CELENT

OPERACIONALIZACIÓN DE LA PREVENCIÓN DEL FRAUDE CON IBM Z16

Reducción de pérdidas en operaciones bancarias, tarjetas y pagos

Neil Katkov

5 de abril de 2022

Este informe fue encargado por IBM, que pidió a Celent que diseñara y ejecutara un estudio en su nombre. El análisis y las conclusiones son exclusivamente de Celent; IBM no tuvo ningún control editorial sobre el contenido de este informe.

CONTENIDO

RESUMEN EJECUTIVO

Los avances en inteligencia artificial (IA), como el aprendizaje profundo, ayudan a que la detección del fraude mejore significativamente. Sin embargo, los grandes bancos y los procesadores de pagos que utilizan modelos de IA suelen ejecutarlos solo en una parte de las transacciones debido a las limitaciones de rendimiento y latencia de sus sistemas de detección de fraudes. Es por ello que muchas transacciones fraudulentas no se controlan ni se detectan.

El IBM Integrated Accelerator for AI, que forma parte del nuevo procesador de sistema principal Telum de IBM, está diseñado para ejecutar inferencias para cargas de trabajo en tiempo real, a escala y con baja latencia. El chip está diseñado para permitir la detección de fraudes en tiempo real incluso en entornos de procesamiento de bancos, tarjetas o pagos de gran volumen.

Para ayudar a los bancos y procesadores de pagos a entender el valor potencial de esta innovación para las operaciones expuestas a fraude, Celent ha elaborado estimaciones que muestran cuánto se podrían llegar a reducir las pérdidas por fraude si estas entidades integraran la inferencia mediante IA en el 100 % de sus transacciones.

Ventajas cuantificables de la detección de fraude basada en IA mediante los sistemas principales IBM z16:

Reducción de las pérdidas por fraude en el sector en		Reducción de las pérdidas por banco en		Reducción de las transacciones con tarjeta rechazadas en
EE. UU.	Globalmente	Banco de EE. UU. de nivel 1	Banco de EE. UU. de nivel 2	
5,6 céntimos por cada 100 dólares	2 céntimos por cada 100 dólares	105 millones de dólares	18 millones de dólares	46 %

Celent estima que la implementación de modelos avanzados de inferencia a, teóricamente, todas las transacciones bancarias, de tarjetas y de pagos que se ejecutan en los sistemas principales de IBM zSystems podría reducir potencialmente las pérdidas por fraude en unos 161 000 millones de dólares en todo el mundo. En ese caso, los bancos podrían evitar 140 000 millones de dólares en pérdidas y, asimismo, las tarjetas y los pagos podrían evitar 21 000 millones de dólares. Solo en Estados Unidos, las pérdidas por fraude bancario podrían reducirse en 44 000 millones de dólares y en 6000 millones en el caso de las tarjetas y los pagos.

Claro que también existen obstáculos para adoptar la inferencia de IA en el sistema principal para las operaciones de fraude, como los problemas de gobernanza de los modelos, los costes de eliminación y sustitución, la disponibilidad de recursos internos de ciencia de datos y la demostración del caso de negocio.

Aun así, la ejecución de modelos avanzados de IA directamente en el entorno del sistema principal es una poderosa innovación en un sector en el que se calcula que el 70 % del valor de las transacciones mundiales se ejecuta en sistemas principales de IBM. La detección del fraude es un importante caso de uso de esta nueva función de IBM, con ventajas demostrables tanto para la cuenta de resultados como para la experiencia del cliente.

EL ALTO COSTE DEL FRAUDE EN LAS OPERACIONES BANCARIAS, LAS TARJETAS Y LOS PAGOS

En 2021, el fraude generó pérdidas de aproximadamente 385 000 millones de dólares a nivel mundial en los sectores de la banca, las tarjetas y los pagos.

El fraude bancario y de pagos adopta muchas formas en los sectores minorista y empresarial. Entre los fraudes dirigidos a los bancos, se incluyen la apropiación de cuentas, el fraude de pagos automáticos autorizados (APP, por sus siglas en inglés), el fraude de facturas y una amplia gama de esquemas de phishing y de ingeniería social diseñados para activar transferencias de dinero ilegítimas u obtener credenciales de cuentas. Las tarjetas y los pagos también son vulnerables a la apropiación de cuentas y a la suplantación de identidad (phishing), así como a esquemas específicos que incluyen la identificación sintética, el fraude de compra máxima sin intención de pago (bust-out) y el fraude de intermediario.

Figura 1: Esquemas comunes de fraude bancario y de tarjetas

Fraude bancario		Fraude con tarjetas	
	Apropiación de cuenta		Fraude con aplicación
	Fraude con APP		Fraude de compra máxima sin intención de pago
	Fraude en cheques		Intermediarios
	Fraude en facturas		Phishing
	Ingeniería social		Identificador sintético

Fuente: Celent

Estos y otros fraudes dirigidos a las cuentas bancarias, las tarjetas y los pagos preocupan mucho a las instituciones financieras. Celent estima que las pérdidas anuales por fraude son de 209 millones de dólares para un banco de nivel 1 en Estados Unidos (activos totales superiores a 100 000 millones de dólares) y de 35 millones de dólares para un banco de nivel 2 (activos totales entre 50 000 y 100 000 millones de dólares). A escala del sector, los bancos tuvieron una pérdida de 328 000 millones de dólares por fraude a nivel mundial en 2021. Los sectores de las tarjetas y los pagos acumularon pérdidas adicionales de 57 000 millones de dólares. En total, en 2021 el fraude generó pérdidas de aproximadamente 385 000 millones de dólares a nivel mundial en los sectores de la banca, las tarjetas y los pagos.

Figura 2: Pérdidas por fraude en los sectores de la banca, las tarjetas y los pagos en 2021

Fuente: Estimaciones de Celent basadas en datos de transacciones del BPI y datos de fraude de los bancos centrales.
Nota: El fraude bancario incluye las transferencias, los débitos directos y los cheques. El fraude con tarjetas y de pagos incluye tarjetas de crédito y débito, pagos electrónicos y otros tipos de pagos.

Aunque los bancos y los procesadores de pagos llevan décadas luchando para evitar el fraude mediante sistemas de detección y seguridad de las tarjetas basadas en chips, las pérdidas han seguido aumentando; esto es porque los estafadores van un paso adelante ideando nuevos esquemas basados en la tecnología y la ingeniería social.

La pandemia de la COVID-19 ha elevado las cifras de fraude. Para los bancos, una fuente importante ha sido el phishing y los esquemas de ingeniería social que se aprovechan de la ansiedad y las necesidades médicas en torno a la pandemia. En cuanto a las transacciones con tarjeta, la pandemia ha aumentado la banca digital y el comercio electrónico, ya que los consumidores han tratado de evitar cualquier transacción presencial en sucursales y tiendas. Dado que las transacciones sin presencia física de la tarjeta (CNP, por sus siglas en inglés) constituyen la mayor parte del fraude con tarjeta —alrededor del 65 %—, las pérdidas por fraude con tarjeta han aumentado.

La ayuda está en camino: modelos de fraude basados en el aprendizaje profundo

Los avances en inteligencia artificial, como el aprendizaje profundo, dan ahora a los bancos las herramientas necesarias para combatir el fraude de forma mucho más eficaz: analizando los datos a escala con el objetivo de encontrar patrones que apunten al fraude, incluyendo nuevas tipologías no vistas anteriormente.

El aprendizaje profundo es un tipo de modelo de aprendizaje automático basado en una red neuronal profunda (DNN, por sus siglas en inglés). Una DNN está formada por nodos computacionales, o neuronas, que utilizan pesos progresivos para reforzar las conexiones entre los nodos. Los nodos se distribuyen en varias capas, de manera que forman una red «profunda», que aumenta la capacidad y la velocidad de aprendizaje del modelo. Los modelos de aprendizaje profundo se entrenan con datos existentes, como las transacciones históricas en el caso de los modelos de fraude. Después, el modelo entrenado se ejecuta en datos reales, como una transacción en tiempo real, para generar un resultado o una inferencia. En el caso de los modelos de fraude, la inferencia suele ser una puntuación que expresa la probabilidad de que la transacción sea fraudulenta.

Basándose en conversaciones e investigaciones del sector, Celent estima que la inferencia de la IA basada en modelos de aprendizaje profundo puede aumentar la precisión de la detección del fraude en un 60 % con respecto a los modelos de fraude existentes.

Sin embargo, el potencial de la inferencia para mejorar los índices de fraude se ve drásticamente limitado por el hecho de que, en los entornos de sistemas principales de gran volumen, estos modelos suelen ejecutarse solo en una pequeña parte de las transacciones —menos del 10 %— debido a problemas de latencia, coste y fricción con el cliente. Esto significa que aproximadamente el 90 % del fraude potencialmente evitable sigue sin detectarse. Esto limita en gran medida la capacidad de los bancos para aprovechar los avances de la IA y recuperar las pérdidas por fraude.

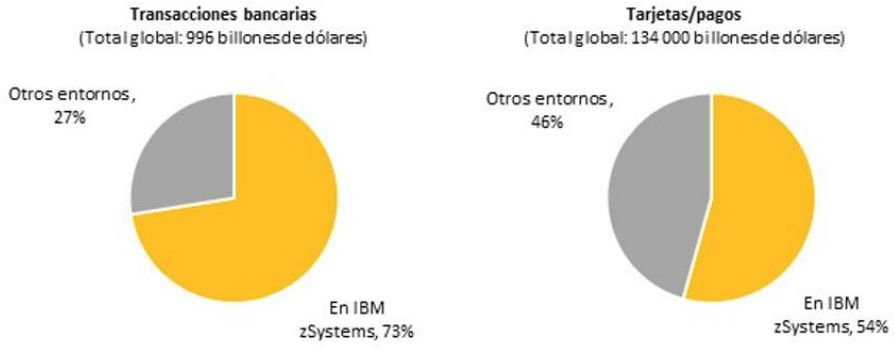
Las barreras de latencia y coste para pasar el 100 % de las transacciones bancarias y de tarjetas a través de modelos avanzados son cosa del pasado. El nuevo procesador IBM z16 Telum incorpora un acelerador de IA que, por primera vez en IBM zSystems, puede ejecutar modelos de IA directamente en el chip y en tiempo real. Esto mejora exponencialmente el desempeño y los tiempos de respuesta, de manera que hace posible —por primera vez— pasar prácticamente todas las transacciones por modelos de detección de fraude basados en el aprendizaje profundo.

LIMITACIONES DE LA DETECCIÓN DEL FRAUDE ACTUALMENTE

La tecnología de detección de fraudes y los enfoques operativos comunes para los entornos de sistema principal incluyen la ejecución de fraudes en sistemas fuera de la plataforma en transacciones seleccionadas o en una etapa posterior a la transacción. Esto limita drásticamente la capacidad de los bancos y procesadores de pagos en lo que se refiere a la incorporación de modelos avanzados de IA en todas sus transacciones.

Los sistemas básicos de muchos de los grandes bancos y procesadores de pagos se ejecutan en entornos informáticos de sistema principal. IBM estima que 45 de los 50 bancos más destacados del mundo funcionan con sistemas principales IBM zSystem. La mayoría de las tarjetas y procesadores de pagos principales también funcionan en la plataforma. A nivel mundial, Celent estima que el 70 % del valor de las transacciones bancarias, de tarjetas y de pagos se ejecuta en entornos IBM zSystems.

Figura 3: Valor de las transacciones bancarias, de tarjetas y pagos en IBM zSystems



Fuente: Celent

La latencia entre los sistemas básicos y los sistemas de detección fuera de la plataforma se puede tolerar en algunas transacciones. Sin embargo, en el caso de las rutinas de inferencia de IA con gran cantidad de datos aplicadas a las transacciones en tiempo real —como los pagos en tiempo real, las transacciones con tarjeta y las transacciones bancarias digitales—, la latencia hace que no sea práctico pasar todas las transacciones por una plataforma de detección de IA cuando se trata de entornos de gran volumen. Cuando las transacciones del sistema básico se envían desde el sistema principal a un sistema de detección fuera de la plataforma para el análisis en tiempo real, los tiempos de respuesta para recibir los resultados de la detección oscilan entre 50 y 80 milisegundos, mientras las transacciones esperan. Esto ralentiza los tiempos de aprobación de las transacciones, lo que puede crear fricciones con los clientes, especialmente en las transacciones con tarjeta.

Pero, fundamentalmente, la alta latencia puede hacer que sea imposible que todas las transacciones pasen por un sistema de detección de fraude fuera de la plataforma. La latencia entre el sistema básico y el software de detección puede retrasar la recepción de los resultados de la detección por el sistema básico hasta el punto que las transacciones en

tiempo real se retrasen. Es por ello que algunos bancos solo utilizan modelos de aprendizaje profundo para detectar el fraude tras la transacción.

Como resultado, los bancos solo envían una pequeña parte de las transacciones —menos del 10 %— a través de sus motores de detección de fraude en tiempo real. Este enfoque conlleva graves consecuencias. Los modelos de aprendizaje profundo actualmente están permitiendo mejoras significativas, alrededor de un 60 %, en las tasas de detección. A pesar de ello, los bancos no están sacando el máximo partido a estos modelos porque solo están procesando una muestra de transacciones. Esto significa que un gran porcentaje de fraude no será detectado, lo que a su vez implica un aumento de pérdidas por fraude. A medida que el fraude se convierte en el centro de atención del cumplimiento de los delitos financieros, si los bancos no son capaces de pasar todas sus transacciones por la detección antifraude, podrían llegar a enfrentarse también al riesgo normativo.

Problemas heredados en un banco estadounidense de nivel 1

Un banco estadounidense de nivel 1 cuyo sistema básico funciona en una plataforma IBM zSystems ha implementado un sistema de detección de fraudes basado en IA fuera de la plataforma. Debido a problemas de coste y latencia, el banco solo procesa transacciones de muy alto riesgo a través del sistema de IA. La mayoría de las transacciones se procesan con una puntuación basada en reglas, se aprueban para comodidad del cliente y se someten a un análisis posterior a la transacción. Los beneficios de la IA se ven muy limitados por la imposibilidad de ejecutar los modelos en todas las transacciones, lo que significa que la IA no se utiliza en todo su potencial.

REDUCCIÓN DE LAS PÉRDIDAS POR FRAUDE CON LA INFERENCIA DE IA EN EL SISTEMA PRINCIPAL

IBM ha desarrollado un procesador para su ordenador central IBM z16 que incluye un acelerador para la IA diseñado para ejecutar inferencias avanzadas directamente en el chip, a escala. Celent estima que el nuevo procesador IBM z16 es compatible con la detección de fraude basada en el aprendizaje profundo en prácticamente todas las transacciones; esto reduce potencialmente las pérdidas por fraude en banca, tarjetas y pagos en 161 000 millones de dólares a nivel mundial.

Los algoritmos de aprendizaje profundo tienden a ser más intensivos en computación que los modelos de fraude heredados. A medida que los bancos implementan la inferencia de IA basada en el aprendizaje profundo para el fraude, se enfrentan a desafíos de gestión relacionados con estas cargas de trabajo críticas. Cuando la detección se realiza en sistemas fuera de la plataforma, los tiempos de respuesta de la detección pueden alcanzar más de 80 milisegundos, con tasas de rendimiento en el rango de 1000 a 1500 transacciones por segundo (tps, por sus siglas en inglés).

Debido a estas limitaciones de latencia y rendimiento, los bancos han experimentado que las transacciones se retrasan mientras esperan los resultados de la detección. Estos y otros problemas llevan a los bancos a enviar solo una parte de las transacciones —menos del 10 %— a través de sus motores de detección.

Aprendizaje profundo en el sistema principal

Basándose en un modelo de aprendizaje profundo para fraudes con tarjetas de crédito, con 32 chips IBM Telum que funcionen en un solo servidor se pueden realizar hasta 3,5 millones de inferencias por segundo con un tiempo de respuesta promedio de 1,2 milisegundos.

Fuente: Microbenchmark de IBM, agosto de 2021

DECLARACIÓN DE LIMITACIÓN DE RESPONSABILIDAD: El resultado del rendimiento se extrapola de las pruebas internas de IBM.

IBM ha desarrollado un acelerador para su ordenador central IBM z16 que puede ejecutar modelos de inferencia de IA directamente en el chip. Según IBM, el rendimiento y las mejoras en la ejecución de los modelos de IA en el sistema principal son suficientes para realizar el análisis del fraude en tiempo real de prácticamente todas las transacciones, incluso en entornos de procesamiento de bancos, tarjetas o pagos de gran volumen.

Además, se puede realizar sin prácticamente afectar los tiempos de procesamiento de las transacciones. IBM afirma que el IBM Integrated Accelerator for AI, el cual forma parte de su nuevo procesador Telum, puede ejecutar modelos de IA en el sistema principal con un tiempo de respuesta muy rápido de solo 1,2 milisegundos para cada solicitud de inferencia. En el caso concreto de la detección de fraudes con tarjetas, las primeras evaluaciones comparativas indicaron que una configuración de 32 chips Telum puede soportar hasta 3,5 millones de inferencias por segundo.

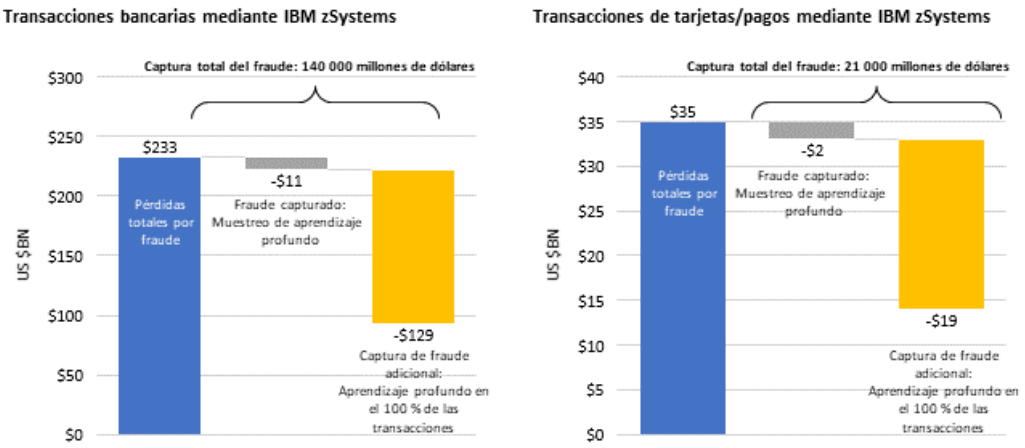
Esta escala es suficiente para soportar incluso los flujos de transacciones máximos, lo que hace posible que los bancos y los procesadores de pagos ejecuten prácticamente todas las transacciones a través de modelos de aprendizaje profundo.

Los bancos y los procesadores de tarjetas y pagos pueden aprovechar todo el potencial de la tecnología moderna de inferencia y ejecutar modelos avanzados con todas las transacciones. Celent estima que la aplicación de modelos avanzados de inferencia a todas las transacciones reduciría potencialmente las pérdidas por fraude en 2 céntimos por cada 100 dólares de transacciones a nivel mundial (2 puntos de base).

En Estados Unidos, donde los índices de fraude son superiores a la media mundial —9,3 céntimos por cada 100 dólares, frente a 3,7 céntimos a nivel mundial—, las pérdidas por fraude podrían reducirse en 5,6 céntimos por cada 100 dólares. Esto equivale a ahorrar al banco 1,33 dólares en una transacción media de 2375 dólares.

Celent estima que, en teoría, pasar todas las transacciones que se ejecutan actualmente en IBM zSystems a través de modelos de aprendizaje profundo podría reducir potencialmente las pérdidas por fraude en 161 000 millones de dólares a nivel mundial. Los bancos podrían evitar 140 000 millones de dólares en pérdidas por fraude, mientras que esta cifra sería de 21 000 millones de dólares en el caso de las tarjetas y los pagos. Solo en Estados Unidos, las pérdidas por fraude se pueden reducir potencialmente en 44 000 millones de dólares para los bancos y en 6000 millones para las tarjetas y los pagos.

Figura 4: Reducción potencial de pérdidas por fraude mediante modelos de aprendizaje profundo



Fuente: Celent

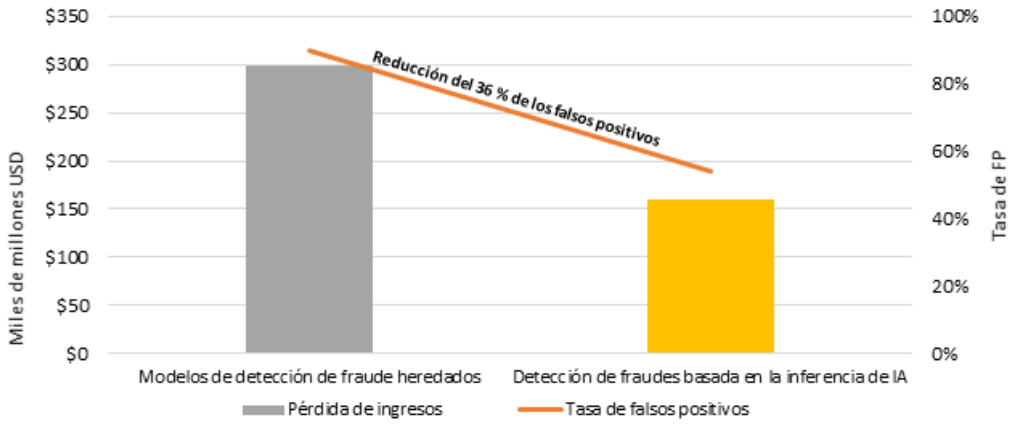
Celent estima que para un banco de nivel 1 en IBM z16, la ejecución de todas las transacciones a través de modelos de inferencia avanzados —en comparación con la práctica actual de aplicar modelos de IA a solo un 10 % de las transacciones— podría reducir las pérdidas por fraude en 105 millones de dólares adicionales. Un banco de nivel 2 podría evitar 18 millones de dólares adicionales en pérdidas. Procesar todas las transacciones mediante modelos avanzados, a su vez, también mejoraría los propios modelos. Un mayor número de transacciones produciría más datos para entrenar los modelos, de modo que se lograría una mayor precisión en la detección del fraude.

CONTROLAR LOS FALSOS POSITIVOS PARA REDUCIR LA FUGA DE CLIENTES

Los modelos antifraude heredados tienen tasas de falsos positivos muy elevadas —normalmente el 90 % de todas las transacciones con alerta o más—, lo que lleva a los bancos a rechazar transacciones legítimas. Los falsos positivos y las transacciones denegadas no solo crean fricción con el cliente, también provocan pérdidas en dólares porque estos mismos clientes, tras la denegación, simplemente proceden a sacar su otra tarjeta de crédito o débito para realizar las compras. Celent estima que las transacciones con tarjeta de crédito denegadas cuestan al sector 298 000 millones de dólares en pérdidas de ingresos por comisiones en todo el mundo.

La necesidad de equilibrar los esfuerzos antifraude con la minimización de la fricción con el cliente es otro motivo por el que los bancos limitan las rutinas de detección del fraude a solo una muestra de todas las transacciones. Los falsos positivos se producen cuando las transacciones legítimas son marcadas erróneamente por el software de detección como fraudulentas. La mayor precisión de los modelos de aprendizaje profundo puede mejorar significativamente las altísimas tasas de falsos positivos del sector, lo que, a su vez, reduciría el número de transacciones rechazadas erróneamente. Esto también ayudaría a mejorar la experiencia del cliente y a reducir la pérdida de ingresos debida a la fuga de clientes. Además, significaría que los bancos pueden pasar todas sus transacciones a través de la detección del fraude con menos perjuicio por la fricción con los clientes.

Figura 5: Los modelos de aprendizaje profundo mejoran las tasas de falsos positivos



Fuente: Celent

Los modelos de aprendizaje profundo aplicados a cada transacción con tarjeta podrían mejorar las tasas de falsos positivos hasta cerca del 55 %. Aunque sigue siendo un porcentaje muy alto, podría suponer una reducción de los ingresos perdidos debido a las comisiones de las tarjetas de entre 137 000 y 161 000 millones de dólares en todo el mundo.

Un menor número de falsos positivos aporta también otras ventajas. Los analistas de fraude tendrían que trabajar con menos alertas, lo que ayudaría a reducir los costes de la investigación posterior a la transacción. En cuanto a los beneficios para la reputación, la reducción de la fricción y de la frustración del cliente aumentaría la buena voluntad y la confianza del cliente.

Los modelos avanzados también pueden conducir a mejoras en la detección de comportamientos sospechosos que puedan indicar blanqueo de dinero. La Ley de Secreto Bancario de EE. UU., las directivas de la UE contra el blanqueo de capitales y otras normativas someten a los programas de lucha contra el blanqueo de capitales (AML, por sus siglas en inglés) de los bancos a un intenso escrutinio por parte de los reguladores. Los reguladores de Estados Unidos son especialmente activos a la hora de citar a los bancos por programas inadecuados de lucha contra el blanqueo de capitales, con multas contra algunos bancos que superan los mil millones de dólares. Las operaciones de lucha contra el blanqueo de capitales también se ven afectadas por las tasas de falsos positivos muy elevadas, normalmente superiores al 95 %, lo que impone una grave carga operativa a los bancos. Además, la supervisión de la lucha contra el blanqueo de capitales suele realizarse después de las transacciones, algo que expone a los bancos a un mayor riesgo. Aprovechar los modelos basados en la IA para las operaciones de AML puede ayudar con estos problemas, ya que mejora la precisión de la detección del comportamiento de AML y reduce los falsos positivos.

AVANZAMOS HACIA EL FUTURO

Nuestro análisis señala los beneficios significativos y cuantificables de ejecutar modelos de aprendizaje profundo en hasta el 100 % de las transacciones. IBM afirma que su nuevo acelerador es compatible con estos modelos para las transacciones que se ejecutan en los sistemas principales IBM z16, incluso en entornos de gran volumen. Sin embargo, sigue habiendo una serie de factores que los bancos y procesadores que den el salto deben tener en cuenta.

Mientras los bancos y los procesadores de tarjetas y pagos sopesan las ventajas de implementar la detección de fraude basada en el aprendizaje profundo en el sistema principal, Celent recomienda que consideren cuestiones como las siguientes:

- **Modelo de gobierno.** Los reguladores y los auditores internos exigen una gobernanza sólida en torno a los modelos de fraude. Esto significa que los modelos de IA deben ser transparentes y explicables. Si bien los proveedores de plataformas de IA se están alejando en general de los enfoques de «caja negra», el gobierno de los modelos de IA sigue siendo una tarea compleja.
- **Resistencia normativa.** Los reguladores se sienten cómodos con la detección tradicional basada en reglas, pero están menos familiarizados con las técnicas avanzadas de aprendizaje profundo. Es posible que los bancos, los científicos de datos y sus proveedores deban, en algunos casos, educar a los reguladores sobre la eficacia y la fiabilidad de la IA avanzada a medida que avanzan.
- **Coste de la sustitución.** Muchas instituciones ya han implantado sistemas de detección de fraudes basados en la IA. Estas empresas tendrán que desarrollar el argumento comercial para trasladar la detección al sistema principal, incluida la decisión de si mantener los sistemas existentes de alguna forma —por ejemplo, para apoyar el análisis posterior a la transacción o las líneas de negocio más pequeñas— o si desecharlos por completo.
- **Recursos para la ciencia de los datos.** El acelerador integrado de IBM para la IA está optimizado para ejecutar modelos, incluidos los construidos con marcos de código abierto como Pytorch y TensorFlow. Sin embargo, todavía no se ha demostrado que sea compatible con los paquetes de software de detección de fraudes, aunque esperamos que algunos proveedores de soluciones antifraude acaben presentando paquetes que puedan funcionar con el acelerador. De todo modos, las instituciones que trasladen la detección basada en IA a IBM z16 necesitarán las capacidades de ciencia de datos para desarrollar y dar soporte a modelos avanzados de aprendizaje profundo para el fraude, ya sea internamente o a través de proveedores de modelos especializados.

Las instituciones financieras deben prestar especial atención a estos factores y hacer las diligencias oportunas en el nuevo acelerador de IA de IBM. Sin embargo, los beneficios potenciales en términos de menos pérdidas por fraude y transacciones rechazadas, así como la reducción de la fricción y la mejora de la experiencia del cliente, son convincentes. Las empresas que utilizan IBM zSystems deberían estudiar detenidamente las ventajas de trasladar la detección del fraude al sistema principal.

APROVECHAR LA EXPERIENCIA DE CELENT

Si este informe le ha parecido interesante, recuerde que puede contratar a Celent para que le ayude a realizar análisis e investigaciones según sus necesidades. Nuestra experiencia colectiva y los conocimientos que hemos adquirido al trabajar en este informe pueden ayudarle a agilizar la creación, el perfeccionamiento o la ejecución de sus estrategias.

Apoyo a las instituciones financieras

Los proyectos a los que solemos dar apoyo son:

Filtrado y selección de proveedores. Realizamos estudios específicos adaptados a usted y a su negocio para ayudarle a entender mejor cuáles son sus necesidades particulares. A continuación, creamos y gestionamos una solicitud de información personalizada para los proveedores seleccionados con el objetivo de ayudarle a tomar decisiones rápidas y precisas.

Evaluaciones de la práctica empresarial. Dedicamos tiempo a la evaluación de sus procesos y requisitos empresariales. Basándonos en nuestro conocimiento del mercado, identificamos las posibles limitaciones de los procesos o de la tecnología y proporcionamos ideas claras que le ayudarán a implementar las mejores prácticas del sector.

Elaboración de estrategias de TI y empresariales. Primero, recogemos las opiniones de su equipo ejecutivo y de TI, de su personal de primera línea y, también, de sus clientes. A continuación, analizamos su posición actual, las capacidades institucionales y la tecnología teniendo en cuenta sus objetivos. De ser necesario, también le ayudamos a reformular sus planes tecnológicos y empresariales para que pueda abordar las necesidades a corto y largo plazo.

Apoyo a los proveedores

Proporcionamos servicios que le ayudan a perfeccionar su oferta de productos y servicios. Algunos ejemplos son:

Evaluación de la estrategia de productos y servicios. Le ayudamos a evaluar su posición en el mercado en términos de funcionalidad, tecnología y servicios. Nuestros talleres sobre estrategia le ayudarán a llegar a los clientes adecuados y a adaptar lo que ofrece a sus necesidades.

Revisión de la comunicación de mercado y del material adjunto. Basándonos en nuestra amplia experiencia con sus clientes potenciales, evaluamos su contenido de comunicación de mercado y ventas —incluyendo el sitio web y cualquier material adicional—.

INVESTIGACIÓN RELACIONADA DE CELENT

Remodelar el riesgo: una taxonomía de la tecnología de regulación
Octubre de 2021

Previsión de tendencias tecnológicas: riesgo, edición de 2022
Octubre de 2021

Gasto informático y operativo en AML-KYC: edición de 2021
Diciembre de 2021

Gasto informático y operativo en el fraude: edición de 2021
Febrero de 2021

Innovación en riesgo: una instantánea a través de la perspectiva del gestor de riesgos del modelo 2021
Abril de 2021

Fino Payments Bank: implementación de la gestión de fraude a distancia en toda la empresa durante la pandemia
Marzo de 2021

Swedbank: modernizar la gestión del fraude con tarjetas y mejorar la experiencia del cliente
Marzo de 2021

AVISO DE COPYRIGHT

Para más información, póngase en contacto con info@celent.com o:

Neil Katkov nkatkov@celent.com

América

EE. UU.
99 High Street, 32nd Floor
Boston, MA 02110-2320

(+1) 617 424 3200

EE. UU.
1166 Avenue of the Americas
Nueva York, NY 10036

(+1) 212 345 8000

EE. UU.
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

(+1) 415 743 7800

Brasil
Rua Arquiteto Olavo Redig
de Campos, 105
Edificio EZ Tower – Torre B – 26º andar
04711-904 – São Paulo

(+55) 11 3878 2000

EMEA

Suiza
Tessinerplatz 5
Zúrich 8027

(+41) 44 5533 333

Francia
1 Rue Euler
París 75008

(+33) 1 45 02 30 00

Italia
Galleria San Babila 4B
Milán 20122

(+39) 02 305 771

Reino Unido
55 Baker Street
Londres W1U 8EW

(+44) 20 7333 8333

Asia Pacífico

Japón
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tokio 107-6216

(+81) 3 6871 7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

(+852) 2301 7500

Singapur
138 Market Street
#07-01 CapitaGreen
Singapur 048946

(+65) 6510 9700