"Código 10" - Su primera línea de defensa

Ya sea que usted venda productos y servicios en persona, o por correo, teléfono o Internet, puede emplear una autorización "Código 10" para verificar información adicional sobre una transacción sospechosa. Su terminal de procesamiento le indicará que llame para obtener una autorización por voz de los cargos (CALL AUTH), o es posible que usted sencillamente no se sienta cómodo con la transacción. En cualquiera de los casos, puede usar el "Código 10" para obtener información adicional antes de entregar su mercancía.

Cómo usar el "Código 10"

- **Llame al número telefónico de autorización por voz que proporciona Servicios a Comerciantes (Merchant Services).** Este número se puede encontrar normalmente en la etiqueta de su terminal, o llame a Servicios a Comerciantes al 1-800-725-1243 y pida que lo transfieran al departamento de Autorización por Voz.
- **Elija la indicación para "Código 10".** Será transferido a un representante de autorización por voz quien le hará una serie de preguntas acerca de la transacción.

  Nunca llame a un número de teléfono del banco que emite la tarjeta que le provea un cliente, ni permita que el cliente llame al banco que emite la tarjeta por usted para obtener un código de autorización. ***No*** acepte un código de autorización que le dé un cliente. No se podrá verificar ningún código de autorización obtenido de una fuente que no sea su Centro de Autorización.
- **Si el pedido es una venta por correo, teléfono o Internet, esté preparado para proporcionar el nombre del titular de la tarjeta, la dirección de facturación y la dirección de envío.** El representante tratará de verificar la información que usted proporcione con el banco que emitió la tarjeta al cliente.
- **El representante tratará de verificar la información del titular de la tarjeta durante su llamada.** Si esto no es posible, los datos se enviarán a un investigador para que se lleve a cabo una investigación adicional. Trataremos de comunicarnos con usted dentro de 24 a 72 horas con el estado actual o el resultado de la investigación.
- **Si una solicitud de autorización es denegada, solicite otra forma de pago que no sea una tarjeta de crédito.** ***No*** divida una transacción denegada en incrementos menores para obtener una autorización.
- **Obtenga un código de autorización por el monto completo de la venta.** Siempre obtenga el código de autorización ***antes*** de enviar la mercancía.

Un código de autorización ***no*** garantiza que una transacción no será disputada más adelante. Un código de autorización sencillamente identifica que el monto de crédito solicitado para esa transacción en particular está disponible en la tarjeta al momento de la venta. Un código de autorización ***no*** lo protege a usted en caso de un contracargo con respecto a transacciones no autorizadas o disputas que tengan que ver con la calidad o la entrega de productos o servicios.

Se recomienda firmemente que use el "Código 10" ***antes*** de que los cargos se hayan cargado a la tarjeta de crédito y ***antes*** de que el producto se haya enviado. Hacer esto le permitirá evitar que sea facturado por cuotas de procesamiento y la pérdida de los costos de envío de la transacción en cuestión. Observe que usted todavía puede solicitar un "Código 10" si el producto ha sido enviado, pero sus probabilidades de recuperar el producto se reducirán.

Fraude en transacciones que no son en persona

A medida que más y más negocios se llevan a cabo por Internet o por teléfono, hay mayor oportunidad de que los defraudadores usen este mercado remoto para hacerse pasar por clientes reales o usar tarjetas o cheques ilegítimos para robar a los negocios. Éstos son algunos ejemplos de las posibles transacciones fraudulentas que debe vigilar en su negocio.

- **Llamadas retransmitidas** - Una llamada retransmitida es una llamada telefónica asistida por operador, normalmente usada por alguien que tiene un impedimento de audición. Aunque éste es un servicio válido, los delincuentes también han usado el servicio para colocar pedidos fraudulentos. Le recomendamos que solicite una autorización "Código 10" para todos los pedidos obtenidos por medio de llamadas retransmitidas.
- **Pedidos a granel** - Los clientes que piden grandes cantidades de artículos idénticos o similares. Debe tener precaución con pedidos a granel con una dirección de entrega en un apartamento o una unidad de almacenamiento propio.
- **Tarjetas múltiples** - Clientes que proporcionan números de tarjetas múltiples para la misma compra, especialmente cuando los números de las tarjetas son diferentes sólo por algunos de los últimos números.
- **El dinero no es una objeción** - Solicitudes de entrega de un día para otro, sin importar el costo.
- **Envío inmediato** - Clientes que solicitan el procesamiento inmediato del pedido y desean el número de rastreo del pedido enseguida.
- **Recogida inmediata** - Clientes que colocan pedidos por teléfono, solicitan el procesamiento inmediato del pedido y luego indican que alguien irá a la tienda a recoger el producto.
- **Dirección de entrega alterna** - Solicitudes de entrega a una dirección que no es la dirección de facturación, o la entrega a un transportista. (Los delincuentes usarán agentes de reembarque basados en los Estados Unidos para evitar la detección de embarques extranjeros.)
- **No se venden aquí** - Solicitudes por teléfono o en línea de mercancía que usted no vende. Las solicitudes más comunes son de teléfonos celulares y computadoras portátiles.
- **Pedidos por correo electrónico gratuito** - Comunicación a través de un servicio de correo electrónico gratuito (Yahoo, Hotmail, Gmail, etc.).
- **Solicitud de fondos en exceso** - Un cliente puede solicitar que usted procese una transacción por un monto mayor que el precio de compra de los productos o servicios y luego envíe los fondos en exceso por transferencia electrónica, giro postal o Western Union® a una empresa transportista o a otra persona. No sólo hay una alta probabilidad de fraude por tal transacción, sino que existe poca probabilidad de que su negocio recupere los fondos. Este tipo de transacción es una violación de las reglamentaciones, así que usted no tendrá la habilidad de resolver favorablemente un contracargo, si éste ocurriera.
- **Esquema de cheque falsificado** - El defraudador paga de más por productos o servicios con un cheque falsificado y solicita que usted envíe la diferencia por transferencia electrónica de regreso a ellos o a un cómplice. Se ha informado que este esquema ha sido realizado con cheques personales, cheques de cuentas comerciales, cheques de cajero y giros postales, y resulta en la pérdida tanto de la mercancía como del dinero en efectivo restante.
- **Identificación fraudulenta del cliente** - Con la tecnología de hoy, es posible alterar una fotocopia de una tarjeta de crédito o una identificación personal, tal como una licencia de conducir o un pasaporte. A veces, un pedido fraudulento incluirá una fotocopia de la tarjeta enviada por fax o por correo electrónico para ganar su confianza. Estas fotocopias no garantizan que usted esté tratando con el titular correcto de la tarjeta. Siempre verifique la información del pedido con el centro de autorización antes de proceder con el pedido.

Países más frecuentes para el fraude

El fraude ya no está localizado. Los negocios que aceptan ordenes internacionales pueden ser susceptibles a esquemas que se originan lejos de sus lugares. Los lugares de peligro actuales donde se originan pedidos de venta por correo, por teléfono, y el fraude por Internet típicamente incluyen:

- África Occidental - Nigeria, Ghana, Gambia
- Asia - Indonesia, Singapur
- Europa Oriental - Bulgaria, Rumania, Rusia

Fraude de empleados - La amenaza interna

A veces los defraudadores de los que se tiene que proteger están dentro de su propia organización. El robo por parte de los empleados de la información de los clientes es un problema creciente para los negocios. Varios avances en la tecnología han hecho fácil para los empleados sin escrúpulos robar la información crediticia de los clientes. Los procedimientos de seguridad relajados también pueden permitir que los empleados roben o hagan mal uso de los datos.

A continuación se proporcionan algunas maneras típicas en que los empleados pueden perpetrar fraude de tarjetas de crédito:

- **Procesar una transacción de crédito a su propia cuenta** - Los empleados pueden emitir créditos a su propia tarjeta de crédito o a la tarjeta de un cómplice usando el dispositivo de Punto de Venta (POS) del Comerciante y utilizando fondos cuyo destino debía ser la cuenta de depósito directo del comerciante.
- **Registrar los números de las tarjetas** - Los empleados podrían echarse al bolsillo los recibos que dejan los titulares de tarjetas o podrían copiar los números de las tarjetas en un papel por separado. Las terminales de POS que truncan el número de la tarjeta en el recibo del cliente pueden ayudar a su negocio a evitar este tipo de fraude.
- **Usar un lector de tarjetas** - Un empleado deshonesto puede robar información valiosa de la tarjeta de un cliente por medio del uso de un "lector de tarjetas" pequeño y operado por baterías. Este dispositivo manual lee la banda magnética de una tarjeta y registra los datos del titular de la tarjeta para después ser descargados a una computadora. De ahí, los números se pueden usar para hacer compras no autorizadas o crear tarjetas falsificadas.

Otras actividades sospechosas de los empleados

El fraude de los empleados también puede tomar otras formas. A veces no consiste en procesar directamente una transacción de tarjeta, pero es sospechosa de todos modos.

Éstos son algunos indicios de posible robo por parte de los empleados.

- Depósitos no hechos dentro de los marcos de tiempo normales (es decir, depósitos diarios que no ocurren diariamente), o depósitos que su banco no ha recibido.
- Recibos de tarjeta de crédito no retenidos según la política de la compañía.
- Errores frecuentes al aplicar pagos de los clientes, o quejas de los clientes de pagos que no han sido aplicados a sus cuentas o que sólo pagos parciales han sido aplicados cuando el cliente pagó en su totalidad.
- Discrepancias entre los recibos de depósitos obtenidos de su banco y los recibos de depósitos que se mantienen internamente.
- Una reducción en el volumen de dinero en efectivo recibido mientras los volúmenes de otros tipos de pagos permanecen sin cambio.
- Vales en las reservas de dinero en efectivo o en la "caja chica."

Cómo combatir el fraude de los empleados

A pesar de la oportunidad de fraude de los empleados, usted como comerciante no está totalmente sin protección. La mayoría de las terminales y las herramientas de software de transacciones le permiten solicitar una contraseña para poder procesar una transacción de crédito, y hay varias otras tácticas que puede usar para prevenir el fraude de empleados:

- Concilie su trabajo diariamente en vez de mensualmente.
- Proteja con contraseña la función de crédito en su dispositivo de POS, o en el dispositivo de POS en sí.
- Asegure su dispositivo de Punto de Venta (POS) mientras que se encuentre fuera de las horas de oficina.
- Tenga una persona separada para que autorice los créditos además de la persona que físicamente procesa un crédito.
- Asegúrese de que todos los créditos tengan documentación interna acompañante de la información del cliente (nombre e información de contacto) y la razón de la devolución o la disputa.
- Empareje los créditos a los productos o servicios devueltos o en disputa, verifique con los clientes qué productos o servicios realmente devolvieron o disputaron.
- Haga que más de una persona revise los estados de cuenta mensuales.
- Envíe todas las transacciones de crédito a una oficina central para su revisión.
- Revise los créditos diariamente o haga que un empleado de confianza lleve a cabo la revisión.
- Investigue completamente los créditos que no tengan ventas correspondientes.
- Revise cualquier lote con un monto en dólares negativo (más créditos que ventas).
- Lleve a cabo auditorias internas regulares en tiempos e intervalos al azar.
- Realice auditorias de los procesos contables y de teneduría de libros trimestralmente.
- Lleve cuenta de los créditos por número de tarjeta, número de terminal, empleado, frecuencia y monto en dólares (informes basados en excepciones).
- Revise cualquier aumento en el volumen de actividad de créditos, devoluciones y disputas.
- Revise sus estados de cuenta mensuales con su inventario físico.
- Pregunte sobre los productos o informes adicionales que hay disponibles para revisar los detalles de las transacciones de tarjetas de crédito, por ejemplo, MerchantConnect Premium.
- Si usted usa otra cosa que no sea una terminal de pagos para procesar transacciones (por ejemplo, una caja registradora electrónica con funciones de pago integradas), hable sobre controles y/o informes adicionales con su proveedor de puntos de venta.
- Proteja sus contraseñas y verifique los controles de acceso interno para informes de cuentas en línea y solicitudes de cambios de cuentas de cheques.

Otros recursos de información para la prevención de fraude

Éstas son fuentes útiles que pueden proporcionar más información y ayuda para evitar el fraude de tarjetas de crédito en su negocio.

En línea

- www.visa.com - Incluye consejos, reglamentaciones, noticias y características del fraude de VISA. (Elija la opción para comerciantes / negocios.)
- www.mastercard.com - Incluye consejos, reglamentaciones, noticias y características del fraude de MasterCard. (Elija la opción para comerciantes.)
- http://zip4.usps.com/zip4/welcome.jsp - El sitio web del Servicio Postal de los Estados Unidos para validar que una dirección existe físicamente. Esto no confirma que una persona vive en la dirección, pero confirma que la dirección es real.
- www.ic3.gov - El Centro de Quejas de Fraude por Internet (Internet Fraud Complaint Center - IFCC). Esta es una sociedad entre el FBI y el Centro Nacional de Delitos de Cuello Blanco (National White Collar Crime Center). Este sitio permite que las víctimas de fraude por Internet informen el fraude en línea a las autoridades apropiadas reglamentarias y del orden público.
- www.forwarders.com - Esta es una lista de transportistas. A menudo los delincuentes internacionales enviarán el pedido a estas direcciones y harán que dicha empresa transportista envíe el pedido al destino final.

Por teléfono

- **Servicio de Verificación de Comerciantes de VISA** 800-847-2750 AUTOMATIZADO
  Opción 1, Verificación de dirección: ingrese la parte numérica de la dirección de la calle, el código postal y el número de la tarjeta VISA y el sistema le indicará si existe un cotejo.
  Opción 2, Números telefónicos del banco emisor: ingrese el número de la tarjeta VISA y se le proporcionará el número 800 del banco emisor, si hay uno disponible.
- **Ayuda de MasterCard** 800-622-7747
  Seleccione el idioma que prefiere, luego la Opción 2. Ingrese el número de la tarjeta MasterCard y se le proporcionará el número 800 del banco emisor, si hay uno disponible.
- **Verificación de la Dirección de Discover** 800-347-1111 AUTOMATIZADO
  Usted necesitará su número de Comerciante de Discover. Ingrese el número de la tarjeta Discover y la información de la dirección y el sistema le indicará si hay un cotejo.
- **Verificaciones de direcciones de American Express** 800-428-7443. La Opción 3 le permite verificar el nombre y la dirección de un número de tarjeta AMEX específica. Para otros servicios en español contacte 800-297-2639

Estos consejos para prevención de fraude no son una modificación de su Acuerdo de Procesamiento de Comerciante, los Términos de Servicio ni la Guía de Operación del Comerciante que rigen su relación de procesamiento con Elavon, Inc. Estos consejos para prevención de fraude se proporcionan para aumentar su conocimiento de las circunstancias en las que la posible actividad fraudulenta puede ocurrir y sugerir medidas para combatir o reducir al mínimo el impacto que produce la aceptación de transacciones fraudulentas.