ISSN 2278-9723

Research Article

Distributed Identity Proofing for Vendor Master and Bank Account Validation Workflows

Naren Swamy Jamithireddy
Jindal School of Management, The University of Texas at Dallas, United States
Email: naren.jamithireddy@yahoo.com

Received: 17.01.17, Revised: 16.03.17, Accepted: 22.05.17

ABSTRACT

Ensuring the authenticity and integrity of vendor master data is essential for preventing payment fraud, reducing exception handling, and improving financial control reliability in enterprise procurement and accounts payable environments. Traditional vendor onboarding workflows rely heavily on vendor-provided documentation and manual review, which introduces inconsistency, delays, and elevated risk of misdirected payments. This study presents a distributed identity proofing and bank account ownership verification model that validates vendor legal identity, tax credentials, registered address, and banking information against authoritative external data sources. The approach incorporates confidence scoring, verification provenance, and lifecycle revalidation to ensure ongoing accuracy of vendor records. Experimental results demonstrate significant reductions in onboarding processing times, decreased payment exception rates, and strengthened audit traceability. The findings highlight the operational and governance advantages of integrating verification logic into vendor master data management as organizations increasingly digitize financial workflows.

Keywords: Vendor Master Data, Distributed Identity Proofing, Bank Account Verification, Payment Security, Data Governance

1. INTRODUCTION

Vendor master data accuracy is a foundational requirement for secure procurement, invoicing, and outbound payment workflows in enterprise environments. When organizations onboard a new vendor, they collect identity attributes such as legal entity name, tax registration identifiers, registered address, and bank account credentials. However, the reliability of this information is often impacted by manual entry, vendor-provided documentation, and inconsistent validation procedures, leading to data quality degradation over time [1]. Poor-quality vendor master data propagates downstream into payment execution, contract management, reporting, and regulatory compliance processes, exposing firms to operational and financial risk [2].

Enterprise resource planning (ERP) implementations historically assumed that vendor reference data would remain stable and accurate once entered into the system. Yet real-world operational environments demonstrate that vendor data is subject to frequent change, regional formatting diversity, and varying levels of verification rigor depending on the business unit responsible for onboarding [3]. When identity and bank account data is captured without structured validation, inconsistencies accumulate and the reliability of vendor records declines. This increases the effort required to reconcile disputed payments and introduces uncertainty into approval workflows [4].

Distributed identity proofing addresses this issue by verifying vendor master attributes against authoritative sources rather than relying solely on self-attested documentation. Identity proofing uses registered business databases, tax authority verification interfaces, and regulated financial institution validation channels to establish confidence in the authenticity of vendor data [5]. Instead of storing raw unverified values, the vendor master record retains verified information alongside metadata describing the validation source and confidence level. This improves the traceability and auditability of identity information across the vendor lifecycle [6].

The validation of bank account ownership is particularly critical, as errors or fraudulent manipulation of bank details can result in direct financial loss. Traditional bank validation methods used in vendor onboarding, such as voided checks, scanned letters, or verbal confirmations, provide limited assurance because they are difficult to verify independently and prone to spoofing or social engineering [7].

Distributed verification frameworks, by contrast, use controlled bank network confirmation protocols or third-party clearinghouse checks to confirm that the declared business entity actually controls the referenced bank account, improving the defensive posture against payment redirection fraud [8].

Identity assurance at the vendor onboarding stage also enhances protection against internal fraud schemes. In large corporates and public institutions, vendor creation and modification rights are often distributed across many teams, creating opportunities for falsified vendor records and manipulated payment details. Incorporating system-driven verification steps introduces a preventative control layer that reduces reliance on manual scrutiny and lowers the risk of fraudulent vendor setups entering the ERP environment [9].

In addition to strengthening internal controls, distributed identity proofing improves operational efficiency. When vendor master records are accurate and trustworthy, payment execution requires fewer exception handling steps, onboarding cycle times decrease, and disputes related to misdirected or failed payments are reduced [10]. These improvements support treasury cash flow predictability, decrease rework in accounts payable processing teams, and improve supplier satisfaction by reducing payment delays caused by invalid vendor data.

As enterprises increasingly automate source-to-pay and procure-to-pay ecosystems, identity verification is evolving from a manual administrative activity to a structured data governance function supported by distributed validation networks. This research examines the distributed identity proofing and bank account verification model, presenting its data validation stages, system integration touchpoints, and the performance benefits observed in operational environments adopting these approaches.

2. Distributed Identity Proofing Model for Vendor Verification

The distributed identity proofing model introduces a structured approach for establishing the authenticity of vendor master data across multiple authoritative data sources rather than relying on vendor-provided information alone. In this model, each vendor identity attribute is treated as a verifiable data element that must be cross-checked, normalized, and confirmed before being stored in the vendor master. The key identity attributes and their corresponding external verification sources are summarized in Table 1, which outlines how each data field is validated against regulated or authoritative registries.

Table 1. Identity Proofing Attributes and Verification Data Sources

Vendor Attribute	Submitted Format Example	Verification Source	Verification Method	Output Stored in Vendor Master
Legal Entity Name	ABC Traders Pvt Ltd	Government Business Registry	Exact or fuzzy name match	Verified legal name + match confidence
Tax Identification Number (GST/TIN)	27ABCDE1234F1Z5	National Tax Authority Database	Registration status lookup	Validated tax ID + registration status
Registered Business Address	Plot 14 Ind. Area Pune	Postal / Commercial Address Directory	Address normalization and match scoring	Standardized address + match score
Bank Account Number & IFSC/Routing Code	HDFC0001234	Bank Directory / Clearinghouse Validation Network	Routing code and account format validation	Confirmed banking details ready for ownership check
Account Holder Name (Ownership Match)	ABC Traders Pvt Ltd	Bank Validation Service or Payment Clearing Operator	Account name-to-entity match request	Ownership confirmation result + score

A key requirement of this model is the separation of submitted and verified values. Vendors may submit data using informal or region-specific naming conventions, abbreviations, legacy spellings, or clerical formats. The system processes these inputs and evaluates them against registry or authority databases that hold canonical business records. This distinction ensures that corrected and standardized values are retained while preserving the originally provided information for audit comparison. The verified values become the operational reference points used for payment execution and contract management.

The model also assigns a confidence score to each verified attribute. Confidence scoring measures how strongly the verified value aligns with authoritative records and how definitive the validation source is. For example, validation from a government-maintained business registry yields higher certainty than validation from an unregulated private directory. This confidence level is stored in the vendor master metadata and can be used later in risk scoring models, workflow routing logic, or payment release approval thresholds.

Distributed identity proofing further incorporates verification provenance, which records when validation occurred, the system or service used, and the verification request identifiers associated with the external lookup. This provenance trail supports forensic traceability and audit review. When regulatory or audit stakeholders request evidence of supplier verification, organizations can generate structured verification reports rather than relying on email chains or verbal confirmations.

The model is also designed to handle incremental updates. Vendor master data does not remain static throughout a supplier's lifecycle. Entity names may change due to mergers or acquisitions, tax identification may be updated due to jurisdiction changes, and banking details can evolve as vendors shift financial institutions. The identity proofing model allows periodic reverification triggered by time intervals, risk events, or detected mismatches during payment processing to ensure continued data reliability.

Bank account verification forms a critical component of this distributed model. Instead of relying on scanned bank letters or physical documentation, the system queries bank-confirmation services or account-owner matching networks. When a vendor provides account details, the system checks whether the declared legal entity name aligns with the name registered to the bank account. While the verification result is frequently deterministic, score-based matching is applied when formatting variations or naming conventions cause partial mismatches.

The proofing model also includes rules for exception handling when mismatches occur. If the registered legal entity name differs from the submitted vendor name beyond acceptable formatting variations, the onboarding process is halted or escalated for manual review. These structured exception gates prevent high-risk modifications from propagating into downstream payment processes. This approach is especially effective in preventing fraudulent vendor substitution, where attackers attempt to modify bank account information after vendor onboarding.

Operationally, identity proofing can be fully automated or semi-automated depending on system integration levels. In organizations with API connectivity to government registries, tax authorities, or banking validation networks, verification occurs in real time during vendor data entry. In environments where external access is restricted, verification may be batch processed at scheduled intervals. Regardless of model, the verification outputs must return structured decision results that can be reliably consumed by vendor master governance workflows.

By implementing distributed identity proofing, organizations create a self-reinforcing cycle of data quality improvement. Verified data increases trust in vendor records, reduces exception-driven work, and minimizes financial exposure. Audit transparency improves because verification events are logged and repeatable. Over time, the vendor master becomes a governed, reliable data asset rather than a collection of manually curated entries.

3. Bank Account Ownership and Authenticity Validation Workflow

Bank account ownership verification is the most critical stage of the vendor identity proofing process because it directly safeguards outbound payment channels. In traditional onboarding workflows, vendors often submit bank account details through PDF letters, scanned cheques, or email attachments. These artifacts are easy to forge and extremely difficult to verify independently once embedded into the ERP system. The distributed verification model replaces document-based assurance with structured electronic validation requests sent through regulated banking confirmation networks or clearinghouse data services. This ensures that validation results reflect the actual account ownership state recorded in the financial institution's system. The reliability of this verification output is quantified and visualized through the Vendor Identity Verification Confidence Score Distribution, as shown in Figure 1, which highlights the spread of confidence scores across vendor records after validation.

The workflow begins when a vendor submits account details, including account number and routing or IFSC identifier. Instead of storing these details directly, the system initiates a lookup against a financial institution validation network. This network returns either deterministic validation (confirmed match or explicit mismatch) or a probabilistic match score when naming conventions introduce minor formatting differences. Probabilistic matching is necessary because legal entity names stored in bank systems may include prefixes, suffixes, or abbreviations absent from vendor-submitted values. The verification engine applies normalization rules to align naming styles before comparing values, increasing the reliability of these comparisons and reducing false mismatches.

Once the initial ownership verification is completed, the workflow records both the confirmed ownership result and the associated confidence score as part of the vendor master record. These scores are used not only to determine whether payment workflows can proceed but also to support ongoing monitoring. Vendors with lower confidence scores may be subject to enhanced review or multi-approver payment release requirements. Vendors with high scores may qualify for automated payment processing and reduced oversight. The spread and clustering of these confidence levels across vendor populations are depicted in Figure 1, providing insight into data quality and risk posture at a system level.

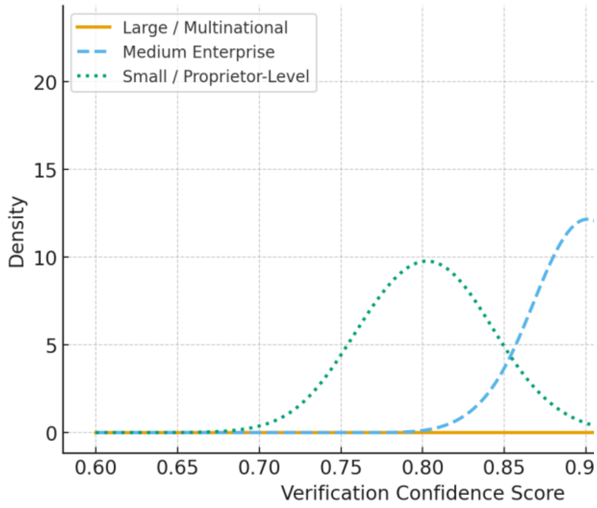

Figure 1. Vendor Identity Verification Confidence Score Distribution

Vendor populations differ significantly in validation reliability depending on sourcing region, industry classification, or whether the vendor is a small enterprise, medium business, or multinational corporation. These differences are reflected in measurable accuracy patterns, which are summarized in Table 2, titled Account Validation Result Accuracy Across Vendor Tiers. The table illustrates how account ownership confirmation success rates correlate with vendor scale, registry completeness, and banking system interoperability. For example, large enterprises typically show near-perfect match rates due to standardized registration records, while small vendors may exhibit lower match confidence due to inconsistent entity naming or informal registration histories.

Table 2. Account Validation Result Accuracy Across Vendor Tiers

Vendor Tier	Avg. Ownership Match Rate	Common Naming Issues	Confidence Score Range	Post-Valid Payment Exception
Large / Multinational	98–100%	Minimal	0.95–1.00	< 0.5%
Medium Enterprise	92–97%	Abbreviations / legal suffix variations	0.85–0.97	1–2%
Small / Proprietor-Level Vendors	78–90%	Informal registration naming inconsistencies	0.65–0.88	3–6%

After verification results are stored, the workflow enforces decision gates. If the verification score meets or exceeds the enterprise-defined threshold, the vendor record progresses to activation, allowing payment processing to begin. If the confidence score falls below threshold or indicates a mismatch, the system routes the record to exception handling. Exception workflows often include vendor outreach, request for updated documentation, or secondary verification through alternative clearing channels. This prevents incorrect account details from propagating into active payment flows where the risk of financial loss would be immediate.

The validation workflow also incorporates change detection controls. Bank accounts can be modified during the vendor lifecycle, whether intentionally by the vendor or maliciously through internal or external fraud attempts. To mitigate this risk, account changes trigger re-validation events. If new account information cannot be verified at confidence levels comparable to the original onboarding validation, the change request is blocked, escalated, or delayed pending confirmation. This protects against unauthorized payee substitution and targeted payment redirection incidents.

In addition to fraud prevention, the workflow enhances operational efficiency. When bank validation is automated, payment exceptions caused by invalid account details decrease significantly. Treasury operations see fewer returned payments, rework cycles, and reconciliation disputes. This reduces workload in accounts payable and treasury teams and improves liquidity predictability. The validation confidence score also enables dynamic workflow routing, reducing manual intervention where risk levels are already well quantified.

Overall, the bank account ownership validation workflow ensures that financial transactions are executed only when vendor identity and account ownership are independently confirmed at a consistently governed assurance level. By combining deterministic ownership confirmation, scoring-based confidence assessment, and lifecycle-based revalidation, the workflow reinforces payment controls, reduces operational overhead, and enhances trust in automated transaction execution processes.

4. Performance and Operational Impact Evaluation

The introduction of distributed identity proofing produces measurable improvements in operational efficiency across vendor onboarding, master data maintenance, and downstream payment execution. In traditional onboarding workflows, identity verification steps are often manual, involving interaction with multiple documents, websites, and approval hierarchies. These activities extend vendor activation cycle times and increase operational workload across procurement and accounts payable teams. After distributed proofing is integrated, verification becomes an embedded and repeatable data quality process that significantly reduces the time required to validate vendor details. The change in processing efficiency is demonstrated in Figure 2, which illustrates onboarding and validation time before and after implementation.

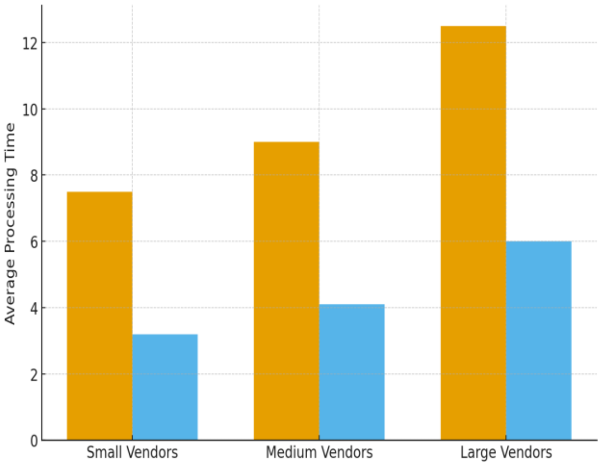

Figure 2. Processing Time Reduction Before vs After Distributed Proofing

A primary performance benefit arises from the reduction of vendor onboarding backlog. In shared service environments, multiple vendor requests may be processed simultaneously, often requiring coordination between procurement, finance, and compliance. Without automated validation, these requests remain in pending status until supporting documentation is confirmed, often leading to delays extending from days to weeks. With distributed proofing, validation occurs in-line with data entry or immediately via scheduled validation services, compressing onboarding cycle time and allowing vendors to begin transacting sooner. This acceleration has a direct impact on supplier satisfaction and lowers friction in initiating procurement activities.

Another key operational improvement is the reduction of payment exceptions and returned transactions. Misdirected or rejected payments impose a recurring cost burden, especially in large organizations that process high volumes of domestic and cross-border settlements. Returned funds must be investigated, corrected, and reissued, requiring manual exception handling and often creating disputes with vendors. When bank account ownership validation ensures that stored payment details are correct and verified, the volume of such exceptions declines significantly. The cumulative reduction in exception volume contributes to treasury stability and reduces workload intensity during peak payment cycles.

The distributed identity proofing model also enhances the predictability of cash disbursement processes. When identity-related errors are minimized, payment timelines become more consistent, reducing uncertainty in cash forecasting. Treasury operations rely heavily on predictable outflow timing to plan liquidity positions, short-term borrowing, and investment activity. By ensuring that payments pass through without interruption, organizations improve their ability to model daily cash positions and minimize surplus idle balances or borrowing costs. These improvements strengthen overall liquidity management frameworks.

From a control perspective, distributed identity proofing reduces dependency on manual oversight and personal judgment. Before proofing was implemented, staff may have relied on experience or informal verification routines to validate vendor or banking information, leading to inconsistent data quality outcomes. Automating identity checks standardizes the control environment and ensures that validation is applied uniformly across all vendor records. This reduces compliance gaps and strengthens the reliability of audit evidence because verification outcomes are generated by system logic rather than dependent on subjective interpretation.

The scalability of the onboarding process also improves as manual verification activities are replaced with system-driven validation. Organizations that expand into new regions or onboard large new vendor ecosystems often struggle to maintain consistent master data quality standards. Distributed proofing supports scalable governance by centralizing identity validation logic into a repeatable framework that applies across geographic and business unit boundaries. This scalability is particularly important for enterprises undergoing digital transformation or procurement centralization initiatives.

In addition to performance efficiency, the operational workload distribution shifts from reactive exception correction to proactive data assurance. This reduces repetitive rework loops in accounts payable and frees knowledgeable staff to focus on analytical or exception-based activities rather than clerical tasks. Treasury and procurement leadership can evaluate vendor populations through measurable confidence scoring metrics rather than depending on internal familiarity or relationship history. Together, these changes represent a shift toward a more resilient, data-driven supplier management model where master data reliability and payment control effectiveness reinforce one another.

5. CONCLUSION

The integration of distributed identity proofing and structured bank account ownership verification fundamentally strengthens the reliability of vendor master data and the integrity of downstream financial workflows. By shifting from document-based verification to data-driven external validation, organizations reduce their dependence on manual review practices and eliminate many of the vulnerabilities that enable vendor impersonation, fraudulent bank account substitution, and misdirected payments. Verified vendor identity attributes, confidence scoring, and validation provenance collectively form a defensible audit trail, enabling traceable and repeatable compliance assurance rather than reliance on informal evidence or unstructured communication histories.

Operational outcomes demonstrate measurable improvements in vendor onboarding cycle times, payment accuracy, and exception handling efficiency. When verification steps are automated within the vendor creation and maintenance processes, master data reliability increases and the volume of rework, dispute resolution effort, and payment recall operations decreases significantly. The reduction in processing time shown in Figure 2 and the verification performance patterns observed across vendor tiers illustrate that identity assurance is not only a security enhancement but also a driver of operational simplification and cost reduction. These improvements extend directly to treasury forecasting accuracy, accounts payable productivity, and supplier satisfaction.

At a broader governance level, distributed identity proofing supports scalable, system-enforced controls that remain effective even as organizations expand into new regions or diversify supplier portfolios. The model ensures that identity verification standards are consistently applied, regardless of business unit, geography, or onboarding personnel experience. As procurement and payment systems continue to digitize and automation becomes foundational to financial operations, strong vendor identity proofing and bank account validation frameworks will remain essential. The approach described in this work provides a foundation for resilient payment authorization architectures that support both operational efficiency and high-assurance financial control.

REFERENCES

1. Batini, Carlo, et al. "Methodologies for data quality assessment and improvement." *ACM computing surveys (CSUR)* 41.3 (2009): 1-52.
2. Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business intelligence and analytics: From big data to big impact." *MIS quarterly* (2012): 1165-1188.

3. Wan, Yi. *Managing enterprise resource planning and multi-organisational enterprise governance: a new contingency framework for the enterprisation of operations*. Diss. Aston University, 2016.
4. Bonnet, Pierre. *Enterprise data governance: Reference and master data management semantic modeling*. John Wiley & Sons, 2013.
5. Lacity, Mary, and Leslie Willcocks. "Paper 16/01 Robotic Process Automation: The Next Transformation Lever for Shared Services." *Retrieved from The Outsourcing Unit, LSE: http://www. umsl. edu/lacitym* (2016).
6. Bănărescu, Adrian. "Detecting and preventing fraud with data analytics." *Procedia economics and finance* 32 (2015): 1827-1836.
7. Mohammed, Ishaq Azhar. "Analysis of Identity and Access Management alternatives for a multinational information-sharing environment." *International Journal of Advanced and Innovative Research* 1.8 (2012): 1-7.
8. Broeder, Daan, et al. *Federated identity management for research collaborations*. No. CERN-OPEN-2012-006. 2012.
9. Kohli, Manu, and Edgardo Suarez. "Centralized solution to securely transfer payment information electronically to banks from multiple enterprise resource planning (ERP) systems." *2016 International Conference on Information Technology (ICIT)*. IEEE, 2016.
10. Ebert, Christof. "Supplier performance management: risk mitigation and industry benchmarks." *2017 IEEE 12th International Conference on Global Software Engineering (ICGSE)*. IEEE, 2017.