Received: 23.08.2026| **Accepted:** 05.10.2026| **Published:** Oct.2026
Citation: EGWARE, E., et al. (2026) Engineering Trust Where Inspection is impossible: A Layered Framework for Digital Marketplaces of Safety-Critical Goods in Low-Trust Markets GAIJIST Vol.2.1.2026 pp.65-78
DOI: https://doi.org/10.5281/zenodo.23877891

ENGINEERING TRUST WHERE INSPECTION IS IMPOSSIBLE: A LAYERED FRAMEWORK FOR DIGITAL MARKETPLACES OF SAFETY-CRITICAL GOODS IN LOW-TRUST MARKETS

EGWARE EROBOGHENE[1], OMOROGBE Osasu Harry (PhD)[2] , Ozobialu Emmanuel Chukwuma[3], OBANDE Bonnie Obeka, Ph.D. (CLN)[4] AMOFORITSE, Fortune Ighotuweyin[5],

[1] Department of Computer Science and Information Technology, College of Natural and Applied Science, Igbinedion University, Okada, Nigeria

Abstract

When buyers cannot inspect a product and the product can injure them if it fails, the usual online trust toolkit (reviews, return policies, branded checkout) is necessary but not sufficient. This article develops a layered framework for building trust in digital marketplaces that sell safety-critical goods in low-trust environments, using motor spare parts in Nigeria as the empirical anchor. Drawing on information economics, technology-acceptance research, two-sided-market theory and recent work on counterfeiting, payment security and data protection, we identify six trust layers: seller identity and accountability, product information and fit, transaction safety, reputation and social proof, regulatory and data governance, and physical assurance and fulfilment. We state six propositions about how the layers interact, including that identity and accountability mechanisms are a precondition for reputation systems to work, that product-fit information reduces return and safety costs more than price information does, and that physical assurance is the layer least reachable by software alone. We illustrate the framework with an integrated spare-parts and mechanic-discovery platform designed for Nigeria, and we set out a measurement agenda. The framework helps designers prioritise features, helps regulators see where platform duties should lie, and gives researchers testable claims.

Keywords: Online trust; counterfeit goods; safety-critical products; digital marketplaces; automotive aftermarket; platform governance; Nigeria

*Corresponding author(s). EGWARE, E., et al. agree that this article remain permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

1. Introduction

Trust research in electronic commerce was built largely on products whose failure is an inconvenience: books, cloth es, and electronics. Safety-critical goods are different. A counterfeit brake pad does not

just disappoint; it can kill. The buyer usually cannot tell the difference at purchase, and in many cases cannot tell afterwards either, because the part is fitted out of sight. Evidence assembled for the automotive sector indicates that automotive parts are among the most dangerous classes of counterfeit goods, that detection by packaging alone is inadequate, and that no single measure suffices (Maasberg et al., 2023). Online marketplaces make the problem more acute because they connect buyers with many independent sellers and rarely verify them: a recent study for the World Intellectual Property Organization found only eight of 50 sampled marketplaces to have coherent anti-counterfeiting strategies (WIPO, 2023).

Low-trust markets amplify the difficulty. Where formal institutions for certification, redress and enforcement are weak, buyers fall back on personal relationships and physical presence, which do not scale to online settings. Nigeria's motor spare-parts and mechanic-services sector is a clear case. Transactions are cash-based and unrecorded, parts identification relies on a seller's verbal assurance, mechanics are found through referral, and estimates attributed to the Standards Organisation of Nigeria (2020) suggest a large share of parts in informal markets are counterfeit. Digital platforms promise to formalise such markets, but they will be adopted only if they are trusted, and they will be trustworthy only if their design addresses the specific sources of risk.

This article asks two questions. *What layers of trust must a marketplace for safety-critical goods supply in a low-trust environment?* And *how do those layers depend on each other?* We answer by synthesising literature and proposing a framework with testable propositions, then illustrating it with a platform designed for the Nigerian aftermarket (Egware & [Supervisor name], in preparation). The contribution is a bridge between three literatures that usually run separately: online-trust theory, counterfeit and supply-chain integrity research, and information-systems design for emerging markets.

2. Approach

This is a narrative, theory-building review and not a systematic review. The literature base comes from a structured review carried out for a postgraduate design project on spare-parts e-commerce, extended with targeted searches in 2026 for recent work on counterfeit control in online marketplaces, automotive e-commerce, payment and application security, and Nigerian data-protection law. We prioritised peer-reviewed theory and evidence, and used standards and regulatory documents where they are the authoritative source. We did not conduct a formal quality appraisal, and we flag where an evidential claim comes from a single or locally reported study. The framework is a theoretical construction offered for empirical testing.

3. Theoretical foundations

Information economics. Akerlof (1970) showed that when sellers know quality and buyers do not, bad goods can drive out good ones. Dimoka et al. (2012) refined this for online markets by separating description uncertainty (what is it?) from performance uncertainty (how will it work?), both of which lower what buyers will pay. For spare parts, description uncertainty includes whether the part fits the vehicle, and performance uncertainty includes whether it is genuine and how it fails. Because both are present, mechanisms that tackle only one will leave a large residual risk.

Trust and acceptance. Gefen et al. (2003) integrated trust with the Technology Acceptance Model, showing that trust and perceived usefulness and ease of use jointly explain online purchase intention, and the unified acceptance models extend this with social influence, facilitating conditions and price value (Venkatesh et al., 2003, 2012). In low-infrastructure settings, facilitating conditions (devices, connectivity, and payment access) can decide whether trust ever has a chance to matter.

Signals and reputation. Written feedback from other buyers helps differentiate sellers and supports price premiums (Pavlou & Dimoka, 2006). But reputation systems work only if the identity behind the reputation is stable and costly to abandon. Peinkofer and

Jin (2023) show that disclosure of who owns inventory and who fulfils an order shapes how consumers assign responsibility when deceptive counterfeits arrive, so identity disclosure is itself a trust-relevant design variable.

Transaction cost and platform theory. Williamson (1985) frames governance as a response to opportunism under asset specificity and uncertainty; in a marketplace the platform operator supplies governance that individual buyers cannot. Two-sided market theory explains the operator's role as a manager of participation on both sides, where decisions on admission, pricing and rules determine the quality of the network (Rochet & Tirole, 2003). A platform that does not hold inventory therefore inherits the duty to curate its sellers.

4. What the evidence says about risk

Three strands of evidence frame the design problem.

Counterfeits are a safety problem, and inspection is weak. Reviews of the automotive supply chain find that parts are commonly validated by packaging marks, that sophisticated counterfeiters copy packaging, and that authenticity is hardest to verify for parts that are not connected to the vehicle's electronics, such as brake pads and tyres. Proposed technical countermeasures include cyber-physical trust anchors linked to tamper-resistant records (Maasberg et al., 2023) and blockchain-based anti-counterfeiting and privacy-preserving vehicle supply chains (Zhang et al., 2022). These are promising but depend on supply-chain participation and cost that retail marketplaces in low-income settings do not control.

Marketplaces under-verify. The WIPO study found that weak seller verification is a fundamental weakness and noted a practice it calls adopted verification, where a marketplace accepts sellers because they already trade elsewhere (WIPO, 2023). The implication is that verification must be done by the platform for its own participants and must be meaningful.

Local evidence on complaints, preferences and logistics is thin but consistent. A six-month study of Ghanaian automotive

platforms reported that about one in five buyer complaints concerned parts that did not match advertised specifications or were suspected counterfeits (Mensah & Agyapong, 2024). A survey of Nigerian vehicle owners reported price comparison as the most valued online feature (Ihejirika & Nwachukwu, 2023). Evidence on adoption suggests peer recommendation can outweigh advertising for first-time use (Osei & Boateng, 2023), while other work argues institutional signals such as registration and certification may dominate for higher-value purchases (Nkemdirim et al., 2022). Delivery of heavy or irregular parts is a persistent barrier outside major cities (Alabi & Olorunfemi, 2023). We treat these as indicative and recommend replication, since most come from single studies.

5. A layered framework

We propose six layers (Table 1). Each answers a distinct source of risk and has its own failure mode.

Table 1. Layers of marketplace trust for safety-critical goods

Layer	Core question for the buyer	Typical mechanisms	Risk addressed	Principal limit
L1. Seller identity and accountability	Who is selling, and can they be held to account?	Credential review, verified badge, business registration, bonding or deposit	Anonymous and disposable sellers	Depends on honesty of submitted documents; bonding requires capital and dispute rules
L2. Product information	Is this the right part for	Structured catalogue, make–	Description uncertainty;	Catalogue accuracy;

Layer	Core question for the buyer	Typical mechanisms	Risk addressed	Principal limit
and fit	my vehicle, exactly as described?	model–year filters, part numbers, standard product identifiers	incompatibility	identifiers do not prove authenticity
L3. Transaction safety	Will my money and card data be safe and recorded?	Certified payment processor, hosted checkout, unique references, order lifecycle	Payment fraud; no proof of purchase	Dependence on third-party processor
L4. Reputation and social proof	What have others experienced?	Ratings, written reviews, recency weighting, endorsements	Performance uncertainty; seller moral hazard	Needs L1 to be credible; can be gamed
L5. Regulatory and data governance	Is my data handled lawfully and is the system secure?	Data protection compliance, security frameworks, audit trails	Privacy harm; breaches; legal exposure	Compliance is uneven; enforcement capacity varies
L6. Physical assurance and fulfilment	Is the part really genuine, and does it arrive intact and on time?	Provenance records, manufacturer authorisation, inspection, logistics partners	Counterfeits; late or damaged delivery	Largely outside software; costly

The layers reflect the governance questions regulators and standards bodies already ask. L5 draws on the NIST Cybersecurity Framework 2.0 (Pascoe et al., 2024), the OWASP Top 10:2025 (OWASP Foundation, 2025), PCI DSS v4.0.1 for card data (PCI Security Standards Council, 2024), and Nigeria's data-protection regime, namely the Nigeria Data Protection Act 2023 and the Nigeria Data Protection Commission's General Application and Implementation Directive 2025, in force since 19 September 2025, which replaced the earlier Nigeria Data Protection Regulation (Federal Republic of Nigeria, 2023; Nigeria Data Protection Commission, 2025). Hosted checkout with a certified processor shrinks L3 compliance scope; Paystack states that it is audited as a PCI DSS Level 1 service provider (Paystack, n.d.).

5.1 Propositions

The following propositions are conceptual and are stated so that they can be tested.

P1 (Identity precedes reputation). Rating and review mechanisms (L4) improve buyers' trust in a marketplace only to the extent that seller identity and accountability (L1) are established; where sellers can re-register at no cost, reputation scores will carry little information. *Rationale:* feedback supports premiums for identifiable sellers (Pavlou & Dimoka, 2006); marketplaces that under-verify allow bad actors to reset (WIPO, 2023).

P2 (Fit information has first-order value). Structured product-fit information (L2) reduces return and safety costs by more than price-transparency features do, even if buyers rate price comparison as the more attractive feature at the point of choice. *Rationale:* description uncertainty is a primary driver of loss (Dimoka et al., 2012); stated preferences for price (Ihejirika & Nwachukwu, 2023) may diverge from realised outcomes.

P3 (Complementarity of L1 and L3). The effect of payment safety (L3) on purchase intention is moderated by seller accountability (L1): secure payment to an unaccountable seller protects the card but not the outcome, so its trust benefit is limited without L1.

P4 (Recency-sensitive reputation). Reputation measures that weight recent experience more heavily than old reviews track seller quality better and discourage coasting than unweighted averages do, particularly for sellers whose service quality changes over time.

P5 (Software ceiling). For safety-critical goods, platform-side measures in L1–L5 reduce but cannot eliminate counterfeit risk; residual risk depends on L6, and the trust gap closes only when physical assurance (provenance, authorised-supplier channels, bonding) is added. *Rationale:* authenticity of installed parts remains hard to verify (Maasberg et al., 2023).

P6 (Contextual weighting). The relative importance of layers varies with context: where formal institutions are weak, buyers will weight L1 and L6 more heavily; where institutions are strong, L5 and L4 will dominate. Peer and institutional signals interact with purchase value (Nkemdirim et al., 2022; Osei & Boateng, 2023).

6. Illustration: an integrated platform for Nigeria

An integrated spare-parts and mechanic-discovery platform designed for Nigeria (Egware & [Supervisor name], in preparation) offers a concrete reading of the framework. At L1, vendors and mechanics submit credentials that an administrator reviews before a verification badge is granted. At L2, a catalogue linked to a vehicle-compatibility table lets buyers filter by make, model, year and category and shows only parts in stock. At L3, checkout is hosted by a certified payment processor, so card data never touch the platform's servers, and an order is committed only after a validated payment confirmation. At L4, vendors and mechanics carry ratings computed with a recency weight, $w = 1/(1 + \alpha \cdot \text{days})$, so that recent service counts for more. At L5, the design anticipates data-minimisation, consent and breach-response duties under the Nigeria Data Protection Act. L6 is where the platform is weakest by design: it records seller identity and transactions but does not authenticate the

physical part, and delivery of bulky parts is handled by sellers pending third-party logistics integration. The platform's recommended upgrades (vendor bonding with escrow, logistics integration, and progressive web delivery) are, in the terms of the framework, reinforcements of L1, L6 and the facilitating conditions that let all layers reach users.

The illustration also shows how the layers interact. The mechanic directory shares the identity and rating infrastructure of the parts marketplace, so a user's trust in one side of the platform can transfer to the other, an example of the cross-side effects emphasised by two-sided market theory (Rochet & Tirole, 2003).

7. Implications

For platform designers. Prioritise by risk, not by fashion. Build identity and fit first, because they condition the value of everything else, then payment safety, then reputation. Do not claim that verification proves authenticity; present it as accountability, and work toward L6 through bonding and authorised channels. Security and privacy are design requirements (Pascoe et al., 2024; OWASP Foundation, 2025), not finishing touches.

For regulators and standards bodies. The framework suggests a division of labour: standards bodies and manufacturers define and enforce authenticity channels (L6); data-protection authorities supervise L5; and platform duties of seller verification and dispute handling (L1) can be made explicit, as policy recommendations for safety-critical categories already propose (Standards Organisation of Nigeria, 2023). Evidence from other jurisdictions shows that clear complaint-handling and transparency strongly influence consumer trust in marketplaces, which supports clear platform obligations.

For researchers. The propositions can be tested with a combination of field experiments (varying L1 and L4 signals), transaction-log analysis (return rate, complaint rate, repeat purchase), and survey instruments for trust and perceived risk grounded in the acceptance literature (Gefen et al., 2003; Venkatesh et al., 2012).

Priority questions are whether seller bonding changes counterfeit incidence, whether guided fit selection lowers returns, and how buyers trade off price and trust in markets where counterfeits are cheaper.

8. Limitations

The framework is theoretical and has not been tested as a whole. Several local sources are single studies whose results need replication, and we have not undertaken a formal systematic review. The layers are analytically distinct but overlap in practice, and the propositions describe tendencies, not laws. The illustration is a design, not a field result. Finally, the framework is developed from automotive parts and may need adaptation for other safety-critical categories, such as medicines or electrical goods, where regulation and physical assurance work differently.

9. Conclusion

Trust in a marketplace for safety-critical goods in a low-trust environment cannot be created by a single feature. It has to be built in layers, with identity and fit at the base, transaction safety and reputation above them, governance around them, and physical assurance as the layer that software can support but not replace. Making these dependencies explicit gives designers a way to prioritise, gives regulators a way to allocate duties, and gives researchers propositions to test. The Nigerian spare-parts market is a demanding but instructive setting in which to do so.

References

Akerlof, G. A. (1970). The market for “lemons”: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics, 84*(3), 488–500. https://doi.org/10.2307/1879431

Alabi, F., & Olorunfemi, T. (2023). Last-mile delivery performance in Nigerian e-commerce: An analysis across product categories. *Journal of Logistics and Supply Chain Management, 11*(1), 22–41.

Dimoka, A., Hong, Y., & Pavlou, P. A. (2012). On product uncertainty in online markets: Theory and evidence. *MIS Quarterly, 36*(2),

395–426. https://doi.org/10.2307/41703461

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023.*

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519

Ihejirika, K., & Nwachukwu, C. (2023). Consumer priorities in Nigerian online spare parts purchasing: A survey of vehicle owners in Port Harcourt and Abuja. *Journal of African Business, 24*(2), 190–208.

Maasberg, M., Butler, L. G., & Taylor, I. (2023). Key parameters linking cyber-physical trust anchors with embedded internet of things systems. *Frontiers in Communications and Networks, 4*, Article 1096841. https://doi.org/10.3389/frcmn.2023.1096841

Mensah, K., & Agyapong, D. (2024). Product authenticity complaints in Ghanaian automotive e-commerce platforms: A six-month empirical study. *African Journal of Business Management, 18*(1), 1–14.

Nigeria Data Protection Commission. (2025). *Nigeria Data Protection Act 2023: General Application and Implementation Directive (GAID) 2025* (NDPC/NDP ACT-GAID/01/2025).

Nkemdirim, O., Obi, K., & Abubakar, J. (2022). Institutional trust versus social recommendations in Nigerian digital commerce adoption: Evidence from the automotive sector. *Electronic Commerce Research, 22*(4), 1431–1458.

Omorogbe, O. H., Eduje, A. I., Anyanwu, L., Obeka, O. B., Ukaoha, K. C., Izevbuwa, O. G., Ighotuweyin, A. F., & Arenvbaguehita, O. D. (2025). The impact of artificial intelligence (AI) on fraud detection in banks in Nigeria. Oil and Gas Journal, 2(9), 10.

https://www.researchgate.net/publication/395988619_The_Impact_of_Artificial_Intelligence_AI_On_Fraud_Detection_in_Banks_in_Nigeria

Omorogbe, O. H., Amoforitse, F. I., & Ozobialu, E. C. (2026). Explainable reinforcement learning for adaptive autonomous agents: A framework for interpretable decision-making in dynamic environments. Pacadpub (IJIS).
https://www.pacadpub.com/index.php/ijis/article/view/49

Omorogbe, O. H., Amoforitse, F. I., Ozobialu, E. C., Eduje, A. I., & Obande, B. (2026). Resolving the scalability–explainability–adaptability trilemma in hybrid optimization systems for disaster management. International Journal of Data Science and Analytics (IJDSA), 2(1).
https://www.pacadpub.com/index.php/ijdsa/article/download/51/36

Osei, K., & Boateng, R. (2023). Social influence and e-commerce adoption in West African markets: Evidence from the automotive sector. *Information Technology & People, 36*(1), 244–268.

OWASP Foundation. (2025). *OWASP Top 10:2025.* https://owasp.org/Top10/2025/

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pavlou, P. A., & Dimoka, A. (2006). The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation. *Information Systems Research, 17*(4), 392–414. https://doi.org/10.1287/isre.1060.0106

Paystack. (n.d.). *Compliance at Paystack.* https://paystack.com/compliance

PCI Security Standards Council. (2024). *Payment Card Industry Data Security Standard: Requirements and testing procedures, v4.0.1.*

Peinkofer, S. T., & Jin, Y. H. (2023). The

impact of order fulfillment information disclosure on consequences of deceptive counterfeits. *Production and Operations Management, 32*(1), 237–260. https://doi.org/10.1111/poms.13833

Rochet, J.-C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association, 1*(4), 990–1029. https://doi.org/10.1162/154247603322493212

Standards Organisation of Nigeria. (2020). *Report on counterfeit automotive parts in Nigerian informal markets.* SON Publications.

Standards Organisation of Nigeria. (2023). *Recommendations for e-commerce platforms trading in safety-critical automotive components* (SON Policy Brief No. 14).

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178. https://doi.org/10.2307/41410412

Williamson, O. E. (1985). *The economic institutions of capitalism: Firms, markets, relational contracting.* Free Press.

World Intellectual Property Organization. (2023). *Practices used by online marketplaces to tackle the trade in counterfeits* (WIPO/ACE/16/11). Advisory Committee on Enforcement, 16th session.

Zhang, C., Zhu, L., Xu, C., Sharif, K., Lu, R.,

& Chen, Y. (2022). APPB: Anti-counterfeiting and privacy-preserving blockchain-based vehicle supply chains. *IEEE Transactions on Vehicular Technology, 71*, 13152–13164. https://doi.org/10.1109/TVT.2022.3196051