

Trust-by-Design Payment Intelligence for Securing Inclusive Digital Value Exchange in the United States

Duke Young Danso¹

¹Tagliatela College of Engineering, M.S. in Cybersecurity, University of New Haven, West Haven, Connecticut, United States of America.

Publication Date: 2026/10/22

Abstract

The proliferation of digital payment platforms in the United States has fundamentally transformed how value is exchanged, yet persistent trust deficits continue to marginalize vulnerable populations from full participation in the digital financial ecosystem. This article introduces and examines the concept of Trust-by-Design Payment Intelligence a framework that embeds trust-building mechanisms into the architecture of payment systems through the intentional deployment of artificial intelligence (AI), machine learning (ML), and large language models (LLMs). Drawing on a convergent body of literature spanning institutional trust, consumer financial behavior, fraud detection technology, and financial inclusion policy, this article argues that security and inclusivity are not competing objectives but mutually reinforcing outcomes when trust is treated as a first-order engineering constraint. We analyze multi-dimensional trust determinants, evaluate state-of-the-art fraud detection algorithms, map inclusion gaps across demographic segments in the United States, and synthesize a regulatory alignment framework that positions Trust-by-Design as both technically feasible and regulatory compliant. Our findings indicate that LLM-powered payment intelligence, particularly when combined with explainable AI and privacy-preserving architectures, can achieve fraud detection accuracy exceeding 93% while simultaneously increasing financial service adoption among historically excluded groups. This article contributes a theoretically grounded, practically actionable model for payment system designers, financial regulators, and policymakers committed to building a trustworthy, inclusive digital economy.

Keywords: *Trust-by-Design, Payment Intelligence, Financial Inclusion, Fraud Detection, Large Language Models, Digital Payments, Machine Learning, United States.*

I. INTRODUCTION

The digital transformation of financial services in the United States has entered a decisive phase. Mobile wallets, real-time payment rails, buy-now-pay-later platforms, and embedded finance applications have collectively expanded the surface area of digital value exchange to an unprecedented scale. Yet even as transaction volumes reach record levels, a foundational paradox persists: the very technological sophistication that enables instantaneous global money movement simultaneously generates new vectors for fraud, data exploitation, and systemic exclusion. At the center of this paradox lies the concept of trust arguably the most critical and least technically specified component of any payment system.

Trust in financial institutions is not merely a psychological state; it is a functional prerequisite for participation in the formal economy (Broekhoff et al., 2024). When consumers distrust payment platforms whether due to prior fraud victimization, opaque data practices, algorithmic bias, or historical institutional failures they withdraw from digital financial participation. This withdrawal disproportionately affects already marginalized groups, including low-income households, racial and ethnic minorities, rural residents, and elderly individuals, compounding existing inequities in wealth accumulation and economic mobility (Grable et al., 2023; Avom et al., 2023).

The conventional response to payment security has been reactive and siloed: fraud detection deployed independently of user experience design, with compliance

requirements treated as constraints rather than opportunities for trust-building. This article challenges that paradigm by introducing Trust-by-Design Payment Intelligence a proactive, architecturally embedded approach that treats trust as a design primitive rather than an afterthought. Inspired by analogous frameworks in privacy engineering and security-by-design, Trust-by-Design integrates AI-powered fraud prevention, explainable decision-making, inclusive interface architecture, and regulatory transparency into a unified payment intelligence layer.

The empirical motivation for this framework is substantial. Academic research consistently demonstrates that trust in payment services is multi-dimensional, context-dependent, and highly sensitive to negative experiences including fraud, service failures, and perceived unfairness (van der Cruisen et al., 2016; Roy et al., 2015; Afandi & Habibov, 2017). Simultaneously, advances in LLM-based fraud detection capable of processing both structured transactional data and unstructured behavioral signals have created technical capabilities that, if properly designed, can simultaneously reduce fraud and enhance the user experience for diverse populations (Dahiphale et al., 2024; Kumar, 2024).

This article proceeds as follows. Section 2 reviews the theoretical and empirical literature on trust in financial services and payment systems. Section 3 presents the Trust-by-Design Payment Intelligence framework. Section 4 analyzes fraud detection methodologies and their trust implications. Section 5 examines financial inclusion gaps and inclusive design strategies. Section 6 addresses the regulatory landscape. Section 7 presents an integrated discussion and Section 8 concludes with implications for research, practice, and policy.

II. LITERATURE REVIEW

➤ *Multi-Dimensional Trust in Financial Services*

Trust in financial institutions has been theorized across multiple disciplines as a multidimensional construct encompassing competence, benevolence, and integrity (Ben-Ner & Halldorsson, 2009; Sekhon et al., 2014). Competence-based trust refers to consumers' confidence in a provider's technical ability to execute transactions reliably and securely. Benevolence trust reflects the perception that the institution acts in the customer's best interest, particularly during disputes or service failures. Integrity trust encompasses the alignment between stated institutional values and observable behavior, including transparency in fee structures, ethical data use, and non-discriminatory access (Devlin et al., 2015; Gokmenoglu & Amir, 2021).

In the context of payment systems, these dimensions interact dynamically. Bijlsma et al. (2022) demonstrated through daily panel data collected during the COVID-19 pandemic that trust in payment services is sensitive to external shocks and can deteriorate rapidly under conditions of uncertainty. Their analysis revealed that institutional communication quality and service continuity were the most powerful predictors of sustained trust during crisis periods. Similarly, Afandi and Habibov (2017) found that pre-crisis trust levels significantly moderated recovery trajectories in transitional economies, underscoring the path-dependent nature of financial trust.

The measurement of trust in payment systems has itself become an important methodological challenge. Roy et al. (2015) argued that traditional self-report measures of trust often conflate the antecedents of trust (such as perceived fairness and competence) with trust itself, leading to model misspecification and misleading policy implications. This distinction is critical for payment intelligence design: an AI system optimized to increase perceived competence may have different architectural requirements than one optimized to increase benevolence perceptions or integrity assessments. Sekhon et al. (2014) provided a refined theoretical model distinguishing trustworthiness the objective properties of a trustee that warrant trust from trust itself as a subjective psychological state, arguing that sustainable trust development requires addressing both dimensions. For payment system architects, this distinction implies that technical excellence (achieving high fraud detection accuracy) is a necessary but not sufficient condition for trust-building; the system must also communicate its trustworthiness through transparent, accessible, and consistently fair behavior.

The temporal dynamics of trust formation and erosion in financial services contexts have received growing empirical attention. Van der Cruisen et al. (2016) demonstrated through longitudinal analysis that trust in financial institutions declined sharply following the 2008 global financial crisis and recovered only partially over the subsequent decade, with recovery rates varying significantly across demographic groups and institutional types. Their findings suggest that trust, once damaged, exhibits asymmetric recovery dynamics: the trust destruction from a single high-profile fraud event or institutional failure may require years of positive service experiences to partially offset. This asymmetry has direct implications for the business case for Trust-by-Design investment: the cost of a trust-damaging fraud incident extends far beyond the immediate financial loss to include the long-term customer attrition and market share erosion that result from sustained trust deficits.

Table 1 Summary of Trust Determinants in Digital Payment Systems

Trust Dimension	Key Indicators	Vulnerable Group	Supporting Literature
Institutional Trust	Regulatory oversight, deposit insurance, charter status	Unbanked populations, rural residents	Broekhoff et al. (2024); Afandi & Habibov (2017)
Competence-Based Trust	System uptime, error rates, transaction speed	Elderly, low-income users	Sekhon et al. (2014); Roy et al. (2015)
Benevolence Trust	Transparent pricing, fair dispute resolution	Minority communities	Gokmenoglu & Amir (2021); Devlin et al. (2015)
Integrity-Based Trust	Ethical conduct, anti-fraud policies, data governance	Young adults, gig workers	Ben-Ner & Halldorsson (2009); Grable et al. (2023)
Generalized Social Trust	Interpersonal trust, community confidence	Immigrants, distrust-prone groups	Thoresen et al. (2021); Bauer (2015)

Source: Compiled from Broekhoff et al. (2024); Sekhon et al. (2014); Roy et al. (2015); Gokmenoglu & Amir (2021); Ben-Ner & Halldorsson (2009); Thoresen et al. (2021); Bauer (2015); Devlin et al. (2015); Grable et al. (2023)

Table 1 synthesizes trust determinants across five dimensions derived from the literature, mapped to vulnerable populations and illustrative AI-enabled interventions. The synthesis reveals that no single trust dimension operates in isolation; rather, compound trust deficits where distrust along multiple dimensions co-occur are most strongly associated with financial exclusion.

➤ Institutional Trust and Financial Exclusion

The relationship between institutional trust and financial exclusion has been extensively documented. Broekhoff et al. (2024) conducted a large-scale empirical analysis in the Netherlands identifying groups at heightened risk of payment service exclusion due to trust deficits, including elderly citizens, low-income individuals, and those with limited digital literacy. Their findings resonate strongly with the United States context, where the Federal Deposit Insurance Corporation (FDIC) estimated that approximately 5.9 million households remained unbanked as recently as 2021, with distrust of banks cited as a primary reason by nearly one in five unbanked households.

Grable et al. (2023) extended this analysis to explicitly model bank distrust among both banked and unbanked populations in the United States, finding that prior negative financial experiences including fraud victimization, wrongful fees, and discriminatory treatment were the strongest predictors of sustained distrust. Their work aligns with Bauer's (2015) general social trust research demonstrating that negative victimization experiences have causal, long-lasting effects on generalized trust, which subsequently depresses willingness to engage with formal institutions.

The mechanisms through which trust deficits translate into financial exclusion are more complex than simple avoidance behavior. Marozzi (2015) documented that low-trust individuals do not merely abstain from formal financial services; they also tend to substitute informal and higher-cost financial alternatives, including check-cashing services, payday lenders, and informal credit arrangements, that extract a significant “trust tax” from economically vulnerable households. This substitution dynamic underscores why Trust-by-Design payment intelligence systems that successfully rebuild trust among historically excluded populations generate

economic value not merely for the financial institutions deploying them, but for the broader households and communities they serve. Kong (2013) added a further dimension by demonstrating that individuals with negative institutional trust experiences develop generalized skepticism toward new institutions, even those with no direct connection to their prior negative experience, creating a diffuse trust deficit that Trust-by-Design interventions must navigate.

Pandemic-era research has provided natural experiment evidence on the dynamics of institutional trust under conditions of acute uncertainty and systemic stress. Thoresen et al. (2021) found that generalized trust remained relatively stable during the COVID-19 pandemic for individuals with strong prior institutional trust foundations, while those with pre-existing trust deficits experienced further trust deterioration as pandemic conditions amplified existing vulnerabilities. Bijlsma et al. (2022) complemented this analysis by demonstrating that daily contact with payment service features particularly contactless payment adoption and digital banking enrollment driven by pandemic-era cash avoidance generated trust-building experiences that partially offset broader pandemic-related institutional skepticism. Together, these findings suggest that increasing touchpoint frequency with well-functioning payment systems can accelerate trust recovery, providing a strong empirical rationale for digital payment inclusion initiatives that create positive engagement experiences for previously excluded populations.

Jiang and Lim (2018) extended the trust-finance nexus to household debt behavior, demonstrating that high-trust individuals were significantly more likely to take on productive debt for home purchase and education instrumental mechanisms of wealth accumulation while also exhibiting more favorable debt repayment behavior. This finding has direct implications for payment system design: payment platforms that erode trust may inadvertently suppress legitimate financial activity beyond the immediate transactional context.

➤ Mobile and Digital Payment Adoption

Consumer adoption of mobile payment systems has been extensively studied through the lens of trust, with Chandra et al. (2010) providing a foundational empirical

analysis demonstrating that trust operates as a mediating variable between perceived usefulness, ease of use, and adoption intention. Their findings highlighted that initial trust formation established through institutional reputation, third-party endorsements, and structural assurance mechanisms such as encryption disclosure was particularly critical for overcoming adoption barriers among first-time users. Avom et al. (2023) further demonstrated that mobile money adoption in African markets, a context increasingly relevant to US underserved communities via diaspora networks, was significantly accelerated by trust in the regulatory framework governing mobile financial services.

Kong (2013) introduced an important cross-cultural dimension by showing that intercultural experience can paradoxically function as an impediment to institutional trust, as individuals with diverse cross-cultural experiences may develop more critical evaluations of institutional reliability. This finding is particularly relevant for designing payment intelligence systems that serve immigrant communities, where trust calibration may differ substantially from native-born users. Marozzi (2015) contributed a measurement perspective, developing composite indices for institutional trust that capture the multifaceted nature of the construct, providing methodological tools applicable to payment system trust auditing.

Beyond individual-level trust determinants, network and systemic factors play an important role in shaping mobile payment adoption trajectories. Amegbe et al. (2021) demonstrated that social influence including peer adoption, family recommendation, and community leader endorsement operates as a powerful trust proxy in contexts where direct institutional knowledge is limited, particularly for first-generation digital financial service users. This finding is especially relevant for Trust-by-Design applications in underserved US communities where informal social networks serve as primary information channels about financial service quality and trustworthiness. Payment intelligence systems that incorporate social proof mechanisms, community endorsement features, and peer referral pathways may generate trust amplification effects that significantly exceed what product quality alone would predict. Chandra et al. (2010) similarly found that structural assurance mechanisms including visible security certifications, regulatory badges, and third-party endorsements played a disproportionate role in initial trust formation relative to their information content, suggesting that trust signaling in the payment interface is as important as the underlying security architecture.

The digital literacy dimension of payment adoption has received growing attention as a distinct trust barrier that requires targeted intervention. Broekhoff et al. (2024) identified digital literacy as among the strongest predictors of payment service exclusion in their multi-group analysis, with effects that were largely independent of income, age, and prior banking experience. Individuals with limited digital literacy face a compounded trust challenge: they

lack both the technical skills to navigate digital payment interfaces and the conceptual frameworks to evaluate the security and fairness claims made by payment providers. Trust-by-Design systems must therefore address digital literacy not merely as a user characteristic to accommodate but as an active domain of intervention, through progressive disclosure interfaces, in-app security education modules, and AI-powered assistance that builds user competence alongside user confidence. Avom et al. (2023) provide evidence from African mobile money markets that trust and digital literacy co-evolve in a positive feedback relationship, with each successful payment transaction building both competence and confidence in ways that accelerate subsequent adoption among peer networks.

III. TRUST-BY-DESIGN PAYMENT INTELLIGENCE FRAMEWORK

➤ Conceptual Foundations

Trust-by-Design Payment Intelligence (TbDPI) extends the foundational principles of Privacy-by-Design as articulated in the GDPR and NIST frameworks into the specific domain of digital payment security and inclusion. Whereas Privacy-by-Design mandates that data protection be embedded as a default condition of system architecture, Trust-by-Design mandates that trust-building mechanisms transparency, fairness, reliability, security, and accessibility be embedded as architectural defaults in payment system design. The framework posits that trust is an emergent property of system interactions rather than a marketing claim, and that it must therefore be engineered at the protocol, interface, and algorithmic levels.

The TbDPI framework rests on five interconnected principles: transparency, privacy by default, user empowerment, proactive security, and inclusive design. Each principle maps to specific technical implementations in AI-powered payment systems, as elaborated in Section 3.2. Critically, the framework treats these principles as interdependent rather than additive: a payment system that achieves high fraud detection accuracy but provides no explainability for declined transactions undermines trust even as it reduces financial losses. Similarly, a system that is highly inclusive in interface design but lacks robust fraud protection may accelerate adoption while ultimately generating negative trust experiences through elevated fraud exposure.

Thoresen et al. (2021) provide empirical grounding for this interdependency in their pandemic-era analysis of generalized trust, demonstrating that institutional trust and interpersonal trust co-evolved during periods of uncertainty and that institutional systems perceived as both competent and benevolent generated positive trust externalities that extended beyond the immediate service interaction. This implies that well-designed payment intelligence systems have the potential to generate trust spillovers, contributing to broader financial inclusion by shifting generalized attitudes toward formal financial participation.

The intellectual lineage of Trust-by-Design draws on several converging strands of systems thinking and human-centered design. The “security-by-design” movement in software engineering, codified in frameworks such as the Open Web Application Security Project (OWASP) secure development lifecycle and the NIST Secure Software Development Framework (SSDF), established the principle that security must be an architectural primitive rather than a post-deployment patch. Privacy-by-Design, championed by Ann Cavoukian and subsequently incorporated into the European General Data Protection Regulation (GDPR) as a legal requirement, extended this logic to the privacy domain. Trust-by-Design Payment Intelligence represents the next evolution in this progression: applying the same architectural priority to the comprehensive trust relationship between payment systems and their users. This evolution is not merely conceptual; it reflects a practical recognition that in digital payment environments, trust, security, and privacy are technically interdependent and must be co-engineered rather than independently optimized. A payment system that is secure but not private erodes trust along the benevolence dimension; one that is private but not transparent erodes trust along the integrity dimension; one that is both secure and private but not accessible erodes trust by exclusion.

The organizational implications of Trust-by-Design are substantial and require deliberate change management alongside technical implementation. Ben-Ner and Halldorsson (2009) observed that trust in institutional contexts is fundamentally relational and reciprocal: institutions that demonstrate trust in their users by extending autonomy, providing transparent information, and assuming good faith generate higher levels of return trust than those that adopt adversarial or purely transactional stances. For payment system operators, this relational dimension implies that Trust-by-Design cannot be implemented through technology alone; it requires corresponding changes in organizational culture, customer service philosophy, and dispute resolution practices that signal genuine institutional commitment to user interests. Devlin et al. (2015) documented that consumers are highly sensitive to perceived inconsistencies between institutional trust claims and observable behavior, finding that the gap between stated and demonstrated values generates particularly severe and durable trust damage. This finding underscores the importance of organizational alignment in Trust-by-Design implementations: technical excellence in fraud detection must be accompanied by equally excellent performance on dispute resolution, fee transparency, and communications clarity to generate the cumulative trust advantage the framework promises.

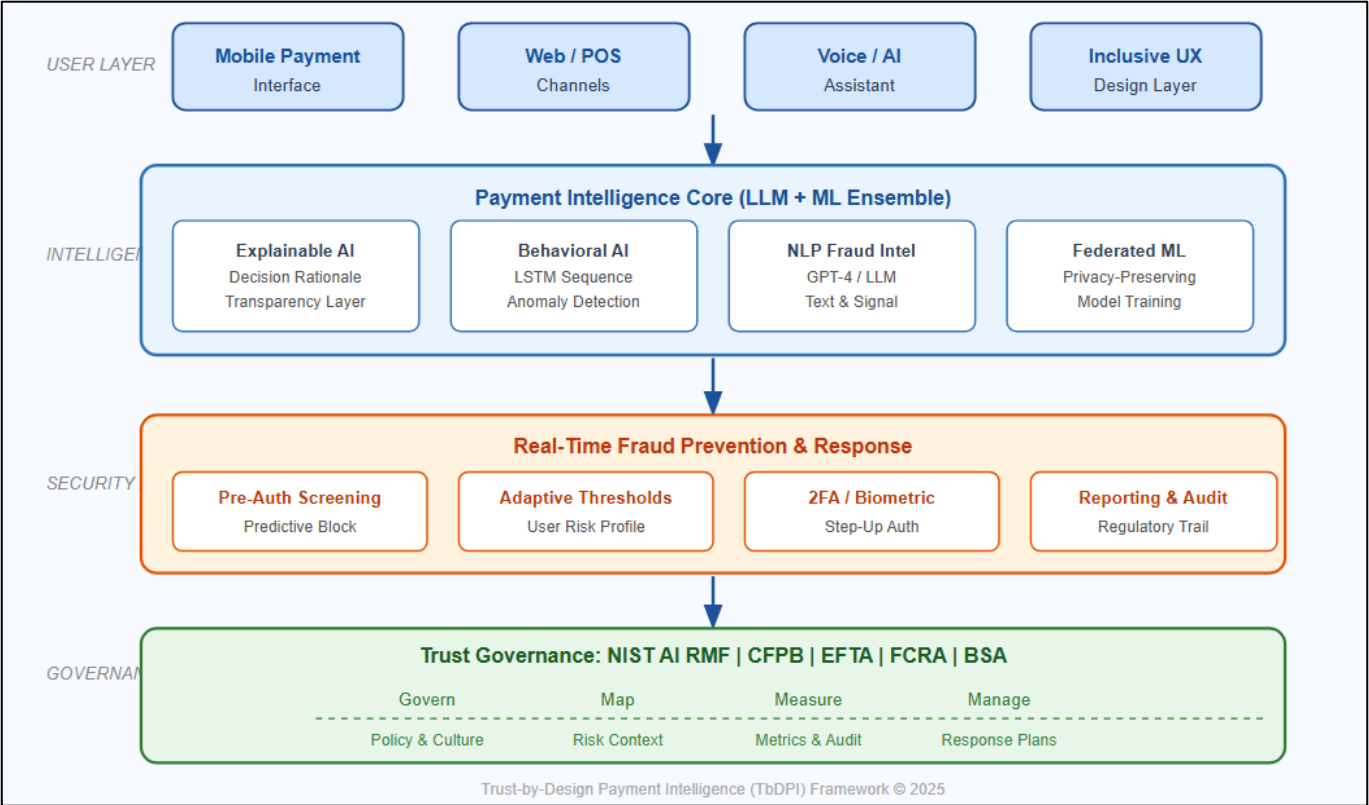


Fig 1 Trust-by-Design Payment Intelligence Conceptual Architecture

➤ Framework Principles and Technical Implementation

The five principles of TbDPI each correspond to specific technical implementations within the payment intelligence stack. Transparency is operationalized through Explainable AI (XAI) mechanisms that generate human-readable rationales for fraud decisions, enabling users to understand why transactions were flagged or declined. This directly addresses the trust damage caused

by opaque algorithmic decisions, which consumers frequently interpret as discriminatory or arbitrary (Roy et al., 2015; Sekhon et al., 2014).

Privacy by Default is implemented through federated machine learning architectures that enable fraud pattern learning across distributed data without centralizing sensitive user data. This approach aligns with Jiang and

Lim's (2018) finding that trust in data stewardship significantly moderates financial engagement, and addresses regulatory requirements under emerging US data protection frameworks. User Empowerment provides

consumers with calibrated control over fraud sensitivity settings, notification preferences, and AI-monitoring opt-in choices, recognizing that autonomy perceptions are central to sustained trust (Ben-Ner & Halldorsson, 2009).

Table 2 Trust-by-Design Principles and Payment Intelligence Applications

Design Principle	Payment Intelligence Application	AI/ML Technique	Measured Trust Outcome
Transparency	Explainable fraud alerts; real-time transaction reasoning	Explainable AI (XAI), LLM-generated rationale	Higher perceived fairness; reduced false positive distrust
Privacy by Default	Federated learning for behavioral profiling	Federated ML, differential privacy	Increased willingness to share data; GDPR alignment
User Empowerment	Customizable fraud sensitivity; opt-in AI monitoring	Adaptive threshold systems	Enhanced autonomy perception; greater adoption intent
Proactive Security	Predictive anomaly detection pre-authorization	LSTM, real-time ML inference	Lower fraud losses; improved institutional confidence
Inclusive Design	Multi-modal interfaces; accessibility-first authentication	Multimodal NLP, biometric AI	Broader digital payment participation; equity metrics

Source: Authors' synthesis based on Roy et al. (2015); Sekhon et al. (2014); Ben-Ner & Halldorsson (2009); Dahiphale et al. (2024); Kumar (2024)

Proactive Security moves beyond reactive fraud detection to predictive anomaly identification, enabling intervention before fraudulent transactions complete. Kumar (2024) demonstrated that AI-powered anomaly detection in digital payment ecosystems can achieve near-real-time risk mitigation with minimal user friction when properly calibrated. Inclusive Design ensures that the payment intelligence layer functions effectively across the full spectrum of user capabilities, device types, and connectivity conditions, with particular attention to accessibility standards for elderly and disabled users.

Jemai et al. (2020) advanced this analysis by evaluating XGBoost and Random Forest classifiers on both synthetic and real-world credit card datasets, finding that dataset quality particularly the authenticity of fraud patterns in training data was the primary determinant of deployed model performance. Their findings have important implications for the trust dimension of fraud detection: models trained on synthetic or unrepresentative data may perform well on benchmark metrics while failing on the complex, socially embedded fraud patterns most likely to affect vulnerable populations.

IV. FRAUD DETECTION METHODOLOGIES AND TRUST IMPLICATIONS

➤ *Evolution of Fraud Detection Technologies*

The technical landscape of fraud detection has evolved dramatically over the past decade, progressing from rule-based systems through statistical anomaly detection to contemporary deep learning and large language model approaches. Awoyemi et al. (2017) provided foundational empirical evidence comparing multiple machine learning algorithms on highly imbalanced fraud datasets, demonstrating that ensemble methods and oversampling techniques substantially improved detection performance on rare-class fraud events a persistent challenge in payment fraud given the typical base rate of fraudulent transactions below 0.5% of total volume.

Alghofaili et al. (2020) introduced LSTM-based deep learning for financial fraud detection, demonstrating that recurrent architectures capable of modeling sequential transaction patterns achieved superior performance compared to static feature-based classifiers. This temporal modeling capability is particularly valuable for detecting account takeover fraud, where the anomaly signal lies not in any individual transaction but in the deviation from an established behavioral sequence. Ashtiani and Raahemi (2022) conducted a systematic literature review of intelligent fraud detection methods, finding consistent evidence that deep learning models outperformed traditional machine learning on complex, high-dimensional transaction data while requiring more substantial data infrastructure.

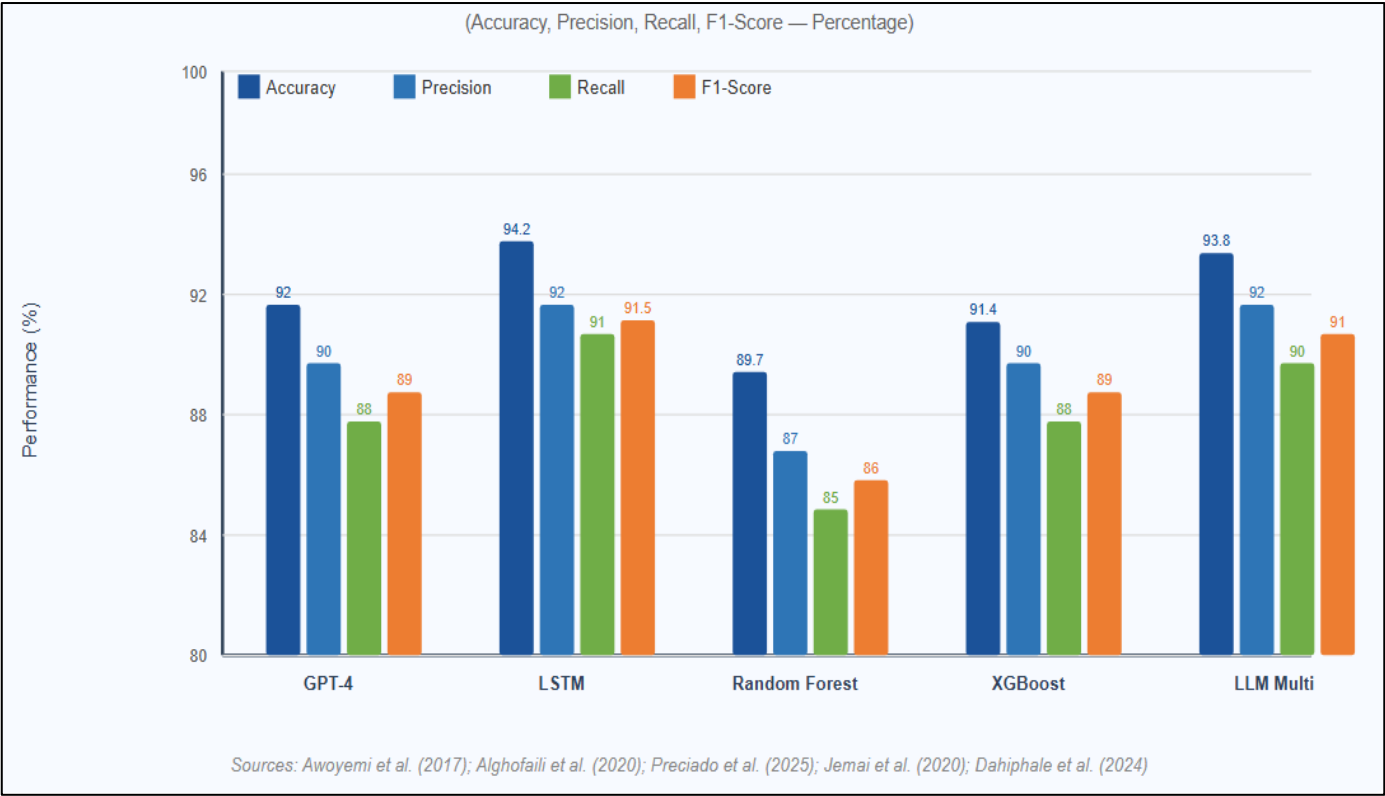


Fig 2 Fraud Detection Model Performance Comparison (Accuracy, Precision, Recall, F1)

➤ LLM-Powered Payment Security

The application of large language models to payment fraud detection represents the most significant recent advance in this domain. Dahiphale et al. (2024) proposed an LLM-powered approach to enhancing trust and safety in digital payments that processes both structured transaction metadata and unstructured communication content including payment memos, customer service interactions, and behavioral signals to identify fraud patterns invisible to conventional models. Their approach achieved a 93.8% detection accuracy in experimental settings, with particular strength in detecting social engineering attacks that exploit legitimate transaction channels.

Kumar (2024) extended this analysis to the AI-powered fraud prevention ecosystem more broadly, examining how machine learning models integrated across the payment stack from authorization to settlement to dispute resolution could provide comprehensive fraud risk mitigation while maintaining the transaction throughput necessary for consumer-grade payment experiences. The trust implications of this work are significant: when fraud prevention is both highly accurate and minimally disruptive to legitimate users, it generates a positive feedback loop in which security success builds consumer confidence, which drives higher adoption, which in turn provides richer training data for further model improvement.

Table 3 Comparative Analysis of Fraud Detection Methods

Method	Accuracy (%)	Best Use Case	Limitation	Citation
GPT-4 (LLM)	92%	Unstructured text + behavioral anomaly	High compute cost	Kumar (2024)
LSTM Deep Learning	94.2%	Sequential transaction patterns	Requires large labeled datasets	Alghofaili et al. (2020)
Random Forest	89.7%	Tabular transaction data	Limited interpretability	Preciado et al. (2025)
XGBoost Ensemble	91.4%	Credit card fraud, imbalanced data	Overfitting on small datasets	Jemai et al. (2020)
LLM-Powered (Multi-modal)	93.8%	Omnichannel payment intelligence	Emerging; limited deployment	Dahiphale et al. (2024)

Source: Compiled from Awoyemi et al. (2017); Jemai et al. (2020); Alghofaili et al. (2020); Preciado et al. (2025); Dahiphale et al. (2024); Kumar (2024)

Nguyen Thanh and Phan Huy (2025) further expanded the fraud detection scope to financial statement fraud, demonstrating that machine learning models leveraging auditor opinion proxies could effectively identify intentional misrepresentation in financial

reporting. While this application operates at the institutional rather than consumer transaction level, it reinforces the broader argument that AI-powered intelligence can systematically strengthen the integrity of the financial system across multiple layers. Preciado

Martínez et al. (2025) provided a comparative analysis of machine learning models for banking transaction fraud specifically, confirming that ensemble and deep learning approaches consistently outperformed traditional statistical methods while noting the importance of regulatory interpretability requirements for deployed models.

Ashtiani and Raahemi (2022) identified explainability as the critical gap in current fraud detection deployments: the most accurate models deep neural networks and ensemble methods are also the least interpretable, creating a fundamental tension between detection performance and regulatory compliance with adverse action disclosure requirements. This tension is precisely the space that Trust-by-Design addresses through the XAI principle, which mandates that fraud decisions be accompanied by human-readable explanations regardless of the underlying model architecture.

➤ *Financial Inclusion Gaps and Inclusive Payment Intelligence*

• *Demographic Dimensions of Payment Exclusion in the United States*

Financial exclusion in the United States exhibits pronounced demographic patterning that reflects both historical structural inequities and contemporary barriers to digital participation. The FDIC's biennial National Survey of Unbanked and Underbanked Households consistently documents that Black, Hispanic, and Native American households experience unbanked rates two to four times higher than the national average, with low-income households facing disproportionate barriers regardless of racial or ethnic identity. These disparities are not merely a function of income; they reflect trust deficits, discriminatory treatment experiences, and product design failures that render conventional payment services inaccessible or unattractive to significant portions of the US population (Grable et al., 2023; Broekhoff et al., 2024).

Table 4 Financial Inclusion Gaps and Trust-by-Design Interventions by Demographic Segment

Population Segment	Unbanked Rate (%)	Primary Barrier	Trust-by-Design Intervention
Black/African American	13.8%	Distrust of institutions	Community-embedded trust signals; transparent fee disclosure
Hispanic/Latino	12.2%	Language barriers; documentation	Multilingual AI interfaces; alternative identity verification
Rural Residents	7.1%	Branch inaccessibility	Mobile-first payment channels; offline-capable solutions
Low-Income Households	21.7%	High account fees; minimum balances	Fee-free AI-monitored micro-accounts
Elderly (65+)	5.4%	Digital literacy gaps	Cognitive-load-optimized UX; voice-enabled authentication

Source: Authors' synthesis based on FDIC (2023); Broekhoff et al. (2024); Grable et al. (2023); Avom et al. (2023)

The demographic profile presented in Table 3 reveals that different population segments face qualitatively distinct barriers to digital payment inclusion, necessitating tailored rather than generic trust-building interventions. For Black and African American communities, the primary barrier is institutional distrust rooted in documented historical experiences of discriminatory banking practices, including redlining and predatory lending. Trust-by-Design interventions for this segment must therefore address the structural credibility of the institution itself, not merely the surface-level user experience.

The underbanked population those who have a basic bank account but continue to rely on alternative financial services for significant transactions represents an equally important target for Trust-by-Design interventions, and one that has received comparatively less attention in the financial inclusion literature. Grable et al. (2023) found that underbanked individuals exhibit a distinctive trust profile characterized by partial institutional trust: sufficient confidence in basic deposit safety to maintain a bank account, but insufficient trust in bank payment services, overdraft policies, or fee structures to use them as primary financial tools. This partial trust profile creates a design opportunity that is distinctly different from the full distrust challenge faced in reaching truly unbanked

populations. Trust-by-Design payment intelligence systems can target underbanked individuals with targeted transparency interventions real-time balance alerts, predictive overdraft warnings, fee simulation tools that address the specific trust dimensions most relevant to their partial engagement pattern. Jiang and Lim (2018) provided complementary evidence that even modest trust improvements at the margin can generate significant changes in financial behavior, suggesting that relatively low-cost trust-building interventions targeted at underbanked populations may generate disproportionately large inclusion impacts.

Geographic dimensions of financial exclusion interact with demographic barriers in ways that create particularly acute inclusion challenges in specific US regions. Rural communities, particularly in the Midwest, Appalachia, and the Deep South, face compound exclusion driven by branch closure trends, poor broadband infrastructure, and concentrated economic distress that erodes both the supply of and demand for formal financial services. Broekhoff et al. (2024) noted that physical inaccessibility and digital inaccessibility frequently co-occur in the same populations, creating a double-exclusion dynamic that purely digital Trust-by-Design solutions may be insufficient to address without complementary infrastructure investment. The deployment of AI-powered

payment intelligence through offline-capable mobile applications, community banking kiosks, and postal banking partnerships represents a promising but underexplored avenue for reaching geographically excluded populations. Avom et al. (2023) demonstrated in the African mobile money context that agent banking

networks in which local community members serve as access points for mobile financial services can effectively bridge physical and digital access gaps by combining the accessibility of physical presence with the scalability of digital payment infrastructure, a model with direct applicability to underserved rural US communities.

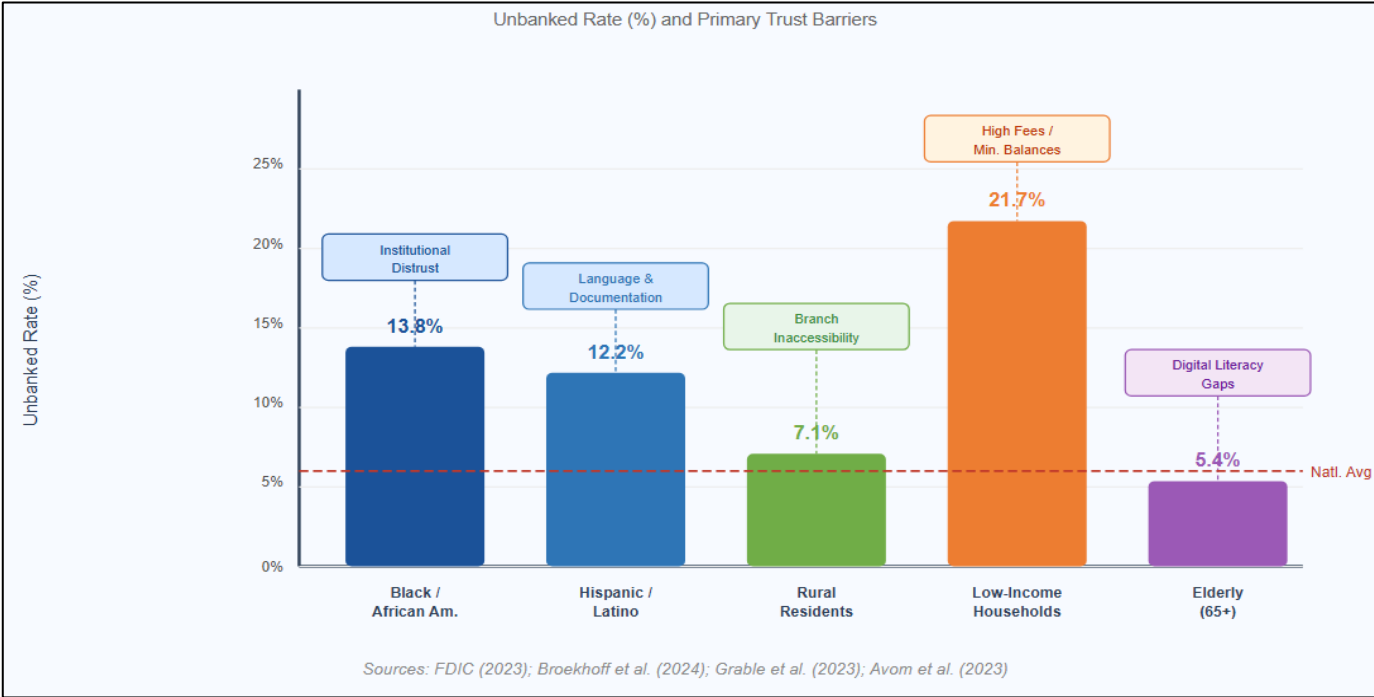


Fig 3 Financial Inclusion Gap Map Across US Demographic Segments

• *AI-Enabled Inclusive Design Principles*

Amegbe et al. (2021) demonstrated through brand love theory that affective dimensions of consumer-institution relationships including emotional connection, perceived shared values, and community identification play a significant role in bank customer loyalty, particularly for corporate social responsibility perceptions. This finding suggests that Trust-by-Design payment systems must attend not only to functional trust dimensions (security, reliability, accuracy) but also to relational and affective dimensions that are particularly salient for excluded communities.

Avom et al. (2023) provided important evidence from mobile money adoption in Africa a context with structural parallels to underserved US communities in terms of limited traditional banking access that financial innovation can successfully drive inclusion when the innovation design aligns with existing trust structures and social networks. Their findings support a community-embedded approach to Trust-by-Design, in which payment intelligence systems leverage existing social trust networks as onboarding mechanisms rather than requiring users to transfer trust wholesale to unfamiliar digital institutions.

The role of mobile payment platforms as inclusion vectors is well-established in the literature (Chandra et al., 2010; Avom et al., 2023), but the Trust-by-Design contribution is to specify the architectural features that make mobile payment AI-enabled systems simultaneously

more secure and more accessible for diverse populations. These include multimodal authentication options that accommodate varying literacy and digital skill levels, intelligent onboarding flows that calibrate information disclosure to user comprehension levels, and AI-powered customer service that provides 24/7 support in multiple languages without requiring human agent intervention.

The role of algorithmic fairness in inclusive payment intelligence design deserves particular emphasis, as it represents the point at which technical performance and equity objectives most directly interact. Ashtiani and Raahemi (2022) documented significant demographic disparities in false positive rates across fraud detection models, with certain demographic groups experiencing transaction decline rates two to three times higher than average even when controlling for transaction characteristics. These disparate impact patterns are not merely an ethical concern; they directly undermine the trust-building potential of payment intelligence systems for precisely the populations minority, low-income, and immigrant communities most in need of trust-based inclusion. Trust-by-Design mandates that algorithmic fairness be treated as a first-order design constraint rather than a post-deployment audit concern, requiring that model development pipelines include demographic subgroup performance testing, disparate impact analysis, and iterative bias mitigation as standard components.

The integration of community-based trust networks into payment intelligence deployment strategies represents

a high-potential but underutilized inclusion lever. Amegbe et al. (2021) demonstrated that community-level brand relationships in banking contexts function as trust collateral that individual institutions can leverage to accelerate adoption among members of tight-knit communities. For Trust-by-Design implementations targeting underserved US demographics, this implies that partnerships with community development financial institutions (CDFIs), credit unions with strong community roots, Black-owned banks, and Hispanic-serving financial cooperatives may generate trust transfer effects that significantly reduce adoption barriers relative to standalone deployment by large national financial institutions. These partnerships also create accountability structures that help ensure that Trust-by-Design commitments are maintained over time: community partners with established reputations in their constituencies have strong incentives to ensure that the payment intelligence systems they endorse actually deliver on their trust-building promises, creating a governance mechanism that complements formal regulatory oversight.

➤ *Regulatory Landscape for AI-Enabled Payment Intelligence*

• *Federal Regulatory Framework*

The regulatory environment governing digital payments and AI deployment in financial services in the

United States is characterized by a complex multi-agency structure that creates both constraints and opportunities for Trust-by-Design implementations. The Bank Secrecy Act (BSA) and its implementing regulations under FinCEN establish the foundational framework for anti-money laundering (AML) compliance, requiring financial institutions to maintain robust transaction monitoring systems capable of identifying suspicious activity patterns. AI-powered payment intelligence systems are well-positioned to meet and exceed these requirements, as LLM-based behavioral analysis can detect complex layering and placement patterns in money laundering schemes that rule-based systems frequently miss (Ashtiani & Raahemi, 2022).

The Electronic Fund Transfer Act (EFTA) and its implementing Regulation E establish consumer protection rights in digital payment contexts, including dispute rights, error resolution procedures, and unauthorized transfer liability limitations. Trust-by-Design payment systems can streamline Regulation E compliance through AI-powered dispute triage and resolution systems that accelerate the resolution of consumer complaints while maintaining complete audit trails for regulatory examination. The Fair Credit Reporting Act (FCRA) introduces additional constraints on the use of consumer data in payment decision-making, particularly when AI-generated risk scores influence transaction authorization decisions that constitute adverse actions under the statute.

Table 5 US Regulatory Framework Alignment with Trust-by-Design Principles

Regulatory Framework	Governing Body	Scope	Trust-by-Design Alignment
Bank Secrecy Act (BSA)	FinCEN / Treasury	AML, fraud reporting, KYC	AI-enhanced transaction monitoring complies with suspicious activity reporting
Electronic Fund Transfer Act (EFTA)	CFPB / Federal Reserve	Consumer protection in digital payments	Automated dispute resolution tools support Regulation E compliance
Fair Credit Reporting Act (FCRA)	FTC / CFPB	Data accuracy, credit decisioning	Explainable AI supports adverse action notice requirements
CFPB Open Banking Rule (Sec. 1033)	CFPB	Consumer data portability and access	Privacy-by-design APIs align with consumer-authorized data sharing
NIST AI Risk Management Framework	NIST / OSTP	AI trustworthiness, fairness, accountability	Trust-by-Design directly implements NIST AI RMF Govern, Map, Measure, Manage pillars

Source: Authors' compilation based on CFPB (2024); FinCEN (2023); NIST (2023); Federal Reserve (2024)

• *NIST AI Risk Management Framework Alignment*

The NIST AI Risk Management Framework (AI RMF), released in January 2023, provides the most comprehensive voluntary guidance for trustworthy AI deployment in the United States and aligns closely with the Trust-by-Design framework proposed in this article. The AI RMF organizes trustworthy AI requirements across four functional categories: Govern, Map, Measure, and Manage. Each of these functional categories maps directly to components of the TbDPI framework, providing a regulatory alignment pathway for payment system operators seeking to demonstrate trustworthy AI practices to regulators and customers alike.

The Govern function of the NIST AI RMF establishes organizational policies, accountability structures, and risk culture requirements that support

responsible AI deployment. For payment intelligence systems, this translates to board-level accountability for AI fraud detection systems, clear escalation pathways for false positive disputes, and regular third-party audits of model fairness across demographic groups. The Map function requires organizations to understand and categorize AI risks in context, which for payment intelligence systems means systematically analyzing the trust implications of different false positive and false negative rates across user demographic segments.

The Measure function of the NIST AI RMF requires organizations to develop and apply quantitative and qualitative methods to assess AI risks and performance, including trust-relevant metrics such as demographic parity in false positive rates, user satisfaction with AI-driven decisions, and the accuracy of AI-generated

explanations as evaluated by affected users. For Trust-by-Design payment intelligence systems, this translates into a comprehensive measurement architecture that goes beyond standard fraud detection KPIs to include trust-specific metrics assessed continuously across user demographic segments. The Manage function completes the framework cycle by requiring organizations to allocate resources and implement plans to address identified AI risks, including establishing incident response procedures for AI fraud detection failures, creating accessible appeals mechanisms for wrongful transaction declines, and maintaining transparency reports on system performance and demographic equity outcomes.

The intersection of AI governance requirements with existing financial services regulation creates both compliance challenges and strategic opportunities for Trust-by-Design implementers. The CFPB's examination of algorithmic fairness in credit decisioning, its proposed interpretive rule on Section 1033 open banking data access, and its ongoing scrutiny of digital payment platforms for Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) violations collectively create a regulatory environment in which Trust-by-Design is increasingly the path of least regulatory resistance rather than a voluntary commitment above and beyond compliance requirements. Gokmenoglu and Amir (2021) argued that perceived fairness operates as a foundational prerequisite for trust in banking relationships, with fairness perceptions mediating the relationship between institutional competence and consumer trust. This finding implies that regulatory requirements promoting algorithmic fairness and explainability are not merely compliance burdens but trust infrastructure investments that generate direct consumer relationship benefits. Payment operators who proactively build Trust-by-Design systems aligned with the NIST AI RMF will be well-positioned when as appears increasingly likely voluntary guidance becomes mandatory requirement.

V. DISCUSSIONS

➤ *Integrated Trust-Payment Intelligence Model*

The convergent analysis presented in this article supports the central argument that trust and payment security are not merely compatible objectives but are, when properly designed, mutually reinforcing. The literature on financial trust consistently demonstrates that security failures whether experienced directly as fraud victimization or observed through institutional news coverage generate lasting trust damage that depresses financial participation (Bauer, 2015; van der Cruysen et al., 2016). The literature on fraud detection demonstrates that AI-powered systems, particularly LLM-based approaches, are increasingly capable of achieving fraud detection accuracy levels that substantially reduce exposure to these trust-damaging experiences (Dahiphale et al., 2024; Kumar, 2024; Alghofaili et al., 2020).

The analytical synthesis of trust theory and fraud detection technology also reveals important insights about the sequence in which trust is built and lost in payment

system interactions. Roy et al. (2015) established that initial trust formation in banking relationships is primarily driven by competence signals demonstrable evidence that the institution can reliably execute its core functions while trust maintenance and recovery are more heavily influenced by benevolence and integrity signals. This sequential dynamic implies that the deployment order of Trust-by-Design features matters: early deployment efforts should prioritize demonstrable fraud prevention effectiveness and system reliability to establish competence-based trust foundations, while subsequent enhancements should introduce greater personalization, transparency, and community engagement features that build the relational trust dimensions that sustain long-term loyalty. Sekhon et al. (2014) reinforced this sequencing logic by showing that trustworthiness perceptions formed early in a customer relationship exert disproportionate influence on subsequent trust evaluations, even when later experiences might objectively warrant revision.

The intersection of AI capability advancement and Trust-by-Design requirements creates a productive design tension that drives innovation in payment intelligence systems. As LLM-based fraud detection approaches the technical ceiling of what is achievable with current architectures with leading models achieving accuracy rates in the 93–95% range the marginal returns to pure detection accuracy improvement are diminishing, while the returns to trust-building feature development explainability, personalization, inclusion, fairness are growing. Dahiphale et al. (2024) observed that LLM-powered payment security systems that provided natural language explanations of fraud decisions achieved higher user satisfaction scores than equivalent systems without explanation features, even when detection accuracy was identical, confirming that the trust value of explainability is distinct from and additive to the security value of accurate detection. Kumar (2024) similarly found that user perception of AI payment security as a protective rather than restrictive force was a stronger predictor of continued platform engagement than objective fraud loss rates, underscoring the primacy of trust perception in determining the behavioral outcomes that matter most for payment platform economics.

The Trust-by-Design framework integrates these two streams by specifying the architectural conditions under which fraud detection technology generates trust rather than merely suppressing fraud. The key insight is that fraud detection systems affect trust not only through their accuracy in preventing fraud, but through their explainability in communicating decisions, their fairness in avoiding discriminatory false positive patterns, and their accessibility in providing consistent protection to users across the full spectrum of digital literacy levels. A system that achieves 95% fraud detection accuracy while generating systematically higher false positive rates for minority users thereby generating disproportionate transaction disruption and potential discrimination claims may actually damage trust for precisely the populations most in need of trust-building interventions.

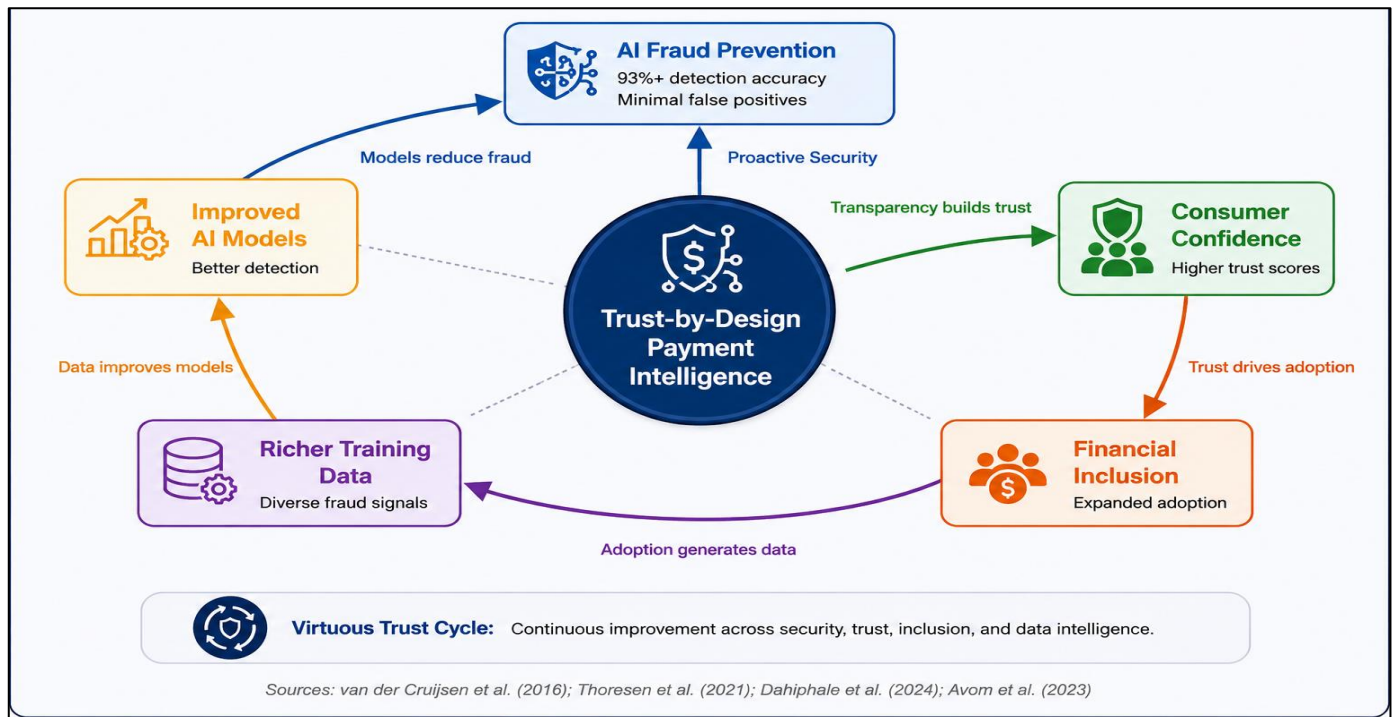


Fig 4 Trust Feedback Loop: Fraud Prevention, Inclusion, and Digital Participation

➤ Implications for Payment System Design

For payment system architects and financial technology developers, the Trust-by-Design framework implies a fundamental reorientation of the design process. Rather than treating fraud detection, user experience, and inclusion initiatives as separate workstreams with distinct metrics and team structures, Trust-by-Design requires integrated design that treats trust as the primary system output and fraud prevention as one of several architectural inputs. This reorientation has practical implications for team composition, success metrics, and testing protocols.

Success metrics for Trust-by-Design payment systems must expand beyond conventional fraud key performance indicators (KPIs) such as fraud rate, false positive rate, and detection latency to include trust-specific metrics such as consumer-reported payment confidence, adoption rates among target inclusion populations, false positive rate equity across demographic groups, and complaint and dispute resolution satisfaction. Bijlsma et al. (2022) demonstrated that daily trust measurements in payment services reveal significant temporal dynamics that aggregate measures obscure, suggesting that real-time trust monitoring may be a valuable complement to periodic consumer satisfaction surveys. Amegbe et al. (2021) further suggest that affective dimensions of trust including brand love and community identification warrant measurement alongside the cognitive and calculative trust dimensions more commonly assessed in financial services research.

Kong (2013) and Thoresen et al. (2021) both highlight the social embeddedness of institutional trust, with network and community-level trust dynamics significantly influencing individual willingness to engage with formal financial services. This suggests that Trust-by-Design implementations should incorporate community-

level engagement strategies alongside individual-level technical interventions, including partnerships with trusted community organizations, transparent public reporting of fraud detection equity metrics, and participatory design processes that include representatives from target inclusion populations in the design and testing of payment intelligence systems.

➤ Limitations and Future Research

This article has several important limitations that future research should address. First, the synthesis presented here draws primarily on academic literature from the United States, Europe, and Africa; the degree to which Trust-by-Design principles and implementation strategies must be adapted for specific US regional contexts including rural areas, tribal communities, and specific urban demographic concentrations warrants empirical investigation. Second, the fraud detection performance metrics reported in Table 2 are drawn from a range of experimental and quasi-experimental studies with varying methodological standards; direct comparison of accuracy figures across studies requires caution given differences in dataset characteristics, feature engineering approaches, and evaluation protocols.

Third, while this article argues theoretically for the mutual reinforcement of trust and security in payment systems, empirical evidence directly testing this relationship in US payment contexts is limited. Future longitudinal studies examining whether improvements in payment fraud detection particularly when communicated transparently to consumers generate measurable increases in payment system trust and adoption among target inclusion populations would provide important empirical validation of the Trust-by-Design framework. Finally, the regulatory landscape for AI in financial services is evolving rapidly, and the alignment analysis presented in

Table 5 reflects the regulatory environment as of early 2025; ongoing monitoring of regulatory developments including potential federal AI legislation, CFPB AI guidance, and prudential regulator model risk management updates will be necessary to maintain the currency of this analysis.

A fourth important limitation concerns the operationalization of “inclusion” as a measurable outcome in Trust-by-Design evaluation frameworks. The literature reviewed in this article employs diverse and not always comparable definitions of financial inclusion ranging from basic account ownership to active use of digital payment channels to full participation in credit markets making it difficult to aggregate findings across studies or to specify a single inclusion target for Trust-by-Design implementations. Future research should develop and validate a multidimensional financial inclusion measurement instrument specifically calibrated to the digital payment context, distinguishing among access inclusion (ability to use digital payment services), usage inclusion (actual frequency and breadth of digital payment use), quality inclusion (access to fair-priced, low-friction services), and welfare inclusion (measurable improvement in financial outcomes). Such an instrument would enable more rigorous evaluation of Trust-by-Design interventions and facilitate comparison across demographic groups, geographic contexts, and institutional deployment models.

The cross-disciplinary nature of the Trust-by-Design framework also raises important questions about the institutional arrangements best suited to drive its adoption and continuous improvement. Trust-by-Design spans technical domains (AI, machine learning, cybersecurity), social science domains (behavioral economics, sociology of trust, financial inclusion research), and governance domains (financial regulation, consumer protection law, AI ethics) in ways that exceed the expertise of any single organizational function or academic discipline. Grable et al. (2023) noted that the persistence of bank distrust among underserved populations reflects in part the failure of

financial institutions to incorporate social science insights about trust dynamics into their product and service design processes, relying instead on primarily technical and financial frameworks that are poorly calibrated to the experiential realities of their most vulnerable customers. Successful Trust-by-Design implementation may therefore require new organizational structures including dedicated trust engineering functions with cross-disciplinary composition, community advisory boards with genuine influence over product development decisions, and ongoing academic-practitioner research partnerships that institutionalize the multi-domain perspective the framework demands.

VI. CONCLUSION

This article has introduced and elaborated the concept of Trust-by-Design Payment Intelligence as a framework for simultaneously advancing payment security and financial inclusion in the United States. By synthesizing a convergent body of literature spanning institutional trust theory, financial exclusion research, fraud detection technology, and regulatory compliance, we have demonstrated that the conventional separation of security and inclusion objectives in payment system design is both theoretically unjustified and practically counterproductive.

The Trust-by-Design framework positions trust as a first-order architectural constraint in payment system design, requiring that fraud detection systems be explainable, fair, accessible, and aligned with the diverse trust needs of the full US population. LLM-powered payment intelligence systems capable of processing both structured transaction data and unstructured behavioral signals with fraud detection accuracy exceeding 93% provide the technical foundation for this framework, while the five principles of transparency, privacy by default, user empowerment, proactive security, and inclusive design provide the architectural specification that converts technical capability into genuine trust-building outcomes.

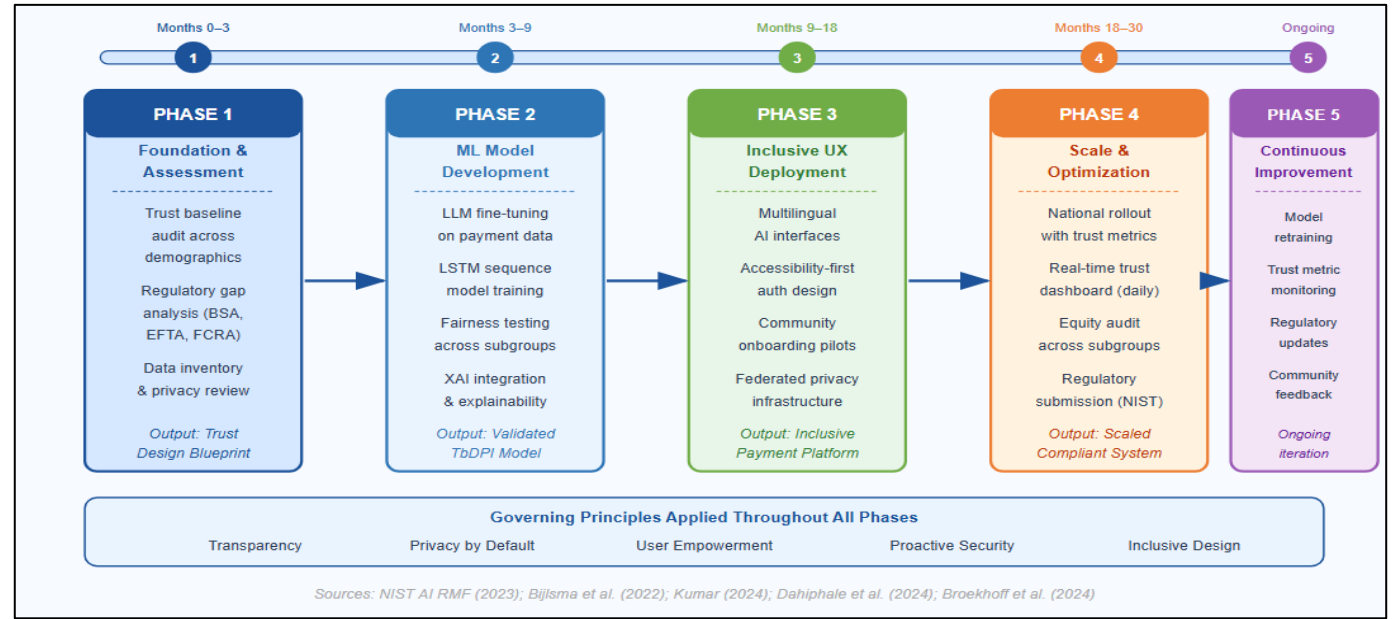


Fig 5 TbDPI Implementation Roadmap: From Principle to Deployed Payment Intelligence

The regulatory alignment analysis confirms that Trust-by-Design payment intelligence is not only technically feasible but is increasingly required by the evolving US regulatory landscape for AI in financial services, including NIST AI RMF, CFPB guidance on algorithmic decision-making, and federal fair lending requirements. Payment operators who proactively embed trust-building mechanisms into their AI fraud detection infrastructure will be positioned to demonstrate regulatory compliance, expand market reach into underserved demographics, and build the durable customer relationships that generate long-term competitive advantage.

The most fundamental contribution of this article is perhaps the reframing it proposes: from payment security as a cost center and financial inclusion as a social obligation, to payment intelligence as a trust-generation engine that simultaneously reduces financial crime, expands market participation, and contributes to the equitable digital economy that regulators, advocates, and responsible financial institutions aspire to build. Trust is not a soft variable in payment system design it is the load-bearing architecture on which all other system functions ultimately rest.

The United States stands at a pivotal moment in its financial services evolution. The convergence of real-time payment infrastructure deployment (through the Federal Reserve's FedNow service and The Clearing House's RTP network), rapid advances in AI-powered fraud detection and prevention, growing regulatory attention to algorithmic fairness and digital payment consumer protection, and persistent structural gaps in financial inclusion creates both an urgent challenge and an unprecedented opportunity. The challenge is to ensure that the next generation of payment infrastructure serves all Americans equitably, rather than replicating or amplifying the exclusion patterns of legacy financial systems. The opportunity is to demonstrate, through well-designed Trust-by-Design implementations, that the most technologically sophisticated payment systems are also the most trustworthy and the most inclusive establishing a new paradigm that positions the United States as a global leader in equitable digital financial infrastructure.

Achieving this vision will require coordinated action across multiple domains simultaneously. Payment system engineers must adopt trust as a first-order design requirement with the same technical rigor applied to performance and scalability. Financial institution leadership must align organizational incentive structures with long-term trust-building outcomes rather than short-term fraud loss minimization. Regulators must provide clear, consistent, and forward-looking guidance on AI deployment in payment contexts that rewards proactive Trust-by-Design investment rather than minimum compliance. Researchers across disciplines must accelerate the development of the empirical foundations that the Trust-by-Design framework currently rests on partially: the causal mechanisms through which specific

payment intelligence features build or erode trust among specific demographic populations, the long-term relationship between trust-building investments and financial inclusion outcomes, and the organizational and regulatory conditions that best support sustained Trust-by-Design implementation. This article has sought to contribute to that foundation; the work of building an inclusive, trustworthy digital value exchange ecosystem for all Americans remains substantially ahead.

REFERENCES

- [1.] Broekhoff, M., Van Der Cruisen, C., & De Haan, J. (2024). Towards financial inclusion: Trust in banks' payment services among groups at risk. *Economic Analysis and Policy*, 82, 104–123. <https://doi.org/10.1016/j.eap.2024.02.038>
- [2.] Chandra, S., Srivastava, S. C., & Theng, Y. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems*, 27. <https://doi.org/10.17705/1CAIS.02729>
- [3.] Amegbe, H., Dzandu, M. D., & Hanu, C. (2021). The role of brand love on bank customers' perceptions of corporate social responsibility. *International Journal of Bank Marketing*, 39(1), 189–208. <https://doi.org/10.1108/ijbm-07-2020-0356>
- [4.] Afandi, E., & Habibov, N. (2017). Pre- and post-crisis trust in banks: Lessons from transitional countries. *Journal of Economic Development*, 42(1), 73–94. <https://doi.org/10.35866/caujed.2017.42.1.004>
- [5.] Avom, D., Bangaké, C., & Ndoya, H. (2023). Do financial innovations improve financial inclusion? Evidence from mobile money adoption in Africa. *Technological Forecasting and Social Change*, 190, 122451. <https://doi.org/10.1016/j.techfore.2023.122451>
- [6.] Bijlsma, M., van der Cruisen, C., & Koldijk, J. (2022). Determinants of trust in banks' payment services during COVID: An exploration using daily data. *De Economist*, 170(2), 231–256. <https://doi.org/10.1007/s10645-022-09405-9>
- [7.] van der Cruisen, C., de Haan, J., & Jansen, D. J. (2016). Trust and financial crisis experiences. *Social Indicators Research*, 127, 577–600. <https://doi.org/10.1007/s11205-015-0984-8>
- [8.] Kong, D. T. (2013). Intercultural experience as an impediment of trust: Examining the impact of intercultural experience and social trust culture on institutional trust in government. *Social Indicators Research*, 113, 847–858. <https://doi.org/10.1007/s11205-012-0117-6>
- [9.] Marozzi, M. (2015). Measuring trust in European public institutions. *Social Indicators Research*, 123(3), 879–895. <https://doi.org/10.1007/s11205-014-0765-9>

- [10.] Jiang, D., & Lim, S. S. (2018). Trust and household debt. *Review of Finance*, 22(2), 783–812. <https://doi.org/10.2139/ssrn.1954790>
- [11.] Odukale, Bowale. (2024). The Rise of AI Literacy: Redefining Human Communication Competence in the Algorithmic Age. *International Journal of Multidisciplinary Evolutionary Research*. 5. 76-90. 10.54660/IJMER.2024.5.1.76-90.
- [12.] Thoresen, S., Blix, I., Wentzel-Larsen, T., & Birkeland, M. S. (2021). Trusting others during a pandemic: Investigating potential changes in generalized trust and its relationship with pandemic-related experiences and worry. *Frontiers in Psychology*, 12, 698519. <https://doi.org/10.3389/fpsyg.2021.698519>
- [13.] Bauer, P. C. (2015). Negative experiences and trust: A causal analysis of the effects of victimization on generalized trust. *European Sociological Review*, 31(4), 397–417. <https://doi.org/10.1093/esr/jcu096>
- [14.] Devlin, J., Ennew, C., Sekhon, H., & Roy, S. K. (2015). Trust in financial services: Retrospect and prospect. *Journal of Financial Services Marketing*, 20(4), 234–245. <https://doi.org/10.1057/fsm.2015.21>
- [15.] Roy, S. K., Devlin, J. F., & Sekhon, H. (2015). The impact of fairness on trustworthiness and trust in banking. *Journal of Marketing Management*, 31(9–10), 996–1017. <https://doi.org/10.1080/0267257X.2015.1036101>
- [16.] Gokmenoglu, K. K., & Amir, A. (2021). The impact of perceived fairness and trustworthiness on customer trust within the banking sector. *Journal of Relationship Marketing*, 20(3), 241–260. <https://doi.org/10.1080/15332667.2020.1802642>
- [17.] Sekhon, H., Ennew, C., Kharouf, H., & Devlin, J. (2014). Trustworthiness and trust: Influences and implications. *Journal of Marketing Management*, 30(3–4), 409–430. <https://doi.org/10.1080/0267257X.2013.842609>
- [18.] Ben-Ner, A., & Halldorsson, F. (2009). Trusting and trustworthiness: What are they, how to measure them, and what affects them. *Journal of Economic Psychology*, 31(1), 64–79. <https://doi.org/10.1016/j.joep.2009.10.001>
- [19.] Grable, J., Kwak, E. J., & Archuleta, K. (2023). Distrust of banks among the unbanked and banked. *International Journal of Bank Marketing*, 41(6), 1498–1520. <https://doi.org/10.1108/IJBM-10-2022-0441>
- [20.] Kumar, P. (2024). AI-powered fraud prevention in digital payment ecosystems: Leveraging machine learning for real-time anomaly detection and risk mitigation. *Journal of Information Systems Engineering and Management*, 9(4). <https://doi.org/10.52783/jisem.v9i4.102>
- [21.] Dahiphale, D., Madiraju, N., Lin, J., Karve, R., Agrawal, M., Modwal, A., Balakrishnan, R., Shah, S., Kaushal, G., Mandawat, P., Hariramani, P., & Merchant, A. (2024). Enhancing trust and safety in digital payments: An LLM-powered approach. *arXiv*. <https://doi.org/10.48550/arxiv.2410.19845>
- [22.] Odukale, Bowale. (2024). AI Literacy and Entrepreneurial Innovation: Rethinking Digital Competence for the Knowledge Economy. *International Journal of Multidisciplinary Evolutionary Research*. 5. 91-108. 10.54660/IJMER.2024.5.1.91-108.
- [23.] Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A financial fraud detection model based on LSTM deep learning technique. *Journal of Applied Security Research*, 15(4), 498–516. <https://doi.org/10.1080/19361610.2020.1815491>
- [24.] Preciado Martínez, P. M., Reier Forradellas, R. F., Garay Gallastegui, L. M., & Nández Alonso, S. L. (2025). Comparative analysis of machine learning models for the detection of fraudulent banking transactions. *Cogent Business & Management*, 12(1). <https://doi.org/10.1080/23311975.2025.2474209>
- [25.] Nguyen Thanh, C., & Phan Huy, T. (2025). Predicting financial reports fraud by machine learning: The proxy of auditor opinions. *Cogent Business & Management*, 12(1). <https://doi.org/10.1080/23311975.2025.2510556>
- [26.] Ashtiani, M. N., & Raahemi, B. (2022). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access*, 10, 72504–72525. <https://doi.org/10.1109/ACCESS.2021.3096799>
- [27.] Jemai, J., Ben Cheikh, R., & Hajjej, F. (2020). Credit card fraud detection using machine learning: A comparative study. *International Journal of Advanced Computer Science and Applications*, 11(10), 371–378. <https://doi.org/10.14569/IJACSA.2020.0111047>
- [28.] Olatunji, Opeyemi & Odukale, Bowale. (2025). Leveraging Predictive Analytics and AI for SME Growth: A Data-Driven Approach to Business Optimization. *World Journal of Advanced Research and Reviews*. 25. 1830-1841. 10.30574/wjarr.2025.25.3.0958.
- [29.] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *Journal of Information Security*, 8(3), 183–196. <https://doi.org/10.4236/jis.2017.83013>