



Financial Inclusion Through Community-Verified Digital Identity

Prof. Ross P. Buckley

Professor, UNSW Sydney, Australia

Abstract

Reliable proof of identity is an important gateway to regulated financial services because financial institutions must determine who their customers are before accounts and other financial relationships can be established. Conventional identity-verification systems, however, may unintentionally exclude people whose official documents are missing, outdated, inconsistent, geographically difficult to obtain, or poorly integrated with digital systems. These barriers can affect rural residents, informal workers, migrants, people with weak civil-registration histories, and other populations at the margins of formal administrative systems. This study develops a community-verified digital identity framework intended to supplement, rather than replace, legally recognized identification and regulated customer-due-diligence processes. In the proposed architecture, identity claims that cannot be adequately established through conventional documentation may be supported by independently recorded attestations from approved community verifiers, combined with digital audit trails, duplicate detection, informed consent, risk-based escalation, institutional review, and accessible appeal mechanisms.

The approach is grounded in identification-for-development literature, digital financial inclusion research, biometric identity scholarship, customer-due-diligence guidance, and principles of inclusive identity governance. Because no primary beneficiary dataset was supplied, the analytical component uses an explicitly labeled simulation involving 200 hypothetical applicants distributed equally across four verification pathways: document-only digital onboarding, assisted electronic know-your-customer verification, community-verified digital identity, and a hybrid community-plus-institutional review pathway.

Simulated first-attempt onboarding completion is 48%, 52%, 80%, and 94%, respectively. These values demonstrate the analytical framework and must not be interpreted as observed field effects. The study argues that community verification can contribute to financial inclusion only when the mechanism is embedded within a legally recognized, privacy-preserving, auditable, non-discriminatory, and risk-sensitive identity ecosystem. Community attestation should therefore function as additional evidence for identity resolution rather than as an uncontrolled substitute for formal identity assurance.

Keywords: digital identity; financial inclusion; community verification; e-KYC; identity exclusion; digital financial services; customer due diligence; inclusive finance.



1. Introduction

Identity is a foundational component of formal economic participation because individuals frequently need a reliable means of proving who they are before accessing regulated services, receiving public transfers, entering contractual relationships, or establishing financial accounts. The World Bank's Identification for Development initiative has emphasized the developmental importance of inclusive and trusted identification systems, while the G20 Digital Identity Onboarding report specifically connects legally recognized, unique, and digital identity with the ability of financial institutions to onboard customers efficiently. Earlier identification-for-development scholarship by Gelb and Clark also documented the rapid expansion of biometric identification programs across developing-country contexts and argued that identification infrastructure should be understood as a component of development policy rather than merely an administrative expense.

The difficulty is that identity systems designed around documentary completeness can reproduce social exclusion when individuals have incomplete documentary histories. The World Bank's Principles on Identification for Sustainable Development were originally developed around inclusion, robust system design, and accountable governance, emphasizing universal access, removal of barriers, privacy, user rights, institutional responsibility, and grievance mechanisms. These principles are particularly important for financial inclusion because inability to satisfy identity or customer-verification requirements can prevent an otherwise eligible individual from accessing an account. At the same time, weakening identity assurance without appropriate safeguards is not a sustainable solution. Financial institutions have legitimate obligations to identify customers, manage fraud risk, and comply with applicable customer-due-diligence and anti-money-laundering requirements. FATF's 2020 digital-identity guidance therefore recommends risk-based assessment of whether a digital identity system provides sufficient reliability for customer due diligence.

Community verification creates a potential bridge between these two requirements. In many communities, an individual whose administrative record is weak may nevertheless possess a socially well-established identity. Local institutions, community organizations, regulated agents, cooperatives, employers, recognized community representatives, or other approved verifiers may have long-standing knowledge of the individual. Converting such knowledge into structured digital attestations could provide supplementary evidence when conventional documents are insufficient. Yet informal recognition cannot simply be digitized and treated as definitive legal identity. Social relationships may contain bias, patronage, collusion, gender exclusion, caste or ethnic discrimination, conflicts of interest, or mistaken recognition. A defensible community-verification mechanism therefore requires multiple independent attestations, verifier accountability, consent, traceable records, conflict controls, duplicate screening, appeal procedures, and institutional escalation.

The financial implications of stronger identity systems are supported by earlier empirical work. Giné, Goldberg, and Yang demonstrated in rural Malawi that improved personal identification affected lending relationships because better identification strengthened a lender's ability to link current applicants with future repayment consequences. Muralidharan, Niehaus, and Sukhtankar found that biometric smartcards in Indian antipoverty programs could improve aspects of state capacity and service delivery, while Gelb and Decker examined the broader potential and operational limitations of biometric technologies in development programs. These studies do not directly establish the effectiveness of



community verification, but they demonstrate why reliable identity resolution matters for service access, institutional accountability, and transactions.

The present study consequently develops a community-verified digital identity model for financial inclusion. Community verification is deliberately defined as a supplementary identity-evidence mechanism operating within a broader regulated identity ecosystem rather than an alternative civil-registry system. The study integrates institutional trust, digital auditability, community knowledge, risk-based customer verification, privacy, and consumer protection. Its analytical contribution is demonstrated through a transparent simulation comparing four hypothetical onboarding pathways. The study does not claim that the simulated results represent actual bank customers or actual fraud-performance outcomes; instead, it provides an operational framework that can subsequently be validated through field pilots, randomized implementation studies, regulatory sandboxes, and longitudinal financial-inclusion research.

2. Objectives of the Study

2.1 Development of an Inclusive Identity-Verification Framework

The first objective is to develop an identity-verification framework capable of reducing avoidable financial exclusion among people who cannot satisfy conventional documentary requirements at the first point of onboarding. The proposed framework recognizes that identity proofing can involve multiple forms of evidence and that the reliability of an identity claim should be evaluated through the quality, independence, consistency, and auditability of that evidence rather than through a simplistic document-versus-no-document distinction.

Community verification is therefore conceptualized as structured attestation. Approved verifiers would not create an individual's legal identity by themselves. Instead, they would digitally attest to specified identity attributes or the continuity of a known individual within a community. Such attestations could supplement available documents, historical records, mobile credentials, institutional information, or other permissible evidence. The approach is consistent with the broader policy principle that identity systems should be inclusive while remaining robust, secure, responsive, and accountable.

2.2 Evaluation of Financial-Onboarding Accessibility and Governance

The second objective is to develop an analytical structure for comparing the accessibility of alternative identity-verification pathways. The study focuses on successful completion of formal financial onboarding because technically available financial products cannot improve inclusion when prospective users cannot cross the identification and verification stage. The comparison therefore considers a conventional document-only pathway, assisted e-KYC, community-supported verification, and a hybrid pathway combining community evidence with institutional review.

The objective is not to identify the pathway that approves the largest number of applicants regardless of risk. A credible financial-inclusion system must jointly consider accessibility, reliability, privacy, error correction, and regulatory acceptability. FATF guidance specifically frames digital identity use through risk-based assessment and appropriate assurance rather than assuming that all digital IDs are equally suitable for customer due diligence. The proposed framework therefore treats

successful inclusion as an outcome requiring both reasonable accessibility and defensible identity assurance.

3. Review of Literature

3.1 Identification Infrastructure and Financial Inclusion

Gelb and Decker's examination of biometric technology emphasized that dependable identification can support transfers and financial-service delivery while also introducing operational and technological challenges. Their work contributed to a larger literature recognizing identity as infrastructure rather than as an isolated administrative document. Gelb and Clark later surveyed extensive use of biometric identification across developing-country programs and argued that identification systems increasingly affected social transfers, financial access, public administration, elections, and other development applications.

The economic relevance of personal identification is also supported by experimental evidence from credit markets. Giné, Goldberg, and Yang's Malawi study showed that fingerprint-based identification changed incentives in a lending environment where weak identification made it difficult to reliably connect borrowers with future credit consequences. The study is important because it demonstrates that identification is not merely an onboarding formality. Identity reliability can influence the information structure governing repeated financial relationships, credit histories, repayment incentives, and institutional risk.

Digital identity extends these possibilities by allowing identity information to be verified electronically. The G20 Digital Identity Onboarding report examines how digital identification can facilitate financial access when the identity has appropriate legal recognition, uniqueness, and digital usability. Digital verification may reduce the reliance on repeated paper handling and can support remote or lower-cost onboarding, but digitalization alone does not resolve exclusion. If the underlying identity database omits an individual or contains incorrect information, digitization can reproduce the same barrier more efficiently.

3.2 Electronic KYC, Biometrics, and Identity Assurance

Electronic know-your-customer processes can reduce the time and administrative burden associated with conventional paper verification when reliable digital identity infrastructure is available. World Bank analysis has highlighted the potential of digital identification to improve the efficiency, security, privacy, and reliability of financial-sector identification while also warning that digital systems introduce technical risks and possible failure modes. Effective financial onboarding therefore depends not merely on digitizing documents but on establishing confidence in the identity-proofing and authentication processes through which a financial institution accepts a customer.

Biometric technologies represent one approach to strengthening uniqueness and authentication. Gelb and Clark's analysis of India's universal identification program showed that biometric identification could operate at very large scale, but accuracy depended on system design and the combined use of multiple biometric modalities. Muralidharan, Niehaus, and Sukhtankar's study of biometric smartcards in India further demonstrated that improved authentication technology can alter program implementation and service delivery. These findings are important for community verification because socially supplied

evidence should not be treated as a technological competitor to biometrics. Community knowledge and biometric uniqueness address different problems and can potentially be complementary.

FATF's digital-identity guidance provides an important governance boundary. The suitability of a digital identity for customer due diligence depends on understanding the assurance provided by identity proofing, enrollment, and authentication.

A community-verified mechanism must therefore specify what has actually been verified. A community member may know that an applicant has lived under a particular name for many years, but that does not necessarily establish date of birth, nationality, or every other legally required attribute. Attribute-level verification and clear assurance labeling are consequently preferable to treating community attestation as an undifferentiated identity certificate.

3.3 Community Verification, Inclusion, and Governance Risks

Community-based verification draws its potential value from information that exists socially but may be absent from formal databases. Local knowledge may help resolve identity continuity for people who lack standard documentary evidence, particularly when they are known to multiple independent institutions or community members. However, community attestation is fundamentally relational evidence. Its quality depends on who is permitted to attest, what they are attesting to, the duration and basis of their knowledge, whether they have conflicts of interest, and whether false attestations create consequences.

The World Bank's identification principles provide a useful governance foundation because they link inclusion with privacy, user control, institutional accountability, and grievance redress rather than treating broader enrollment as the only objective. This balance is essential. A community verification program could increase access while simultaneously producing new forms of social surveillance if individuals must disclose unnecessary personal information to local gatekeepers. It could also reproduce existing power inequalities if only dominant community actors are authorized to validate identity.

The literature therefore suggests that the strongest identity systems combine accessibility with graduated assurance. The present study extends this insight by proposing a hybrid evidence model in which community attestation contributes additional evidence when ordinary documentation is insufficient, while institutional review remains available for ambiguous or higher-risk cases. This approach also reflects FATF's emphasis on risk-based digital-identity assessment and the G20's broader concern with trusted digital identity for financial onboarding. Community verification is thus positioned as one layer within a larger identity-governance architecture rather than as an autonomous replacement for regulated identity proofing.

4. Research Methodology

4.1 Research Design and Simulated Population

The study adopts a conceptual-methodological research design supported by reproducible simulation. No actual applicants, bank customers, community verifiers, institutions, or geographic locations are represented in the analytical dataset. The simulation is used because primary field data were not supplied and presenting invented identity outcomes as observed empirical results would be methodologically inappropriate.



The hypothetical analytical population contains 200 applicants, divided equally among four identity-verification pathways. Each group therefore contains fifty simulated applicants. The first pathway represents document-only digital onboarding. The second represents assisted e-KYC in which an authorized agent supports applicants in completing digital identity verification. The third uses a community-verified digital identity process involving structured local attestations. The fourth applies a hybrid model in which community evidence is digitally recorded and then subjected to risk-based institutional review.

The principal simulated outcome is successful first-stage financial onboarding. The simulation does not attempt to estimate actual fraud or money-laundering rates because those outcomes require validated event data and long-term observation. A future empirical study should separately measure identity-verification accuracy, duplicate detection, false rejection, false acceptance, fraud incidence, appeal outcomes, onboarding time, cost per verified customer, demographic disparities, customer satisfaction, privacy incidents, and subsequent account activity.

4.2 Community-Verification Protocol

Under the proposed model, an applicant first provides available identity evidence and consents to the use of the community-verification pathway. Community attestation would be activated only where legally permissible and where ordinary evidence is insufficient for the relevant assurance level. At least two independently approved verifiers would confirm narrowly specified attributes based on direct knowledge of the applicant. The verifier's own identity would need to be established before the attestation could be accepted.

Every attestation would generate an auditable digital record containing the verifier identity, time of verification, attribute attested, basis of knowledge, consent record, and declared conflicts of interest. The system would check for repeated relationships between particular verifiers and applicants, unusually concentrated attestation patterns, duplicate identity signals, and contradictory information. Cases crossing predefined risk thresholds would not be automatically rejected; they would move to institutional review.

4.3 Measurement Framework and Proposed Questionnaire

The quantitative demonstration focuses on onboarding completion, but a responsible empirical evaluation must also measure trust, comprehension, autonomy, fairness, and perceived privacy. Five questionnaire items are therefore proposed for a future field study. They are proposed questions only and were not administered to the hypothetical applicants

Table 1: Proposed Measurement Framework for Community-Verified Digital Identity

No.	Evaluation Construct	Proposed Questionnaire Item	Measurement Purpose
1	Accessibility	“The identity-verification process allowed me to provide reasonable evidence even when standard documents were unavailable or	Assesses whether the process reduces documentary



No.	Evaluation Construct	Proposed Questionnaire Item	Measurement Purpose
		incomplete.”	exclusion
2	Comprehension	“I understood who was verifying my identity and how the information would be used.”	Evaluates transparency and informed participation
3	Community Trust	“I was comfortable with the approved community verifiers involved in confirming my identity information.”	Measures perceived legitimacy of the attestation process
4	Privacy and Control	“I felt that I could control which identity information was shared during the verification process.”	Evaluates perceived privacy and user agency
5	Appeal and Fairness	“I believe I would have a fair way to challenge or correct a verification decision if the system made a mistake.”	Measures procedural fairness and confidence in redress mechanisms

A future instrument should undergo cognitive testing, translation validation where necessary, expert review, pilot administration, and psychometric assessment. Responses should also be disaggregated across population groups because an average trust score can conceal exclusion concentrated among women, migrants, minority communities, people with disabilities, or socially marginalized groups.

5. Analysis

5.1 Comparative Simulated Onboarding Outcomes

The simulation generates different first-stage completion levels across the four verification pathways. The document-only digital pathway successfully onboards 24 of 50 simulated applicants, corresponding to 48%. Assisted e-KYC produces 26 completions, or 52%. The community-verified pathway produces 40 successful completions, representing 80%, while the hybrid community-plus-institutional pathway produces 47 completions, corresponding to 94%.

These values are synthetic scenario outputs, not estimates of real-world performance. Their purpose is to illustrate how an empirical study could test whether alternative verification architectures reduce identity-related onboarding failure. The relatively high simulated performance of the hybrid model reflects the analytical assumption that applicants who cannot be resolved through a single evidence source have an additional structured review opportunity rather than being immediately rejected.

Table 2: Simulated Financial-Onboarding Results by Identity-Verification Pathway

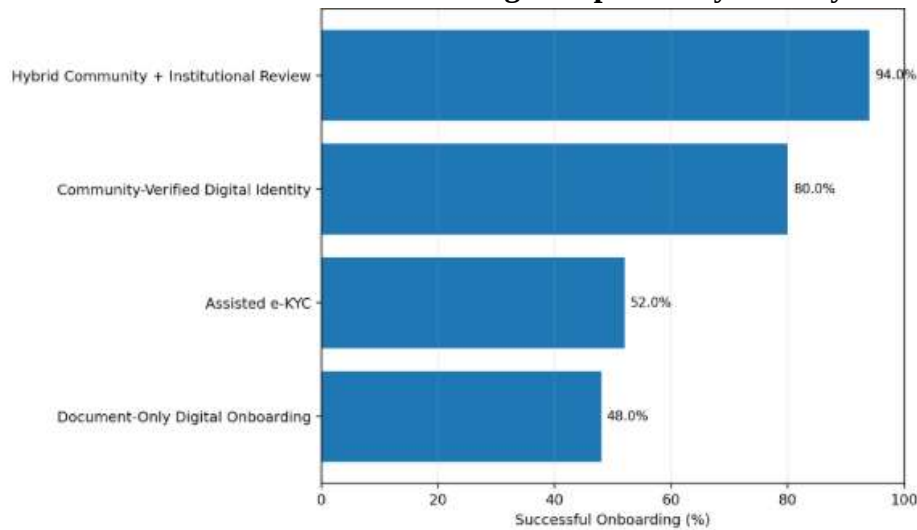
Verification Pathway	Simulated Applicants	Successful First-Stage Onboarding	Not Successfully Onboarded	Completion Rate	Difference From Document-Only Pathway
Document-Only Digital Onboarding	50	24	26	48.0%	Baseline
Assisted e-KYC	50	26	24	52.0%	+4 percentage points
Community-Verified Digital Identity	50	40	10	80.0%	+32 percentage points
Hybrid Community + Institutional Review	50	47	3	94.0%	+46 percentage points
Total	200	137	63	68.5% overall	—

The simulated progression illustrates an important distinction between verification standards and verification pathways. Reducing documentary exclusion does not necessarily require lowering identity requirements. It may instead involve giving applicants additional evidence channels through which the same underlying identity can be resolved. In this interpretation, inclusion emerges from evidence diversity and structured escalation rather than from unverified approval.

5.2 Identity Pathways and Financial-Inclusion Accessibility

The graph below presents the same simulated onboarding-completion outcome visually. It is an actual graph generated from the synthetic analytical dataset rather than a placeholder.

Graph 1: Simulated Formal-Finance Onboarding Completion by Identity Verification Pathway



The graph highlights the potential analytical value of layered verification. Document-only and assisted e-KYC pathways show similar simulated completion levels, suggesting that assistance alone cannot resolve every case if the fundamental problem is missing or inconsistent identity evidence. Community verification produces a substantial simulated increase because socially available evidence is converted into a structured digital form. The hybrid model produces the highest simulated completion because ambiguous cases receive an institutional escalation route.

The pattern should not be interpreted to mean that community verification inevitably produces higher approval rates in practice. Actual outcomes would depend on legal rules, civil-registration coverage, quality of community institutions, verifier training, system design, fraud controls, population mobility, user consent, and the underlying distribution of identity-document deficiencies.

5.3 Accessibility, Assurance, and Error Management

The most important analytical insight is that onboarding completion cannot serve as the sole performance indicator. A verification system approving 100% of applicants would be unacceptable if it could not reliably distinguish genuine identity claims from fraudulent or duplicate identities. Conversely, a highly restrictive system could achieve low fraud rates partly by excluding legitimate users. A meaningful evaluation therefore needs to analyze an accessibility-assurance frontier rather than maximize only one outcome.

Community verification may move this frontier when independent local knowledge adds credible information at comparatively low administrative cost. Its contribution is strongest when social evidence addresses a specific uncertainty, such as whether an applicant is consistently known under the claimed identity within a local setting. It is weaker for attributes that community verifiers cannot reasonably establish. The system should consequently store evidence at the attribute level and avoid claiming higher assurance than the evidence supports.

Error correction is equally important. No documentary, biometric, digital, or community system is completely error-free. The World Bank identification principles explicitly emphasize accountability,



privacy, user rights, and grievance mechanisms, while FATF digital-identity guidance emphasizes understanding system assurance and reliability. An inclusive verification architecture must therefore make correction and appeal part of the system design rather than treating them as exceptions occurring after system failure.

6. Discussion

6.1 Community Verification as Supplementary Identity Evidence

The conceptual contribution of this study is the separation of community evidence from legal identity authority. A person may be widely known within a village, neighborhood, cooperative, workplace, refugee community, or informal occupational network, but social recognition alone does not automatically satisfy the legal or regulatory requirements applied to a financial institution. Treating community attestation as equivalent to a national identity credential could create significant legal, fraud, and accountability risks.

A stronger interpretation treats community evidence as one input into identity resolution. This resembles the broader evolution of identity assurance toward multiple pieces of evidence, differentiated assurance levels, and risk-sensitive verification. FATF's 2020 guidance encourages regulated entities and authorities to understand the reliability and independence of digital identity systems used for customer due diligence. Community verification should therefore be acceptable only within a regulatory framework that defines when it can be used, which attributes it can support, and what additional review is required.

This distinction also protects community verifiers. Local actors should not be expected to make judgments about matters outside their knowledge. A verifier may be able to attest that an individual has been known locally for ten years under a particular name, while having no reliable knowledge of citizenship, precise birth date, or previous identities in other jurisdictions. Attribute-specific attestation allows the system to use social knowledge without transforming community members into unqualified compliance officers.

6.2 Financial Inclusion Without Weakening Identity Integrity

Financial inclusion and customer verification are sometimes framed as competing objectives. Such framing is unnecessarily restrictive. The G20 Digital Identity Onboarding work presents trusted digital identity as an enabler of financial access rather than as an obstacle to it, while FATF guidance supports risk-based approaches capable of recognizing reliable digital identity systems. The policy challenge is therefore to improve identity assurance while reducing avoidable procedural exclusion.

Earlier empirical evidence illustrates the economic importance of reliable identification. Giné, Goldberg, and Yang found that stronger personal identification changed incentives within Malawi's rural credit market, demonstrating that identity reliability can affect the functioning of financial relationships rather than merely account-opening paperwork. Similarly, biometric smartcard evidence from India demonstrates how identity-linked technology can alter program implementation when combined with institutional systems. These findings reinforce the argument that inclusive identity reform should improve both access and accountability.



The simulated results in the present study should consequently be understood as a hypothesis-generating illustration. The 94% hybrid completion result does not imply that real institutions can achieve that rate. Rather, it shows what should be tested: whether applicants rejected by standard documentary pathways can be safely resolved when independent community evidence and institutional review are added. A real pilot would need to compare not only acceptance rates but also false matches, duplicate identities, fraud attempts, appeals, verification costs, customer retention, and subsequent account activity.

6.3 Privacy, Social Power, and Responsible Governance

Community verification introduces ethical risks that differ from those of centralized digital identity. A centralized system may create concerns about surveillance, data concentration, cybersecurity, unauthorized linkage, and institutional misuse. A community system introduces additional risks involving interpersonal power. Applicants may fear that local leaders will learn sensitive personal information or that access to financial services will depend on social conformity.

The system must therefore minimize the information visible to community verifiers. A verifier does not need access to an applicant's bank balance, financial history, intended financial product, transaction data, or unrelated personal information merely because the verifier is confirming an identity attribute. Data minimization and purpose limitation are fundamental. The World Bank's identification principles explicitly connect trusted identification with privacy and user rights, and its ID4D work treats governance as a central component of inclusive system design.

Verifier diversity is equally important. Requiring two attestations is not sufficient when both verifiers belong to the same tightly connected authority structure. Systems should prevent systematic exclusion by allowing multiple categories of approved verifier, enabling confidential complaints, periodically auditing approval patterns, and examining whether particular groups experience unusually high rejection rates. Community verification becomes genuinely inclusive only when it provides an additional route into formal systems without transferring uncontrolled gatekeeping power from distant bureaucracies to local elites.

7. Conclusion

This study develops a community-verified digital identity framework intended to address one of the less visible barriers to financial inclusion: the inability of legitimate applicants to satisfy conventional identity-verification requirements despite possessing a socially established identity. The proposed model does not advocate replacing civil registration, national identity systems, regulated customer due diligence, or reliable digital identification. Instead, it introduces structured community attestation as supplementary evidence within an auditable and risk-based verification process.

The simulated comparison illustrates how the framework could be evaluated. Among 200 hypothetical applicants, first-stage onboarding completion is 48% for document-only digital onboarding, 52% for assisted e-KYC, 80% for community-verified digital identity, and 94% for the hybrid community-plus-institutional review pathway. These differences are intentionally synthetic and provide no empirical estimate of actual implementation effects. Their methodological purpose is to show how identity-accessibility outcomes can be compared without fabricating field evidence.



The broader conclusion is that community knowledge can be valuable only when transformed into accountable evidence. Effective implementation requires independently approved verifiers, informed consent, restricted attribute-level attestations, auditable digital records, conflict-of-interest controls, duplicate screening, risk-based escalation, privacy safeguards, accessible appeals, and institutional oversight. Community attestation should never become an informal permission system through which local elites determine who may participate in formal finance.

Future research should test the framework using controlled pilot programs in settings where documentary identity gaps materially restrict formal financial access. Studies should measure onboarding completion alongside false rejection, false acceptance, identity fraud, verification time, cost, privacy perceptions, demographic disparities, appeal outcomes, and subsequent account usage. Longitudinal analysis will also be required to determine whether better identity onboarding leads to durable financial inclusion rather than one-time account creation. The most valuable community-verified identity system will therefore be neither the system that approves the most applicants nor the system that imposes the strictest verification.

References

1. Chowdhry, B., Goyal, A., & Ahmed, S. (2021). Digital Identity in India. In *India Studies in Business and Economics*. Springer/Palgrave Macmillan.
2. Carrière-Swallow, Y., Haksar, V., & Patnam, M. (2021). *Stacking Up Financial Inclusion Gains in India*. IMF Finance & Development.
3. Khera, P., Ng, S. Y., Ogawa, S., & Sahay, R. (2021). Is Digital Financial Inclusion Unlocking Growth? *IMF Working Paper*, 2021/167.
4. Addo, A., & Senyo, P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly*, 38(2), 101568.
5. Krishna, S. (2021). Digital identity, datafication and social justice: Understanding Aadhaar use among informal workers in south India. *Information Technology for Development*, 27(1).
6. Allen, F., Demirgüç-Kunt, A., Klapper, L., & Martinez Peria, M. S. (2016). The foundations of financial inclusion: Understanding ownership and use of formal accounts. *Journal of Financial Intermediation*, 27, 1–30.
7. Demirgüç-Kunt, A., Klapper, L., Singer, D., & Van Oudheusden, P. (2015). *The Global Findex Database 2014: Measuring Financial Inclusion around the World*. World Bank.
8. Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. World Bank.
9. Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2022). *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*. World Bank.
10. Karlan, D., Ratan, A. L., & Zinman, J. (2014). Savings by and for the poor: A research review and agenda. *Review of Income and Wealth*, 60(1), 36–78.
11. Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106(10), 2895–2929.



12. Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution. *Center for Global Development Working Paper No. 315*.
13. Gelb, A., & Metz, A. D. (2018). Identification revolution: Can digital ID be harnessed for development? *Center for Global Development*.
14. D'Silva, D., Filková, Z., Packer, F., & Tiwari, S. (2019). The design of digital financial infrastructure: Lessons from India. *BIS Papers No. 106*. Bank for International Settlements.
15. Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science*, 354(6317), 1288–1292.
16. Jack, W., & Suri, T. (2014). Risk sharing and transactions costs: Evidence from Kenya's mobile money revolution. *American Economic Review*, 104(1), 183–223.
17. Kumar, C., & Mishra, S. K. (2011). Banking access and household welfare: Evidence from India. *Journal of Development Economics*.
18. Swamy, V. (2014). Financial inclusion, gender dimension, and economic impact on poor households. *World Development*, 56, 1–15.
19. Gupta, S., & Kanungo, R. P. (2022). Financial inclusion through digitalisation: Economic viability for the bottom of the pyramid segment. *Journal of Business Research*, 148, 262–276.
20. Financial Stability Board. (2021). *Digital ID to Enhance Financial Inclusion: A Toolkit for Regulatory Authorities*. Financial Stability Board.