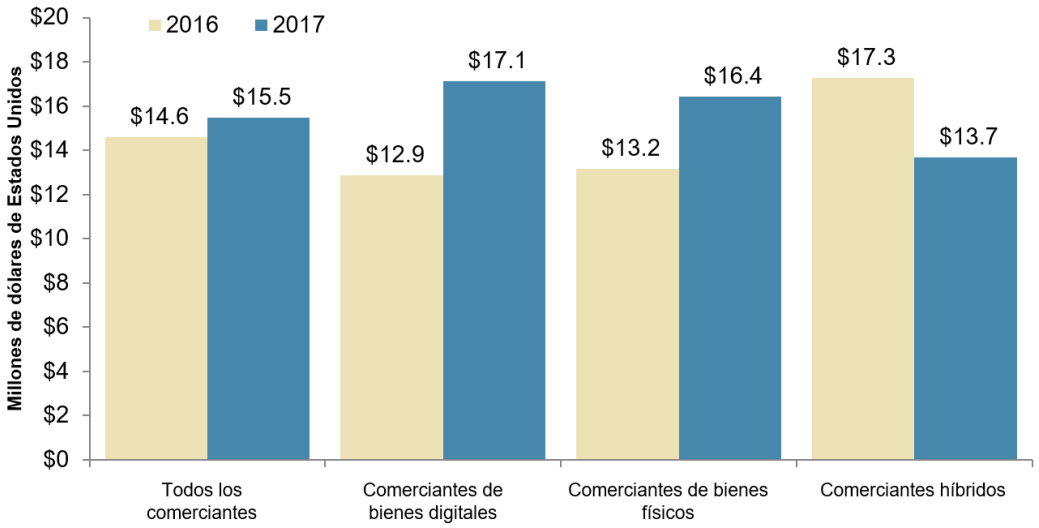
En tanto los riesgos a sus negocios aumentan, los comerciantes deben dedicar una porción cada vez mayor de gastos operativos a la actividad de mitigación del fraude, logrando un equilibrio razonable entre asegurar y autenticar las operaciones de los clientes y conservar la experiencia del cliente y aumentar al máximo la rentabilidad. Muchos comerciantes examinarán la subcontratación externa de sus actividades a un tercero dedicado y experto, permitiendo a esos comerciantes combatir con eficacia el fraude, mientras que se centran más en atraer nuevos clientes e incrementar sus ingresos a través de los canales emergentes.

Las herramientas y técnicas del fraude se desarrollan muy rápidamente, y los comerciantes pueden esperar que continúen aumentando los intentos de fraude tanto en número como en tipo. Los defraudadores tienen los motivos, habilidades y herramientas que necesitan para constituir un desafío considerable para los controles del fraude de los comerciantes y su capacidad para autorizar en forma precisa una operación. La gestión de fraudes continuará siendo un área fundamental de la inversión en el futuro previsible.

APÉNDICE

Los comerciantes gastaron en promedio casi $1 millón más en costos relacionados con fraudes en 2017

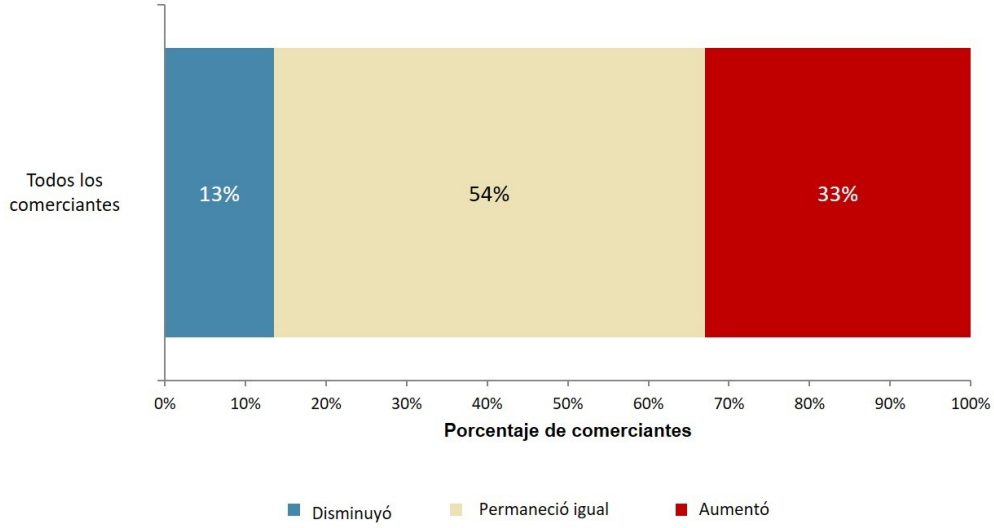
Figura 20: Promedio de costos por fraude totales en dólares (2016-17).



Fuente: Javelin Strategy & Research, 2017

La preocupación por el fraude de TNP ha aumentado en 1 de cada 3 comerciantes

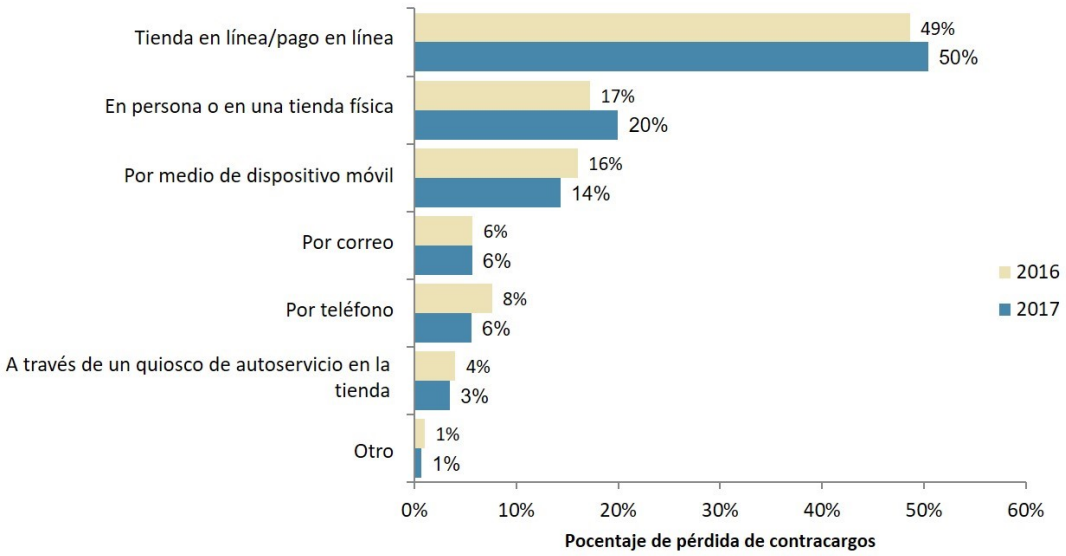
Figura 21: Cambio en la preocupación por fraude de TNP en los últimos 12 meses.



Fuente: Javelin Strategy & Research, 2017

Los comerciantes en línea reciben aún más golpes del fraude en línea

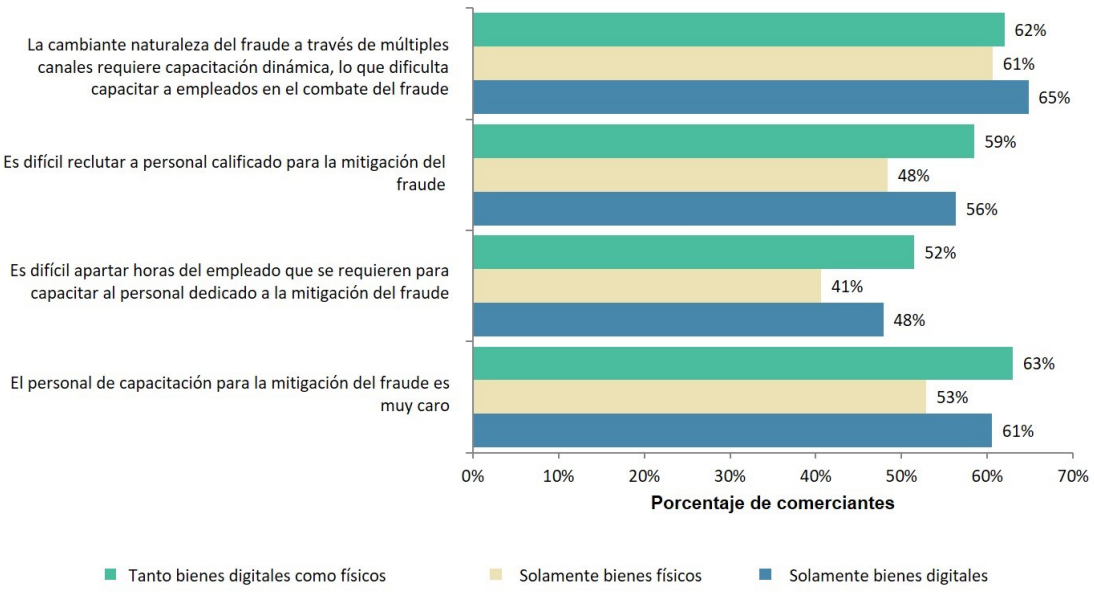
Figura 22: Porcentaje de todas las pérdidas por contracargos por canal.



Fuente: Javelin Strategy & Research, 2017

Fraud Generalmente, los comerciantes son pesimistas acerca de la capacitación del personal para combatir el fraude

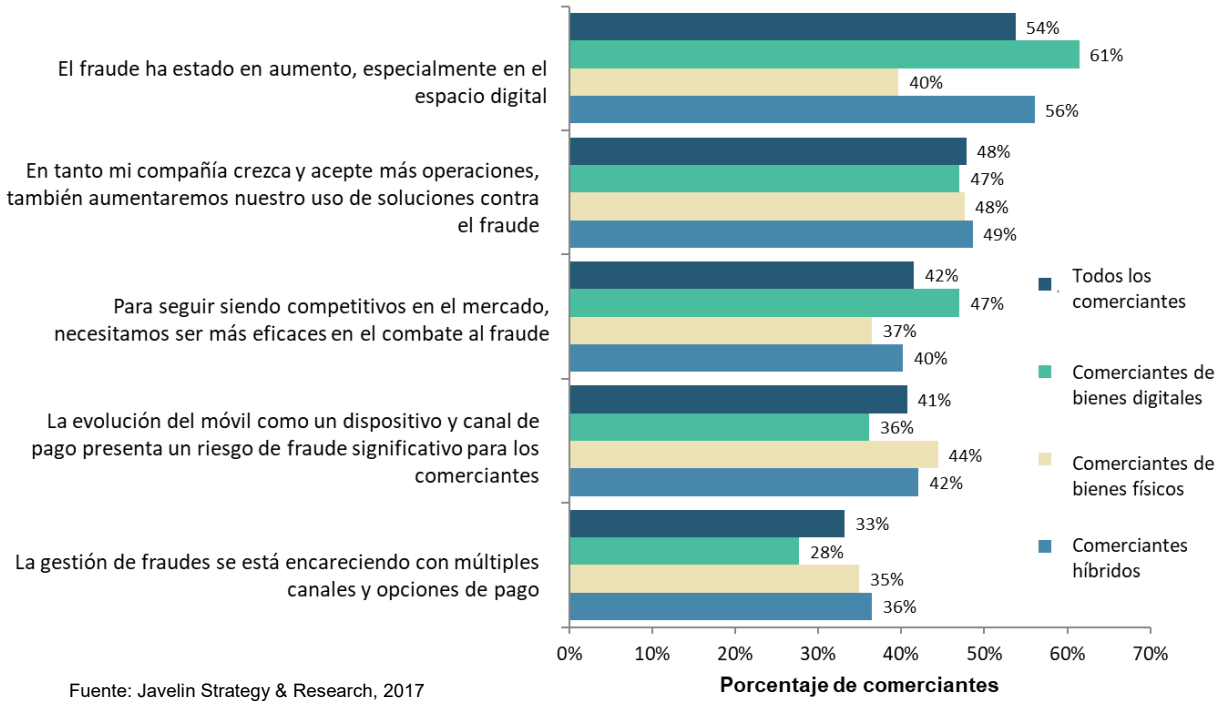
Figura 23: Actitudes en torno a la capacitación del personal de gestión de fraudes.



Fuente: Javelin Strategy & Research, 2017

El crecimiento del fraude en el canal digital motiva el aumento de la inversión

Figura 24: Motivos para el aumento de la inversión en la gestión de fraudes.



Fuente: Javelin Strategy & Research, 2017

METODOLOGÍA

En junio de 2017, Vesta contrató a Javelin Strategy & Research para llevar a cabo un estudio independiente e integral acerca del gasto de los comerciantes en todas las operaciones relacionadas con la gestión de fraudes y administración de cargos a usuarios. Javelin Strategy & Research realizó una encuesta en línea a 497 comerciantes que utilizan el comercio electrónico que ganaban $1 millón o más anualmente, y que pertenecen a los segmentos de comerciantes clave:

- 142 comerciantes que venden solamente bienes digitales.
- 155 comerciantes que venden solamente bienes físicos.
- 200 comerciantes híbridos, que venden ambos tipos de bienes.

Asimismo, se llevaron a cabo entrevistas a profundidad con ejecutivos de la industria que desempeñan roles que tienen influencia sobre los gastos operativos relacionados con la gestión de fraudes y administración de cargos a usuarios.

ACERCA DE JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, una empresa de Greenwich Associates LLC, es una firma de consultoría basada en investigaciones que asesora a sus clientes para que tomen decisiones económicas más inteligentes en un mundo financiero digital. Nuestros analistas ofrecen perspectivas imparciales, factibles y descubren oportunidades que ayudan a que las instituciones financieras, dependencias gubernamentales, compañías de pago, comerciantes, y otros proveedores de tecnología aumenten sus utilidades de manera sustancial.

Autores: Al Pascual, director de Investigación y Jefe del Área de Fraude y Seguridad; Kyle Marchini, analista de Alto Rango, Área de Fraude y Seguridad; Ginger Schmeltzer, Asesora de Alto Rango

Fecha de publicación: Septiembre de 2017.

SOBRE VESTA

Vesta Corporation es líder mundial en soluciones de pago que generan ingresos para socios empresariales en los sectores de telecomunicaciones, medios, financieros y digitales. La tecnología patentada de protección contra fraudes de la compañía ha demostrado que aumenta la conversión y la aceptación, al mismo tiempo que elimina operaciones fraudulentas y responsabilidad de los comerciantes. Vesta ha sido reconocida como empresa innovadora líder en tecnologías de pagos, posee múltiples patentes, y ha ganado numerosos premios como una de las empresas que crece con mayor rapidez en los Estados Unidos. Fundada en 1995 y con oficinas principales en Portland, las operaciones de Vesta abarcan América, Europa y Asia. Para mayor información, visite https://trustvesta.com/es/