IDTECH UNICO

The Identity-Credit Paradox

WHITE PAPER

Identity Verification Intelligence for Financial Instituions

The failure begins with identity, but the loss is often booked somewhere else.

Financial institutions rarely experience identity fraud as a cleanly labeled identity problem. More often, it appears later, after onboarding, in categories that look operational or financial rather than foundational: first-payment default, credit loss, chargebacks, promotional abuse, mule activity, account takeover, or abandoned accounts created for later exploitation.

KEY METRICS FROM INDUSTRY DATA

That is the identity-credit paradox. The failure begins with identity, but the loss is often booked somewhere else.

This is critically important because classification drives investment. If a loss is treated as a credit problem, institutions will look to underwriting, scoring, collections, or portfolio controls. If it is treated as a payments problem, they will focus on transaction monitoring and chargeback controls. Those layers address downstream symptoms. The upstream failure persists: an identity that should never have entered the system was allowed through.

$27.3B
U.S. Identity fraud losses in 2025[1]

+31%
of all FinCEN reports identity related[1]

18M
U.S victims of Identity fraud in 2025[1]

Traditional Know Your Customer processes remain essential. Institutions need to verify that a user is real, that documents are valid, that data is consistent, and that a person is present during onboarding. But the threat model has changed. Traditional KYC was built around an isolated session, where a user presents information and the institution checks whether that information appears internally consistent. Modern fraud operates across sessions, institutions, and markets. It is automated, adaptive, synthetic, and networked.

The Problem at a Glance

1.6M
BSA reports tied to identity (2021)[1]

42%
of all FinCEN reports identity related[1]

$212B
in suspicious activity linked to identity[1]

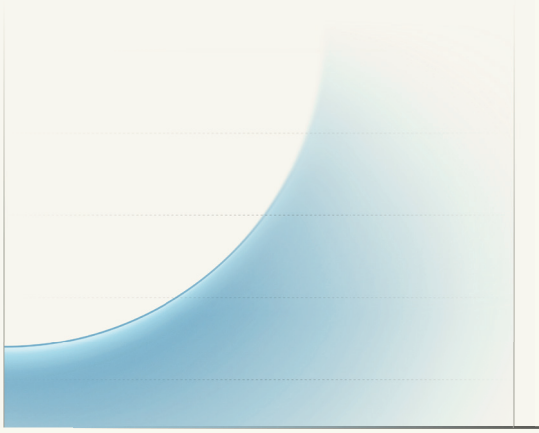
The result is a widening gap between the way fraud operates and the way many institutions still defend against it.

FinCEN's analysis of Bank Secrecy Act reports shows how deeply identity is embedded in financial crime. The agency found that approximately 1.6 million BSA reports filed in 2021, or 42 percent of all reports filed that year, relate to identity, representing $212 billion in suspicious activity. The most frequently reported typologies included fraud, false records, identity theft, third-party money laundering, and circumvention of verification standards.[1]

That makes identity a financial-crime layer in its own right.

At the same time, identity fraud is becoming more difficult to separate from credit behavior. The U.S. Government Accountability Office has noted that the true cost of synthetic identity fraud is likely underestimated because many cases may go undetected and be reported as credit loss rather than fraud.[2] The Federal Reserve has made a similar point in its work on synthetic identity fraud, warning that misclassification can make the scope of the problem harder to quantify, distort fraud models, and allow bad actors to reuse identities across the system.[3]

For banks, fintechs, marketplaces, gig platforms, and other scaled digital businesses, the implication is direct. The next generation of identity defense must move beyond adding friction to the same isolated process. It needs to make identity verification more intelligent, more coordinated, and more capable of recognizing repeat patterns before they become downstream losses.



SECTION 01

New-account fraud has moved upstream

Criminals are creating new accounts that should not exist - and the attack surface is shifting earlier in the customer lifecycle than traditional controls were built to catch.

01

New-Account Fraud Has Moved Upstream

New-account fraud has become one of the clearest expressions of this shift. The Federal Reserve has warned that digital account openings, while more convenient for legitimate customers, create new opportunities for criminals. It notes that new-account fraud has become easier to commit and harder to detect because of more sophisticated technology, generative AI, and the widespread availability of personally identifiable information on the dark web.[4]

> **Javelin Strategy & Research - 2026 Identity Study**
>
> New-account fraud victims rose 31% (4.2M - 5.4M) with losses up 13% to $7B in 2025.

Javelin Strategy & Research's 2026 Identity Fraud Study provides a useful snapshot of the trend. Traditional U.S. identity fraud losses remained roughly flat at $27.3 billion in 2025, affecting 18 million victims. But new-account fraud was the category with the sharpest victim growth, rising 31 percent from 4.2 million victims in 2024 to 5.4 million in 2025. Losses from new-account fraud rose 13 percent year over year to $7 billion.[5]

That contrast is important. Overall identity fraud losses may appear stable at a high level, but the attack surface is shifting. Criminals are moving earlier in the customer lifecycle. Beyond hijacking existing accounts, they are creating new ones that should not exist.

$1.2B

Fraudulent Pix transactions in Brazil in 2024

Even as the absolute frud rate heid at 0.03% of transaction value. [7]

The pattern appears at a global level. The Financial Action Task Force of Latin America, GAFILAT, recently described fraud as one of the most widespread threats facing the region, with intensifying risks around digital financial services and cross-border payments.[6] In Brazil, where the Pix instant-payment system has reshaped consumer banking, industry research drawing on central bank data found that approximately USD 1.2 billion was involved in fraudulent Pix transactions in 2024, even though the absolute fraud rate stayed at roughly 0.03 percent of transaction value.[7] That contrast illustrates a broader principle. High-volume digital rails turn small fraud rates into large loss pools, and when those rails are accessed through digital onboarding, the integrity of identity verification becomes the rails' single most important upstream defense.

SECTION 02

Traditional KYC was built for a narrower threat

1:1 KYC answers whether this person matches this documento. It cannot ask whether the same identity signal has appeared before - at other institutions, under other names.

02

Traditional KYC was built for a narrower threat

A typical 1:1 KYC process asks whether the applicant matches the identity evidence they present. Does the selfie match the photo on the ID? Is the document valid? Do the attributes appear consistent? Is the person physically present in the session?

Those are necessary questions. They catch obvious mismatches, forged documents, impersonation attempts, low-quality presentation attacks, and many forms of identity theft. Strong liveness detection and presentation attack detection have become even more important as deepfakes, injection attacks, and synthetic media have improved.

But 1:1 KYC is still bounded by the session. While it answers whether this person appears to match this document or account application, a different and increasingly important question goes unanswered: has this same identity signal appeared before under other names, documents, accounts, institutions, or geographies?

What 1:1 KYC CAN detect

- Document forgery
- Face mismatch
- Liveness spoof
- Presentation attacks
- Low-quality fakes

What 1:1 KYC CAN detect

- Cross-instituion reuse
- Mule networks
- Serial synthetic IDs
- Ring-level patterns
- Memory across markets

This is a critical issue because modern fraud often depends less on one perfect fake identity than on repeatability. A fraud ring can test variations across institutions. A real person can act as a mule repeatedly. A synthetic identity can be assembled from valid fragments of data. A biometric signal can appear in different contexts with different personal information. A single institution may see only one apparently plausible application, while the broader pattern reveals serial abuse.

FinCEN described this problem years ago in its analysis of synthetic identity fraud, noting that criminals can use a single synthetic identity to acquire several credit cards from different financial institutions.[8] That same logic applies more broadly to networked fraud: each institution sees only the part of the pattern that touches its own perimeter.

Generative AI compounds the problem. FinCEN has warned that GenAI tools have reduced the resources required to produce high-quality synthetic content, and that criminals use those tools to lower the cost, time, and resources needed to exploit financial institutions' identity verification processes.[9] The FBI's 2025 IC3 report similarly found that AI-related complaints produced more than $893 million in reported losses in 2025, while noting that synthetic content is becoming easier to make and harder to detect.[10]

$893M+

AI-related complaint losses reported in 2025[10]

Beyond producing more convincing fake images, videos, documents, and messages, AI changes the economics of attack. It reduces the cost of testing. It reduces the effort required to scale. It improves the quality of social engineering and synthetic content. It allows fraud operations to iterate faster than manual or siloed controls can adapt.

A process built to verify one session at a time is now facing adversaries that operate across sessions, institutions, and markets.

SECTION 03

The blind spot outside the session

A fraudster who passes one institution’s onboarding can try again somewhere else. the cross-institutional pattern is the risk signal - and isolated KYC systems cannot detect it.

03

The Blind Spot Outside the Session

The most important blind spot in traditional KYC is one of scope. Session-level controls, no matter how rigorous, are bounded by the session.

That distinction is crucial. Advanced liveness detection can determine whether a real, present person is participating in an onboarding flow. Presentation attack detection can help protect against masks, replayed videos, synthetic media, and other attempts to spoof biometric systems. Document verification can validate identity evidence. Device and behavioral signals can add context.

All of that is essential. None of it automatically creates memory across the market.

A fraudster who passes one institution's onboarding can try again somewhere else. A mule can be used repeatedly. A synthetic profile can evolve over time. A face can appear with different credentials. A fraud ring can attack many institutions at once, learning from each attempt. The cross-institutional pattern is the risk signal, and isolated KYC systems lack the visibility to detect it.

150+

account-opening attempts from a single biometric signature

Observed across ~30 institutions before network-level detection triggered.[11]

Unico's own network observations illustrate how concentrated this reuse can become. The company has documented cases in which a single biometric signature attempted to open accounts more than 150 times across roughly 30 different institutions before being identified at the network level.[11] At each institution, the application looked plausible enough to investigate. Across the network, the pattern was unambiguous.

This is where the misclassification loop becomes dangerous. When identity-driven losses are booked as credit losses or operational losses, institutions may underinvest in identity infrastructure. When fraud models are trained on misclassified outcomes, they can learn the wrong lesson. When fraudsters succeed in one environment, they can reuse the same pattern elsewhere.

The Federal Reserve's synthetic identity fraud materials warn that misclassification can understate the problem and allow bad actors to reuse identities.[3] The U.S. GAO has similarly noted that synthetic identity fraud may be hidden when cases are treated as credit loss rather than fraud.[2]

There are strategic implications for executive decision-makers. If the organization cannot identify which losses began as identity failures, it cannot know whether its identity stack is performing. A portfolio may appear to have a credit problem when it also has an onboarding problem. A fraud team may chase downstream abuse when the stronger intervention point was account creation.

That is why the architecture matters.

Liveness is now foundational

The rise of AI-generated media has made strong liveness and presentation attack detection a baseline requirement for modern identity verification. Financial institutions cannot rely on static document checks or simple selfie matching when attackers can produce more convincing synthetic images, manipulate video streams, or attempt digital injection attacks.

> **NIST SP 800-63A-4 — Digital Identity Guidelines (August 2025)**
>
> "Credential service providers must implement presentation attack detection to confirm the genuine presence of a live human being and mitigate spoofing and impersonation attempts." [12]

NIST's current digital identity guidance reflects this shift. In remote biometric collection, NIST says credential service providers must implement presentation attack detection to confirm the genuine presence of a live human being and mitigate spoofing and impersonation attempts. Its authentication guidance also states that facial-recognition biometric systems must implement presentation attack detection.[12]

This is a foundational acknowledgment: Without strong liveness, remote identity verification becomes vulnerable to the very AI-enabled tools now changing the fraud landscape.

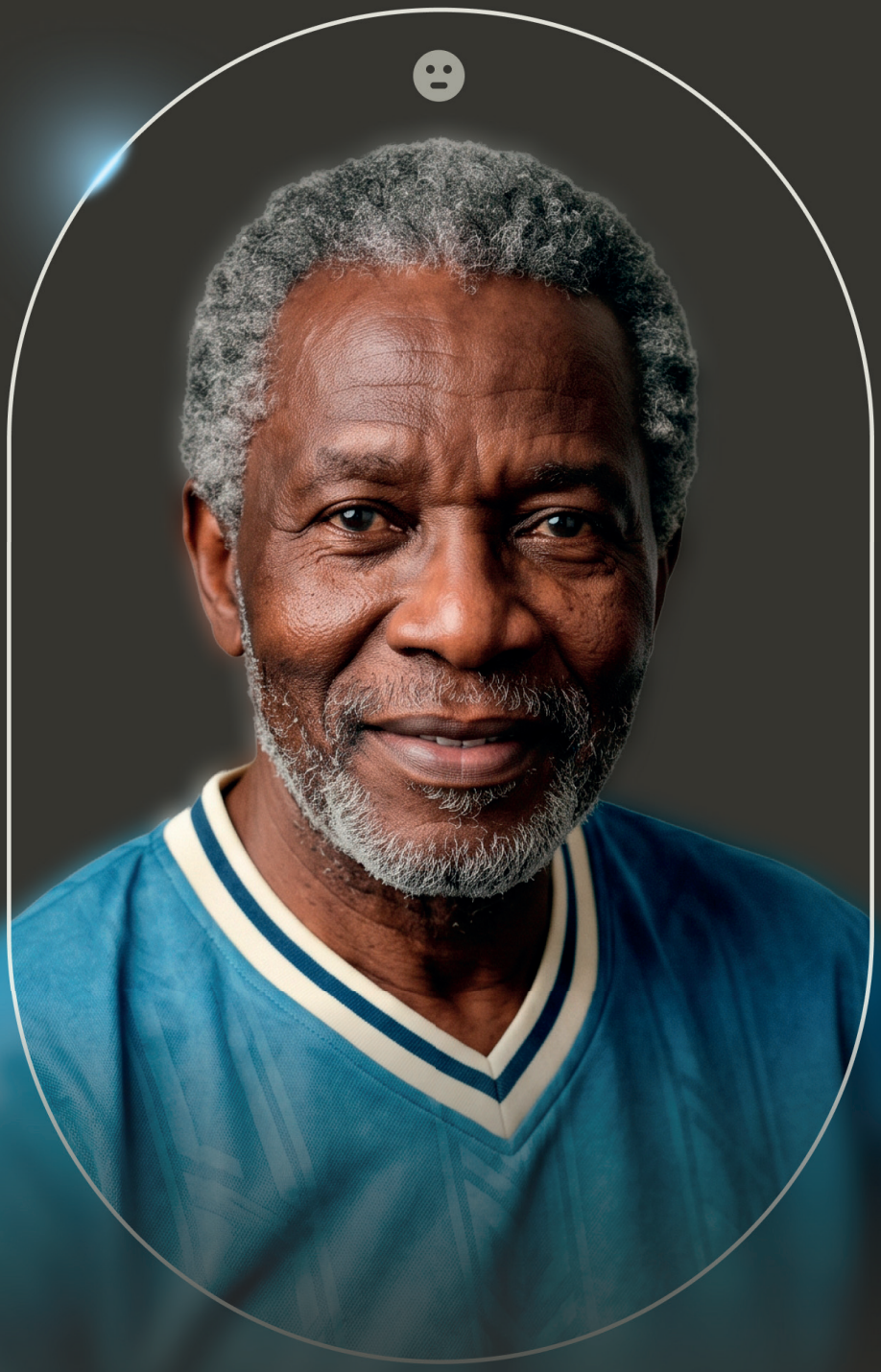
The most robust modern liveness systems take a multi-layered approach designed to defeat increasingly sophisticated attacks. Unico's architecture, for example, uses a four-layer liveness model built to block video injection attacks and sensor-level device attacks while confirming in real time that the person in front of the camera is genuine, present, and legitimate.[13]

But even the most advanced liveness, on its own, answers only part of the question. Liveness asks whether the person in the current session is real, present, and not using a spoofing or injection technique. Network intelligence asks whether the identity signal has appeared before in a suspicious pattern across other contexts. A strong identity architecture needs both.

NIST makes a similar distinction in its discussion of digital injection and forged media. It warns that emerging attacks pair digital injection with increasingly effective GenAI tools to defeat document validation, biometric operations, and visual comparisons. It also notes that even controls such as live capture and presentation attack detection are not sufficient to address all possible cases.[14]

Liveness has a precise role. It secures the front door. The deeper question, whether the person at the door has appeared under different names, at different institutions, in suspicious contexts, sits outside its scope.

This is the point where modern KYC needs to evolve from a checkpoint into an intelligence layer.



Modern KYC needs to evolve from a checkpoint into an intelligence layer.

Liveness secures the front door. Network intelligence answers whether the person at the door has appeared under different names, at different institutions, in suspicious contexts.

KYC Needs a Memory Layer

A networked fraud problem requires a network-aware defense.

The shift from 1:1 to 1:N identity verification is best understood in that context. In a 1:1 process, the institution compares the person to the identity evidence they present. In a 1:N process, the system can also evaluate whether the same biometric identity signal appears elsewhere in a relevant population, potentially under a different name or identity record.

SESSION-LEVEL MATCH

1:1

Person vs. their document
Bounded by the current session

NETWORK INTELLIGENCE

1:N

Person vs. all known signals
Memory across institutions & markets

NIST explicitly recognizes this concept. Its identity proofing guidance describes a 1:N search as checking an applicant's collected biometric characteristics against a database to determine whether the applicant is already present, possibly under a different name. It also requires safeguards, including manual review before enrollment is declined based on automated 1:N results.[15]

A responsible 1:N model surfaces identity conflicts and suspicious reuse patterns for risk evaluation. It must be governed by consent, disclosure, privacy controls, independent testing, demographic performance evaluation, and appropriate human review.

1.5B
Authentications processed last year[13]

20+
Contries of operation[13]

$7B+
In financial fraud prevented last year[13]

3 sec
Average biometric verification time[13]

That privacy context is especially important for biometrics. The architecture is privacy-conscious by design, working through hashed biometric matching, cross-network risk signals, and fraud-pattern recognition. These mechanisms protect institutions and legitimate users without functioning as a raw face database or a tracking system.

Precedent: FinCEN Section 314(b)

Financial institutions already share intelligence to identify money laundering. Identity fraud now requires the same architectural thinking.[16]

The same principle already exists in other areas of financial crime. FinCEN's Section 314(b) framework allows financial institutions to share information under defined conditions to identify and report activity that may involve money laundering or terrorist activity. FinCEN has also emphasized that information sharing can help address fraud and cybercrime when appropriately connected to financial-crime risks.[16]

Identity fraud now requires the same architectural thinking.

Unico's position is built around that combined model: strong session-level verification, advanced liveness, and network-level identity intelligence. The company describes its IDCloud platform as delivering three-second verification, liveness detection, fraud-radar capabilities, and network-wide monitoring for serial patterns. Unico also says it processed more than 1.5 billion authentications last year across more than 20 countries, and prevented more than $7 billion in financial fraud last year.[13]

Scale matters here because it changes the fraud signal. The more legitimate and fraudulent patterns a network can observe, the more useful the network becomes for each participating institution. In a siloed model, every institution learns alone. In a networked model, fraud intelligence can compound.

That is the defensive architecture modern fraud demands.

Smarter fraud control means smarter friction

Fraud and conversion are often treated as opposing goals. Tighten controls, and good users abandon the process. Reduce friction, and fraudsters exploit the opening.

50%

Of U.S consumers abandon if > 10 questions are asked

Many

Customers tolerate tougher checks when they understand why

That tradeoff is real when institutions rely on blunt controls. But better identity intelligence changes the calculation.

A risk-calibrated system applies stronger scrutiny where the signal warrants it. Low-risk users move quickly, while suspicious sessions, identity conflicts, or repeated patterns are escalated for deeper review.

Make the easy cases easier. Make the suspicious cases harder.

Identity verification has expanded from a compliance checkbox into a growth control and trust infrastructure decision.

This is increasingly important because user patience is limited. FICO research found that half of U.S. consumers abandon digital bank onboarding if they must answer more than ten questions.[17] More recent FICO research complicates the picture in a useful way: many customers say they will tolerate tougher identity checks when they understand the security value.[18] Unexplained, repetitive, or poorly targeted friction harms conversion. Intelligent security can preserve trust.

That matters for banks and fintechs. It also matters for marketplaces, gig platforms, iGaming operators, e-commerce companies, and any digital business that has to approve legitimate users quickly while stopping account farming, mule activity, synthetic identities, bonus abuse, and repeat fraud attempts.

The goal is better friction.

A modern identity architecture should make the easy cases easier and the suspicious cases harder. It should distinguish between a returning trusted user and an identity signal linked to suspicious reuse. It should recognize when the session is genuine but the broader pattern is suspect. It should prevent downstream losses without forcing every customer through a slower, more repetitive process.

This is where the business case and the security case converge. Identity verification has expanded from a compliance requirement into a growth control, a fraud-control layer, and a trust infrastructure decision.

The End of Isolated KYC

Traditional KYC still has a role. But in its isolated form, it is incomplete.

The financial system still needs document validation, identity evidence, biometric comparison, liveness, and compliance workflows. Those controls remain necessary. The threat model has expanded beyond what they were built to address.

They can ask whether this applicant matches this application. They can ask whether this person appears live in this session. They can ask whether the document appears valid. The cross-institutional question lies outside their reach: whether the same identity signal has appeared repeatedly under different names, at different institutions, in suspicious contexts. That is the missing memory layer.

The next era of identity verification will not be defined by asking for more documents or adding more friction. It will be defined by whether institutions can recognize identity patterns before those patterns become losses. Financial institutions cannot fight 2026 fraud with 2010 tools.

For executives responsible for risk, fraud, identity, product, and customer experience, the choice is becoming clearer. Institutions can keep strengthening individual silos, or they can move toward architectures where visibility scales with participation.

Modern fraud is already collaborative, automated, and global. Identity defense has to catch up.

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, internal network observation data. Provided by Unico to ID Tech for this paper.

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