O Paradoxo da Identidade e do Crédito

WHITE PAPER

Inteligência de Verificação de Identidade para Instituições Financeiras

A falha começa com a identidade, mas a perda geralmente é registrada em outro lugar.

As instituições financeiras raramente experienciam a fraude de identidade como um problema de identidade claramente rotulado. Com mais frequência, ela aparece mais tarde, após o onboarding, em categorias que parecem operacionais ou financeiras, em vez de estruturais: inadimplência no primeiro pagamento (first-payment default), perda de crédito, estornos (chargebacks), abuso promocional, atividade de mulas, invasão de contas ou contas abandonadas criadas para exploração posterior.

PRINCIPAIS MÉTRICAS DE DADOS DA INDÚSTRIA

Esse é o paradoxo identidade-crédito. A falha começa com a identidade, mas a perda é frequentemente contabilizada em outro lugar.

Isso é criticamente importante porque a classificação impulsiona o investimento. Se uma perda é tratada como um problema de crédito, as instituições buscarão soluções em subscrição (underwriting), pontuação (scoring), cobrança ou controles de portfólio. Se for tratada como um problema de pagamentos, elas focarão no monitoramento de transações e controles de estorno. Essas camadas abordam os sintomas posteriores (downstream). A falha anterior (upstream) persiste: uma identidade que nunca deveria ter entrado no sistema foi Liberada.

$27.3B
em perdas devido a fraude de identidade nos EUA em 2025[1]

+31%
de todos os relatórios da FinCEN relacionados à identidade[1]

18M
de vítimas de fraude de identidade nos EUA em 2025[1]

Os processos tradicionais de "Conheça seu Cliente" (KYC) continuam essenciais. As instituições precisam verificar se um usuário é real, se os documentos são válidos, se os dados são consistentes e se a pessoa está presente durante o onboarding. Mas o modelo de ameaça mudou. O KYC tradicional foi construído em torno de uma sessão isolada, na qual um usuário apresenta informações e a instituição verifica se essas informações parecem internamente consistentes. A fraude moderna opera através de sessões, instituições e mercados. Ela é automatizada, adaptável, sintética e em rede.

O problema à primeira vista

1.6M
de relatórios da BSA vinculados à identidade (2021)[1]

42%
de todos os relatórios da FinCEN relacionados à identidade[1]

$212B
em atividades suspeitas ligadas à identidade[1]

O resultado é um abismo crescente entre a forma como a fraude opera e a maneira como muitas instituições ainda se defendem dela.

A análise da FinCEN sobre os relatórios da Lei de Sigilo Bancário (BSA) mostra o quão profundamente a identidade está inserida no crime financeiro. A agência descobriu que aproximadamente 1,6 milhão de relatórios BSA arquivados em 2021 — ou 42% de todos os relatórios arquivados naquele ano — referem-se à identidade, representando US$ 212 bilhões em atividades suspeitas. As tipologias relatadas com maior frequência incluíram fraude, registros falsos, roubo de identidade, lavagem de dinheiro por terceiros e padrões de verificação burlados.[1]

Isso torna a identidade uma camada de crime financeiro por si só.

Ao mesmo tempo, a fraude de identidade está se tornando mais difícil de separar do comportamento de crédito. O Escritório de Responsabilidade Governamental dos EUA (GAO) observou que o custo real da fraude de identidade sintética é provavelmente subestimado, pois muitos casos podem passar despercebidos e ser relatados como perda de crédito em vez de fraude.2 O Federal Reserve fez uma observação semelhante em seu trabalho sobre fraude de identidade sintética, alertando que a classificação incorreta pode tornar o escopo do problema mais difícil de quantificar, distorcer modelos de fraude e permitir que maus atores reutilizem identidades em todo o sistema.[3]

Para bancos, fintechs, marketplaces, plataformas de gig economy e outros negócios digitais em escala, a implicação é direta. A próxima geração de defesa de identidade deve ir além de adicionar fricção ao mesmo processo isolado. É necessário tornar a verificação de identidade mais inteligente, mais coordenada e mais capaz de reconhecer padrões de repetição antes que se tornem perdas posteriores (downstream).

SEÇÃO 01

A fraude deslocou-se para as etapas iniciais do processo.

Criminosos estão criando novas contas que não deveriam existir, e a superfície de ataque está se deslocando para um estágio anterior do ciclo de vida do cliente, para o qual os controles tradicionais não foram projetados.

01

A fraude de contas deslocou-se para as etapas iniciais (upstream)

A fraude de abertura de contas (ou fraude de novas contas) tornou-se uma das expressões mais claras dessa mudança. O Federal Reserve alertou que as aberturas de contas digitais, embora mais convenientes para clientes legítimos, criam novas oportunidades para criminosos. O órgão observa que a fraude de abertura de contas tornou-se mais fácil de cometer e mais difícil de detectar devido a tecnologias mais sofisticadas, IA generativa e à ampla disponibilidade de informações de identificação pessoal (PII) na dark web.[4]

> **Javelin Strategy & Research - Estudo de Identidade 2026**
> O número de vítimas de fraudes em novas contas aumentou 31% (de 4,2 milhões para 5,4 milhões), e as perdas aumentaram 13%, atingindo US$ 7 bilhões em 2025.

O Estudo de Fraude de Identidade de 2026 da Javelin Strategy & Research fornece um panorama útil da tendência. As perdas tradicionais por fraude de identidade nos EUA permaneceram praticamente estáveis em US$ 27,3 bilhões em 2025, afetando 18 milhões de vítimas. No entanto, a fraude de abertura de contas foi a categoria com o crescimento mais acentuado de vítimas, subindo 31%, de 4,2 milhões de vítimas em 2024 para 5,4 milhões em 2025. As perdas decorrentes de fraudes em novas contas aumentaram 13% em relação ao ano anterior, atingindo US$ 7 bilhões.[5]

Esse contraste é importante. As perdas globais por fraude de identidade podem parecer estáveis em um nível macro, mas a superfície de ataque está mudando. Os criminosos estão se direcionando para fases mais precoces do ciclo de vida do cliente. Além de sequestrar contas existentes, eles estão criando novas que não deveriam existir.

$1.2B

Transações fraudulentas com Pix no Brasil em 2024
Mesmo quando a taxa absoluta de fraude permaneceu em 0,03% do valor da transação.[7]

O padrão aparece em nível global. O Grupo de Ação Financeira da América Latina, GAFILAT, descreveu recentemente a fraude como uma das ameaças mais difundidas enfrentadas pela região, com riscos intensificados em torno de serviços financeiros digitais e pagamentos transfronteiriços.6 No Brasil, onde o sistema de pagamentos instantâneos Pix remodelou o setor bancário de consumo, pesquisas da indústria baseadas em dados do banco central revelaram que aproximadamente US$ 1,2 bilhão estiveram envolvidos em transações Pix fraudulentas em 2024, embora a taxa absoluta de fraude tenha permanecido em cerca de 0,03% do valor das transações.[7] Esse contraste ilustra um princípio mais amplo: canais (rails) digitais de alto volume transformam pequenas taxas de fraude em grandes pools de perdas e, quando esses canais são acessados por meio de onboarding digital, a integridade da verificação de identidade torna-se a defesa upstream mais importante desses canais.

Uma nova conta pode ser monetizada de várias maneiras. Um fraudador pode obter crédito sem intenção de reembolso. Pode movimentar fundos ilícitos. Pode depositar cheques forjados ou falsificados. Pode explorar bônus ou incentivos promocionais. Pode fazer compras e contestá-las mais tarde. Pode criar contas que ficam inativas até serem úteis para golpes, atividade de mulas ou esquemas de identidade sintética.

Do ponto de vista da instituição, esses comportamentos podem aparecer em diferentes departamentos e sistemas. A equipe de crédito vê a inadimplência (default). A equipe de pagamentos vê disputas. A equipe de fraude vê abuso de conta. A equipe de conformidade vê atividade suspeita. No entanto, muitos desses resultados compartilham a mesma dependência anterior (upstream): se a identidade era legítima no ponto de entrada.

É aí que o KYC 1:1 tradicional — o modelo no qual um proponente é verificado apenas contra as evidências de identidade que ele mesmo apresenta — começa a mostrar seus limites.

SEÇÃO 02

O KYC tradicional foi construído para uma ameaça mais limitada

O sistema KYC 1:1 informa se esta pessoa corresponde às informações deste documento. Ele não pode perguntar se a mesma marca de identidade já apareceu antes, em outras instituições ou sob outros nomes.

O KYC tradicional foi construído para uma ameaça mais limitada

Um processo típico de KYC 1:1 pergunta se o proponente corresponde à evidência de identidade que apresenta. A selfie corresponde à foto no documento de identidade? O documento é válido? Os atributos parecem consistentes? A pessoa está fisicamente presente na sessão?

Essas são perguntas necessárias. Elas detectam incompatibilidades óbvias, documentos forjados, tentativas de falsificação de identidade, ataques de apresentação de baixa qualidade e muitas formas de roubo de identidade. Uma detecção robusta de prova de vida (liveness) e de ataques de apresentação tornou-se ainda mais importante à medida que deepfakes, ataques de injeção e mídias sintéticas evoluíram.

Mas o KYC 1:1 ainda é limitado pela sessão. Embora responda se esta pessoa parece corresponder a este documento ou solicitação de conta, uma pergunta diferente e cada vez mais importante fica sem resposta: esse mesmo sinal de identidade já apareceu antes sob outros nomes, documentos, contas, instituições ou geografias?

O que o KYC 1:1 pode detectar

- Falsificação de documentos
- Incompatibilidade/discrepância facial
- Imitação de identidade para comprovação de vida
- Ataques de apresentação
- Falsificações de baixa qualidade

O que o KYC 1:1 não pode detectar

- Reutilização de dados entre diferentes instituições
- Redes de contas de laranjas
- Identidades sintéticas criadas em série
- Padrões no nível de gangues/organizações criminosas
- Histórico ou registros compartilhados em diferentes mercados

Este é um problema crítico porque a fraude moderna muitas vezes depende menos de uma única identidade falsa perfeita do que da repetibilidade. Uma rede de fraude pode testar variações em várias instituições. Uma pessoa real pode agir como mula repetidamente. Uma identidade sintética pode ser montada a partir de fragmentos válidos de dados. Um sinal biométrico pode aparecer em diferentes contextos com diferentes informações pessoais. Uma única instituição pode ver apenas uma solicitação aparentemente plausível, enquanto o padrão mais amplo revela um abuso em série.

A FinCEN descreveu esse problema anos atrás em sua análise de fraude de identidade sintética, observando que criminosos podem usar uma única identidade sintética para adquirir vários cartões de crédito de diferentes instituições financeiras.8 Essa mesma lógica se aplica de forma mais ampla à fraude em rede: cada instituição vê apenas a parte do padrão que toca seu próprio perímetro.

A IA generativa agrava o problema. A FinCEN alertou que as ferramentas de GenAI reduziram os recursos necessários para produzir conteúdo sintético de alta qualidade, e que os criminosos usam essas ferramentas para diminuir o custo, o tempo e os recursos necessários para explorar os processos de verificação de identidade das instituições financeiras.9 O relatório IC3 de 2025 do FBI descobriu, de forma semelhante, que as queixas relacionadas à IA produziram mais de US$ 893 milhões em perdas relatadas em 2025, observando que o conteúdo sintético está se tornando mais fácil de criar e mais difícil de detectar.[10]

$893M+

Prejuízos relatados em 2025 devido a reclamações relacionadas à IA[10]

Além de produzir imagens, vídeos, documentos e mensagens falsas mais convincentes, a IA altera a economia do ataque. Ela reduz o custo dos testes. Reduz o esforço necessário para escalar. Melhora a qualidade da engenharia social e do conteúdo sintético. Permite que as operações de fraude refaçam mais rápido do que os controles manuais ou em silos podem se adaptar.

Um processo construído para verificar uma sessão de cada vez enfrenta agora adversários que operam através de sessões, instituições e mercados.

SEÇÃO 03

O ponto cego fora da sessão

Um fraudador que conclui com sucesso o processo de cadastro em uma instituição pode tentar novamente em outra. Esse padrão interinstitucional é o sinal de alerta, e sistemas KYC isolados não conseguem detectá-lo.

03

O ponto cego fora da sessão

O ponto cego mais importante no KYC tradicional é o de escopo. Controles em nível de sessão, por mais rigorosos que sejam, estão limitados pela sessão.

Essa distinção é crucial. A detecção avançada de prova de vida (liveness) pode determinar se uma pessoa real e presente está participando de um fluxo de onboarding. A detecção de ataques de apresentação pode ajudar a proteger contra máscaras, vídeos reproduzidos, mídias sintéticas e outras tentativas de burlar (spoofing) sistemas biométricos. A verificação de documentos pode validar as evidências de identidade. Sinais de dispositivos e comportamentais podem adicionar contexto.

Tudo isso é essencial. Nada disso cria automaticamente memória em todo o mercado.

Um fraudador que passa pelo onboarding de uma instituição pode tentar novamente em outro lugar. Uma mula pode ser usada repetidamente. Um perfil sintético pode evoluir ao longo do tempo. Um rosto pode aparecer com diferentes credenciais. Uma rede de fraude pode atacar muitas instituições ao mesmo tempo, aprendendo com cada tentativa. O padrão interinstitucional é o sinal de risco, e os sistemas de KYC isolados carecem da visibilidade para detectá-lo.

150+

Tentativas de abertura de conta a partir de uma única assinatura biométrica
Observado em aproximadamente 30 instituições antes da ativação da detecção em nível de rede.[11]

As próprias observações de rede da Unico ilustram o quão concentrada essa reutilização pode se tornar. A empresa documentou casos em que uma única assinatura biométrica tentou abrir contas mais de 150 vezes em cerca de 30 instituições diferentes antes de ser identificada no nível de rede.11 Em cada instituição, a solicitação parecia plausível o suficiente para ser investigada. Em toda a rede, o padrão era inequívoco.

É aqui que o ciclo de classificação incorreta se torna perigoso. Quando as perdas impulsionadas pela identidade são contabilizadas como perdas de crédito ou perdas operacionais, as instituições podem investir subestimadamente na infraestrutura de identidade. Quando modelos de fraude são treinados com resultados classificados incorretamente, eles podem aprender a lição errada. Quando fraudadores têm sucesso em um ambiente, eles podem reutilizar o mesmo padrão em outro lugar.

Os materiais do Federal Reserve sobre fraude de identidade sintética alertam que a classificação incorreta pode subestimar o problema e permitir que maus atores reutilizem identidades.[3] O GAO dos EUA observou de forma semelhante que a fraude de identidade sintética pode ser ocultada quando os casos são tratados como perda de crédito em vez de fraude.[2]

Existem implicações estratégicas para os tomadores de decisão executivos. Se a organização não consegue identificar quais perdas começaram como falhas de identidade, ela não pode saber se seu stack de identidade está performando. Um portfólio pode parecer ter um problema de crédito quando também tem um problema de onboarding. Uma equipe de fraude pode perseguir o abuso posterior (downstream) quando o ponto de intervenção mais forte era a criação da conta.

É por isso que a arquitetura importa.

A prova de vida (liveness) é agora fundamental

O surgimento de mídias geradas por IA tornou a detecção robusta de prova de vida (liveness) e de ataques de apresentação um requisito básico para a verificação de identidade moderna. As instituições financeiras não podem confiar em verificações estáticas de documentos ou simples correspondência de selfies quando os atacantes podem produzir imagens sintéticas mais convincentes, manipular transmissões de vídeo ou tentar ataques de injeção digital.

> **NIST SP 800-63A-4 — Diretrizes de Identidade Digital (agosto de 2025)**
>
> "Os provedores de serviços de credenciais devem implementar a detecção de ataques de apresentação para confirmar a presença real de um ser humano e mitigar tentativas de falsificação de identidade e fraude."[12]

As diretrizes atuais de identidade digital do NIST refletem essa mudança. Na coleta biométrica remota, o NIST afirma que os provedores de serviços de credenciais devem implementar a detecção de ataques de apresentação para confirmar a presença genuína de um ser humano vivo e mitigar tentativas de spoofing e falsificação de identidade. Suas diretrizes de autenticação também estabelecem que os sistemas biométricos de reconhecimento facial devem implementar a detecção de ataques de apresentação.[12]

Este é um reconhecimento fundamental: sem uma prova de vida robusta, a verificação remota de identidade torna-se vulnerável às mesmas ferramentas habilitadas por IA que agora estão transformando o cenário da fraude.

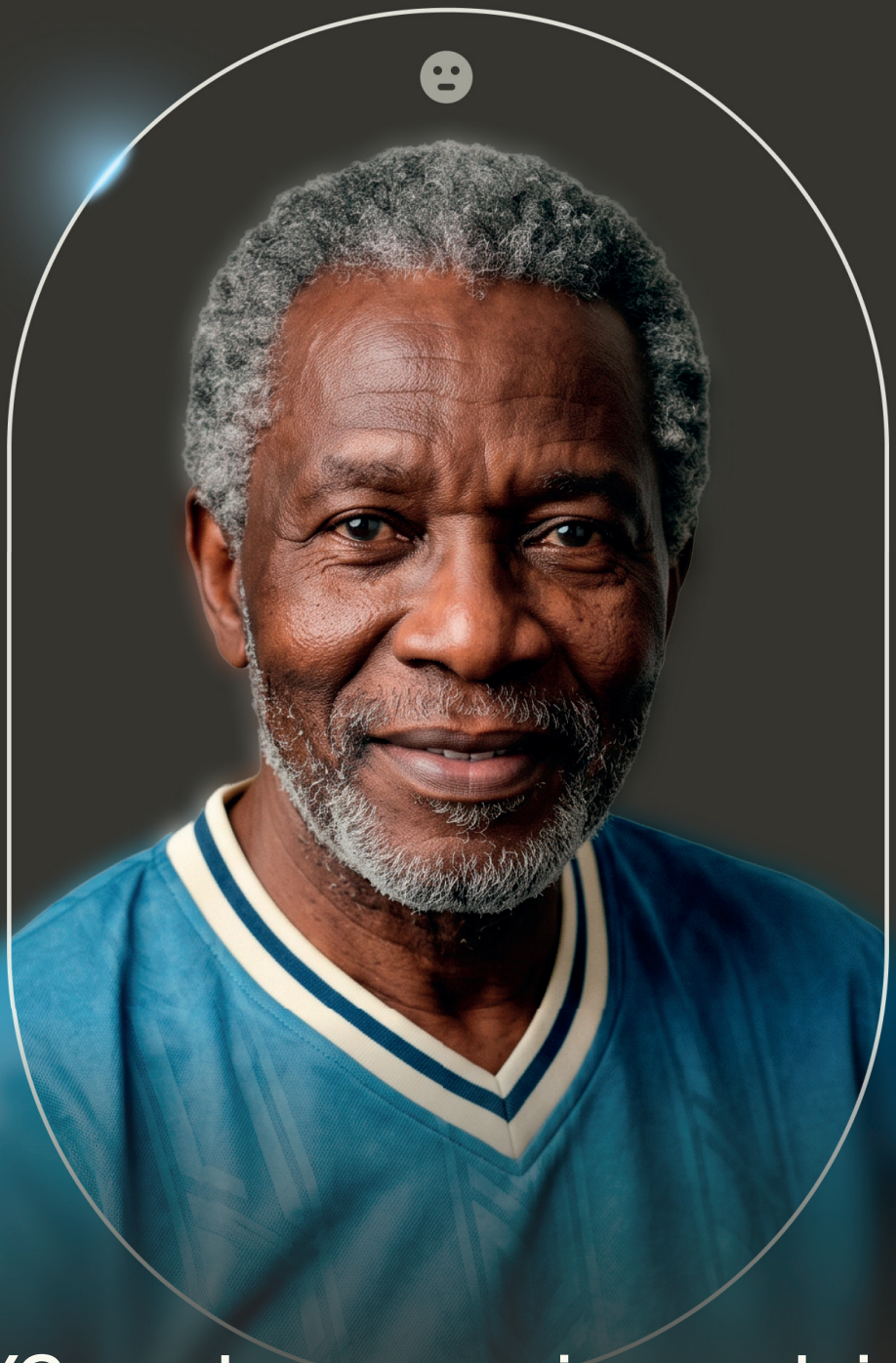
Os sistemas de prova de vida modernos mais robustos adotam um enfoque em múltiplas camadas projetado para derrotar ataques cada vez mais sofisticados. A arquitetura da Unico, por exemplo, utiliza um modelo de liveness de quatro camadas construído para bloquear ataques de injeção de vídeo e ataques a dispositivos no nível do sensor, enquanto confirma em tempo real que a pessoa à frente da câmera é genuína, está presente e é legítima.[13]

Mas mesmo o liveness mais avançado, por si só, responde apenas a parte da pergunta. O liveness pergunta se a pessoa na sessão atual é real, está presente e não está usando uma técnica de spoofing ou injeção. A inteligência de rede pergunta se o sinal de identidade já apareceu antes em um padrão suspeito em outros contextos. Uma arquitetura de identidade sólida precisa de ambos.

O NIST faz uma distinção semelhante em sua discussão sobre injeção digital e mídia forjada. Ele alerta que os ataques emergentes combinam a injeção digital com ferramentas de IA generativa (GenAI) cada vez mais eficazes para derrotar a validação de documentos, as operações biométricas e as comparações visuais. Também observa que mesmo controles como a captura ao vivo e a detecção de ataques de apresentação não são suficientes para lidar com todos os casos possíveis.[14]

A prova de vida tem um papel preciso. Ele protege a porta de entrada. A questão mais profunda — se a pessoa na porta apareceu sob diferentes nomes, em diferentes instituições ou em contextos suspeitos — fica fora de seu escopo.

Este é o ponto em que o KYC moderno precisa evoluir de um ponto de verificação para uma camada de inteligência.



O KYC moderno precisa evoluir de um mero ponto de verificação para uma camada de inteligência.

O sistema de verificação de presença protege a porta da frente. A inteligência de rede responde se a pessoa na porta apareceu com nomes diferentes, em instituições diferentes ou em contextos suspeitos.

O KYC precisa de uma camada de memória

Um problema de fraude em rede exige uma defesa consciente da rede.

A mudança da verificação de identidade 1:1 para 1:N é melhor compreendida nesse contexto. Em um processo 1:1, a instituição compara a pessoa com a evidência de identidade que ela apresenta. Em um processo 1:N, o sistema também pode avaliar se o mesmo sinal de identidade biométrica aparece em outro lugar em uma população relevante, potencialmente sob um nome ou registro de identidade diferente.

CONCORDÂNCIA A NÍVEL DA SESSÃO

1:1

Pessoa em frente ao seu documento
Limitado à sessão atual

INTELIGÊNCIA DE REDE

1:N

Pessoa que apresenta todos os sinais conhecidos
Histórico/registro compartilhado entre instituições e mercados

O NIST reconhece explicitamente esse conceito. Suas diretrizes de comprovação de identidade descrevem uma busca 1:N como a verificação das características biométricas coletadas de um proponente em um banco de dados para determinar se o proponente já está presente, possivelmente sob um nome diferente. Ele também exige salvaguardas, incluindo revisão manual antes que uma inscrição seja recusada com base em resultados 1:N automatizados.[15]

Um modelo 1:N responsável traz à tona conflitos de identidade e padrões de reutilização suspeitos para avaliação de risco. Ele deve ser regido por consentimento, divulgação, controles de privacidade, testes independentes, avaliação de desempenho demográfico e revisão humana apropriada.

1.5B
de autenticações processadas no ano passado[13]

20+
países de operação[13]

$7B+
em fraude financeira prevenida no ano passado[13]

3 sec
é o tempo médio para verificação biométrica[13]

Esse contexto de privacidade é especialmente importante para a biometria. A arquitetura é consciente da privacidade por design, trabalhando por meio de correspondência biométrica com hash, sinais de risco entre redes e reconhecimento de padrões de fraude. Esses mecanismos protegem as instituições e os usuários legítimos sem funcionar como um banco de dados de rostos brutos ou um sistema de rastreamento.

Precedente: Seção 314(b) da FinCEN

As instituições financeiras já compartilham informações para identificar lavagem de dinheiro. A fraude de identidade agora exige a mesma abordagem arquitetônica.[16]

O mesmo princípio já existe em outras áreas do crime financeiro. A estrutura da Seção 314(b) da FinCEN permite que as instituições financeiras compartilhem informações sob condições definidas para identificar e relatar atividades que possam envolver lavagem de dinheiro ou atividade terrorista. A FinCEN também enfatizou que o compartilhamento de informações pode ajudar a lidar com a fraude e o cibercrime quando apropriadamente conectado aos riscos de crimes financeiros.[16]

A fraude de identidade exige agora o mesmo pensamento arquitetônico.

O posicionamento da Unico é construído em torno desse modelo combinado: verificação robusta em nível de sessão, liveness avançado e inteligência de identidade em nível de rede. A empresa descreve sua plataforma IDCloud como fornecedora de verificação em três segundos, detecção de liveness, capacidades de radar de fraude e monitoramento em toda a rede para padrões seriais. A Unico também afirma ter processado mais de 1,5 bilhão de autenticações no ano passado, incluindo mais de 170 milhões de rostos de usuários únicos em mais de 20 países, e evitado mais de US$ 7 bilhões em fraudes financeiras no último ano.[13]

A escala importa aqui porque ela altera o sinal de fraude. Quanto mais padrões legítimos e fraudulentos uma rede puder observar, mais útil a rede se torna para cada instituição participante. Em um modelo em silos, cada instituição aprende sozinha. Em um modelo em rede, a inteligência de fraude pode ser potencializada.
Essa é a arquitetura defensiva que a fraude moderna exige.

Um controle de fraude mais inteligente significa uma fricção mais inteligente

Fraude e conversão são frequentemente tratadas como objetivos opostos. Aperte os controles, e os bons usuários abandonam o processo. Reduza a fricção, e os fraudadores exploram a brecha.

50%

dos consumidores americanos abandonam uma compra se forem questionados sobre mais de 10 assuntos.

Muitos

clientes toleram controles mais rigorosos quando entendem o motivo.

Esse tradeoff é real quando as instituições dependem de controles rudimentares. Mas uma inteligência de identidade melhor altera esse cálculo.

Um sistema calibrado pelo risco aplica um escrutínio mais rigoroso onde o sinal o justifica. Usuários de baixo risco avançam rapidamente, enquanto sessões suspeitas, conflitos de identidade ou padrões repetidos são escalonados para uma revisão mais profunda.

Isso é cada vez mais importante porque a paciência do usuário é limitada. Uma pesquisa da FICO revelou que metade dos consumidores dos EUA abandona o onboarding de bancos digitais se tiverem que responder a mais de dez perguntas.17 Pesquisas mais recentes da FICO complementam esse cenário de uma forma útil: muitos clientes afirmam que tolerariam verificações de identidade mais rigorosas quando entendem o valor da segurança. Fricção inexplicável, repetitiva ou mal direcionada prejudica a conversão.18 A segurança inteligente pode preservar a confiança.

Isso é importante para bancos e fintechs. Também é relevante para marketplaces, plataformas de gig economy, operadores de iGaming, empresas de e-commerce e qualquer negócio digital que precise aprovar usuários legítimos rapidamente, ao mesmo tempo em que interrompe o account farming, a atividade de mulas, identidades sintéticas, abuso de bônus e tentativas repetidas de fraude.

O objetivo é uma fricção melhor.

Uma arquitetura de identidade moderna deve tornar os casos fáceis ainda mais fáceis e os casos suspeitos mais difíceis. Ela deve distinguir entre um usuário de confiança que retorna e um sinal de identidade vinculado a uma reutilização suspeita. Deve reconhecer quando a sessão é legítima, mas o padrão mais amplo é suspeito. Deve evitar perdas posteriores (downstream) sem forçar cada cliente a passar por um processo mais lento e repetitivo.

É aqui que o business case e o security case convergem. A verificação de identidade expandiu-se de um requisito de conformidade para um controle de crescimento, uma camada de controle de fraude e uma decisão de infraestrutura de confiança.

O fim do KYC isolado

O KYC tradicional ainda tem um papel. Mas, em sua forma isolada, ele é incompleto.

O sistema financeiro ainda precisa de validação de documentos, evidência de identidade, comparação biométrica, prova de vida (liveness) e fluxos de trabalho de conformidade (compliance). Esses controles continuam sendo necessários. O modelo de ameaça expandiu-se para além do que eles foram construídos para enfrentar.

Eles podem perguntar se este proponente corresponde a esta solicitação. Podem perguntar se esta pessoa parece estar presente (live) nesta sessão. Podem perguntar se o documento parece válido. A questão interinstitucional está fora do alcance deles: se o mesmo sinal de identidade apareceu repetidamente sob nomes diferentes, em diferentes instituições ou em contextos suspeitos. Essa é a camada de memória que falta.

A próxima era da verificação de identidade não será definida pelo pedido de mais documentos ou pelo aumento da fricção. Será definida pela capacidade das instituições de reconhecer padrões de identidade antes que esses padrões se tornem perdas. As instituições financeiras não podem combater a fraude de 2026 com ferramentas de 2010.

Para executivos responsáveis por risco, fraude, identidade, produto e experiência do cliente, a escolha está se tornando mais clara. As instituições podem continuar fortalecendo silos individuais ou podem avançar em direção a arquiteturas onde a visibilidade escala com a participação.

A fraude moderna já é colaborativa, automatizada e global. A defesa da identidade tem que se atualizar.

References

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, dados internos de observação. Fornecidos pela Unico à ID Tech para este artigo.

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