SECURITY ADVISOR
SU DEFENSA DIGITAL

Fraude de identidad en banca digital

El ataque que parece legítimo

Soraya Suárez
Consultora, Security Advisor
Con la colaboración de OneSpan

EN ESTE ANÁLISIS

Resumen ejecutivo

Cuatro ideas para llevarse, antes de entrar en el detalle:

— El fraude ya no rompe la puerta. Entra con credenciales válidas y se comporta como un cliente legítimo — por eso la autenticación tradicional deja de alcanzar por sí sola.

— Hay al menos cinco formas de suplantación activas hoy en banca digital, desde la apropiación de cuentas hasta los deepfakes en canales asistidos.

— Las identidades no humanas — APIs, bots y agentes de IA — ya son el próximo vector de riesgo y exigen credenciales propias, delegación explícita y verificación criptográfica del mandato.

— La respuesta no es más fricción: es fricción proporcional al riesgo, un enfoque que además la regulación (PSD2/SCA en Europa, y exigencias equivalentes en América Latina) empieza a exigir.

El fraude que ya no se nota

Durante años la seguridad bancaria se midió en barreras: contraseñas más largas, más preguntas, más pasos. Pero el fraude aprendió a moverse más rápido que esas barreras. El atacante de hoy no necesita romper nada — le alcanza con parecer legítimo. Compra credenciales filtradas en la dark web, copia el comportamiento esperado y se mueve dentro de lo que el propio banco considera "normal".

El resultado es un fraude que no hace ruido. La transacción se aprueba, la sesión se cierra, y el cliente recién se entera cuando revisa su saldo. Para la entidad, la pregunta que importa deja de ser ¿quién está accediendo? Pasa a ser: ¿este comportamiento es realmente el del cliente que dice ser?

Las caras del ataque en banca

En el contexto financiero, la suplantación adopta formas concretas:

— Apropiación de cuentas (ATO): uso de credenciales robadas para vaciar fondos, modificar beneficiarios o solicitar productos de crédito a nombre de la víctima.

— Fraude de apertura de cuenta: identidades sintéticas —mezcla de datos reales y falsos— que superan un onboarding débil para defraudar después.

— Ingeniería social y estafas autorizadas (APP fraud): el cliente, manipulado, autoriza la transferencia él mismo. Técnicamente todo es legítimo; el engaño está en la intención. Es el escenario donde la autenticación por sí sola no alcanza.

— Ataques al canal: phishing, SIM swap, malware móvil y técnicas de hombre en el navegador (MitB) que interceptan o alteran la operación en tiempo real.

— Deepfakes en canales asistidos: voz o video sintéticos para convencer al call center o al propio cliente, y para intentar vencer la prueba de vida en el onboarding remoto.

Cuando el que opera no es una persona

Hasta acá, todo el razonamiento asume que del otro lado hay un humano — legítimo o impostor. Esa premisa se está cayendo, y es probablemente el cambio de fondo más relevante que enfrenta la banca en los próximos años.

Las identidades no humanas (NHI) —cuentas de servicio, APIs, bots y, cada vez más, agentes de IA— ya son la mayor parte de los accesos en cualquier ecosistema digital. En banca aparecen en dos planos bien distintos, y conviene no mezclarlos:

— Hacia adentro: las integraciones que sostienen el open banking y los servicios embebidos. APIs y cuentas de servicio con privilegios amplios, credenciales de larga vida y poca trazabilidad son un vector de fraude a escala: un solo secreto filtrado no compromete una cuenta, compromete un canal.

— Hacia afuera: los agentes de IA que empiezan a operar en nombre del cliente —comparar productos, ejecutar pagos, gestionar trámites—. El banco deja de ver a la persona y pasa a ver a su delegado automático.

"El atajo peligroso es el evidente: que el cliente entregue su usuario y contraseña al agente para que "haga las cosas por él". Eso destruye de un golpe la trazabilidad, el no repudio y cualquier análisis de comportamiento."

Los CAPTCHA, además, dejan de servir como filtro: no distinguen un agente legítimo de un bot fraudulento, solo agregan fricción al humano.

La respuesta que se está consolidando en la industria va por otro camino: credenciales digitales verificables y delegación explícita. Que el agente tenga identidad propia. Que el cliente defina los límites de lo que puede hacer — montos, destinatarios, vigencia. Y que el banco pueda verificar criptográficamente esa delegación en cada operación. La pregunta se vuelve triple: ¿es un humano, un agente autorizado o un bot? Y si es un agente, ¿está actuando dentro del mandato que le dio su titular?

Para el banco, esto significa gobernar sus identidades no humanas con la misma seriedad que las de sus clientes: credenciales de vida corta, mínimo privilegio, inventario, auditoría. Y diseñar cada flujo de autorización asumiendo que quien opera puede no ser una persona.

Del muro al semáforo: seguridad basada en riesgo

La respuesta no es subir la fricción para todos por igual. Es aplicar la fricción correcta en el momento correcto. Un enfoque de autenticación adaptativa evalúa cada interacción según su riesgo: si todo encaja —dispositivo conocido, ubicación habitual, operación de rutina— el cliente avanza sin obstáculos; si algo se desvía, el sistema pide verificación adicional o bloquea.

Esa lógica de semáforo depende de capas que trabajan juntas: identidad verificada en el origen, autenticación resistente a la suplantación en cada acceso, integridad del canal y

del dispositivo, y monitoreo continuo del comportamiento durante toda la sesión. Basta que falte una capa para que el atacante encuentre el hueco.

Marco regulatorio: la fricción inteligente es ley

Normativas como PSD2 en Europa —y su discusión hacia PSD3— convirtieron en obligación lo que antes era buena práctica. La Autenticación Reforzada de Cliente (SCA) exige combinar al menos dos factores independientes (algo que el cliente sabe, tiene o es) para operaciones sensibles, pero permite exenciones basadas en análisis de riesgo.

En América Latina el enfoque no llega por una norma única, sino por la vía de los reguladores y los esquemas de pagos locales: requisitos de autenticación reforzada para operaciones sensibles, exigencias de gestión de riesgo tecnológico y presión creciente de los sistemas de pagos instantáneos, donde la irreversibilidad de la transacción no deja margen para detectar el fraude después. El fondo es el mismo en todas partes: más seguridad donde hay riesgo, menos fricción donde no lo hay.

Dónde encaja OneSpan

OneSpan es un proveedor especializado en autenticación e identidad para el sector financiero. Su valor no está en un producto suelto, sino en orquestar verificación, autenticación y señales de riesgo bajo una sola decisión. Hoy esa oferta vive en la plataforma DigipassONE, pensada para modernizar sin reemplazar de golpe lo que ya funciona: tokens de hardware, autenticadores móviles y passkeys, conviviendo.

Componente	Qué resuelve
DigipassONE Authenticate	Autenticación basada en riesgo con un portafolio amplio de factores —passkeys y FIDO2, autenticadores de hardware y software, OTP— para login y aprobación de transacciones resistentes a phishing.
Firma de transacciones (Cronto)	El cliente confirma en un display de confianza exactamente lo que está autorizando, frustrando la manipulación de datos aun cuando el canal esté comprometido. Contramedida directa al MitB.

Digipass FX (FIDO2)	Llaves de autenticación sin contraseña que vinculan criptográficamente cada acceso al dominio legítimo, neutralizando phishing, SIM swap y ataques de intermediario.
DigipassONE Verify	Emisión y verificación de credenciales digitales sobre ecosistemas de wallets. Habilita el onboarding verificado y el modelo de delegación e identidad verificable para agentes de IA.
DigipassONE Insights	Analítica y visibilidad transversal —incluida la telemetría de amenazas móviles— para medir la efectividad de las políticas y ajustar el umbral de riesgo con datos.
Protección de la app móvil	Blindaje en tiempo de ejecución y detección de dispositivo comprometido, malware y overlays, para que la app siga siendo una fuente de señal confiable.
Verificación de identidad	Validación documental y biometría facial con detección de vivacidad en el onboarding, para cerrar la puerta al fraude de apertura y a las identidades sintéticas.

La ventaja: confianza sin fricción innecesaria

Juntas, estas capacidades permiten aplicar seguridad proporcional al riesgo. El cliente legítimo no siente nada — la experiencia es fluida. El impostor, en cambio, choca con verificaciones que no puede superar: le falta el factor físico, la biometría, el patrón de comportamiento genuino. La seguridad deja de ser un costo de experiencia. Se vuelve un diferenciador de confianza.

Conclusión

El fraude de identidad en la banca digital ya no se reconoce por lo que rompe, sino por lo bien que imita. Defenderse exige dejar de preguntar únicamente "¿quién entra?" y empezar a evaluar "¿cómo se comporta quien entra?" a lo largo de toda la relación. Y, cada vez más, sumar una tercera pregunta: "¿es una persona la que está operando, o alguien —o algo— actuando en su nombre?".

"Verificación sólida en el origen, autenticación resistente al engaño, integridad del canal y análisis continuo del comportamiento son las claves para preparar el terreno frente a las identidades no humanas que ya están tocando la puerta."

SECURITY ADVISOR

Diseñemos juntos tu estrategia de verificación de identidad

Te ayudamos a diseñar tu estrategia de verificación, autenticación adaptativa y detección de fraude en tiempo real. Escribinos para coordinar una evaluación de riesgo de identidad y una demostración.