DETECCION DE FRAUDE EN CUENTA BANCARIA

DESCRIPCION DEL PROYECTO:
Detección de Fraude en Cuenta Bancaria con Tarjeta de Crédito

Uno de los fraudes más extendidos en el sector bancario es de la tarjeta de crédito. Teniendo un histórico de datos de transacciones bancarias del usuario se podría construir un modelo de machine learning de clasificación (aprendizaje supervisado) que categorice en tiempo real cada transacción financiera del usuario como 'correcta' o 'anómala' (o que al inicio del día categorice las transacciones del día anterior). Y a continuación emita un mensaje de alerta o pide un segundo factor de autenticación al usuario para autorizar la transacción (por ejemplo, introduciendo un código numérico enviado por SMS al usuario o autorizando la transacción desde la página web o la app móvil de su banco o desde aplicaciones móviles genéricas de autenticación como 'Google Authenticator' o 'Microsoft Authenticator'.
O si en un plazo de tiempo determinado (24 o 48 horas) se detectan 3 o más transacciones anómalas sin segunda autenticación por parte del usuario la entidad financiera podría proceder directamente al bloqueo del medio de pago del usuario.

Esta aplicación de machine learning no sólo podría detectar fraudes para el usuario a través de su cuenta bancaria, sino que también podría detectar fraudes o delitos financieros que el usuario este cometiendo. Por ejemplo, si un cliente durante un corto periodo de tiempo realiza ingresos de dinero efectivo en pequeñas cantidades (y no asociadas a ninguna factura o catalogadas como ingresos del trabajo) que sumadas superan el umbral permitido por el estado para realizar transacciones con dinero en efectivo. Esta técnica de lavado de dinero (Money Laundering) se conoce como smurfing.
O por ejemplo si hace o recibe transacciones a países (ya que las transacciones estarán geolocalizadas) u organizaciones que estén dentro de una lista negra (por ser paraísos fiscales o bien países u organizaciones en guerra o con organizaciones terroristas asentadas) del ministerio del interior o de cualquier otro organismo europeo o internacional. En dicho caso se podría enviar una alerta al banco o directamente al ministerio de economía o al de interior.

También se podrían marcar como sospechosas transacciones que tengan un importe elevado con relación al importe medio del histórico de transacciones en cada categoría o en relación con cualquier otra transacción que haya hecho el usuario en su histórico de transacciones. Igualmente, la sucesión de pequeños y frecuentes gastos en una determinada categoría también podría ser obligatorio autenticarla por un segundo canal adicional a partir de un determinado número de transacciones.

Transacciones sospechosas que requerirían doble autenticación serían las realizadas en empresas de envío de remesas de dinero (MoneyGram, Western Union, Ria) o bien compras de BitCoin o aportaciones a un bitcoin wallet.

También sería obligatorio pedir un segundo factor de autenticación para aquellas transacciones de pagos realizadas en casa de apuestas online o físicas.

Igualmente se pueden calificar como sospechosas aquellas transacciones que tengan información inconsistente o incoherente. Por ejemplo, que esté a nombre de una persona distinta y sin relación al titular de la tarjeta o asignada a una dirección distinta a la del titular de la tarjeta o por trabajos realizados en un vehículo distinto al del usuario. O compras realizadas a multinacionales tecnológicas cargadas en países distintos a los de su sede económica (Amazon fuera del Luxemburgo (y que la sociedad de cargo no se llame 'Amazon Media EU S.à.r.l.'), LinkedIn y Facebook fuera de Irlanda, Netflix fuera de Holanda (y que la sociedad de cargo no se llame 'Netflix International B.V.'), etc.),

Se pueden catalogar como sospechosas retiradas de grandes cantidades de efectivo de un cajero o bien frecuentes retiradas de cantidades pequeñas de efectivo. Sobre todo, si es un usuario que, de acuerdo con su histórico de transacciones, suele pagar casi siempre por medios electrónicos como tarjetas, aplicaciones como bizum, etc.

También son transacciones sospechosas aquellas que un usuario haga en una categoría de gasto en la que no tenga transacciones asignadas en su histórico, sobre todo si el importe de la transacción es de cierta cuantía. Por ejemplo, nuevas compras de artículos de joyería, piedras preciosas u obras de arte.
Igualmente se debería requerir una segunda autenticación o emitir una alerta en aquellas compras o pagos de servicios a proveedores nunca antes utilizados como concesionarios físicos u online de coches/motos, agencias de viaje, compra de artículos nuevos o de segunda mano a través de aplicaciones móviles como eBay, Wallapop, etc.

La geolocalización también puede utilizarse como otro parámetro para catalogar una transacción como sospechosa. Sobre todo, si su geolocalización no coincide con su patrón típico de comportamiento. Por ejemplo, un usuario que trabaja en Madrid en el distrito de Chamartín y vive en Tres Cantos y un día de diario por la mañana realiza una transacción en distrito de Villa de Vallecas.
O bien si se empiezan a registrar varias transacciones de un usuario en Alemania sin figurar en su histórico la compra de un billete de avión a ese país.
O incluso si efectivamente el modelo de machine learning detecta que las transacciones realizadas fuera de sus geolocalizaciones habituales son 'normales' también puede catalogar como sospechosas aquellas transacciones aquellas transacciones cuya cuantía sea superior a un umbral económico realizadas fuera de las geolocalizaciones habituales conocidas del usuario (domicilio habitual, segunda residencia, lugar de trabajo, etc.).

BENEFICIOS ESPERADOS
Aumento de la seguridad para el usuario, para el banco y para la administración pública al disponer de otro medio adicional de detección de transacciones fraudulentas.

IMPACTO ESPERADO
Aumento de la lealtad del usuario del banco o medio de pago al contar con una capa más de seguridad.

ESTIMACION CREACION NETA DE EMPLEO
Depende del alcance final del proyecto y del plazo previsto para el proyecto. A priori este proyecto podría ser realizado por un Ingeniero de Datos, un Científico de Datos y un Desarrollador de Software de Backend.

SECTOR
FinTech: Financiero y de Tecnologías de la Información. Con especial foco en las disciplinas de Big Data (Ingeniería de Datos), Aprendizaje Automático (Machine Learning y Deep Learning) y Desarrollo Software de Backend.

OBJETIVO DE TRANSFORMACION DIGITAL
Añadir una capa de seguridad adicional a los medios de pago utilizados sobre la cuenta corriente de un usuario.

PRESUPUESTO ESTIMADO
Depende del alcance final del proyecto. Para el alcance más básico: 2 meses de trabajo de un Ingeniero de Datos, 2 meses de trabajo de un Científico de Datos, 1 mes de trabajo de un desarrollador de software Backend.
Adicionalmente, el proyecto necesitaría de una fase indefinida de mantenimiento debido a los continuos cambios y evoluciones en proveedores, medios de pagos, hábitos de vida del usuario y aparición de nuevas formas de fraude.

PORCENTAJE DE FINANCIACION PUBLICA SOLICITADO
A concretar tras la aceptación de una oferta concreta por parte de un cliente.