La Paradoja de la Identidad-Crédito

WHITE PAPER

Inteligencia de Verificación de Identidad para Instituciones Financieras

La falla comienza con la identidad, pero la pérdida suele registrarse en otro lugar.

Las instituciones financieras rara vez experimentan el fraude de identidad como un problema de identidad claramente etiquetado. Con mayor frecuencia, este aparece más tarde, después del onboarding, en categorías que parecen operativas o financieras en lugar de estructurales: incumplimiento del primer pago, pérdida crediticia, contracargos, abuso de promociones, actividad de mulas, robo de cuentas o cuentas abandonadas creadas para su posterior explotación.

MÉTRICAS CLAVE DE LOS DATOS DE LA INDUSTRIA

Esa es la paradoja identidad-crédito. El fallo comienza con la identidad, pero la pérdida a menudo se contabiliza en otro lugar.

Esto es de vital importancia porque la clasificación impulsa la inversión. Si una pérdida se trata como un problema de crédito, las instituciones recurrirán a la suscripción de riesgos, el scoring, la cobranza o los controles de cartera. Si se trata como un problema de pagos, se centrarán en el monitoreo de transacciones y los controles de contracargos. Esas capas abordan los síntomas posteriores (downstream). El fallo inicial (upstream) persiste: se permitió el ingreso de una identidad que nunca debió haber entrado al sistema.

↑ **$27.3B**
en pérdidas por fraude de identidad en EE. UU. en 2025[1]

↑ **+31%**
de todos los informes de FinCEN relacionados con la identidad[1]

↑ **18M**
de víctimas de fraude de identidad en EE. UU. en 2025[1]

Los procesos tradicionales de "Conoce a tu Cliente" (KYC) siguen siendo esenciales. Las instituciones deben verificar que un usuario sea real, que los documentos sean válidos, que los datos sean consistentes y que la persona esté presente durante el onboarding. Pero el modelo de amenaza ha cambiado. El KYC tradicional se construyó en torno a una sesión aislada, donde un usuario presenta información y la institución verifica si esa información parece internamente consistente. El fraude moderno opera a través de sesiones, instituciones y mercados. Es automatizado, adaptativo, sintético y en red.

El problema a primera vista

1.6M
de informes de la BSA vinculados a la identidad (2021)[1]

42%
de todos los informes de FinCEN relacionados con la identidad[1]

$212B
en actividades sospechosas vinculadas a la identidad[1]

El resultado es una brecha cada vez mayor entre la forma en que opera el fraude y la manera en que muchas instituciones aún se defienden de él.

El análisis de FinCEN sobre los informes de la Ley de Secreto Bancario (BSA) muestra cuán profundamente está arraigada la identidad en los delitos financieros. La agencia descubrió que aproximadamente 1.6 millones de informes BSA presentados en 2021, o el 42 por ciento de todos los informes presentados ese año, se relacionan con la identidad, lo que representa 212 mil millones de dólares en actividad sospechosa. Las tipologías reportadas con mayor frecuencia incluyeron fraude, registros falsos, robo de identidad, lavado de dinero por parte de terceros y elusión de los estándares de verificación.[1]

Eso convierte a la identidad en una capa de delitos financieros por derecho propio.

Al mismo tiempo, el fraude de identidad se está volviendo más difícil de separar del comportamiento crediticio. La Oficina de Rendición de Cuentas del Gobierno de los EE. UU. (GAO) ha señalado que es probable que se subestime el costo real del fraude de identidad sintética, ya que muchos casos pueden pasar desapercibidos y reportarse como pérdida crediticia en lugar de fraude.[2] La Reserva Federal ha planteado un punto similar en su trabajo sobre el fraude de identidad sintética, advirtiendo que una clasificación errónea puede dificultar la cuantificación del alcance del problema, distorsionar los modelos de fraude y permitir que los actores malintencionados reutilicen identidades en todo el sistema.[3]

Para los bancos, las fintechs, los marketplaces, las plataformas de economía colaborativa (gig platforms) y otros negocios digitales a escala, la implicación es directa. La próxima generación de defensa de la identidad debe ir más allá de añadir fricción al mismo proceso aislado. Necesita hacer que la verificación de identidad sea más inteligente, más coordinada y más capaz de reconocer patrones repetitivos antes de que se conviertan en pérdidas posteriores (downstream).

SECCIÓN 01

El fraude se ha desplazado hacia las etapas iniciales (upstream)

Los delincuentes están creando cuentas nuevas que no deberían existir, y la superficie de ataque se está desplazando a una etapa más temprana del ciclo de vida del cliente de lo que los controles tradicionales fueron diseñados para detectar.

01

El fraude se ha desplazado hacia las etapas iniciales (upstream)

El fraude de cuentas nuevas se ha convertido en una de las expresiones más claras de este cambio. La Reserva Federal ha advertido que las aperturas de cuentas digitales, aunque son más convenientes para los clientes legítimos, crean nuevas oportunidades para los delincuentes. Señala que el fraude de cuentas nuevas se ha vuelto más fácil de cometer y más difícil de detectar debido a una tecnología más sofisticada, la IA generativa y la amplia disponibilidad de información de identificación personal en la dark web.[4]

> **Javelin Strategy & Research - Estudio de Identidad 2026**
> Las víctimas de fraude de cuentas nuevas aumentaron un 31% (de 4.2 millones a 5.4 millones), y las pérdidas se incrementaron un 13%, alcanzando los $7 mil millones en 2025.

El Estudio de Fraude de Identidad de 2026 de Javelin Strategy & Research proporciona una instantánea útil de la tendencia. Las pérdidas por fraude de identidad tradicional en EE. UU. se mantuvieron prácticamente estables en 27,300 millones de dólares en 2025, afectando a 18 millones de víctimas. Sin embargo, el fraude de cuentas nuevas fue la categoría con el crecimiento de víctimas más pronunciado, aumentando un 31 por ciento, de 4.2 millones de víctimas en 2024 a 5.4 millones en 2025. Las pérdidas por fraude de cuentas nuevas aumentaron un 13 por ciento interanual, alcanzando los 7,000 millones de dólares.[5]

Ese contraste es importante. Las pérdidas globales por fraude de identidad pueden parecer estables a un nivel general, pero la superficie de ataque está cambiando. Los delincuentes se están desplazando hacia etapas más tempranas del ciclo de vida del cliente. Más allá de secuestrar cuentas existentes, están creando cuentas nuevas que no deberían existir.

$1.2B

Transacciones fraudulentas de Pix en Brasil en 2024
Incluso cuando la tasa absoluta de fraude se mantuvo en el 0.03% del valor de las transacciones.[7]

El patrón aparece a nivel global. El Grupo de Acción Financiera de Latinoamérica (GAFILAT) describió recientemente el fraude como una de las amenazas más extendidas que enfrenta la región, con riesgos cada vez mayores en torno a los servicios financieros digitales y los pagos transfronterizos.[6] En Brasil, donde el sistema de pagos instantáneos Pix ha remodelado la banca de consumo, investigaciones de la industria basadas en datos del banco central revelaron que aproximadamente 1,200 millones de dólares estuvieron involucrados en transacciones fraudulentas de Pix en 2024, a pesar de que la tasa de fraude absoluta se mantuvo en aproximadamente el 0.03 por ciento del valor de las transacciones.[7] Ese contraste ilustra un principio más amplio: los rieles (rails) digitales de alto volumen convierten pequeñas tasas de fraude en grandes focos de pérdidas, y cuando se accede a esos rieles a través del onboarding digital, la integridad de la verificación de identidad se convierte en la defensa inicial (upstream) más importante de dichos canales.

Una cuenta nueva puede monetizarse de varias maneras. Un defraudador puede obtener crédito sin intención de reembolso. Puede mover fondos ilícitos. Puede depositar cheques falsificados o adulterados. Puede explotar bonos o incentivos promocionales. Puede realizar compras y disputarlas más tarde. Puede crear cuentas que permanecen inactivas hasta que resultan útiles para estafas, actividades de mulas o esquemas de identidad sintética.

Desde la perspectiva de la institución, estos comportamientos pueden aparecer en diferentes departamentos y distintos sistemas. El equipo de crédito ve el incumplimiento (default). El equipo de pagos ve las disputas. El equipo de fraude ve el abuso de cuentas. El equipo de cumplimiento ve actividad sospechosa. Sin embargo, muchos de esos resultados comparten la misma dependencia inicial (upstream): si la identidad era legítima en el punto de entrada.

Es ahí donde el KYC 1:1 tradicional —el modelo en el que se verifica a un solicitante únicamente contra la evidencia de identidad que él mismo presenta— comienza a mostrar sus límites.

SECCIÓN 02

El KYC tradicional fue diseñado para una amenaza más limitada

El sistema KYC 1:1 responde si esta persona coincide con este documento. No puede preguntar si la misma señal de identidad ha aparecido anteriormente, en otras instituciones o con otros nombres.

02

El KYC tradicional fue diseñado para una amenaza más limitada

Un proceso típico de KYC 1:1 pregunta si el solicitante coincide con la evidencia de identidad que presenta. ¿Coincide la selfie con la foto de la identificación? ¿Es válido el documento? ¿Los atributos parecen consistentes? ¿Está la persona físicamente presente en la sesión?

Esas son preguntas necesarias. Detectan discrepancias obvias, documentos falsificados, intentos de suplantación, ataques de presentación de baja calidad y muchas formas de robo de identidad. La detección robusta de prueba de vida (liveness) y la detección de ataques de presentación se han vuelto aún más importantes a medida que los deepfakes, los ataques de inyección y los medios sintéticos han mejorado.

Pero el KYC 1:1 sigue limitado por la sesión. Si bien responde a si esta persona parece coincidir con este documento o solicitud de cuenta, una pregunta diferente y cada vez más importante queda sin respuesta: ¿ha aparecido antes esta misma señal de identidad bajo otros nombres, documentos, cuentas, instituciones o geografías?

Lo que el KYC 1:1 SÍ PUEDE detectar

- Falsificación de documentos
- Incompatibilidad/discrepancia facial
- Suplantación de prueba de vida
- Ataques de presentación
- Falsificaciones de baja calidad

Lo que el KYC 1:1 NO PUEDE detectar

- Reutilización de datos entre distintas instituciones
- Redes de cuentas mula
- Identidades sintéticas creadas en serie
- Patrones a nivel de bandas/organizaciones criminales
- Historial o registro compartido entre diferentes mercados

Este es un problema crítico porque el fraude moderno a menudo depende menos de una identidad falsa perfecta que de la repetibilidad. Una red de fraude puede probar variaciones en múltiples instituciones. Una persona real puede actuar como mula repetidamente. Una identidad sintética puede ensamblarse a partir de fragmentos de datos válidos. Una señal biométrica puede aparecer en diferentes contextos con diferente información personal. Una sola institución puede ver solo una solicitud aparentemente plausible, mientras que el patrón más amplio revela un abuso en serie.

FinCEN describió este problema hace años en su análisis del fraude de identidad sintética, señalando que los delincuentes pueden usar una sola identidad sintética para adquirir varias tarjetas de crédito de diferentes instituciones financieras.[8] Esa misma lógica se aplica de manera más amplia al fraude en red: cada institución ve solo la parte del patrón que toca su propio perímetro.

La IA generativa agrava el problema. FinCEN ha advertido que las herramientas de IA generativa (GenAI) han reducido los recursos necesarios para producir contenido sintético de alta calidad, y que los delincuentes utilizan esas herramientas para disminuir el costo, el tiempo y los recursos necesarios para explotar los procesos de verificación de identidad de las instituciones financieras.9 El informe IC3 de 2025 del FBI encontró de manera similar que las denuncias relacionadas con la IA produjeron más de 893 millones de dólares en pérdidas reportadas en 2025, señalando además que el contenido sintético es cada vez más fácil de crear y más difícil de detectar.[10]

$893M+

Pérdidas por reclamaciones relacionadas con la IA registradas en 2025[10]

Más allá de producir imágenes, videos, documentos y mensajes falsos más convincentes, la IA cambia la economía del ataque. Reduce el costo de las pruebas. Reduce el esfuerzo requerido para escalar. Mejora la calidad de la ingeniería social y del contenido sintético. Permite que las operaciones de fraude iteren más rápido de lo que los controles manuales o aislados pueden adaptarse.

Un proceso diseñado para verificar una sesión a la vez se enfrenta ahora a adversarios que operan a través de sesiones, instituciones y mercados.

SECCIÓN 03

El punto ciego fuera de la sesión

Un estafador que supera el proceso de registro (onboarding) de una institución puede volver a intentarlo en otro lugar. El patrón interinstitucional es la señal de riesgo, y los sistemas KYC aislados no pueden detectarlo.

03

El punto ciego del KYC

El punto ciego más importante en el KYC tradicional es el del alcance. Los controles a nivel de sesión, por muy rigurosos que sean, están limitados por la sesión.

Esa distinción es crucial. La detección avanzada de prueba de vida (liveness) puede determinar si una persona real y presente está participando en un flujo de onboarding. La detección de ataques de presentación puede ayudar a proteger contra máscaras, videos reproducidos, medios sintéticos y otros intentos de suplantar los sistemas biométricos. La verificación de documentos puede validar la evidencia de identidad. Las señales de dispositivo y de comportamiento pueden añadir contexto.

Todo eso es esencial. Nada de ello crea automáticamente memoria en todo el mercado.

Un defraudador que supera el onboarding de una institución puede intentarlo de nuevo en otro lugar. Una mula puede ser utilizada repetidamente. Un perfil sintético puede evolucionar con el tiempo. Un rostro puede aparecer con diferentes credenciales. Una red de fraude puede atacar muchas instituciones a la vez, aprendiendo de cada intento. El patrón interinstitucional es la señal de riesgo, y los sistemas de KYC aislados carecen de la visibilidad para detectarlo.

150+

intentos de apertura de cuenta a partir de una única firma biométrica

Se observó en más de 30 instituciones antes de que se activara la detección a nivel de red.[11]

Las propias observaciones de red de Unico ilustran cuán concentrada puede llegar a ser esta reutilización. La empresa ha documentado casos en los que una sola firma biométrica intentó abrir cuentas más de 150 veces en aproximadamente 30 instituciones diferentes antes de ser identificada a nivel de red.[11] En cada institución, la solicitud parecía lo suficientemente plausible como para ser investigada. A través de la red, el patrón era inequívoco.

Aquí es donde el bucle de clasificación errónea se vuelve peligroso. Cuando las pérdidas impulsadas por la identidad se contabilizan como pérdidas crediticias o pérdidas operativas, las instituciones pueden invertir insuficientemente en infraestructura de identidad. Cuando los modelos de fraude se entrenan con resultados mal clasificados, pueden aprender la lección equivocada. Cuando los defraudadores tienen éxito en un entorno, pueden reutilizar el mismo patrón en otros lugares.

Los materiales de la Reserva Federal sobre el fraude de identidad sintética advierten que la clasificación errónea puede subestimar el problema y permitir que los actores malintencionados reutilicen identidades.[3] La GAO de los EE. UU. ha señalado de manera similar que el fraude de identidad sintética puede ocultarse cuando los casos se tratan como pérdida crediticia en lugar de fraude.[2]

Existen implicaciones estratégicas para los tomadores de decisiones ejecutivas. Si la organización no puede identificar qué pérdidas comenzaron como fallos de identidad, no puede saber si su stack de identidad está funcionando. Una cartera puede parecer tener un problema de crédito cuando también tiene un problema de onboarding. Un equipo de fraude puede perseguir el abuso posterior cuando el punto de intervención más sólido era la creación de la cuenta.

Por eso la arquitectura importa.

La prueba de vida (liveness) es ahora fundamental

El auge de los medios generados por IA ha convertido a la detección robusta de prueba de vida (liveness) y de ataques de presentación en un requisito básico para la verificación de identidad moderna. Las instituciones financieras no pueden confiar en verificaciones de documentos estáticos o en un simple cotejo de selfies cuando los atacantes pueden producir imágenes sintéticas más convincentes, manipular transmisiones de video o intentar ataques de inyección digital.

> **NIST SP 800-63A-4 — Directrices sobre identidad digital (agosto de 2025)**
>
> "Los proveedores de servicios de credenciales deben implementar sistemas de detección de ataques de presentación para confirmar la presencia real de una persona y mitigar los intentos de suplantación de identidad."[12]

Las directrices actuales de identidad digital del NIST reflejan este cambio. En la recolección biométrica remota, el NIST señala que los proveedores de servicios de credenciales deben implementar la detección de ataques de presentación para confirmar la presencia genuina de un ser humano vivo y mitigar los intentos de suplantación (spoofing) e identidad falsa. Sus directrices de autenticación también establecen que los sistemas biométricos de reconocimiento facial deben implementar la detección de ataques de presentación.[12]

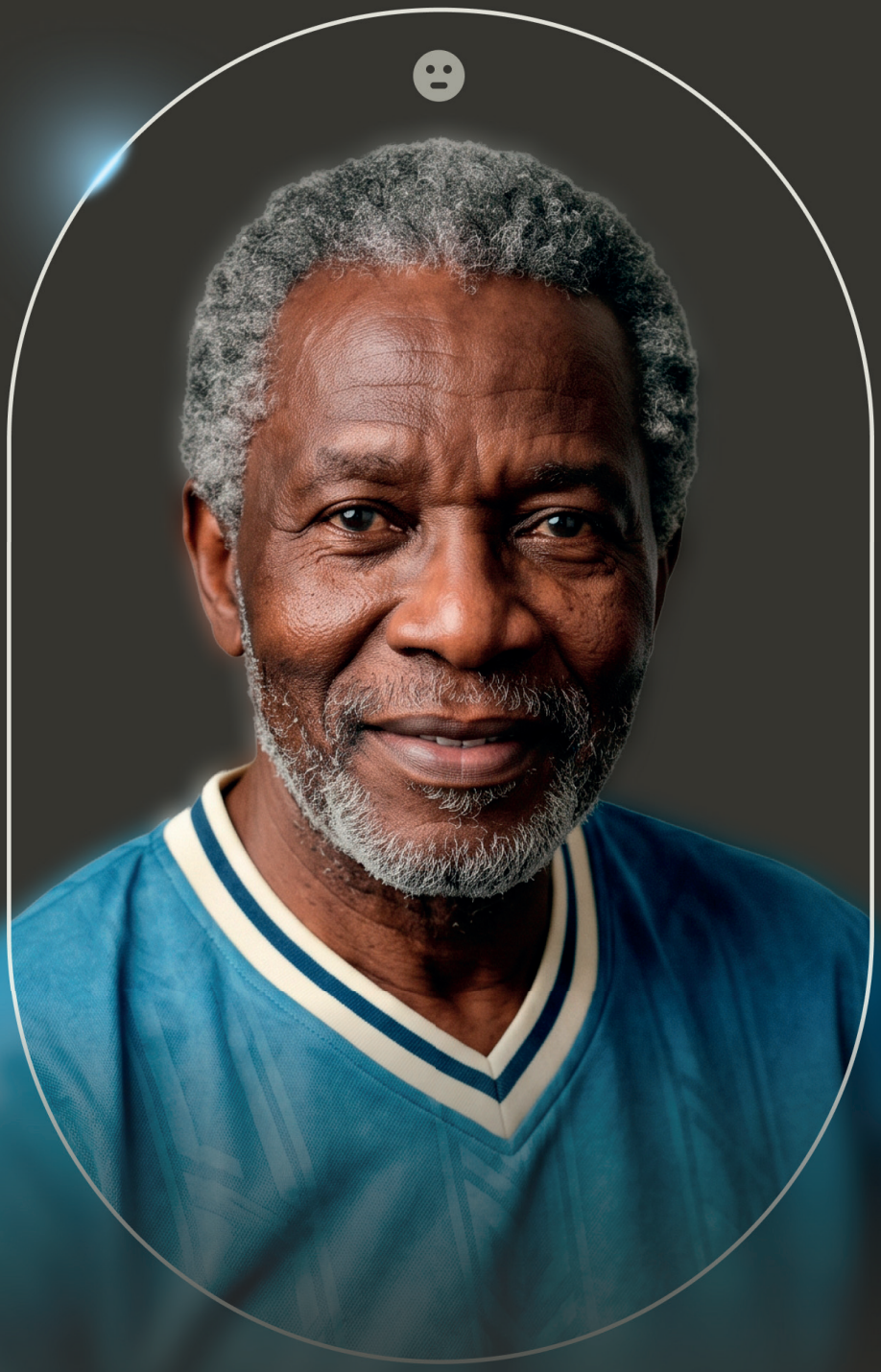
Este es un reconocimiento fundamental: sin una prueba de vida sólida, la verificación de identidad remota se vuelve vulnerable a las mismas herramientas habilitadas por IA que ahora están transformando el panorama del fraude. Los sistemas modernos de prueba de vida más robustos adoptan un enfoque multicapa diseñado para derrotar ataques cada vez más sofisticados. La arquitectura de Unico, por ejemplo, utiliza un modelo de liveness de cuatro capas diseñado para bloquear ataques de inyección de video y ataques a dispositivos a nivel de sensor, mientras confirma en tiempo real que la persona frente a la cámara es genuina, está presente y es legítima.[13]

Pero incluso la prueba de vida más avanzada, por sí sola, responde solo a una parte de la pregunta. El liveness pregunta si la persona en la sesión actual es real, está presente y no utiliza una técnica de suplantación o inyección. La inteligencia de red pregunta si la señal de identidad ha aparecido antes en un patrón sospechoso a través de otros contextos. Una arquitectura de identidad sólida necesita ambas.

El NIST hace una distinción similar en su análisis sobre la inyección digital y los medios falsificados. Advierte que los ataques emergentes combinan la inyección digital con herramientas de IA generativa cada vez más efectivas para burlar la validación de documentos, las operaciones biométricas y las comparaciones visuales. También señala que incluso los controles como la captura en vivo y la detección de ataques de presentación no son suficientes para abordar todos los casos posibles.15

La prueba de vida tiene un papel preciso: asegura la puerta de entrada. La pregunta más profunda —si la persona en la puerta ha aparecido bajo diferentes nombres, en diferentes instituciones o en contextos sospechosos— queda fuera de su alcance.

Este es el punto en el que el KYC moderno debe evolucionar de ser un punto de control a ser una capa de inteligencia.



Los procesos modernos de KYC (Conozca a su cliente) deben evolucionar de un punto de control a una capa de inteligencia.

La verificación de presencia garantiza la seguridad en la puerta principal. La inteligencia de red permite determinar si la persona que llama ha aparecido con nombres diferentes, en distintas instituciones o en contextos sospechosos.

KYC necesita una capa de memoria

Un problema de fraude en red requiere una defensa que tenga en cuenta la red.

El cambio de la verificación de identidad 1:1 a 1:N se entiende mejor en ese contexto. En un proceso 1:1, la institución compara a la persona con la evidencia de identidad que presenta. En un proceso 1:N, el sistema también puede evaluar si la misma señal de identidad biométrica aparece en otro lugar dentro de una población relevante, potencialmente bajo un nombre o registro de identidad diferente.

AJUSTE AL NIVEL DE LA SESIÓN

1:1

La persona frente a su documento
Limitado por la sesión actual

INTELIGENCIA DE RED

1:N

Persona contra todas las señales conocidas
Memoria en instituciones y mercados

El NIST reconoce explícitamente este concepto. Su guía de comprobación de identidad describe una búsqueda 1:N como el cotejo de las características biométricas recolectadas de un solicitante contra una base de datos para determinar si el solicitante ya está presente, posiblemente bajo un nombre distinto. También exige salvaguardas, incluida la revisión manual antes de que se rechace el registro basándose en resultados 1:N automatizados.

Un modelo 1:N responsable saca a la luz conflictos de identidad y patrones de reutilización sospechosos para la evaluación de riesgos. Debe regirse por el consentimiento, la divulgación, los controles de privacidad, las pruebas independientes, la evaluación del desempeño demográfico y una revisión humana adecuada.

1.5B	**20+**	**$7B+**	**3 sec**
Autenticaciones procesadas el año pasado[13]	Países de operación[13]	En fraude financiero prevenido el año pasado[13]	Tiempo promedio de verificación biométrica[13]

Ese contexto de privacidad es especialmente importante para la biometría. La arquitectura es consciente de la privacidad por diseño, funcionando a través de cotejos biométricos mediante hashing, señales de riesgo a través de la red y el reconocimiento de patrones de fraude. Estos mecanismos protegen a las instituciones y a los usuarios legítimos sin funcionar como una base de datos de rostros en bruto ni como un sistema de rastreo.

Precedente: Sección 314(b) de FinCEN

Las instituciones financieras ya comparten información para identificar el blanqueo de capitales. El fraude de identidad ahora requiere el mismo enfoque arquitectónico.[16]

El mismo principio ya existe en otras áreas de los delitos financieros. El marco de la Sección 314(b) de la FinCEN permite que las instituciones financieras compartan información bajo condiciones definidas para identificar y reportar actividades que puedan involucrar lavado de dinero o actividades terroristas. La FinCEN también ha enfatizado que el intercambio de información puede ayudar a abordar el fraude y el cibercrimen cuando se conecta adecuadamente con los riesgos de delitos financieros.[16]

El fraude de identidad requiere ahora el mismo pensamiento arquitectónico.

El posicionamiento de Unico se construye en torno a ese modelo combinado: verificación robusta a nivel de sesión, prueba de vida (liveness) avanzada e inteligencia de identidad a nivel de red. La empresa describe su plataforma IDCloud como proveedora de verificación en tres segundos, detección de prueba de vida, capacidades de radar de fraude y monitoreo en toda la red de patrones en serie. Unico también afirma que procesó más de 1,500 millones de autenticaciones el año pasado, incluye más de 170 millones de rostos de usuarios únicos en más de 20 países y previno más de 7,000 millones de dólares en fraudes financieros el año pasado.[13]

La escala es importante aquí porque cambia la señal de fraude. Cuantos más patrones legítimos y fraudulentos pueda observar una red, más útil se vuelve para cada institución participante. En un modelo aislado, cada institución aprende por su cuenta. En un modelo en red, la inteligencia de fraude puede potenciarse.

Esa es la arquitectura defensiva que exige el fraude moderno.

Un control de fraude más inteligente significa una fricción más inteligente

El fraude y la conversión a menudo se tratan como objetivos opuestos. Si se endurecen los controles, los buenos usuarios abandonan el proceso. Si se reduce la fricción, los defraudadores aprovechan la oportunidad.

50%

Los consumidores estadounidenses abandonan el proceso si se les hacen más de 10 preguntas.

Muchos

Los clientes toleran controles más estrictos cuando entienden el porqué.

Ese intercambio (tradeoff) es real cuando las instituciones dependen de controles rudimentarios. Pero una mejor inteligencia de identidad cambia el cálculo.

Un sistema calibrado según el riesgo aplica un escrutinio más riguroso donde la señal lo justifica. Los usuarios de bajo riesgo avanzan rápidamente, mientras que las sesiones sospechosas, los conflictos de identidad o los patrones repetidos se derivan a una revisión más profunda.

Simplifica los casos sencillos. Dificulta los casos sospechosos.

La verificación de identidad ha pasado de ser una casilla de verificación de cumplimiento a una decisión sobre la infraestructura de control del crecimiento y la confianza.

Esto es cada vez más importante porque la paciencia del usuario es limitada. Una investigación de FICO reveló que la mitad de los consumidores estadounidenses abandonan el onboarding de la banca digital si deben responder más de diez preguntas.17 Investigaciones más recientes de FICO complejizan el panorama de una manera útil: muchos clientes dicen que tolerarán controles de identidad más estrictos cuando comprenden el valor de la seguridad.[18] La fricción inexplicable, repetitiva o mal dirigida perjudica la conversión. La seguridad inteligente puede preservar la confianza.

Eso es importante para los bancos y las fintechs. También es importante para los marketplaces, las plataformas de economía colaborativa (gig platforms), los operadores de iGaming, las empresas de comercio electrónico y cualquier negocio digital que deba aprobar rápidamente a los usuarios legítimos mientras detiene el cultivo de cuentas (account farming), la actividad de mulas, las identidades sintéticas, el abuso de bonificaciones y los intentos repetidos de fraude.

El objetivo es una mejor fricción. Una arquitectura de identidad moderna debe hacer que los casos fáciles sean más sencillos y los casos sospechosos sean más difíciles. Debe distinguir entre un usuario de confianza que regresa y una señal de identidad vinculada a una reutilización sospechosa. Debe reconocer cuándo la sesión es legítima pero el patrón más amplio es sospechoso. Debe prevenir pérdidas posteriores (downstream) sin obligar a cada cliente a pasar por un proceso más lento y repetitivo.

Aquí es donde el caso de negocio y el caso de seguridad convergen. La verificación de identidad se ha expandido de ser un requisito de cumplimiento a convertirse en un control de crecimiento, una capa de control de fraude y una decisión de infraestructura de confianza.

El fin del KYC aislado

El KYC tradicional aún tiene un papel que desempeñar.
Pero, en su forma aislada, es incompleto.

El sistema financiero sigue necesitando validación de documentos, evidencia de identidad, comparación biométrica, prueba de vida (liveness) y flujos de trabajo de cumplimiento (compliance). Esos controles siguen siendo necesarios. Sin embargo, el modelo de amenaza se ha expandido más allá de lo que fueron diseñados para abordar.

Pueden preguntar si este solicitante coincide con esta solicitud. Pueden preguntar si esta persona parece estar presente (live) en esta sesión. Pueden preguntar si el documento parece válido. Pero la pregunta interinstitucional queda fuera de su alcance: si la misma señal de identidad ha aparecido repetidamente bajo diferentes nombres, en diferentes instituciones o en contextos sospechosos. Esa es la capa de memoria que falta.

La próxima era de la verificación de identidad no se definirá pidiendo más documentos ni añadiendo más fricción. Se definirá si las instituciones pueden reconocer patrones de identidad antes de que esos patrones se conviertan en pérdidas. Las instituciones financieras no pueden combatir el fraude de 2026 con herramientas de 2010. Para los ejecutivos responsables de riesgo, fraude, identidad, producto y experiencia del cliente, la elección se está volviendo más clara. Las instituciones pueden seguir fortaleciendo sus silos individuales o pueden avanzar hacia arquitecturas donde la visibilidad escale con la participación.

Referencias

1 FinCEN, Financial Trend Analysis: Identity-Related Suspicious Activity: 2021 Threats and Trends, January 2024.
https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf

2 U.S. Government Accountability Office, Social Security Administration: Actions Needed to Help Ensure Success of Electronic Verification Service, GAO-24-106770, June 2024.
https://www.gao.gov/assets/gao-24-106770.pdf

3 Federal Reserve / FedPayments Improvement, Miscategorization of Synthetic Identity Fraud, toolkit brief.
https://fedpaymentsimprovement.org/wp-content/uploads/miscategorization-synthetic-identity-fraud.pdf

4 Federal Reserve Financial Services, "New Account Fraud and Digital Account Openings," September 2025.
https://www.frbservices.org/news/fed360/issues/090225/industry-perspective-new-account-fraud

5 Javelin Strategy & Research, 2026 Identity Fraud Study: The Illusion of Progress, April 2026.
https://javelinstrategy.com/whitepapers/2026-identity-fraud-study-illusion-progress

6 GAFILAT, International Dialogue for Strengthening Regional AML/CFT Policies Report, January 2026.
https://biblioteca.gafilat.org/wp-content/uploads/2026/01/Informe-Dialogo-Internacional-EN.pdf

7 Zetta, Pix: The New Gold, 2025, citing Banco Central do Brasil data.
https://somoszetta.org.br/wp-content/uploads/2025/08/Zetta_Pix2025_V4-1.pdf

8 FinCEN, Synthetic Identity Fraud, Intelligence Assessment, 2017.
https://www.fincen.gov/system/files/shared/267546_Synthetic%20ID%20Fraud_IA.pdf

9 FinCEN, Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004, November 2024. https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

10 FBI Internet Crime Complaint Center, 2025 IC3 Annual Report, April 2026.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

11 Unico, datos de observación de la red interna de Unico. Proporcionados por Unico a ID Tech para este artículo.

12 NIST, SP 800-63A-4 (Identity Proofing and Enrollment) and SP 800-63B-4 (Authentication and Authenticator Management), Digital Identity Guidelines, August 2025. https://pages.nist.gov/800-63-4/sp800-63a.html and https://pages.nist.gov/800-63-4/sp800-63b.html

13 Unico, IDCloud platform and company materials.
https://www.unico.io/id-cloud-one

14 NIST, SP 800-63A-4, Digital Injection Prevention and Forged Media Detection, August 2025.
https://pages.nist.gov/800-63-4/sp800-63a.html

15 NIST, SP 800-63A-4, 1:N biometric identification guidance, August 2025.
https://pages.nist.gov/800-63-4/sp800-63a.html

16 FinCEN, "Section 314(b)" program guidance and December 2020 statement on information sharing.
https://www.fincen.gov/section-314b

17 FICO, "New FICO Research Shows an Accelerated Digital-First Mindset," August 2021.
https://fico.gcs-web.com/news-releases/news-release-details/new-fico-research-shows-accelerated-digital-first-mindset-71-us

18 FICO, "FICO Survey Shows Americans Prepared to Be Dishonest to Meet Financial Needs," August 2025.
https://fico.gcs-web.com/news-releases/news-release-details/fico-survey-shows-americans-prepared-be-dishonest-meet-financial

unico.io