REPORTE OFICIAL | OCTUBRE DE 2014

Autenticación 3-D Secure con modelos avanzados

Los modelos que se usan para la autenticación basada en el riesgo y el comportamiento de las transacciones de comercio electrónico pueden reducir las pérdidas y proporcionar operaciones de pago fluidas para las transacciones de bajo riesgo.

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies, Análisis avanzado y ciencia de los datos

ca technologies

Tabla de contenidos

Resumen

Reto

Los emisores necesitan equilibrar la seguridad de las transacciones de pago de comercio electrónico y una experiencia del cliente de pago sin inconvenientes. La cuestión es cómo proporcionar una experiencia de pago sin problemas a los clientes legítimos para que no abandonen la transacción o usen otro método de pago y, al mismo tiempo, detener los intentos ilegítimos de realizar transacciones. La utilización de la autenticación basada en el comportamiento para determinar en qué transacciones se debe pedir al cliente que atraviese pasos adicionales de autenticación es clave para reducir la fricción del cliente y garantizar mejor que la transacción sea legítima. Las reglas son un componente importante para brindar autenticación basada en el riesgo y el comportamiento. Cuando se agregan modelos y se los usa para guiar la aplicación de reglas basadas en el riesgo, el impacto en los intentos ilegítimos de autenticación se puede incrementar considerablemente, a la vez que se proporciona una mejor experiencia a los titulares de tarjetas y se reducen las pérdidas para el emisor.

Oportunidad

El canal 3-D Secure presenta muchas oportunidades para los emisores. Ante el gran aumento del fraude del comercio electrónico, combinado con el cambio de responsabilidad, la autenticación 3-D Secure proporciona una primera línea de defensa a los emisores. No obstante, es importante utilizar esa primera línea de defensa con inteligencia y de la mejor manera posible. CA Risk Analytics ofrece la oportunidad de examinar las transacciones de comercio electrónico durante la autenticación con información única que no está disponible para los sistemas de detección de fraudes de autorización y, por lo tanto, de prevenir una transacción ilegítima. Se debe realizar una evaluación del riesgo de autenticación a fin de brindar una experiencia de pago ininterrumpida a la mayoría de los titulares de tarjetas legítimos. Con la solución CA Risk Analytics instalada, los emisores pueden reducir las pérdidas y limitar la fricción en la experiencia del cliente.

Beneficios

CA Risk Analytics puede ayudar a los emisores a evaluar el nivel de riesgo de las actividades en línea en comercios protegidos por 3-D Secure. Evalúa de manera transparente el riesgo de que alguien que no sea el titular de la tarjeta legítimo intente realizar una transacción de comercio electrónico, en tiempo real. Puede identificar una parte importante de intentos de transacciones legítimas y permitir que los clientes continúen con la compra sin afectarlos y, a la vez, de manera similar, identifica los intentos de transacciones ilegítimas que se deben detener. La identificación del dispositivo, la ubicación geográfica, las características de la conexión y los patrones históricos se pueden usar para evaluar el riesgo de cada intento de transacción.

Un aspecto clave de CA Risk Analytics es la disponibilidad de modelos regionales avanzados que evalúan el nivel de riesgo de un intento de transacción determinado con análisis sofisticados, incluido un modelo de red neuronal de comportamiento, y que proporcionan una calificación que indica el riesgo de ese intento. Luego, las reglas en CA Risk Analytics pueden combinar esta calificación del modelo con otros factores empresariales para determinar el mejor procedimiento que se debe seguir con un intento de transacción determinado, lo que da como resultado un incremento considerable de la efectividad de la solución.

Sección 1

3-D Secure proporciona las bases para la reducción de la pérdida en el comercio electrónico

El protocolo 3-D Secure brinda a los emisores muchas oportunidades que se deben aprovechar para obtener el máximo beneficio y protección que ofrece el canal 3-D Secure.

El canal 3-D Secure se centra en la autenticación de los intentos de transacciones de comercio electrónico. Es importante comprender la diferencia entre autenticación y autorización. La autenticación se refiere al intento de confirmar que la persona que inicia una transacción (u otra actividad) sea el titular de la tarjeta legítimo y genuino. La autorización se refiere al intento de validar que el titular de la tarjeta (confirmado) tenga la autoridad para realizar la transacción (según la política, los saldos disponibles, el estado de cuenta y otras cuestiones). Tenga en cuenta que el fraude puede ocurrir y detectarse en ambos pasos, la autorización y la autenticación, pero existen diferencias clave; por ejemplo, la autenticación no contrarresta el fraude de primera instancia. Sin embargo, independientemente del tipo de fraude, la autenticación de la persona que intenta realizar una transacción es el punto de inicio para garantizar que la transacción en sí sea válida.

En el caso de las transacciones en las que se presenta la tarjeta, la presencia física de la tarjeta ha sido aceptada por mucho tiempo como un componente clave de la autenticación. A medida que los usuarios ilegítimos se vuelven más sofisticados, los emisores responden con una mejor seguridad en las tarjetas (banda magnética, CVV [valor de verificación de la tarjeta], CVC [código de verificación de la tarjeta], CID [número de identificación de la tarjeta] y tarjetas inteligentes). Estos datos, o el resultado de la autenticación con estos datos, se envían generalmente en una solicitud de autorización.

Para las transacciones CNP (sin tarjeta), la autenticación física mediante la tarjeta ya no es posible y la responsabilidad suele recaer en el comercio. No obstante, con la llegada del comercio electrónico, ha sido necesario desarrollar una autenticación sólida de las transacciones de comercio electrónico. Los datos de la solicitud de autorización, si bien son suficientes para autorizar una transacción, no alcanzan para la autenticación de una transacción de comercio electrónico. Como resultado, surgió la transacción 3-D Secure, que requiere otra información en comparación con la solicitud de autorización y que está diseñada para autenticar a la persona que intenta realizar una transacción. Esta tarea, que es totalmente diferente de la autorización, requiere una perspectiva única. Sin embargo, los resultados de esta autenticación se pueden utilizar en el flujo de autorización para proporcionar un mejor contexto al sistema de autorización.

Para ser claros, cuando nos referimos a un fraude en este documento, hacemos referencia a un fraude de autenticación en transacciones 3-D Secure de comercio electrónico.

Con el protocolo 3-D Secure, existe la posibilidad de examinar los intentos de autenticación de comercio electrónico mediante el uso de información única que no está disponible para los sistemas de detección de fraudes de autorización y, por lo tanto, de prevenir una transacción ilegítima antes de que genere una solicitud de autorización. Cuando se usa el sistema CA Risk Analytics, esta información única incluye un identificador único para cada dispositivo (identificador de dispositivo), una dirección URL [localizador uniforme de recursos] a la que accede el titular de la tarjeta para efectuar la transacción (URL del comercio), la dirección IP (protocolo de Internet) actual del dispositivo e información adicional de proveedores de datos independientes, como ubicación del dispositivo, velocidad de la conexión, tipo, identificación del anonimizador, etc. Esta información aumenta considerablemente (pero no reemplaza) la información tradicional, como el monto, la moneda, el nombre y el identificador del comercio, el identificador de la tarjeta, etc. Con este aumento, los modelos de autenticación 3-D Secure pueden proporcionar más beneficios que solo ven la información tradicional, ya que brindan una detección fuerte de los intentos de autenticación ilegítimos y afectan únicamente a una pequeña parte de los intentos legítimos.

El canal 3-D Secure proporciona información en tiempo real para el análisis de las transacciones de autenticación; en particular, tenemos la oportunidad de actualizar información sobre la tarjeta, el dispositivo u otras entidades centrales de la transacción en tiempo real. Esto permite que todas las transacciones siguientes aprovechen el beneficio de la información y el contexto incrementados cuando se las evalúa para calcular el riesgo de autenticación. Esto puede ser especialmente potente cuando se analizan entidades entre bancos en un entorno de SaaS (software como servicio).

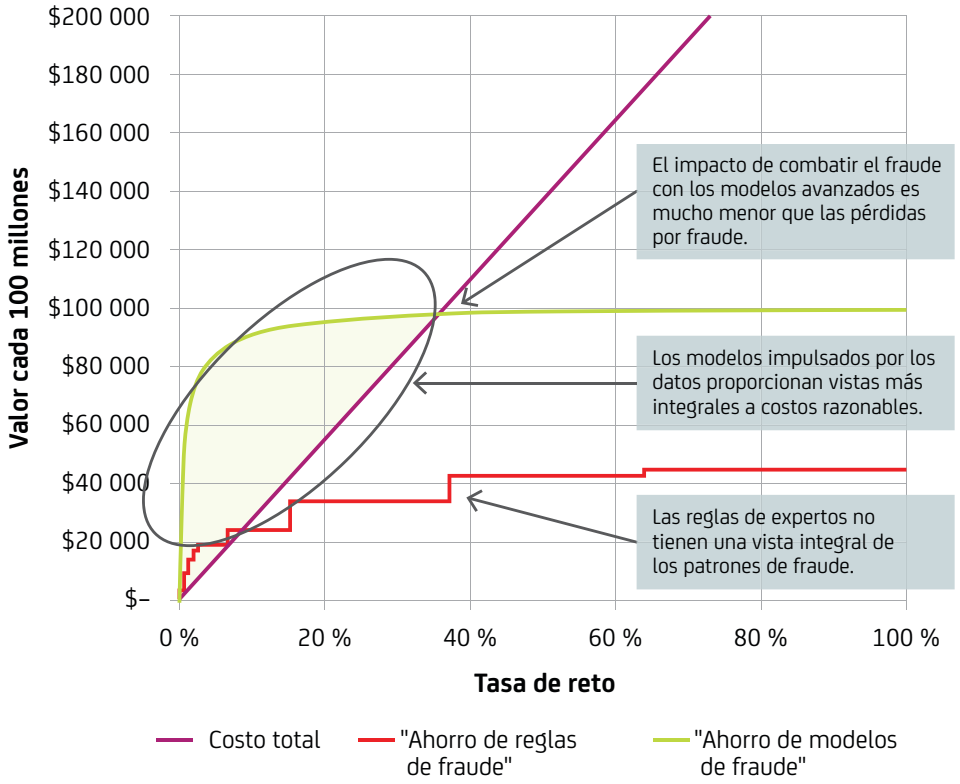
También existe la posibilidad de hacer que la compra por comercio electrónico sea relativamente fluida. Las implementaciones iniciales de 3-D Secure presentan preguntas de seguridad a todos los compradores de comercios protegidos por 3-D Secure. Si la seguridad es sólida, como el uso de OTP (contraseñas de un solo uso), esto puede ser razonablemente efectivo; si las preguntas no son seguras, como solicitar información necesaria para realizar la transacción en sí (fecha de caducidad o CVV2 [valor de verificación de tarjeta 2]), esto no hace mucho para combatir las pérdidas. Pero existe un efecto secundario: realizar preguntas de seguridad a los titulares de tarjetas introduce “fricción” en la transacción, lo que incrementa la resistencia a completar la transacción y afecta negativamente la experiencia del cliente.

El impacto negativo de la fricción en la experiencia del cliente no es completamente cualitativo, tiene un componente cuantitativo también: incrementa considerablemente el abandono y las tasas de “error falso”. El abandono genera pérdida de comisiones de intercambio y tiene otros impactos más importantes, como la pérdida de saldo rotativo para tarjetas de crédito o la posible deserción de los clientes, que es un problema grave tanto para cuentas de débito como de crédito. Estos impactos permiten cuantificar parte del impacto que una experiencia del cliente negativa tiene para los emisores y proporcionan una gran motivación para reducir la fricción de la transacción. En el caso extremo en el que se presentan preguntas de seguridad a todos los clientes, los costos del abandono pueden superar cualquier posible ahorro de pérdida. Por lo tanto, es esencial evaluar el riesgo de una transacción determinada e intervenir en el proceso solo cuando haya una buena justificación. Esto se realiza mejor con la autenticación basada en el comportamiento.

En el gráfico 1 de la página siguiente, se muestra un ejemplo del costo total de la detección de fraude (incluidas las oportunidades perdidas debido al abandono) (línea violeta), el ahorro de un sistema de reglas típico (línea roja) y el ahorro de un modelo regional típico de CA Risk Analytics (línea verde). Observe que a medida que se incrementa la tasa de reto, también lo hace el costo de operar el sistema. Con un sistema de reglas, que generalmente no tiene una vista completa del fraude, el costo de operar el sistema puede sobrepasar rápidamente el ahorro obtenido con las reglas. Con un modelo avanzado impulsado por los datos, se puede obtener una vista completa del fraude a un costo razonable. El área marcada en verde muestra la ventaja que tiene un modelo en comparación con las reglas.

Gráfico 1.

Costo total de la detección de fraude.



Sección 2

Autenticación basada en el comportamiento

La autenticación basada en el comportamiento incluye analizar la transacción actual en el contexto de patrones usuales del titular de la tarjeta, el comercio y la actividad del dispositivo del usuario para ver si solo esta información puede generar un alto grado de confianza en cuanto a que el usuario sea el titular de la tarjeta auténtico. De ser así, no es necesario molestar al usuario en el medio de la transacción y esta se puede completar sin impacto alguno, lo que reduce considerablemente la fricción y la probabilidad de abandono y, por lo tanto, mejora la experiencia del titular de la tarjeta[1]. Por otro lado, si hay un alto grado de certeza de que este no es el titular de la tarjeta auténtico, la transacción puede ser denegada rotundamente, lo que previene una solicitud de autorización o pago y elimina la oportunidad de fraude, aunque el estafador conozca información de autenticación. Por último, en las transacciones en las que no hay un alto grado de certeza de legitimidad o ilegitimidad, lo aconsejable sería implementar una interacción de autenticación fuerte con el titular de la tarjeta. La idea clave de la autenticación basada en el comportamiento es utilizar patrones de comportamiento para disminuir la incertidumbre en cuanto a si la persona que intenta realizar la autenticación es el titular de la tarjeta legítimo y, por lo tanto, de forma simultánea, (a) reducir la cantidad de transacciones legítimas afectadas por la autenticación secundaria y, a la vez, (b) lograr que más fraudes pasen a la autenticación secundaria y (c) denegar de forma rotunda más fraudes.

Modelos como autenticadores basados en el comportamiento

Los modelos regionales de CA Risk Analytics se desarrollan con los datos de emisores regionales que permiten la utilización de sus datos en el CA eCommerce Consortium y que aportan "datos reales"[2]. Estos datos incluyen transacciones 3-D Secure de tarjetas de crédito y débito.

Los modelos regionales abarcan diversos elementos. Primero, los modelos utilizan información de la transacción actual. Esto incluye la fecha y la hora, el monto, la ubicación de la persona que intenta autenticarse para una transacción (en el caso del comercio electrónico, el equipo o el dispositivo móvil del titular de la tarjeta), la información del comercio (nombre, identificador y dirección URL), la información sobre la dirección IP del dispositivo, las características de la conexión y la información adicional de proveedores de datos independientes. Esta información es esencial para que el modelo comprenda la transacción actual. No obstante, no es suficiente para comprender los comportamientos involucrados.

Segundo, los modelos utilizan información de comportamientos previos de las entidades centrales del intento de autenticación actual, como la tarjeta, el dispositivo o el comercio. De la información de los comportamientos previos, se extraen los factores importantes que se deben analizar en los patrones de comportamiento. Esto incluye la siguiente información: los comercios que se han visitado; los montos, las ubicaciones y los dispositivos usados en cada una de estas visitas; y los dispositivos únicos que se han utilizado con esta tarjeta. Asimismo, se buscan patrones similares en otras entidades centrales. Estos "destilados centrales", como se denomina a los historiales, se actualizan con cada intento observado de autenticación para una transacción.

Tercero, los modelos utilizan variables complejas, incluidos minimodelos, que aíslan los patrones de comportamiento de los destilados centrales involucrados en la transacción y determinan si la transacción actual se adecúa a algunos de los patrones y cómo lo hace. Estas variables pueden ser tan simples como identificar si se trata de un dispositivo nuevo para usar con una tarjeta determinada o la velocidad de gasto de una tarjeta o un dispositivo. Sin embargo, también pueden ser complejas, como comparar la tendencia de un titular de tarjeta determinado de realizar compras reiteradas y la cantidad de veces que ha visitado este comercio con los mismos patrones de otras personas.

Cuarto, los modelos utilizan tablas basadas en datos históricos. Estas tablas proporcionan información sobre las tendencias anteriores de transacciones legítimas y fraudulentas en los datos históricos, incluida la tendencia y las métricas Naïve-Bayesian.

Finalmente, todos estos elementos diferentes se presentan a un modelo numérico no lineal que sopesa las diversas predicciones sobre anormalidades de comportamiento y el riesgo de que se trate de un intento ilegítimo. Estos modelos capturan los comportamientos no lineales: relaciones importantes entre variables y la probabilidad de fraude que no son una simple relación lineal. Comparan indicadores de riesgo con factores mitigantes (este es un comercio con un nivel alto de fraude y el monto tiene un nivel alto de fraude, pero esta persona ya ha realizado este tipo de transacción antes desde este dispositivo) y analizan diferentes relaciones.

La manera en que estos distintos factores se sopesan se determina con un algoritmo de capacitación en un gran conjunto de datos de transacciones históricas y "datos reales", es decir, estos tipos de modelos están inherentemente "impulsados por los datos". Esto permite que los modelos "descubran" relaciones relevantes que no son fáciles de capturar en reglas y que presenten la mejor estimación sobre la probabilidad de que esta sea una transacción ilegítima.

El resultado de estos modelos es un número que proporciona una estimación de la probabilidad de que este intento de autenticación sea *ilegítimo*. Esto admite la jerarquización de las transacciones de autenticación, lo que permite que se adopten diferentes medidas y la priorización de esas medidas. Específicamente, esto permite la "autenticación silenciosa" de las transacciones, sin afectar al titular de tarjeta, según los patrones de comportamiento que figuran en los datos y que muestran una baja probabilidad de ilegitimidad.

Modelado numérico no lineal que usa redes neurales unilaterales

Entre la gran variedad de estrategias de modelado numérico, las FFNN (redes neuronales unilaterales) proporcionan la combinación ideal de desempeño, flexibilidad y viabilidad.

Las FFNN son extremadamente flexibles, ya que no requieren suposiciones estructurales o distributivas sobre el espacio de la característica de entrada. Demuestran un desempeño avanzado, incluso en los datos extremadamente no lineales, ya que son aproximadores de funciones universales. Además, sin importar el tamaño o la complejidad de los datos, aprenden en tiempo real y generan una calificación en tiempo constante, lo que hace que sean muy prácticas aun para conjuntos de datos sumamente grandes.

Estructura de la red neural

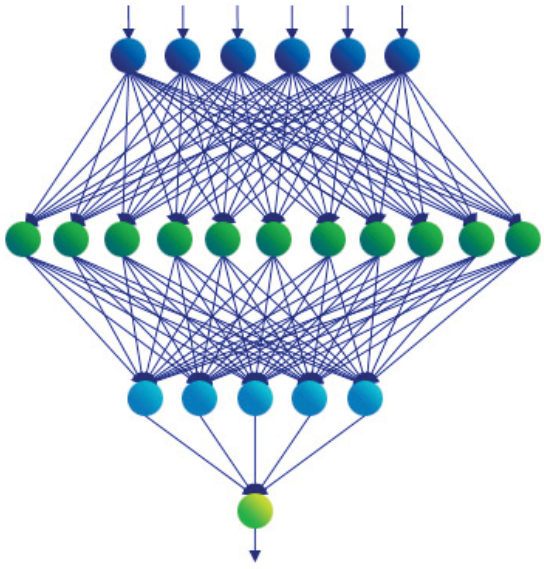
Una FFNN es esencialmente un gráfico acíclico de flujo de señal no lineal, cuya información de entrada es una representación numérica de la transacción según la capturan las técnicas mencionadas previamente, y su valor de salida, en el contexto actual, se interpreta como una medida ordinal de la probabilidad de que un intento de autenticación sea fraudulento (la calificación).

Para explicarlas de una manera más descriptiva, se puede pensar que las FFNN están compuestas de una secuencia de “capas”, cada una de las cuales está compuesta por un conjunto de “neuronas” (véase el gráfico 2). El intento de autenticación de entrada se presenta a la primera capa (de entrada), donde comienza su propagación por la red. Esta propagación continúa por capas internas (“capas ocultas”) y, finalmente, llega a la capa de salida. Cada capa realiza una transformación no lineal en su entrada y pasa el resultado a la capa subsiguiente. Cada capa puede tener una cantidad arbitraria de neuronas, pero, en el contexto actual, la capa final (de salida) tiene una única neurona (que genera la calificación).

El poder expresivo de las FFNN radica en estas transformaciones secuenciales no lineales, que, colectivamente, permiten que la FFNN modele cualquier función de su entrada.

Gráfico 2.

Ejemplo de una FFNN.



Sección 3

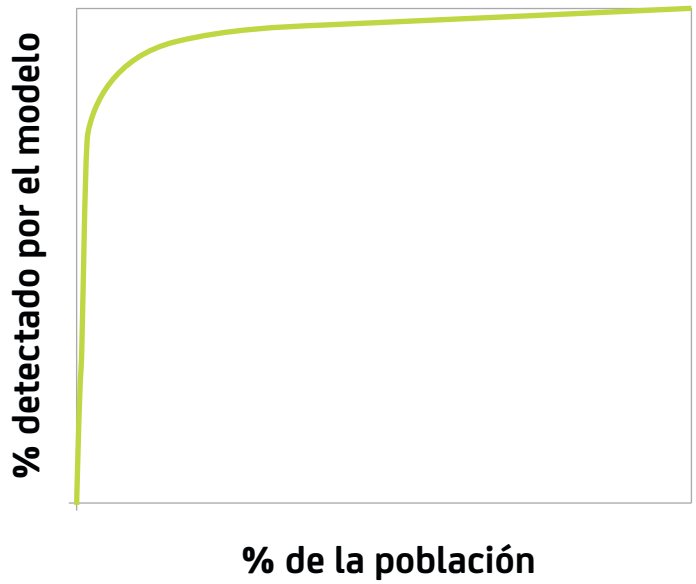
Ventajas de los modelos avanzados

Desempeño del modelo

Los modelos regionales de CA permiten la denegación o la autenticación incrementada en la mayoría de las transacciones fraudulentas y solo afectan una pequeña parte de las transacciones legítimas. El desempeño general se muestra en el gráfico 3. El modelo maximiza la detección de fraudes, a la vez que minimiza el impacto en los clientes. Tenga en cuenta que el gráfico no muestra toda la curva, sino que se centra en el área operativa de la curva.

Gráfico 3.

La detección de fraude del modelo como una función del porcentaje de todas las transacciones marcadas por el modelo. Tenga en cuenta que el gráfico solamente abarca una porción de la población y se centra en el área operativa de la curva.



Calificaciones de modelos y reglas

Las reglas son adecuadas para abordar indicadores precisos y bien definidos de fraude. Se implementan rápido y se comprenden fácilmente. No obstante, no están impulsadas por los datos y están, por lo tanto, limitadas por el conocimiento que tiene el creador de la regla en cuanto a los posibles indicadores de fraude. Las reglas no pueden capturar comportamientos complejos con facilidad ni permiten la rápida combinación de múltiples riesgos en una única decisión. Finalmente, no pueden jerarquizar las transacciones para permitir el ajuste de la denegación, la autenticación secundaria y los volúmenes de casos.

Los modelos capturan patrones complejos mediante el uso de variables sofisticadas. Las variables se basan en la transacción actual y los destilados centrales (información clave de transacciones previas sobre identificadores centrales en las transacciones, que se han destilado). Mediante el uso de variables no lineales y lineales, junto con técnicas de capacitación establecidas, los modelos permiten la ponderación de diferentes factores mediante el uso de una estrategia impulsada por los datos y generan una jerarquización de las transacciones según la probabilidad de fraude. Sin embargo, los modelos no adoptan medidas por sí mismos; las reglas son un complemento esencial de los modelos.

Reglas y modelos juntos

Debido a las diferentes fortalezas de los modelos y las reglas, la mejor estrategia consiste en usarlos juntos. Primero, utilice un modelo fuerte para separar las transacciones fraudulentas de las que no lo son y jerarquizarlas con una calificación. Segundo, escriba reglas que utilicen esta calificación de diversas maneras: (i) las calificaciones altas indican una probabilidad alta de fraude y se las debe usar para la toma de medidas (se debe ajustar el límite de calificación para lograr los volúmenes y la intensidad de fraude que la institución desea), y (ii) las calificaciones más bajas se pueden usar junto con reglas contra fraude relámpago u otras reglas, lo que posibilita el filtrado de las transacciones que tienen una probabilidad alta de ser legítimas y permite que las reglas funcionen en un conjunto de datos más rico. Finalmente, habrá reglas de políticas, que son independientes de la probabilidad de fraude, que la institución implementará (que tal vez requieran una autenticación secundaria para dispositivos nuevos sin importar la probabilidad de fraude).

Sección 4

Conclusión

El uso de la autenticación basada en el comportamiento para determinar qué transacciones se deben ver afectadas por la autenticación o la denegación es clave para reducir el impacto en el cliente (es decir, la fricción), a la vez que se garantiza mejor la legitimidad de la transacción. Las reglas son un componente importante para brindar autenticación basada en el riesgo y el comportamiento. Sin embargo, tienen varias limitaciones. Cuando se agregan modelos sofisticados basados en el comportamiento que guían la aplicación de reglas basadas en el riesgo, el impacto en los intentos ilegítimos se puede incrementar considerablemente, a la vez que se proporciona una mejor experiencia a los titulares de tarjetas y se reducen las pérdidas para el emisor.

Sección 5

Información sobre los autores

Paul Dulany ha estado en el ámbito del análisis avanzado y la ciencia de los datos durante 14 años. Se unió a CA Technologies en 2013 y lideró el desarrollo de la infraestructura de modelado analítico y el primer modelo producido por el equipo de ciencia de los datos de CA. Antes de unirse a CA Technologies, trabajó en SAS Institute por más de 8 años, donde formó parte del equipo que desarrolló los primeros modelos de la solución SAS Enterprise Fraud Management; además, lideró el desarrollo de los primeros modelos de tarjetas de débito y creó muchas técnicas nuevas. Antes de SAS, Paul trabajó en HNC y Fair Isaac durante más de 5 años como científico y, posteriormente, como administrador del equipo de modelado predictivo de fraude, donde desarrolló varios modelos de tarjetas de pago Falcon y trabajó en otras áreas. Paul tiene patentes de esta época en HNC y SAS. Tiene un doctorado en Física Teórica.

Hongrui Gong tiene una vasta experiencia en el ámbito del análisis avanzado y la ciencia de los datos. Se unió a CA Technologies en abril de 2013 y cumplió una función importante en las iniciativas de creación de una infraestructura de modelado y desarrollo de modelos para los productos 3-D Secure. Antes de unirse a CA, trabajó durante más de 15 años con importantes empresas de análisis (SAS, FICO y HNC), donde desarrolló modelos para productos como la detección de fraudes de tarjetas de pago, la detección de fraudes de seguros, la identificación de personas que no realizan las declaraciones de impuestos correspondientes para el Gobierno federal y estatal, productos contra el lavado de dinero, el pronóstico de pérdida de préstamos, la administración del riesgo de margen de préstamo de corretaje y la

calificación de riesgo crediticio para empresas públicas y privadas. Hongrui tiene un doctorado en Dinámica de Fluidos Computacional y pasó 4 años en el Laboratorio Nacional de Los Álamos, donde se centró en la investigación del modelado teórico y las simulaciones informáticas del flujo turbulento. Tiene varias patentes de su trabajo previo.

Kannan Shah ha estado en el ámbito del análisis avanzado y la ciencia de los datos durante 6 años. Se unió a CA Technologies en 2013 y contribuyó al desarrollo de la infraestructura de modelado analítico y el primer modelo producido por el equipo de ciencia de los datos de CA. Antes de unirse a CA Technologies, fue científico sénior de planta en SAS Institute, donde desarrolló modelos y técnicas estadísticas y proporcionó soporte al cliente para la solución SAS Enterprise Fraud Management. Ha contribuido al desarrollo de modelos de detección de fraude para tarjetas de pago y transferencias ACH (Cámara de Compensación Automatizada) y electrónicas, que se implementaron en Estados Unidos, el Reino Unido, México y la región Asia-Pacífico. Kannan tiene varias patentes de su trabajo en SAS. Kannan tiene una maestría en Ingeniería Eléctrica de Drexel University de Filadelfia. Entre las áreas en las que se centró durante sus estudios académicos, se incluyeron la detección y la estimación, el procesamiento de señales estocásticas, la inteligencia de las máquinas, el reconocimiento de patrones estadísticos, las redes neurológicas, la teoría de la información, el análisis espectral de orden superior, y el diseño y la complejidad de algoritmos.

Comuníquese con CA Technologies en ca.com/ar.

CA Technologies (NASDAQ: CA) crea un software que impulsa la transformación en las empresas y les permite aprovechar las oportunidades de la economía de la aplicación. El software es el centro de cada empresa, en cada industria. Desde la planificación hasta el desarrollo, la administración y la seguridad, CA trabaja con empresas en todo el mundo para cambiar la forma de vivir, realizar transacciones y comunicarse, mediante entornos móviles, de nube pública y privada, y centrales y distribuidos. Obtenga más información en **ca.com/ar**.

1 En las regiones donde se ha realizado una educación importante de los titulares de tarjetas para que busquen indicadores de 3-D Secure, puede ser tranquilizador para el titular de tarjeta ver una ventana emergente con un mensaje en el que se indique que la transacción está protegida por 3-D Secure.

2 El término “datos reales” se refiere a información sobre las transacciones y las tarjetas que se utiliza para identificar las transacciones que el proceso de autenticación debe detener.