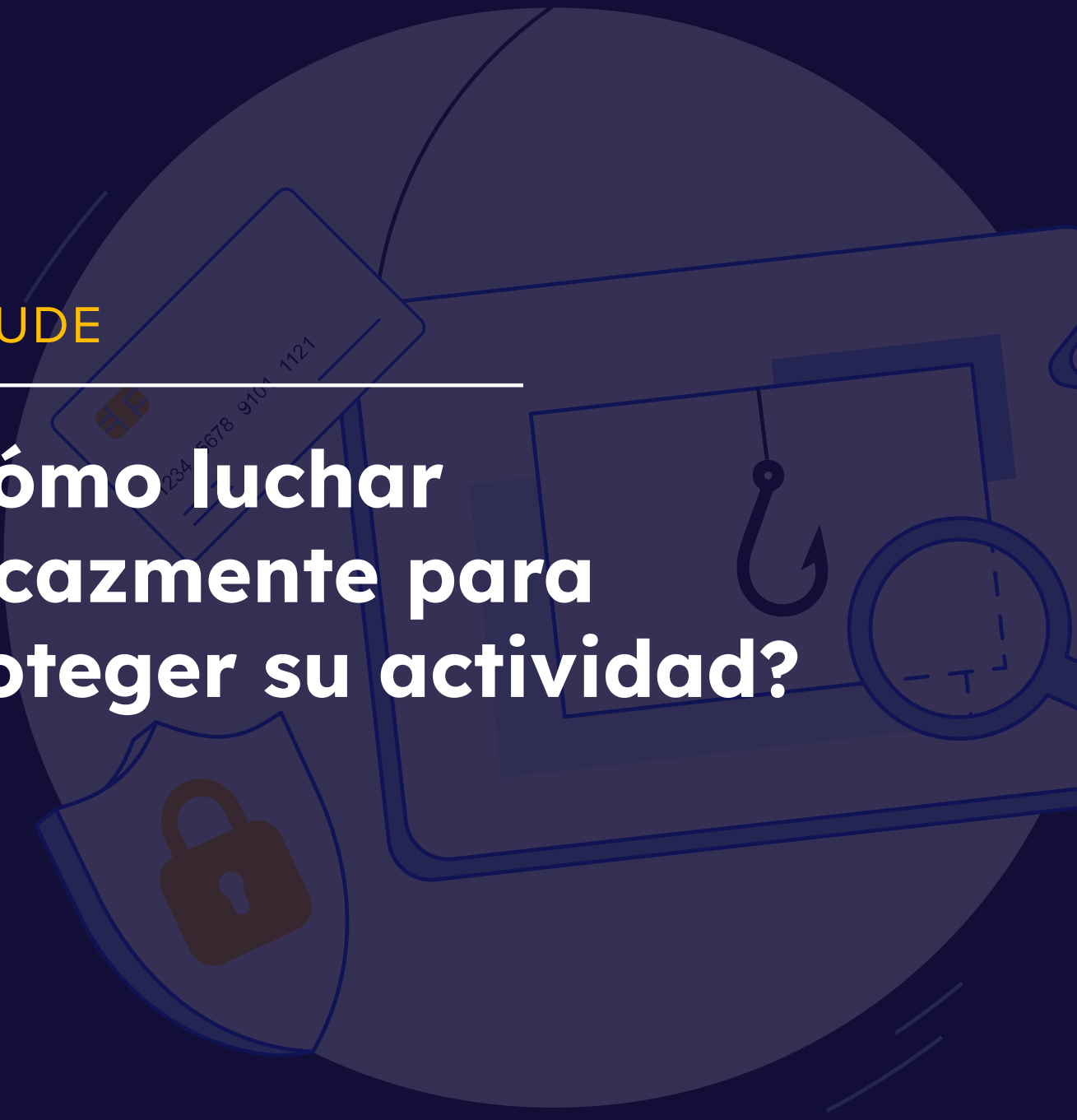
Lyra

FRAUDE

¿Cómo luchar eficazmente para proteger su actividad?



E-COMMERCE & IN-STORE

ÍNDICE

CONTEXTO DEL FRAUDE

Cada año, miles de comercios ven cómo pagos aparentemente validados se transforman en pérdidas muy reales. Una transacción aceptada no garantiza siempre un cobro efectivo: el fraude y los chargebacks pueden duplicar rápidamente el coste de una venta y afectar a la rentabilidad de una actividad.

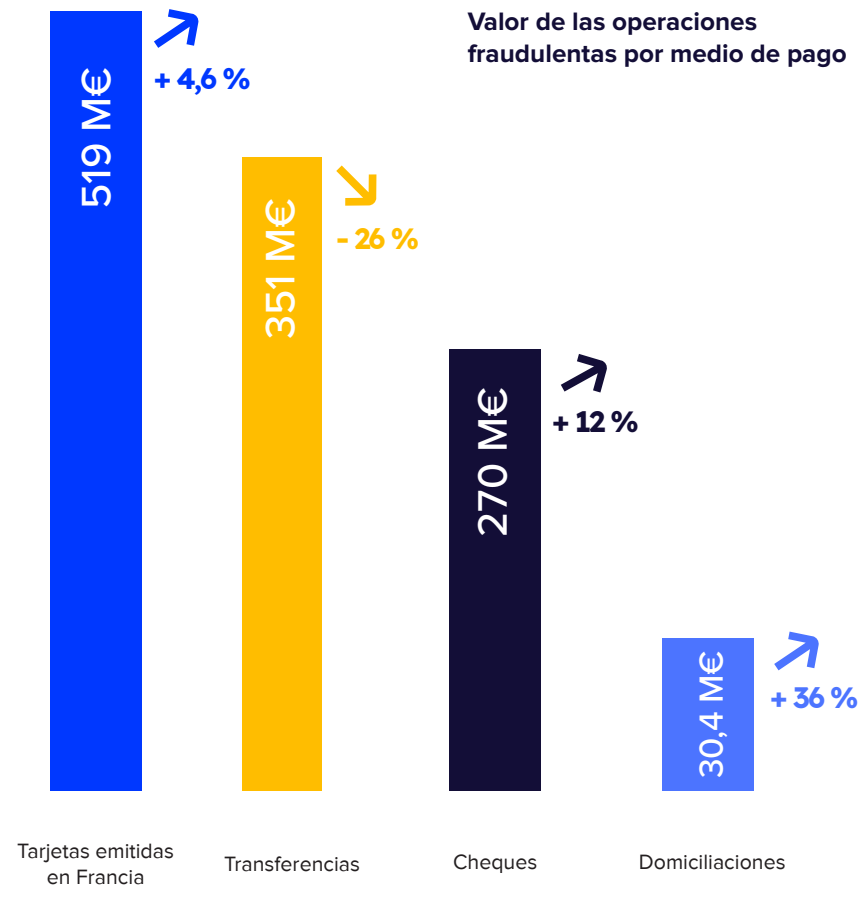
Según el Observatorio de la Seguridad de los Medios de Pago (OSMP), el fraude en Francia representó 1.200 millones de euros en 2024, correspondientes a 7,8 millones de transacciones.

La tarjeta, principal medio de pago en el día a día, concentra el 40,2 % del fraude en valor y el 94 % en volumen. Las transferencias, seguidas de los cheques y las domiciliaciones, representan respectivamente el 29,5 % (350 M€), el 22,7 % (270 M€) y el 2,6 % (30 M€).Estas cifras demuestran que el fraude afecta a todos los medios de pago, tanto en e-commerce como en el punto de venta físico.

Ante esta realidad, una constatación es clara: el fraude no desaparecerá. Sin embargo, puede anticiparse, controlarse y transformarse en un factor de fiabilidad y confianza.

Proteger su actividad implica adoptar los reflejos adecuados, comprender los comportamientos fraudulentos, anticipar su evolución y desplegar defensas sólidas, flexibles e inteligentes.

Este libro blanco ofrece un análisis de los principales riesgos, de los métodos utilizados por los defraudadores y de las buenas prácticas para prevenirlos. Porque una infraestructura de pago bien dominada no solo protege: impulsa el rendimiento y se convierte en una palanca estratégica de crecimiento.



Datos recopilados por el Observatorio de la Seguridad de los Medios de Pago (OSMP) en 2024

¿QUÉ ES EL FRAUDE **EN LOS MEDIOS DE PAGO?**

Definición

Este fraude se produce cuando un medio de pago (tarjeta, transferencia, domiciliación, cheque) se utiliza sin la autorización de su titular o es objeto de una reclamación abusiva. En ambos casos, el comercio sufre consecuencias directas: pérdida del importe del pedido, costes adicionales y una relación de confianza con sus clientes debilitada. Comprender los mecanismos del fraude permite recuperar el control de la infraestructura de pago y transformar un riesgo en un factor de fiabilidad y rendimiento.

Fraude externo

El titular de la tarjeta o del medio de pago no es el origen de la transacción. Sus datos bancarios han sido comprometidos (robo, phishing, piratería informática) y son utilizados por un tercero para realizar una compra fraudulenta. El comercio sufre entonces una pérdida inmediata con la recepción de un impago, difícilmente impugnable si la transacción no ha sido objeto de una autenticación reforzada (como 3D Secure).

Fraude amistoso

Más insidiosa, el denominado fraude amistosa se basa en una declaración falsa. El cliente sí es el origen del pago, pero lo impugna voluntariamente ante su banco. El objetivo es obtener un reembolso abusivo conservando el bien o el servicio. Este tipo de fraude se observa especialmente en los modelos de suscripción.

El titular de la tarjeta valida el primer pago (autenticado mediante 3D Secure) y, posteriormente, impugna los pagos siguientes —denominados MIT (Merchant Initiated Transactions)— con el fin de interrumpir su suscripción sin pasar por un procedimiento clásico de cancelación.

Ya sea externo o "amistoso", el fraude no se limita a un pedido perdido.
Impacta directamente en:

- **La tesorería,** debido a flujos financieros inestables.
- **La productividad,** por el tiempo dedicado a la gestión de litigios.
- **La relación con el cliente,** por una confianza degradada que amenaza la fidelización.

EL RETO DE **UN COMERCIO**

El principal desafío de un comercio hoy en día es claro: **conciliar crecimiento y seguridad.**

En otras palabras, autorizar las transacciones legítimas al tiempo que se limita el fraude que reduce los márgenes.

Tres objetivos clave, que vinculados a los retos de la empresa, pueden aumentar el riesgo de fraude.

Objetivo		Reto	
Recorrido de compra fluido	VS	Competitivos	**Un recorrido de compra debilitado.** Un proceso demasiado restrictivo hace que los clientes se decanten por competidores que ofrecen una experiencia más fluida.
Incremento de la facturación	VS	Financieros	**Transacciones impugnadas.** Cada chargeback conlleva el reembolso del importe inicial, así como costes adicionales. Un impacto inmediato en los márgenes.
Fidelización y captación de clientes	VS	Imagen y reputación	**Una confianza debilitada.** Los incidentes repetidos alteran la percepción de fiabilidad y deterioran la relación con el cliente a largo plazo.

La cuestión, por tanto, no es únicamente reducir el fraude. Se trata de apropiarse de la infraestructura de pago para convertirla en un catalizador de confianza y rendimiento. Al dominar los riesgos, el comercio agiliza sus recorridos de compra, protege sus márgenes y respalda un crecimiento sostenible.

¿QUÉ ES UN **CHARGEBACK?**

Definición

Una transacción validada no siempre es sinónimo de un cobro efectivo.

En e-commerce, una venta puede parecer finalizada… hasta que el cliente impugna la operación ante su banco. En ese caso, los fondos ya abonados se retiran de la cuenta del comercio y se restituyen al comprador. Se trata entonces de un **impago**, también denominado **chargeback**.

Nota: un impago puede ser impugnado en función de su motivo, aportando documentos justificativos. No obstante, la resolución a favor del comercio no está garantizada.

El **chargeback** / **impago** puede clasificarse en dos **categorías**.

Impago por fraude

El comprador impugna la transacción alegando no ser el origen de la misma.

- Si la transacción ha sido autenticada mediante 3D Secure con transferencia de responsabilidad, el comercio está protegido financieramente y el riesgo es asumido por el banco del comprador.
- En los demás casos, el comercio recibe un impago, lo que puede generar un coste directo y un impacto inmediato en el rendimiento de su actividad. No obstante, los impagos siguen siendo impugnables y los fondos pueden recuperarse según los procedimientos establecidos.

Impago por servicio

El comprador impugna la transacción por un motivo de litigio comercial. Por ejemplo, declara no haber recibido el producto o que el servicio prestado no se corresponde con la descripción inicial.

- Este tipo de impago puede ser impugnado mediante **pruebas tangibles** (justificantes de entrega, capturas del pedido, seguimiento logístico).
- La capacidad del comercio para **documentar** cada etapa de su proceso se convierte entonces en un factor clave para asegurar sus ingresos.

Impactos de un impago

Un impago no se limita a una simple venta perdida. Afecta directamente a la rentabilidad de una actividad comercial. Sus consecuencias son múltiples:

- **Pérdida de facturación** correspondiente al importe del pedido.
- **Costes adicionales** facturados por el banco.
- Tiempo de gestión administrativa que **reduce** la productividad.
- Tesorería **desestabilizada**.
- Confianza del cliente e imagen de marca **deterioradas**.

EL OBJETIVO DE **LOS DEFRAUDADORES**

La finalidad de un fraude relacionado con un medio de pago es siempre la misma para el defraudador: **obtener un beneficio económico.**

Esto se traduce en distintas estrategias:

- **Desviar medios de pago legítimos:** recopilación de datos de pago para su reutilización o reventa.
- **Explotar datos robados:** multiplicación de transacciones para probar datos de pago y generar un beneficio inmediato antes de ser detectado.
- **Convertir el beneficio:** reventa rápida de bienes, solicitud de reembolsos mediante otro medio de pago, etc.

Riesgos variables según los medios de pago

Cada medio de pago presenta **niveles de vulnerabilidad distintos**:

- **Riesgo financiero directo:** pagos con tarjeta sin transferencia de responsabilidad, domiciliaciones SEPA impugnadas, etc.
- **Riesgo de fraude:** pagos con tarjeta sin autenticación reforzada, por ejemplo.

Las técnicas de fraude evolucionan constantemente. Por ello, la lucha contra el fraude no puede limitarse únicamente a herramientas técnicas. Exige un **control** continuo, una **vigilancia** activa y una capacidad de **anticipación** frente a los distintos escenarios de ataque.

¿CÓMO **PROTEGERSE?**

La lucha contra el fraude no se basa en una única solución. Requiere un enfoque global que combine el control de los riesgos, la vigilancia activa, el conocimiento del cliente y el uso óptimo de las herramientas de prevención. Es esta combinación la que convierte la protección en un **factor sostenible de fiabilidad y rendimiento.**

Conocer los riesgos

El primer paso para reforzar la seguridad de una actividad consiste en **cartografiar sus vulnerabilidades.** No todos los medios de pago implican el mismo nivel de riesgo.

- **Las transacciones sin autenticación reforzada,** como los pagos MOTO (Mail Order / Telephone Order) o las introducciones manuales, se encuentran entre las más expuestas.
- Por el contrario, un pago con tarjeta validado mediante **3D Secure** con transferencia de responsabilidad ofrece una mayor protección al comercio, ya que el riesgo es asumido por el banco del comprador. La transferencia de responsabilidad implica que, cuando la autenticación 3D Secure se realiza con éxito, es el banco del comprador —y no el comercio— quien asume las pérdidas financieras en caso de fraude.

Algunas situaciones requieren asimismo una vigilancia reforzada:

- Pedidos **internacionales** procedentes de zonas sensibles.
- Carritos **atípicos** o importes excepcionalmente elevados.
- **Nuevos** clientes sin historial suficiente para analizar su comportamiento.

Anticipar estos factores permite adoptar una postura proactiva, en lugar de defensiva, y optimizar las decisiones de validación.

Conocer a sus clientes

Más allá del análisis de los medios de pago, el conocimiento detallado de los comportamientos de los clientes constituye **un pilar esencial de la prevención**. Cuanto mejor conoce un comercio los hábitos de sus compradores, más fácil le resulta detectar rápidamente las anomalías.

Que un cliente fiel cambie repentinamente de país, de dirección o de importe medio de compra puede justificar un control adicional. Por el contrario, un nuevo cliente que multiplica los intentos de pago o solicita una entrega fuera de la zona geográfica definida por el comercio representa una señal de alerta que no debe ignorarse.

En muchos casos, **un simple contacto directo** (correo electrónico o teléfono) basta para despejar las dudas. Sin embargo, si persiste la incertidumbre, es preferible bloquear un pedido sospechoso que exponer la actividad a un impago con consecuencias significativas.

Utilizar las herramientas disponibles

Las soluciones de pago integran hoy en día **módulos potentes y eficaces** de detección y prevención del fraude. Aún es necesario saber activarlos y configurarlos de manera óptima.

Entre las reglas y herramientas que puede poner a disposición un PSP como Lyra se encuentran:

- **Módulos de seguridad:** autenticación reforzada 3D Secure, filtros antifraude, scoring dinámico.
- **Bloqueo geográfico e IP:** rechazo automático de transacciones procedentes de determinadas zonas o direcciones IP sospechosas.
- **Rechazos selectivos:** exclusión de tarjetas prepago o de uso único, frecuentemente utilizadas por los defraudadores.
- **Alertas inteligentes:** activación de una validación manual en caso de comportamiento sospechoso.

Un seguimiento **periódico** de los chargebacks ya registrados permite ajustar y perfeccionar las reglas de filtrado, reforzando así la precisión y la eficacia del dispositivo.

En caso de duda, el PSP puede acompañar al comercio en el análisis de transacciones sensibles y en la optimización de los parámetros de seguridad.

Mantener la vigilancia

El fraude evoluciona constantemente: los defraudadores perfeccionan sus escenarios, explotan nuevas vulnerabilidades y ponen a prueba de forma continua los límites de los sistemas. Para seguir siendo competitivo, un comercio debe implantar una vigilancia activa y regular de su actividad.

Algunos indicios deben llamar la atención:

- Pedidos **urgentes** o solicitudes atípicas de entrega exprés.
- **Incoherencias** entre las direcciones de facturación y de entrega.
- **Múltiples** intentos de pago fallidos en serie.
- **Cambios** repentinos en la información (dirección, correo electrónico, número de teléfono).
- Conexiones desde una dirección IP **sospechosa** o incoherente con el perfil del cliente.

La vigilancia no es responsabilidad exclusiva del **gestor**: debe ser compartida por todos los **colaboradores**, desde el soporte hasta la logística, para detectar y comunicar rápidamente los comportamientos sospechosos.

Estos indicios no siempre constituyen un fraude probado, pero requieren una verificación rápida. Mientras el producto no haya sido enviado o el servicio prestado, el comercio conserva el control: **bloquear, reembolsar o anular la transacción sigue siendo posible.**

Lyra

Los escenarios de fraude que conviene conocer

EL CARDING

“El defraudador intenta pagar utilizando varias tarjetas con el mismo BIN (primeros dígitos de la tarjeta).”

Definición

El carding es un fraude en e-commerce que consiste en probar de forma masiva números de tarjetas bancarias robadas o falsificadas con el fin de identificar aquellas que siguen activas. Los defraudadores utilizan bots o scripts automatizados que envían, en cuestión de minutos, cientos de intentos de pago. A menudo, estos intentos proceden del mismo BIN y se basan en datos obtenidos mediante phishing, malware o bases de datos revendidas en foros clandestinos.

Incluso sin que se complete una compra real, el carding genera impactos:

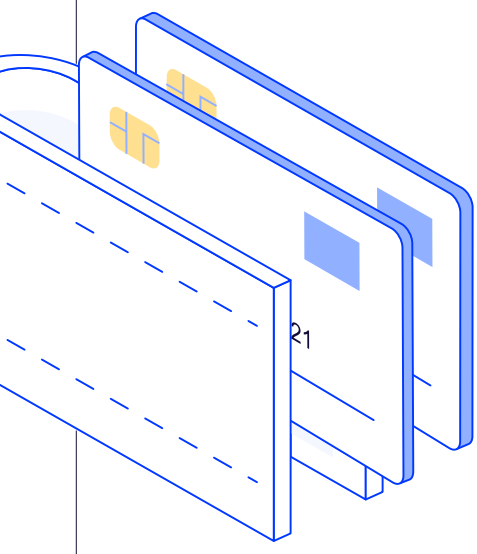
- Técnicos: saturación del servidor de pago, ralentizaciones, bloqueos.
- Financieros: multiplicación de los costes de autorización.
- Reputacionales: pérdida de confianza de clientes y socios.

Las tarjetas validadas se utilizan posteriormente para cometer otros fraudes en distintos comercios.

Detectar el carding

Varios indicadores pueden alertar al comercio de una actividad sospechosa:

- Una **misma dirección de correo electrónico o IP** intenta numerosas transacciones con tarjetas diferentes.
- **BIN o fechas de caducidad** idénticas en varios intentos.
- **Fallos** repetidos seguidos de uno o dos pagos validados.
- Pedidos realizados en horarios **inusuales**, en ocasiones durante la noche.
- Actividad elevada procedente de zonas **geográficas poco habituales.**



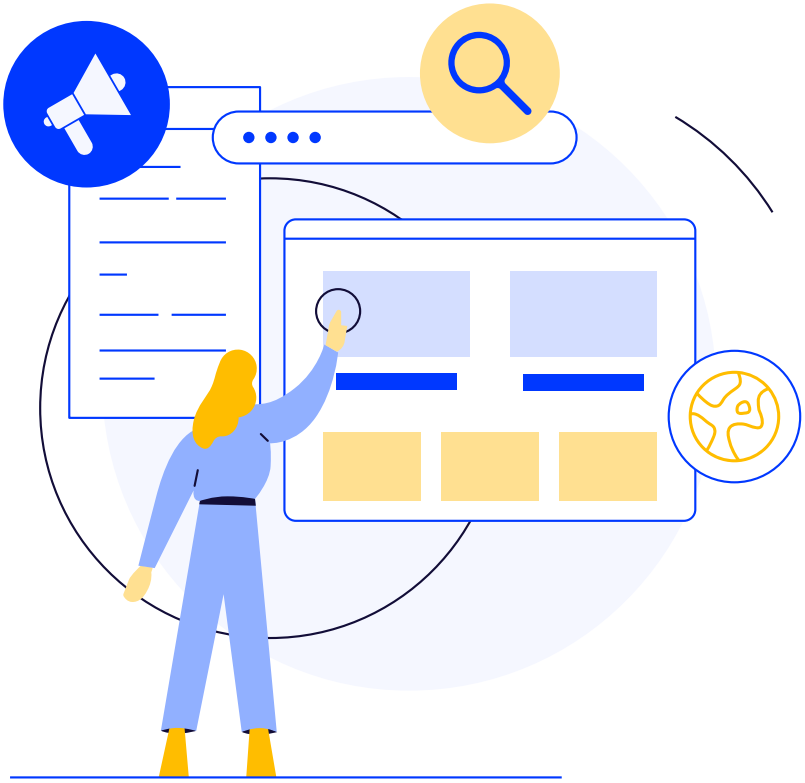
El carding nunca es invisible.
Con herramientas de seguimiento adecuadas, puede detectarse rápidamente.

¿Cómo protegerse?

Para contrarrestar el carding, no basta con reaccionar a posteriori: el enfoque debe ser **preventivo y proactivo**. Entre las buenas prácticas esenciales se incluyen:

- Implantar **reglas de velocidad**, por ejemplo, bloquear una dirección de correo electrónico que utilice más de tres tarjetas en cinco minutos.
- Utilizar **herramientas y filtros** inteligentes proporcionados por el PSP: scoring dinámico, supervisión en tiempo real, alertas automatizadas.
- Desplegar **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart), pruebas que permiten diferenciar a un humano de un robot y frenar los scripts automatizados.
- **Supervisar** los intentos de pago fallidos, que suelen ser señales precursoras de un ataque de carding.
- **Bloquear** o anular las transacciones sospechosas antes del envío, incluso si el pago parece validado.

Al reforzar la vigilancia y aprovechar plenamente las herramientas de prevención, un comercio puede **neutralizar el carding antes de que afecte a su rendimiento y comprometa la fiabilidad de su sitio.**



ABUSO DE CONFIANZA – **MOTO**

"El defraudador solicita realizar un pago a distancia mediante la introducción manual de los datos de la tarjeta por parte del comercio (MOTO: Mail Order / Telephone Order)."

Definición

El **MOTO** (Mail Order / Telephone Order) designa una transacción introducida manualmente por el comercio, ya sea en un **TPV físico en tienda** o a través de un **formulario de pago en e-commerce**, sin autenticación reforzada. Esta práctica, aún utilizada en determinados sectores para responder a solicitudes a distancia, representa una **vulnerabilidad importante.**

Los defraudadores explotan este canal poco seguro contactando directamente con el comercio, a menudo bajo el pretexto de una urgencia o de una situación excepcional, y utilizan números de tarjetas bancarias robadas.

La transacción se valida, el producto se entrega, pero unos días más tarde el verdadero titular de la tarjeta impugna la operación.

Resultado: el comercio sufre un impago y asume en solitario la pérdida financiera.

Modo operativo

Comercio (víctima)		Cliente (defraudador)
Recibe un pedido por teléfono, en línea o por correo electrónico.	1	Se presenta como un cliente con prisa, incapaz de desplazarse, y exige una entrega rápida.
El pedido resulta atractivo, lo que le incita a aceptarlo.	2	Facilita varios números de tarjeta hasta que uno de ellos funciona.
Introduce manualmente los datos de las tarjetas utilizadas por el defraudador.	3	Solicita rápidamente la confirmación de la entrega.
Una vez validada la transacción, expide el pedido.	4	Envía a un tercero para recoger el paquete en un plazo muy corto.
Días después, recibe impagos no impugnables vinculados a las tarjetas utilizadas.	5	Desaparece con el pedido, con el objetivo de revenderlo, y deja de estar localizable.

¿Cómo protegerse?

- Extremar la vigilancia en productos con **alto valor de reventa.**
- Desconfiar de pedidos atípicos o con importes anormalmente elevados, especialmente cuando incluyen una **entrega urgente**.
- Solicitar un documento de identidad o **una prueba** de titularidad de la tarjeta antes de aceptar la transacción..
- Concienciar a los equipos para que aprendan a decir no, incluso bajo presión.
- Limitar al máximo el uso del **MOTO** y priorizar pagos con **autenticación reforzada**, por ejemplo mediante un **enlace de pago seguro.**

ABUSO DE CONFIANZA – **GOLD DIGGER**

“El defraudador muestra un gran interés por lo que vendo, ya que podrá revenderlo fácilmente.”

Definición

El fraude por **abuso de confianza** se dirige especialmente a los comercios que venden productos de **alto valor y fácil reventa**, como smartphones, productos electrónicos o piezas mecánicas.

El defraudador se presenta como un cliente legítimo: realiza un pedido, insiste en una entrega urgente y, posteriormente, recoge el producto para revenderlo rápidamente.

Unos días más tarde, el verdadero titular de la tarjeta impugna el pago.

Para maximizar sus beneficios, el defraudador multiplica los intentos con distintas tarjetas, a menudo procedentes de países diversos, y utiliza una misma dirección de entrega, en ocasiones la de cómplices.

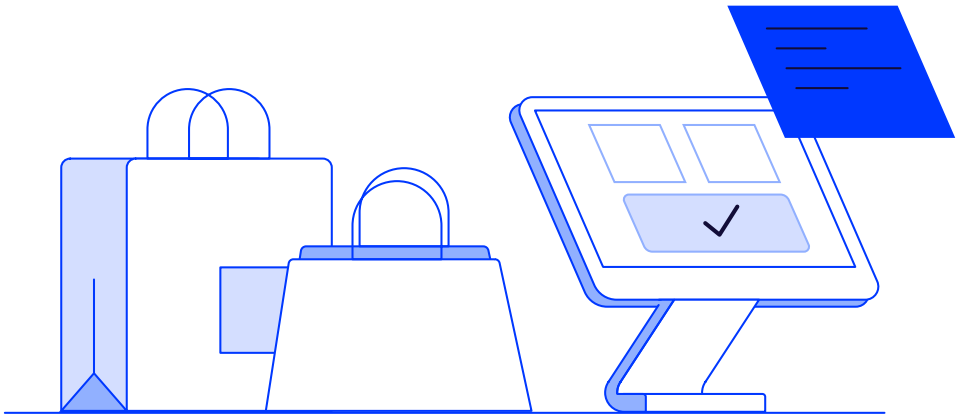
En este escenario, el comercio asume **en solitario la pérdida financiera.**

Detectar al “gold digger”

Algunos indicios permiten identificar este tipo de fraude:

- Una **misma dirección de correo electrónico** prueba varias tarjetas en muy poco tiempo, a menudo desde zonas geográficas diferentes.
- Varias cuentas o compradores distintos utilizan la misma **dirección de entrega**.
- Tras realizar el pedido, el cliente contacta con el servicio de atención para **acelerar la entrega**, insistiendo de forma reiterada en la urgencia.

Atención: un defraudador experimentado sabe mostrarse cooperativo y tranquilizador. Por ello, contactar directamente con el cliente no siempre es suficiente para identificar el fraude.



¿Cómo protegerse?

Controlar la velocidad y las zonas de riesgo:

- **Bloquear** o generar una alerta cuando una misma dirección de correo electrónico prueba varias tarjetas en pocos minutos.
- **Filtrar** por zona geográfica: si la clientela es mayoritariamente local, restringir determinadas zonas de riesgo o fuera de Europa.
- **Verificar** las direcciones de entrega: una misma dirección utilizada por varias cuentas debe activar una alerta, salvo en el caso de puntos de recogida conocidos.

Formar a los equipos:

- **Sensibilizar** al servicio de atención al cliente sobre los pedidos de riesgo: cualquier solicitud insistente debe activar la vigilancia.
- **Fomentar la prudencia:** retrasar o bloquear un envío en caso de duda es preferible a asumir una pérdida directa.
- **Documentar** cada interacción sospechosa para crear un historial útil en caso de litigio.

Combinar vigilancia humana y herramientas automáticas:

Incluso cuando están bien camuflados, estos intentos pueden contrarrestarse mediante una combinación de reglas sencillas y vigilancia humana.

Los filtros y sistemas de detección no siempre identifican todas las señales. Un control manual dirigido a pedidos de alto valor o que presenten varios criterios de riesgo refuerza la detección y preserva las ventas.

EL CAMUFLAJE

“El defraudador intenta hacerse pasar por un cliente normal.”

Definición

El **camuflaje** es una de las formas de fraude más insidiosas para los comercios. A diferencia de los ataques masivos o evidentes, el defraudador apuesta por la discreción.

Su objetivo es imitar en todos los aspectos a un cliente legítimo para realizar una transacción fraudulenta sin despertar la menor sospecha.

Este escenario resulta especialmente peligroso porque, en cuanto el defraudador llama la atención, es bloqueado de inmediato. Por ello, se adapta jugando con los detalles: comportamiento de compra realista, importes plausibles, información creíble.

El comercio descubre el fraude demasiado tarde, generalmente en el momento del **chargeback**, una vez que el pedido ha sido enviado y las pérdidas ya son irreversibles.

Detectar el camuflaje

Identificar a un defraudador camuflado es complejo y constituye una de las formas de fraude más difíciles de detectar en tiempo real. No obstante, algunos indicios pueden alertar:

- **Transacciones inusuales:** varios pedidos de pequeño importe realizados en poco tiempo con la misma tarjeta o el mismo correo electrónico.
- **Direcciones sospechosas:** una misma dirección de entrega utilizada por distintos compradores.
- **Identidades dudosas:** nombres escritos íntegramente en minúsculas, formulaciones extrañas, juegos de palabras sospechosos o incluso suplantación de celebridades como clientes.
- **Reclamaciones frecuentes:** impugnaciones repetidas de compras o múltiples devoluciones por motivos discutibles.

Nota: una señal aislada no siempre basta para detectar a un defraudador camuflado. En cambio, la observación de un **patrón recurrente a lo largo del tiempo** suele permitir identificar estos comportamientos discretos y proteger la actividad.

¿Cómo protegerse?

Para contrarrestar el camuflaje, es esencial combinar **reglas automáticas, vigilancia humana y análisis continuo de los datos históricos.**

Implementar reglas reactivas

- **Bloquear** correos electrónicos sospechosos: cualquier dirección ya utilizada en fraudes debe excluirse automáticamente.
- **Supervisar** las direcciones de entrega utilizadas por varias cuentas y activar una alerta o un bloqueo en caso de sospecha.
- **Reglas de velocidad:** varias transacciones cercanas en el tiempo con la misma tarjeta o el mismo correo electrónico deben ser señalizadas.

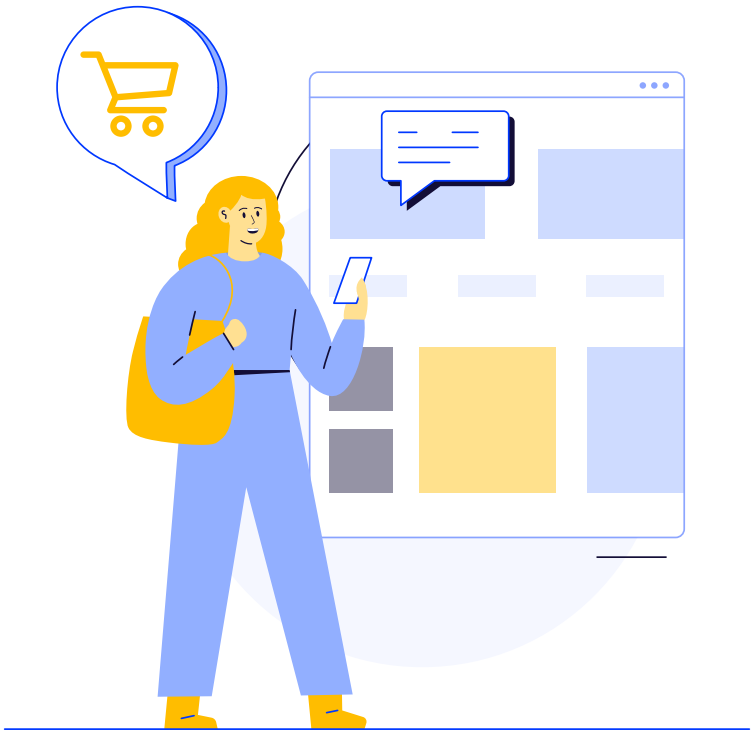
Sensibilizar a los equipos

- Formar a los equipos para identificar estas señales débiles refuerza considerablemente la protección.

Conservar y analizar los datos para enriquecer las reglas de protección

- Cada fraude pasado es una oportunidad de aprendizaje. El análisis de los chargebacks y de las transacciones fraudulentas permite mejorar las reglas existentes, afinar las alertas y reducir las oportunidades que se dejan a los defraudadores.

En resumen, frente al camuflaje, la **adaptación continua** es la clave: cuanto más domina y enriquece un comercio sus reglas a partir de la experiencia, más refuerza la fiabilidad de sus pagos y protege de forma duradera su rendimiento



EL ESPEJISMO

“El pedido es demasiado bueno para ser verdad”

Definición

El **espejismo** es un fraude sutil que juega con la emoción y la urgencia. El defraudador busca suscitar entusiasmo o generar una sensación de presión para empujar al comercio a ayudarle cueste lo que cueste.

Bajo esta influencia, el comercio puede perder vigilancia, ignorar ciertas señales de alerta y validar una transacción de riesgo.

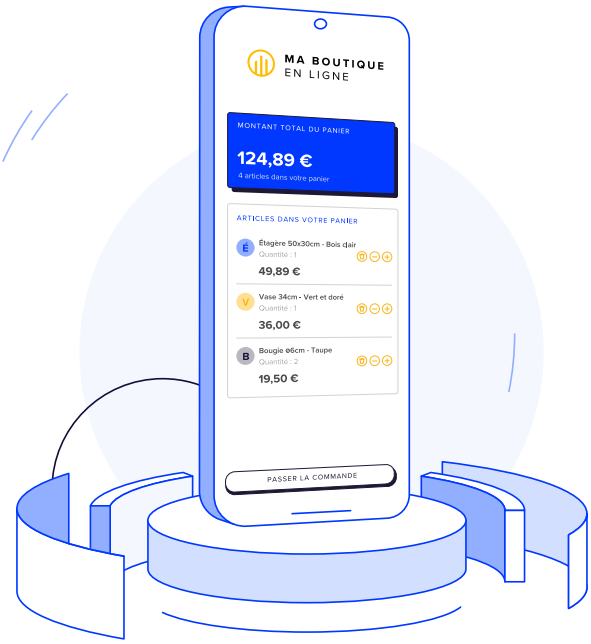
El objetivo es claro: **obtener la autorización de una transacción de alto importe antes de que se identifique el riesgo.**

Detectar el espejismo

El espejismo se detecta mediante una combinación de comportamientos insistentes e inusuales:

- **Importes atípicos:** un pedido especialmente elevado o desproporcionado.
- **Medios de pago dudosos**: insistencia en un pago sin autenticación reforzada, como el pago MOTO, a menudo justificado por una situación excepcional.
- **Urgencia excesiva:** presión para procesar la transacción de inmediato, explotando el estrés o la prisa del comercio.
- **Excusas repetitivas:** prueba de varias tarjetas (cónyuge, familiar, vecino...), mientras el comercio siga siendo cooperativo.

Tomados de forma aislada, estos indicios pueden parecer triviales. Sin embargo, su acumulación dibuja un **escenario típico de espejismo.**



¿Cómo protegerse?

Señalar y bloquear este comportamiento

Cualquier situación que active varias alertas (importe inusual, pago MOTO, presión relacionada con la urgencia) debe ser señalada de inmediato y evaluada por los equipos responsables de la seguridad.

Sensibilizar a los equipos

La vigilancia humana es crucial y debe apoyarse en el sentido común. La regla de oro es clara: si es demasiado bueno para ser verdad, probablemente no lo sea.

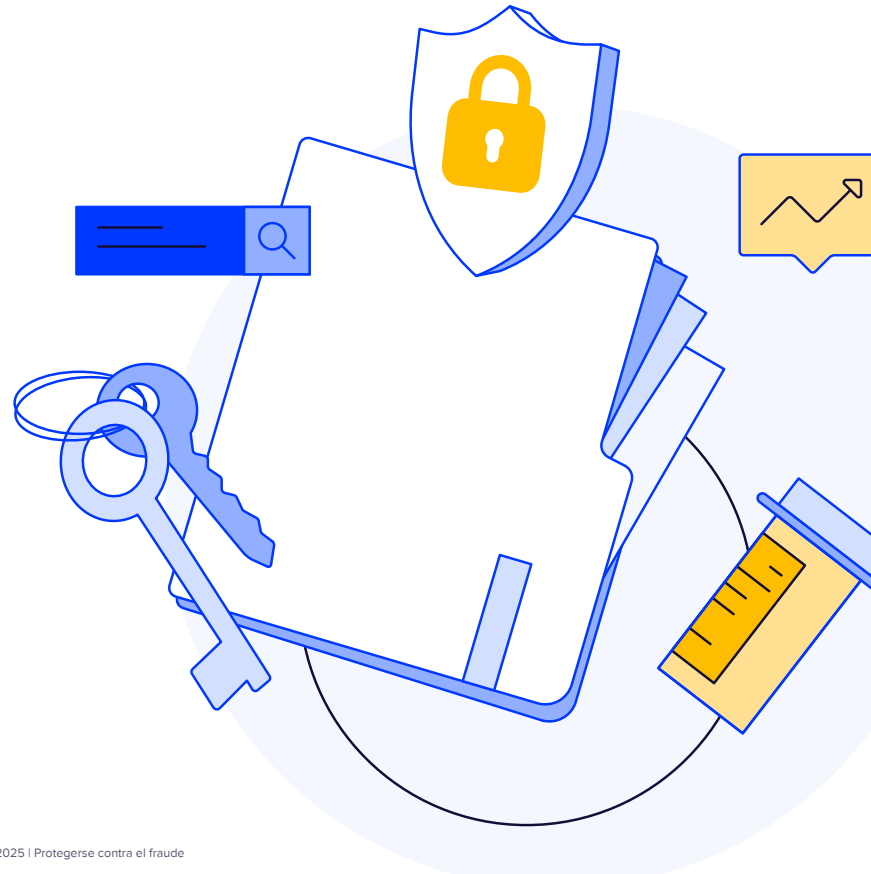
Los equipos deben saber reconocer los patrones típicos del espejismo y resistir la presión del cliente.

Poner fin a la transacción de riesgo

Nunca se debe dejar que el escenario continúe. Un defraudador persistente solo se detendrá cuando la transacción sea rechazada. Los intentos repetidos con distintas tarjetas o excusas deben conllevar la **suspensión inmediata del pedido.**

En resumen, el espejismo explota la psicología del comercio: entusiasmo, empatía y urgencia son sus principales palancas. La prevención se basa en la vigilancia, el conocimiento de las señales débiles y la firmeza frente a comportamientos sospechosos.

Actuando con rapidez y criterio, el comercio protege sus ventas, su rentabilidad y su fiabilidad.



INGENIERÍA **SOCIAL**

“El defraudador llama haciéndose pasar por un compañero o un socio de confianza con el fin de obtener información sensible.”

Definición

Aunque el fraude suele apoyarse en la tecnología, también recurre a un arma más sutil: **la manipulación humana.**

La **ingeniería social** consiste en llevar a un empleado o a un comercio a revelar, a veces sin darse cuenta, información sensible o a realizar una acción comprometedora. En este caso, no es la tecnología la que falla, sino la **vigilancia humana.**

Este tipo de fraude representó **382 millones de euros en 2024** (fuente: OSMP).

Los defraudadores explotan la confianza, la urgencia o la credulidad para desbloquear el acceso a datos críticos. Su objetivo es claro: **eludir las protecciones técnicas manipulando directamente a quienes las utilizan.**

Con el auge de la inteligencia artificial (imitación de voces, deepfakes, redirección de líneas telefónicas), estos ataques se vuelven más sofisticados, más creíbles y, por tanto, más peligrosos.

Ejemplos habituales de ingeniería social

“Buenos días, le llamamos desde el soporte de su proveedor de servicios de pago. Necesitamos verificar urgentemente sus accesos al back office para evitar el bloqueo de sus cobros. ¿Podría facilitarnos sus credenciales? ”

“Buenos días, realicé un pedido ayer pero me equivoqué en el importe. ¿Podría reembolsarme rápidamente en esta nueva cuenta bancaria? Es muy urgente.”

“Buenos días, le rogamos que encuentre a continuación nuestros nuevos datos bancarios. Le agradecemos que los registre y los utilice para el pago de sus próximas compras.”

— Su proveedor

“Tiene un nuevo mensaje. Para escucharlo, haga clic aquí.”

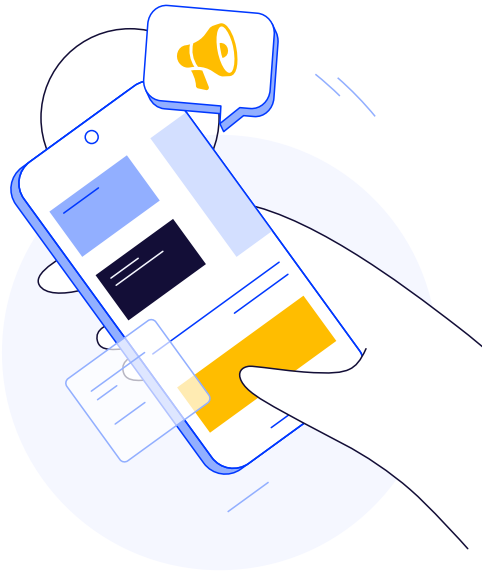
Detectar la ingeniería social

PRETEXTING

El defraudador inventa un escenario creíble (problema urgente, solicitud ficticia de un cliente, autoridad jerárquica simulada) para incitar a la divulgación de información confidencial.

PHISHING

Un correo electrónico o un SMS que imita a una fuente legítima incita a la víctima a hacer clic en un enlace fraudulento y a introducir sus datos en un sitio web falsificado.



IMPERSONATING

El defraudador se hace pasar por una persona de confianza con el fin de obtener una acción comprometedora.
Ejemplo: ***transferencia urgente sin justificante.***

¿Cómo protegerse?

La lucha contra la ingeniería social se basa menos en herramientas técnicas que en una **cultura de seguridad compartida.**
Cada colaborador debe convertirse en un **actor de fiabilidad.**

Algunas buenas prácticas clave:

- **No divulgar nunca información sensible bajo presión:** todo lo que parece urgente debe verificarse.
- **Limitar la difusión de datos personales o profesionales:** incluso una información aparentemente inocua (dirección de correo electrónico, fechas de vacaciones, nombre de un familiar) puede ser explotada.
- **Verificar siempre la legitimidad del interlocutor:** una llamada de confirmación o una validación a través de un canal oficial reduce considerablemente los riesgos.
- **Anonimizar o cifrar los datos sensibles siempre** que sea posible, para limitar su explotación.
- **Formar regularmente a los equipos:** comprender los métodos de los defraudadores permite anticiparlos mejor y resistirlos.

TOMA DE **CONTROL**

“Un hacker desvía mi sitio web en la fase de pago”

Definición

La toma de control se produce cuando un defraudador consigue piratear el sitio web de un comercio.

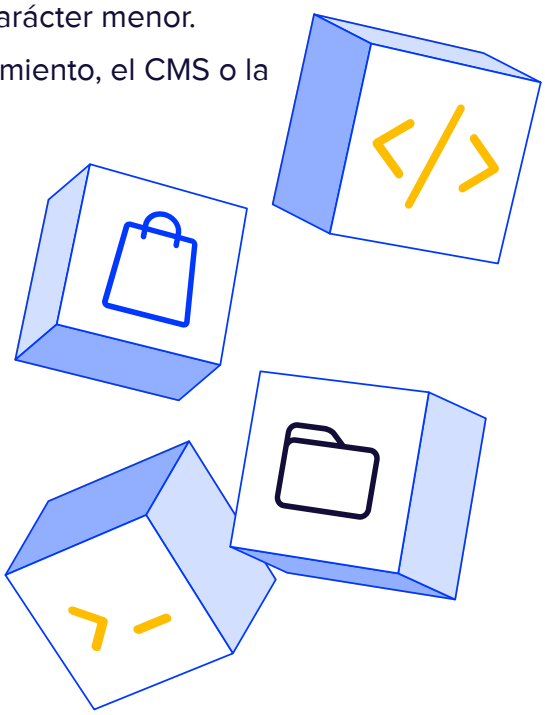
En la fase de pago, desvía los fondos a su propia cuenta o redirige a los clientes a una página de pago falsa con el fin de capturar sus datos bancarios.

El ataque es dirigido y sus efectos son inmediatos: cada transacción validada desaparece antes de llegar a la cuenta del comercio. El riesgo es crítico, ya que el fraude suele detectarse únicamente cuando se constata la ausencia de pedidos finalizados o, en el peor de los casos, la no recepción de los fondos.

Detectar la toma de control

El indicio más evidente es la ausencia de fondos ingresados a pesar de que las transacciones figuren como validadas. No obstante, otros signos deben alertar:

- **Redirecciones inusuales** hacia páginas externas o no reconocidas.
- **Modificaciones** no previstas en el sitio web, incluso de carácter menor.
- **Alertas de seguridad emitidas** por el proveedor de alojamiento, el CMS o la **agencia web.**



¿Cómo protegerse?

Ante una toma de control, la **rapidez de actuación** es esencial:

- **Suspender temporalmente la actividad del sitio:** detener las ventas evita nuevas pérdidas y protege a los clientes mientras se restablece la situación.
- **Asegurar y recuperar el control:** tras analizar la intrusión, aplicar las medidas de seguridad necesarias (actualización de contraseñas o de plugins) y restaurar el código o la configuración. En caso necesario, recurrir al proveedor de servicios de pago para verificar el correcto funcionamiento antes de reanudar la actividad.
- **Reforzar la seguridad del sitio a largo plazo:** activar una autenticación reforzada, desplegar un sistema de monitorización continua y configurar alertas en tiempo real para detectar cualquier anomalía antes de que se vuelva crítica.

ÉSUSTITUCIÓN DEL **TERMINAL DE PAGO**

“El defraudador entra en mi tienda para sustraer mi TPV”

Definición

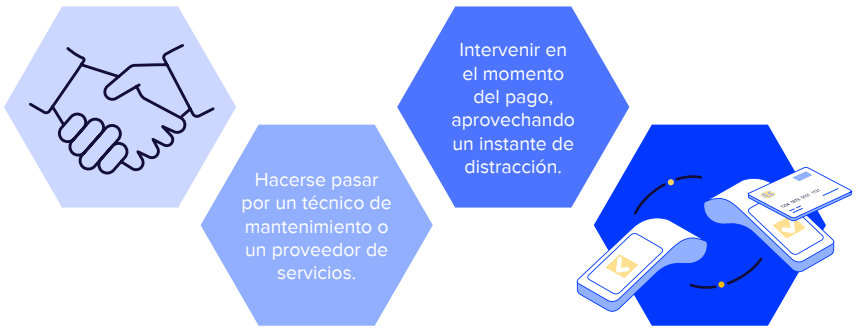
La sustitución del terminal se produce cuando un defraudador toma el control del punto de cobro físico. Desvía la atención del comercio para reemplazar el TPV legítimo por un terminal fraudulento.

Los fondos cobrados se redirigen entonces a una cuenta de terceros, que el defraudador puede recuperar fácilmente.

Este método también puede dirigirse a los códigos QR estáticos mostrados en el punto de venta, que son manipulados para desviar los pagos.

Modo operativo

El defraudador puede:



Detectar la sustitución del TPV

El indicio más evidente es que **los fondos dejan de recibirse**. Sin embargo, otros signos pueden alertar:

- Falta de visibilidad de los pagos en el back office.
- Incoherencias entre los importes validados y las cantidades realmente ingresadas.
- Mensajes inusuales en el terminal.
- Apariencia modificada del TPV.
- Información errónea en los recibos.

¿Cómo protegerse?

- **Vigilar el terminal:** no dejar nunca un TPV sin supervisión, ni durante el horario de apertura ni en el de cierre. Comprobar sistemáticamente su integridad antes de usarlo y detectar cualquier signo de manipulación.
- **Actuar con rapidez:** ante la menor duda o cualquier manipulación sospechosa, aislar y sustituir inmediatamente el terminal afectado.
- **Reforzar la vigilancia colectiva:** formar a los equipos para reconocer los intentos de suplantación y verificar la identidad de los técnicos o proveedores.
- **Asegurar los controles diarios:** comparar importes, identificadores del comercio y códigos bancarios en los recibos y cierres de caja, y verificar la autenticidad de los códigos QR utilizados.

FRAUDE MEDIANTE **FACTURA CRÉDITO**

“El defraudador realiza reembolsos en sus propias tarjetas desde un TPV fraudulento utilizando los fondos de mi cuenta”

Definición

El **fraude mediante factura crédito** consiste en que un defraudador **desvía el mecanismo de reembolso**. Con la ayuda de un **TPV fraudulento**, abona importes en tarjetas prepago que controla directamente desde la cuenta del comercio. A continuación, los fondos se retiran o transfieren de inmediato, dejando al comercio ante una **pérdida irreversible y sin posibilidad de recurso**.

Detectar el fraude mediante factura crédito

La detección se basa en una supervisión detallada de los flujos financieros. Algunos indicios deben alertar de forma inmediata:

- **Reembolsos no autorizados:** cualquier operación que no haya sido iniciada por los equipos internos debe tratarse como crítica.
- **Patrones repetitivos:** mismos importes, mismas tarjetas o una serie de reembolsos concentrados en pocos minutos.
- **Flujos inusuales:** reembolsos realizados en horarios atípicos, en tarjetas poco utilizadas o con un volumen superior al habitual.
- **Descuadres contables:** comparar periódicamente los recibos del TPV con los extractos bancarios permite detectar rápidamente cualquier anomalía.

Estos indicios, aunque sean mínimos, constituyen **señales débiles valiosas** para anticipar y detener un fraude antes de que comprometa la rentabilidad.

¿Cómo protegerse?

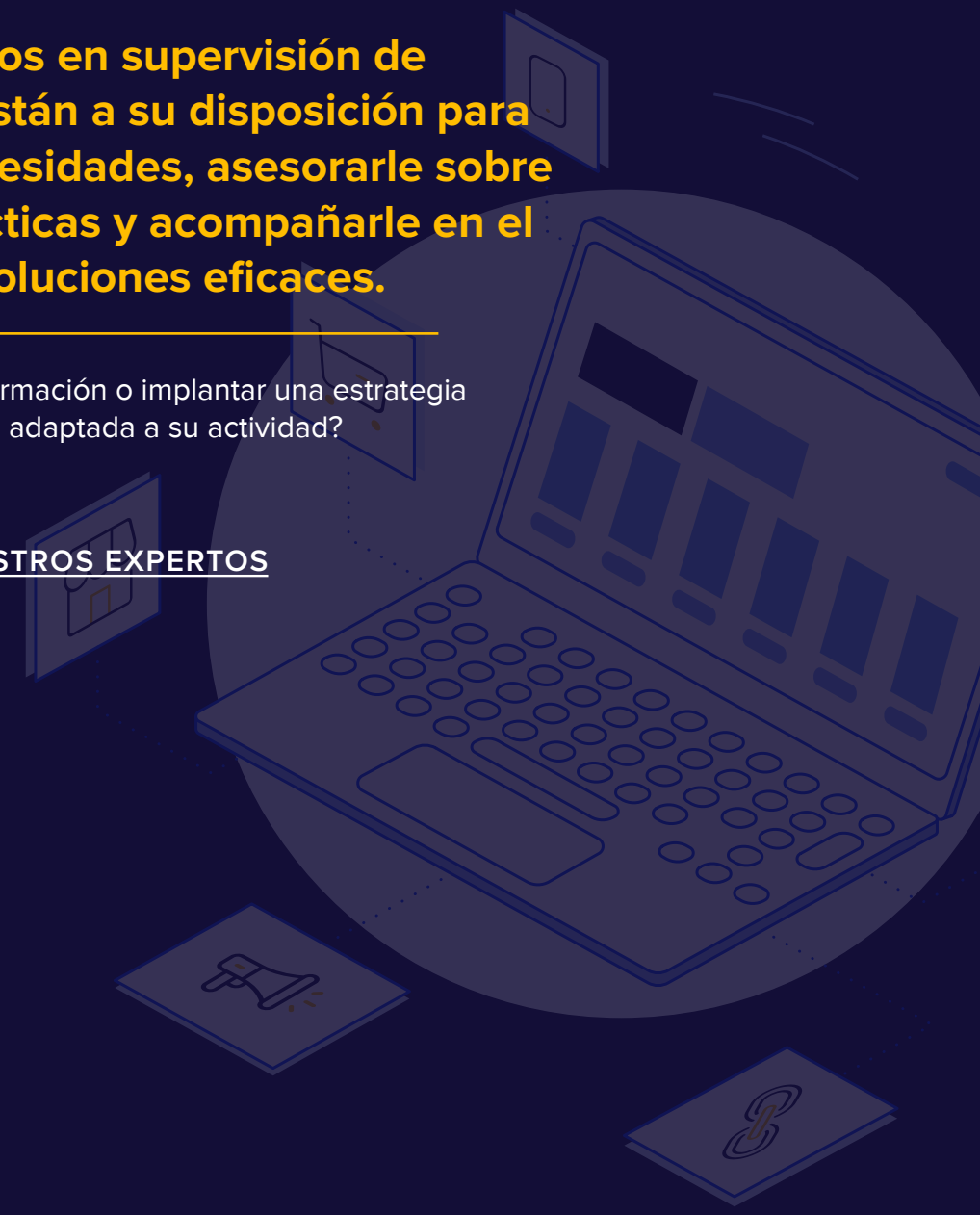
La protección frente al fraude mediante factura crédito se basa en una combinación de **control operativo y reacción inmediata:**

- **Controlar los flujos a diario:** verificar sistemáticamente los reembolsos y conciliarlos con las ventas reales para detectar cualquier desviación.
- **Reaccionar sin demora:** ante la menor duda, bloquear el TPV sospechoso e iniciar una investigación antes de que se lleven a cabo nuevas operaciones.
- **Implantar alertas automáticas:** activar una notificación en cuanto aparezca un reembolso inusual (importe idéntico repetido, frecuencia acelerada, volumen anormal).
- **Reforzar la gestión de accesos:** limitar los permisos únicamente a los colaboradores autorizados para configurar o validar un reembolso.
- **Capitalizar la experiencia:** documentar cada intento de fraude con el fin de mejorar los procedimientos internos y reforzar la formación de los equipos.

Nuestros expertos en supervisión de transacciones están a su disposición para analizar sus necesidades, asesorarle sobre las mejores prácticas y acompañarle en el despliegue de soluciones eficaces.

¿Desea obtener más información o implantar una estrategia de lucha contra el fraude adaptada a su actividad?

CONTACTE CON NUESTROS EXPERTOS



Juntos, hagamos de su infraestructura de pago una palanca estratégica contra el fraude.

Lyra
LYRA.COM

> Acceso directo a nuestra guía de conocimiento sobre el fraude