



# Banco Internacional utiliza aprendizaje Inteligente en la investigación de fraude

[hola@optaris.com](mailto:hola@optaris.com)

"Los bancos están constantemente pendientes del monitoreo de patrones y tendencias y evolucionando rápidamente sus técnicas para mantenerse un paso por delante de los estafadores".

James Chessen,  
EVP. ABA's Centro de pagos y ciberseguridad

## Banca en fraude

Las estadísticas sobre el fraude bancario son simplemente asombrosas.

De acuerdo con el Reporte de las Naciones, de la Asociación de Examinadores de Fraude Certificados del 2018, los casos de fraude le costaron a las organizaciones más de \$ 7 mil millones a nivel mundial en 2017. No es de extrañar, entonces que los bancos están recurriendo a las últimas soluciones tecnológicas para combatir el fraude, proteger los ingresos y mantener la confianza del consumidor.

Por ejemplo, un banco internacional bien establecido recurrió a Bottomline Technologies para ayudar a mitigar su exposición al fraude.

En 2010 el banco implementó la plataforma de Fraude Cibernético y Administración de Riesgos (CFRM) de Bottomline para detectar y evitar rápidamente el fraude de pagos. La solución proporciona una evaluación continua a través de canales y tipos de pago. Cuando se detectan anomalías, las alertas se generan y se envían al equipo de investigación del banco. Las alertas proporcionan al banco con una rica visualización e información forense detallada sobre las transacciones a través de un tablero de control fácil de usar, lo que permite a los investigadores intervenir y detener el fraude antes de que ocurra.

"El 74% de los profesionales financieros informaron que sus empresas habían tenido experiencia De fraude de pagos el año pasado." Según la Encuesta de fraude y control de pagos del 2017

# Banco Internacional utiliza aprendizaje Inteligente en la investigación de fraude

## Ataques en escala

En 2016, los investigadores del banco notaron que el número de alertas había ido aumentando año tras año.

El banco maneja 250.000 transacciones diarias y las alertas había aumentado a un promedio de 1.5%, llegando a 3750 alertas por día. De esas alertas, solo el 8% eran verdaderos intentos de fraude.

El equipo de investigación se enfrentó entonces, con el desafío de monitorear cada alerta y decidir un curso de acción para evitar la interrupción de las operaciones comerciales. Esto puso a prueba los recursos y aumentó el riesgo de errores. Fue un proceso lento que tomó un promedio de 20 minutos por investigador por alerta.

El banco necesitaba encontrar una solución que tuviera la capacidad de manejar el creciente número de transacciones y reducir los falsos positivos sin agregar recuento a su equipo de investigación. Para lograr esto, la solución debería proporcionar menos falsos positivos y disminuir el tiempo de investigación.

Bottomline Technologies recomendó que el banco actualice a la última versión de la plataforma CFRM para aprovechar los últimos avances de las capacidades analíticas de su motor.

El motor de análisis CFRM combina el aprendizaje inteligente, la detección basada en reglas y los perfiles de comportamiento reduciendo el riesgo de fraude y los falsos positivos. Captura el comportamiento del usuario en tiempo real y proporciona protección contra amenazas externas donde las credenciales del usuario estén comprometidas y donde se visualicen las amenazas internas de los usuarios autorizados.

Actualmente y con las nuevas tecnologías, el banco puede ahora identificar el comportamiento anómalo y reducir los falsos positivos y priorizar los verdaderos positivos agrupándolos en las siguientes categorías:

- **Detener la transacción** - que cierra inmediatamente la transacción de pago
- **Llamar al cliente**, que genera una lista clasificada de clientes para contactar antes de tomar acción
- **Llamada infructuosa**: que genera una lista clasificada de clientes para ser llamados nuevamente

La lista de llamadas a clientes prioriza las alertas al generar una puntuación de "probabilidad de fraude" para cada transacción. Este ranking permite al equipo de investigación del banco determinar a quién llamar primero, llamando de esta manera, a los clientes con la mayor probabilidad de fraude primero.

Con este sistema de puntuación de las alertas, se obtienen varias ventajas; prevención efectiva del fraude, reducción de falsos positivos, menor molestia a los clientes por llamadas infructuosas y mayor capacidad para el equipo de trabajo.

## Beneficios claves



Mejor visibilidad y control



Menor tiempo de investigación



Mejor toma de decisiones

## Ganancias de Eficiencia

Con el panorama de amenazas fraudulentas en constante evolución, es imperativo que las organizaciones se protejan a sí mismas mediante la adopción de las últimas soluciones que se centran en el real comportamiento del usuario y en su capacidad de adaptación para responder de forma rápida y precisa a los nuevos mecanismos de fraude.

La plataforma de Ciber Fraude y Gestión de Riesgos de Bottomline le permite al banco reducir el riesgo, prevenir el fraude y cumplir con los requisitos de cumplimiento normativo con una plataforma flexible.