Cinco tipos de fraudes internos muy sutiles en el sector de *retail*

y cómo detectarlos utilizando datos

Zebra
Prescriptive Analytics™

Powered by Zebra Savanna™

En este *ebook* abordamos los siguientes temas:

- Cinco tipos de fraudes internos en el sector de *retail*
- Los comportamientos de datos que los revelan
- Cómo identificarlos y prevenirlos con análisis avanzado

Introducción

El fraude es un problema muy serio para un sector tan brutalmente competitivo como el de *retail*. El estrechamiento progresivo de los márgenes como consecuencia de las guerras de precios exige que los comercios minoristas combatan la pérdida de efectivo provocada por el fraude, sobre todo cuando lo cometen los propios empleados. Además de conocer bien los procedimientos de seguridad del comercio minorista (y, por ende, cómo evitarlos), los empleados tienen acceso a funciones de las cajas registradoras que generan riesgos, así como a mercancía sin protección en trastiendas, almacenes y camiones. Este conocimiento de los procesos dificulta la detección del fraude interno aunque se utilicen cámaras u otras medidas de seguridad.

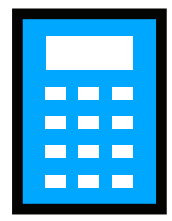
Para combatir este problema, muchos comercios minoristas están aprovechando los datos de que disponen para identificar actividades sospechosas de los empleados. Son conscientes de que los datos no son manipulables y de que el uso de una solución adecuada de análisis avanzado, como el análisis prescriptivo, permite identificar comportamientos específicos que indican fraude y otras actividades que erosionan los márgenes. En este *ebook* abordamos cinco ejemplos extremadamente sutiles de fraudes de empleados y los datos que nos advierten de su presencia y que el análisis prescriptivo permite identificar.


ZEBRA

Cinco tipos de fraudes internos muy sutiles en el sector de *retail*

1. *Sliding*

2. Uso no autorizado del PIN del gerente

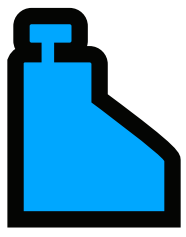


3. Fraude de programas de fidelización

4. Cambio de precios y *sweethearting*

5. Fraude en el servicio al cliente de comercio electrónico

Fraude n.º 1



Sliding

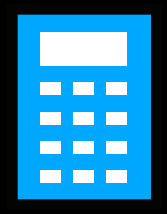
El *sliding* (deslizamiento) se produce cuando un empleado de caja pasa un artículo por el escáner ocultando intencionadamente el código de barras. El cliente (por lo general un conocido) puede entonces embolsar el artículo y abandonar la tienda sin pagarlo. Identificar esta actividad como fraude puede resultar complicado, ya sea con cámaras de seguridad o incluso estando presente. Aunque pueda confirmar que no se ha escaneado un código, es difícil demostrar que se trate de *sliding* y no de un simple error.

Los datos pueden ser de gran utilidad en este caso. Una forma de identificar el *sliding* consiste en analizar el índice de escaneados por minuto o por hora de empleados de caja concretos. Este proceso comienza con una buena solución de análisis como el análisis prescriptivo, que permite agrupar en clústeres (es decir, agrupar

por características similares) empleados de caja y tiendas para determinar las medias de referencia para determinados KPI, como la velocidad de escaneado. Se indicará como posible defraudador a todo empleado cuya velocidad de escaneado se sitúe tres desviaciones estándar por debajo del valor de referencia.

Una circunstancia así es particularmente sospechosa si se produce durante un periodo de «alto riesgo» (mediodía, temporada alta de compras o descansos o días libres del gerente, etc.). El análisis prescriptivo tiene en cuenta estas circunstancias para identificar fraudes.

Fraude n.º 2



Uso no autorizado del PIN del gerente

Para mitigar el riesgo intrínseco de las anulaciones de operaciones, los cambios de precio manuales y otras actividades, muchos comercios minoristas exigen que los gerentes las autoricen mediante la introducción de un número de identificación personal (PIN). Lamentablemente, es fácil hacer un uso indebido de este PIN si un empleado de caja lo memoriza o si el gerente lo revela para ahorrar tiempo. Si este comportamiento no se evita, un solo empleado de caja podría sustraer miles de euros en efectivo o en artículos.

Existen numerosas formas de identificar el fraude en los PIN utilizando, por ejemplo, los datos de recursos humanos. Las soluciones de análisis más avanzadas integran datos de múltiples aplicaciones y proveedores. Permiten visualizar fácilmente conjuntos de datos independientes y cualquier información que proporcionen mediante una sola interfaz.

Para detectar el uso no autorizado del PIN del gerente, puede implementar un «patrón» (un algoritmo que busca comportamientos de datos específicos) que cruce cada uso de un PIN con los datos de la nómina. El patrón le avisa cada vez que se utiliza el PIN del gerente durante un periodo en el que este no está de servicio.

Como alternativa, si sus gerentes llevan consigo ordenadores móviles con servicios de localización, una solución de análisis permite comprobar la proximidad del gerente a la caja registradora en la que se introdujo el PIN. Si el gerente se encontraba trabajando en otro punto del establecimiento en ese momento, se avisa al equipo de protección de activos.

Fraude n.º 3

Fraude de programas de fidelización

La mayoría de los comercios minoristas permiten que, al pasar por caja, los clientes introduzcan un número de teléfono como medio para acceder a su cuenta de puntos de fidelización. Ha habido casos de empleados de caja que han aprovechado este servicio para introducir subrepticiamente su propio número de teléfono en lugar del número del cliente para robarle las recompensas de programas de fidelización. A no ser que el cliente se tome la molestia de contar sus puntos de fidelización, este comportamiento pasa inadvertido.

Las mencionadas capacidades de generación de valores de referencia y clústeres que ofrece el análisis avanzado permiten obtener pruebas de fraude a partir de los datos. Para ello, se analizan las cuentas de fidelización de los propios dependientes para detectar saldos de puntos excesivos. El sistema avisa de aquellas cuentas de empleados que de pronto comienzan a acumular puntos a una velocidad superior a la media.

Otro tipo de fraude de programas de fidelización consiste en que los empleados utilizan *phishing* para obtener los números de teléfono asociados a cuentas con saldos de puntos elevados y posteriormente emplean los puntos para comprar productos o combustible con un descuento muy alto.

Al igual que en el ejemplo anterior, puede configurarse una solución adecuada que indique las cuentas de clientes con un gasto inexplicable de puntos, especialmente en compras propensas a hurtos, como productos electrónicos, combustible o tarjetas regalo. Estas cuentas pueden haber sido hackeadas de algún modo y deben ser investigadas.

Fraude n.º 4

Cambio de precios y *sweethearting*

Este método es el preferido de las bandas organizadas que cometen delitos contra el sector de *retail*. Suelen utilizarlo empleados que trabajan en departamentos en los que los productos se venden al peso, como la carne u otros productos frescos. Dado que las etiquetas de precios se imprimen in situ, es fácil adherir etiquetas de artículos de valor reducido a paquetes de productos de alto valor (por ejemplo, poner a un solomillo de ternera de 21 euros/kg el precio del pollo troceado de 1,99 euros/kg).

Siguiendo un método similar conocido como *sweethearting* (regalo de productos a amigos), un empleado de caja puede escanear un código de un producto barato (por ejemplo, un paquete de chicles de 25 céntimos) en lugar del artículo de precio elevado que su conocido ha llevado a la caja (por ejemplo, un perfume de gama alta de 89 €).

Aunque detecte estos comportamientos inusuales en un informe de inventario, le resultará difícil determinar si son fraude o un simple cambio en la demanda.

Una forma simple de identificar los cambios de precio es supervisando los movimientos de inventario. Esas ventas falsas originarán un número inusualmente alto de movimientos de productos baratos y un número inusualmente bajo en el caso de los productos sustraídos. Juntos, estos dos comportamientos conforman una prueba clara de fraude en el precio, sobre todo si solo se producen en algunas tiendas.

Una solución de análisis avanzado permite detectar fácilmente estos fraudes. Al detectar los mencionados patrones de ventas, la solución identifica la caja registradora en la que se han procesado la mayoría de los artículos de precio bajo. Posteriormente, extrae la grabación de las cámaras correspondiente al momento del escaneado, lo que le permite ver rápidamente lo que se escaneó en realidad y el importe registrado. Esto agiliza las investigaciones y permite una intervención más rápida y precisa.

Fraude n.º 5

Fraude en el servicio al cliente de comercio electrónico

Las empresas de comercio electrónico experimentan la pérdida de paquetes en tránsito que nunca llegan al cliente. La mayoría de los comercios minoristas sustituyen gratis los productos perdidos. Algunos también envían al cliente una tarjeta regalo o un descuento para futuras compras por las molestias ocasionadas.

Esta práctica supone un riesgo elevado de fraude por parte de los representantes de atención al cliente. Algunos comercios minoristas han sorprendido a representantes de atención al cliente enviándose pedidos de sustitución a sí mismos o a conocidos, a veces en connivencia con una red delictiva más amplia. La acumulación de estos incidentes puede suponer miles de euros en pérdidas, lo que hace imprescindible su identificación y prevención.

Existen numerosos flujos de datos que permiten revelar esta actividad antes de que se acumulen las pérdidas. Estos son algunos ejemplos:

- **Destino de los pedidos de sustitución.** Los pedidos de sustitución con destino a direcciones próximas al centro de llamadas tienen una probabilidad superior de ser fraudulentos. De igual modo, el envío de múltiples pedidos de sustitución a las mismas direcciones debe se investigado de inmediato —sobre todo si coinciden con el domicilio de empleados actuales. El análisis prescriptivo permite identificar y alertar de estas anomalías fácilmente.

- **Frecuencia de las sustituciones.** Como hemos explicado anteriormente, las soluciones de análisis avanzado permiten establecer medias de referencia para comportamientos como las sustituciones de pedidos. Comparando los valores medios para todos los representantes de atención al cliente con los índices de sustitución de representantes concretos, la solución permite identificar fácilmente a cualquier empleado que procese más sustituciones de las esperadas.

Cualquiera de los comportamientos de datos mencionados anteriormente puede ser indicativo de fraude. Una solución de análisis adecuada permite identificarlos y alertarle para que ponga en marcha una investigación antes de que las pérdidas alcancen niveles críticos.

Conclusión

El profesional de protección de activos de *retail* de hoy en día necesita herramientas nuevas y potentes para identificar y eliminar el fraude interno. Sobre todo, es imprescindible que estas herramientas aumenten la eficiencia (es decir, que le permitan identificar los casos rápidamente antes de que se acumulen las pérdidas) y la eficacia (es decir, que ofrezcan un índice elevado de alertas positivas verdaderas) para optimizar los recursos humanos y agilizar las investigaciones. Invertir en una solución de análisis avanzado como el análisis prescriptivo puede proporcionarle la ventaja competitiva que necesita para detectar incluso los casos más sutiles de fraude y proteger sus márgenes y beneficios.

Para obtener más información sobre el análisis prescriptivo y cómo puede ayudar al equipo de protección de activos a combatir el fraude y el incumplimiento de la legislación, visite www.zebra.com/prescriptiveanalytics o póngase en contacto con nosotros en fran@zebra.com.

Zebra
Prescriptive Analytics™

Powered by Zebra Savanna™