Cómo está cambiando el fraude y cómo responder

Los riesgos y la pandemia de COVID-19

La crisis de COVID-19 representa uno de los mayores problemas en la historia del sector de los pagos electrónicos.Con la caída del PIB, una recesión mundial en curso, y un posible cambio en el comportamiento de los consumidores, los préstamos con tarjetas de crédito y débito se verán afectados en muchos aspectos. Sin embargo, en el corto plazo, son los cambios repentinos en el entorno de riesgo los que probablemente causen un fuerte impacto en el desempeño comercial en general.

Visa Consulting & Analytics (VCA) investigó, desde diversos ángulos, el aspecto cambiante del riesgo en los pagos electrónicos. En este documento nos enfocaremos en la administración de fraude.

Casi todos los expertos en gestión de riesgo seguramente tendrán algo de experiencia en trabajar durante una recesión económica. Algunos también pueden haber hecho frente a una verdadera crisis económica, como la crisis financiera mundial de 2008 y 2009. Si bien todavía no podemos medir el alcance del impacto de esta crisis sin precedentes, sabemos del impacto que está teniendo en el comportamiento diario de los consumidores..

A principios de mayo, por ejemplo, *Oxford Economics* informó que el gasto global de los hogares había caído aún más y más rápido que el PIB.[1]

Mientras tanto, el servicio de noticias de la industria de pagos *PYMNTS.com* informó que, en un período de tan solo ocho semanas, se observó: "seis veces más consumidores trabajando desde casa, cuatro veces más consumidores comprando comestibles *online* en vez de ir a la tienda, cuatro veces más consumidores pidiendo comida para llevar por medio de un agregador o a su restaurante favorito, y tres veces más consumidores comprando online otros productos no comestibles."[2]

Los estafadores aprovechan la oportunidad que surge como producto de la confusión, distracción y vulnerabilidad durante la crisis de COVID-19. Pueden esconderse entre los cambios de comportamiento, aprovechar el hecho de que los bancos y los comercios están implementando cambios y se aprovechan de los consumidores desprevenidos.

La tormenta perfecta para un gestor de riesgos. Es presión en su máxima expresión durante todas las fases del ciclo de vida del crédito, todo al mismo tiempo. Y para empeorar las cosas, no hay certeza alguna de cómo evolucionará la crisis, cuánto podría durar o cómo sería la recuperación.

La crisis de COVID-19 pone toda la presión sobre las cuatro fases del ciclo de riesgo

Con un cambio en los fundamentos económicos, es necesario repensar el apetito de riesgo, ajustar la política de adquisiciones y reducir el costo de las mismas.

Con un mayor riesgo en todo el portafolio, el volumen se impulsa hacia la función de cobros, que es el último paso para proteger el rendimiento y la reputación.

A medida que surgen nuevos riesgos, es necesario repensar los modelos de suscripción, pensar seriamente en el sistema de precios basado en riesgos, y prestar especial atención al fraude.

A medida que evolucionan los comportamientos de los clientes, las prácticas de gestión de clientes deben seguir el mismo camino, incluida la gestión de líneas de crédito, los planes de pago, la gestión de autorizaciones y la detección de fraudes.

1 *"Coronavirus Watch As restrictions ease, a slow revival", Oxford Analytics,* 4 de mayo de 2020: *http://resources.oxfordeconomics.com/coronavirus-watch-as-restrictions-ease-a-slow-revival?oe most recent content download id=0000029&interests trending topics=coronavirus*
2 *"Why Consumers Aren't In A Rush To Reopen The Economy" PYMNTS.com,* 4 de mayo de 2020: *https://www.pymnts.com/coronavirus/2020/no-rush-to-reenter-physical-world/*

Por lo tanto, la industria de los pagos está experimentando un cambio profundo y repentino en la naturaleza del riesgo de los pagos electrónicos. Se espera que, en el corto plazo, este cambio impactará fuertemente en el rendimiento general de cualquier negocio de pagos electrónicos. En este documento nos enfocamos en la gestión de clientes, que comprende la detección y administración de fraudes.

Existen tres puntos clave en materia de detección y administración de fraudes.

1 Primero, y más importante, es saber que la situación actual es el terreno ideal para los atacantes.

Entre los tipos de actividad que se reportaron: ataques de fuerza bruta, intentos de retiro de efectivo en cajeros automáticos, estafas de *phishing* y compras falsas de criptomonedas, donaciones y maniobras de *click-and-collect*. Mientras tanto, los incidentes que involucran a la seguridad cibernética siguen siendo un motivo grave de preocupación. Emisores, comercios y adquirentes deben permanecer alertas en todo momento y entorno.

Esto se suma al hecho de que los índices de fraude tienden a ser más altos en el canal de *eCommerce*, por lo que cualquier cambio en la combinación de pagos con tarjeta presente (CP) a tarjeta no presente (CNP) probablemente traerá un aumento en la relación fraude-ventas.

2 Segundo, la crisis ha hecho que muchos de los sistemas que utilizan los equipos de prevención de fraude se vuelvan menos útiles.

Por ejemplo, desde el punto de vista de detección de fraude, muchas herramientas analizan la actividad de gasto fuera de lo normal, sin seguir un patrón. Sin embargo, durante la crisis, el comportamiento de compra difícilmente siga un patrón. Entonces, el índice de falsos positivos aumenta inevitablemente.

3 Tercero, los emisores, comercios y adquirentes deben prepararse para un aumento de "fraude en primera instancia".

A raíz de las dificultades financieras que algunos clientes pueden estar atravesando, es posible que algunos se vean tentados de cuestionar transacciones legítimas. Del mismo modo, con consumidores confinados en sus casas que se embarcan en una racha de compras compulsivas online, también podría aumentar la cantidad de consumidores que se arrepienten de su compra y generar una "oleada" de reclamos y disputas. También puede haber un aumento de eventos de fraude por solicitud de cuenta.

Mientras tanto, con el crecimiento de transacciones CNP, quizás sea inevitable que también aumente el "fraude amigable". Cuando los tarjetahabientes revisan sus resúmenes de cuenta, es posible que encuentren transacciones que parecen fraudulentas —categorías nuevas en las que nunca antes había comprado online, nombres de comercios que no son lo suficientemente descriptivos para relacionar el artículo comprado con el monto de la transacción y múltiples cargos relacionados con una sola compra (por ejemplo, si los minoristas dividen los cargos según el monto de la compra y los gastos de envío).

Si bien es muy temprano para evaluar el impacto total de esto, la industria de pagos se está preparando para grandes desarreglos. Por ejemplo, aparentemente varios grandes procesadores de pagos están reteniendo los depósitos para protegerse de un aumento esperado de contracargos y, a raíz de la crisis, se dice que la disputa de transacciones por parte de los tarjetahabientes en EUA se ha duplicado y hasta triplicado.[3]

Ante este panorama, el desafío del gestor de riesgos consiste en mantenerse alerta y adaptarse a las nuevas realidades, todo esto sin descuidar la calidad en la experiencia del cliente. En momentos en que los comportamientos de pago están cambiando y es probable que se formen nuevos hábitos, un enfoque demasiado rígido en la administración de fraude podría llevar fácilmente a un consumidor a usar otra tarjeta.

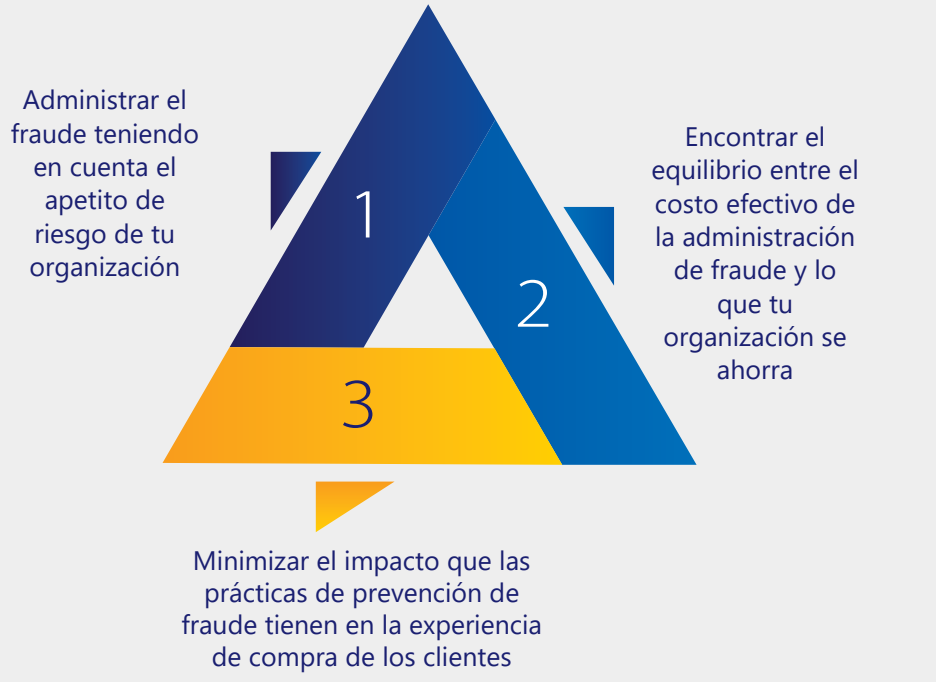
3 "Hit by Coronavirus—and a 30% Holdback by the Payment Processor", Wall Street Journal, 15 June 2020: https://www.wsj.com/articles/hit-by-coronavirusand-a-30-holdback-by-the-payment-

Verdades universales

Si bien todavía tenemos que determinar cómo evolucionará la crisis y cuáles pueden ser los impactos a largo plazo, podemos basarnos en algunas verdades universales.

En lo que al momento de pago respecta, el consumidor siempre ha buscado —y lo seguirá haciendo— la combinación ideal de confianza, conveniencia, velocidad, simplicidad y aceptación universal.

Paralelamente, la función de la administración de fraude siempre ha sido, y será, girar en torno a tres parámetros que se relacionan entre sí:



Estos tres parámetros siempre determinarán el papel y la actividad de la función de administración de fraude. La forma del triángulo puede cambiar, pero estos principios se mantienen intactos. La tarea del gestor de riesgo es mantener un balance y equilibrio.

Los detalles de la respuesta deben ajustarse a cada circunstancia en particular en la que se encuentre el emisor, tamaño y naturaleza de su portafolio, el entorno de fraude en el que opere y el nivel de crisis en el que se encuentre su mercado local. VCA ha recopilado nueve imperativos que considera relevantes para cualquier emisor sin importar dónde opere.

Nueve imperativos para los equipos de fraude durante la pandemia COVID-19

#1

Prepárate para maniobras de fraude de prueba de cuenta - como los ataques de enumeración o fuerza bruta

Es posible que este sea el riesgo actual más grande de todos.

Los estafadores están aprovechando la crisis que sacude al *eCommerce* en todo el mundo para camuflar sus maniobras de prueba de cuenta. Utilizando los ataques de enumeración o fuerza bruta, envían solicitudes de autorización de manera sistemática al BIN de un emisor para obtener credenciales de pago legítimas.

Entonces debes estar atento a cualquier incremento inusual durante la contabilización de transacciones. Presta atención a los rechazos por número de cuenta no válido y permanece atento a los aumentos de actividad de solicitudes de autorización (por ej.: solicitudes muy seguidas con unos segundos entre cada una y del mismo origen).

Si sospechas que está por cometerse un fraude, analiza la situación rápidamente. También, identifica aquellas solicitudes de autorización con números de cuenta secuenciales y aplica protección adicional as cuentas con números similares.

#2

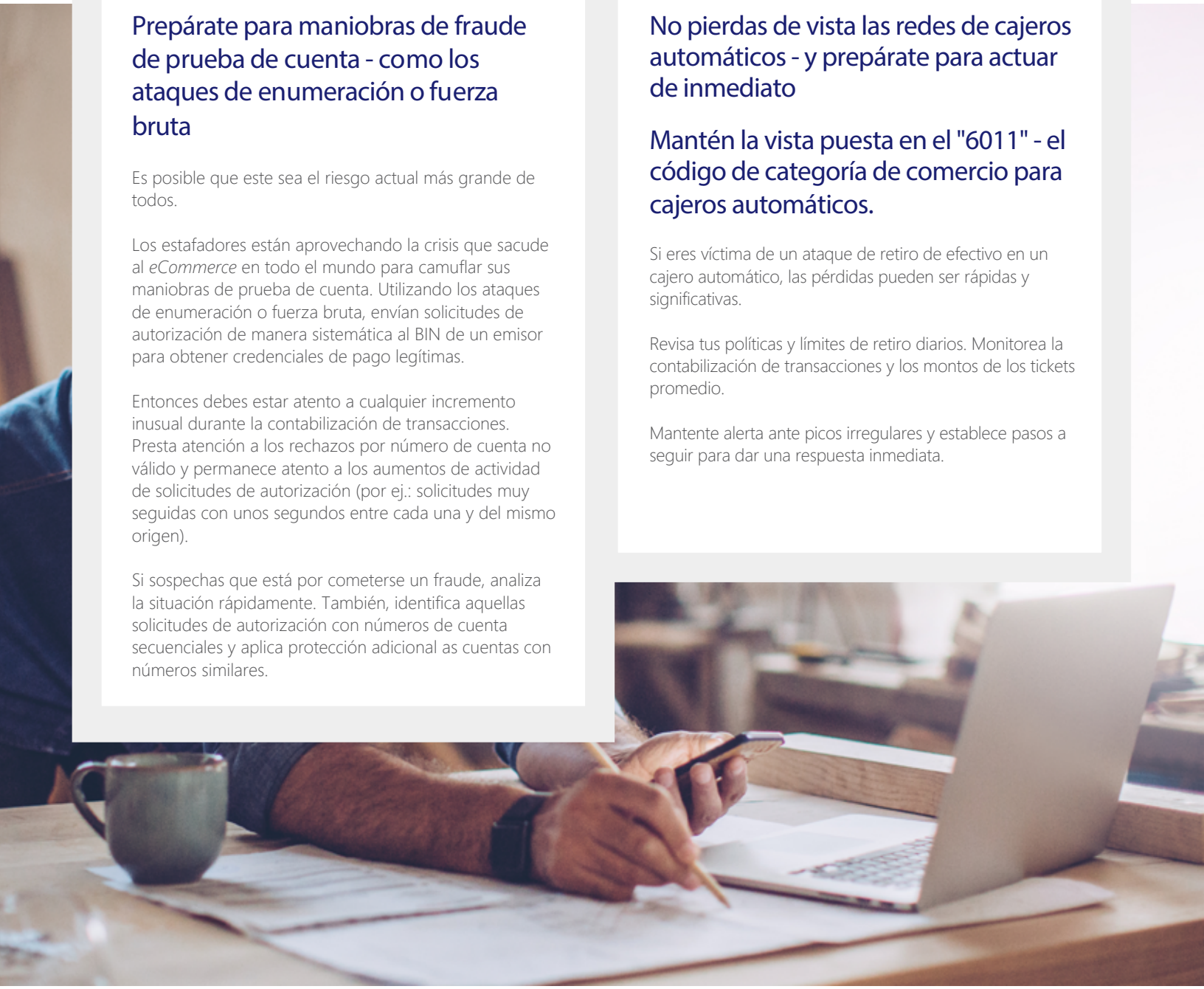
No pierdas de vista las redes de cajeros automáticos - y prepárate para actuar de inmediato

Mantén la vista puesta en el "6011" - el código de categoría de comercio para cajeros automáticos.

Si eres víctima de un ataque de retiro de efectivo en un cajero automático, las pérdidas pueden ser rápidas y significativas.

Revisa tus políticas y límites de retiro diarios. Monitorea la contabilización de transacciones y los montos de los tickets promedio.

Mantente alerta ante picos irregulares y establece pasos a seguir para dar una respuesta inmediata.



#3

Interactúa con todo el ecosistema - y ayuda a tus pares a ayudarte

El trabajo de todo el sector unido es una de las mejores defensas que tenemos. Participa activamente en los foros de la industria, colabora con las autoridades del ámbito de la seguridad pública y comparte con tus pares tendencias y posibles soluciones. Es muy importante que no pierdas de vista tus reportes de fraude. Cuanto más pronto hagas los reportes, más pronto los sistemas de Visa tomarán los datos para nutrir su red. Con herramientas como *Visa Advanced Authorization* (VAA) y *Visa Risk Manager* (VRM), los riesgos emergentes se pueden erradicar antes de que se conviertan en tendencia.

#4

Ten en cuenta que cualquier fisura en tu sistema de seguridad podría verse fácilmente y quedar expuesta

Los estafadores estarán al acecho buscando puntos vulnerables en tus operaciones y en la seguridad de tus portafolios.

Por ejemplo, si hasta hoy no contabas con personal de prevención de fraude durante el horario nocturno o fines de semana, es momento de que lo hagas. Del mismo modo, si tienes personal trabajando desde casa, pero sin acceso a las herramientas y a la tecnología que sí podrían acceder estando en las instalaciones de la empresa, sería conveniente que les ofrezcas algo de respaldo.

No pierdas de vista los riesgos que también pueden enfrentar tus proveedores. Por ejemplo, si tercerizas parte de tus operaciones de prevención de fraude a otro, ¿sabes cómo está manejando esta crisis?

En momentos como este, debes optimizar tu capacidad de prevenir el fraude y evitar que se vea comprometida.

#5

Comunica, educa y alienta a tus tarjetahabientes

Mantén una comunicación proactiva con tus tarjetahabientes y aprovecha para educarlos y trasmitirles seguridad.

Procura comunicarles que, a raíz de que estás muy atento a cuestiones de seguridad, es posible que reciban más comunicados y/o solicitudes de verificación de lo normal.

Además, adviérteles sobre cualquier tipo de fraude frecuente o nuevo en tu mercado. Recuérdales también qué tipo de alertas o mensajería SMS envías.

.

#6

Confía en tus recursos analíticos

La clave para identificar patrones de fraude nuevos o desconocidos muy probablemente radique en los datos de tus transacciones existentes. Desafía continuamente a tus equipos de analítica a estar en la búsqueda constante de indicadores de comportamiento de fraude.

Y, lo que es aún más importante, si hasta ahora los reportes eran trimestrales o mensuales, probablemente quieras agilizar las cosas llevándolos a una frecuencia semanal o diaria.

Además, antes de la pandemia, es muy probable que los índices de fraude CNP de tu organización estuvieran sesgados debido al alto volumen de transacciones relacionadas con viajes. Para hacer una comparación homogénea, debes excluir las transacciones relacionadas con viajes, que probablemente serán minúsculas una vez que pase el confinamiento.

#7

Responde al aumento de alertas de fraude rápidamente, de forma sistemática y sensata

Inevitablemente recibirás muchas alertas de riesgo de fraude. Deberás aceptar el hecho de que, a causa de la migración masiva al eCommerce y el aumento en el comportamiento de gasto sin seguir un patrón, el sistema de puntuación de riesgos de tu organización se debilitará un poco.

Entonces, analiza nuevamente las reglas que has implementado para la prevención de fraude y asegúrate de que están alineadas a los cambios forzosos que se generan en el comportamiento de pago diario priorizando tus acciones de investigación.

Procede cuanto antes para actualizar tus modelos de riesgo. Por ejemplo, los modelos de fraude bajo supervisión deberán ajustarse rápidamente y con más frecuencia debido a los cambios de comportamiento. A partir de esta pandemia, casi todos los gastos se hacen sin seguir un patrón, y el índice de falsos positivos aumenta. Con este escenario en mente, es importante que reportes nuevos eventos de fraude lo antes posible, incluyendo nuevos hallazgos, y que hagas los ajustes necesarios. Y si aún trabajas con técnicas basadas en reglas, esta puede ser una llamada de atención a actualizarte y adoptar lo último en activos de datos, herramientas y tecnologías.

#8

Revisa tus planes de manejo de crisis y gestión de eventos cibernéticos a la luz del COVID-19

Es muy probable que los planes de manejo de crisis y contingencias, y los análisis de seguridad cibernética que tenías, se hayan diseñado bajo circunstancias totalmente diferentes. Sería oportuno echarles un vistazo con ojos de COVID-19 y analizar qué se debe cambiar y cómo.

Por ejemplo, ¿con qué rapidez y eficiencia podrías lidiar con un compromiso grande o un evento cibernético importante? ¿Qué tan expuesto quedarías? La capacidad de tus equipos y sistemas, ¿está preparada para dar respuesta rápida?

#9

No olvides el toque humano

Si sucediera lo peor, y una cuenta se viera comprometida, inicia una comunicación abierta y activa con tu cliente. ¿Qué espera generalmente?

- Que le informes en caso de que haya fraude
- Que le creas
- Que el problema se resuelva en pocos días
- Que lo mantengas informado de cada paso
- Que lo guíes durante todo el proceso de recuperación
- Que le recomiendes pasos a seguir para evitar fraudes futuros

También es una oportunidad para convertir una posible situación difícil en un motivo para que tu cliente sea leal a tu marca.

Si bien la crisis de COVID-19 ha afectado a empresas de todas partes, es cierto que los desafíos pueden traer oportunidades. El equipo de Visa Consulting & Analytics puede asesorarte para que tu empresa responda mejor a esta pandemia.

Sobre Visa Consulting & Analytics

Somos un equipo global de cientos de consultores de pago, científicos de datos y economistas en los seis continentes.

- Nuestros consultores cuentan con décadas de experiencia en la industria de pagos y son expertos en estrategia, producto, gestión de portafolio, riesgos, recursos digitales y más.
- Nuestros científicos de datos son expertos en estadísticas, analítica avanzada y machine learning con acceso exclusivo a datos obtenidos a través de VisaNet, una de las redes de pago más grandes del mundo.
- Entender las condiciones económicas que afectan al consumo permite a nuestros economistas brindar información única y oportuna sobre las tendencias de consumo global.

La combinación de nuestra amplia experiencia en consultoría de pagos, nuestra inteligencia en estrategias económicas y la amplia variedad de datos con la que contamos, nos permite identificar conocimientos prácticos y recomendaciones que ayudan a tomar mejores decisiones comerciales.

Para obtener ayuda para abordar cualquiera de las ideas o principios anteriores, puedes contactar a tu ejecutivo de cuenta Visa y coordinar un horario con nuestro equipo Visa Consulting & Analytics o enviar un correo electrónico a **VCA@Visa.com**. También puedes visitarnos en **Visa.com/VCA.**

