

Managing fraud risks in humanitarian E-voucher systems

Journal of Information Technology
Teaching Cases
2025, Vol. 0(0) 1–9
© Association for Information
Technology Trust 2025



Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/20438869251393287

journals.sagepub.com/home/jitcc



Chinomso Nwagboso¹ and Chibuzo Nwagboso²

Abstract

In Gwoza, a conflict-affected region in northeast Nigeria, a digital e-voucher system designed to streamline humanitarian food distribution is undermined by identity duplication and unauthorised enrolment practices. This teaching case follows Sa'adatu, a frontline Food and Livelihood Assistant, as she uncovers multiple cards issued to members of the same household, exposing the system's vulnerability to manipulation. The system was developed as part of the World Food Programme's digital transformation agenda, supported by Nigerian state authorities and INGOs, aiming to replace bulk food distribution with transparent, biometric-based entitlements. The case explores the technological limits of biometric verification in low-infrastructure contexts, the governance challenges posed by stakeholder influence, and the ethical challenges in enforcing accountability and protecting access to aid. Failure of this system risks not only exclusion of vulnerable households but also reputational harm and donor withdrawal. With no formal audit trails, limited escalation mechanisms, and competing demands for integrity and inclusion, this case allows students to examine digital identity systems, fraud risk management, and ethical discretion in humanitarian information systems, encouraging thoughtful discussion on technology governance in fragile and complex environments.

Keywords

Crime and security, data quality, digitalisation, ethics, ICTs and society, IS in developing countries, IS management and governance, social analysis of technology, teaching cases

Learning outcomes

By engaging with this case, students will be able to:

- (1) Analyse the design and operational challenges of implementing biometric-linked digital aid systems in low-infrastructure and conflict-affected settings.
- (2) Evaluate the risks and limitations of identity duplication, weak audit trails, and informal governance structures in e-voucher platforms.
- (3) Critically assess the ethical dilemmas faced by frontline staff navigating between system integrity and humanitarian inclusion.
- (4) Propose practical and context-appropriate improvements to digital verification systems, fraud detection protocols, and field-level decision support mechanisms.
- (5) Discuss how stakeholder power dynamics and local adaptations can influence the effectiveness and fairness of humanitarian technology systems.

displaced tens of thousands of people, severed access to farmland, and made food production nearly impossible for many households. For internally displaced persons (IDPs), the monthly food assistance provided through international aid organisations is often the only reliable source of sustenance.

The e-voucher system in Gwoza was introduced through a partnership between the World Food Programme (WFP) and international non-governmental organisations (INGOs), with operational oversight from Nigerian state authorities. The policy logic behind the programme was to move away from bulk food distributions – plagued by inefficiencies, diversion, and security risks – towards a household-size-based entitlement system. Larger families would receive proportionally higher monthly allocations, while biometric verification at vendor shops was intended to ‘close

Too many cards, too little food

In the conflict-affected region of Gwoza, Borno State, humanitarian aid is a lifeline. Years of insurgency have

¹Nottingham Trent University, Nottingham, UK

²International Food and Policy Research Institute, Abuja, Nigeria

Corresponding author:

Chinomso Nwagboso, Nottingham Business School, Nottingham Trent University, 50 Shakespeare Street, Nottingham NG1 4FQ, UK.

Email: Chinomso.nwagboso@ntu.ac.uk

loopholes' and ensure that only authorised beneficiaries accessed aid. Donor conditionalities reinforced this emphasis on transparency, linking continued funding to demonstrable reductions in fraud, leakage, and inequity (Table 1).

When beneficiaries visited approved vendors, they thumbprinted at the point-of-sale terminal, viewed their card balance, and redeemed food items – typically maize, beans, cereal, and vegetable oil – within a fixed redemption period. According to Sa'adatu, a Food and Livelihood Assistant working for an international medical NGO in Gwoza, the e-voucher system was designed to offer beneficiaries dignity of choice while reducing fraud and minimising logistical bottlenecks.

'The number of people in your household determines how much you receive on your card. If you have more people, your money is more. If less, your money is less – that's how it works on the e-voucher'.

Yet, despite its intended efficiencies, the system was vulnerable to manipulation. During a routine field visit to monitor vendor shops, Sa'adatu observed an unusual pattern: multiple e-voucher cards being used by individuals claiming to belong to the same household. In one case, three different people visited the same vendor over the course of 2 days, each presenting a valid card linked to the same surname and claiming some variant of kinship – 'we are cousins', 'we have the same mother but different fathers', 'our grandmother registered us'. Each cardholder thumbprinted successfully and collected food. None of the cards were flagged by the system.

Sa'adatu's suspicion grew. She had heard rumours from colleagues and local residents that some households were gaming the system by registering multiple cards using slightly varied household compositions or vague family connections. Without a national digital ID system or centralised biometric database, it was difficult to verify claims of kinship or household boundaries. What was meant to be a simple system of accountability had created its own moral grey zones.

'Some families have found a way to register two or three cards under different names', she explained later. 'You can't say it's fake, because maybe they are really related. But the same household ends up collecting food more than once'.

The vulnerability of the system is both technical and social. Beneficiary registration often depends on lists provided by local leaders or stakeholders, who are expected to nominate the most vulnerable households. In practice, these

community gatekeepers sometimes prioritise their relatives or accept payment in exchange for inclusion. According to Sa'adatu:

'Sometimes the stakeholders bring their family and friends as beneficiaries. And in some cases, people give them money to be included'.

The result is a skewed distribution system where eligibility is partially determined by connections rather than need. At the same time, the e-voucher system does not currently support cross-verification or flagging of suspected duplicate records. Without such controls, frontline staff like Sa'adatu are left to rely on intuition, pattern recognition, and incomplete information.

The logic of the e-voucher system

The e-voucher system deployed in Gwoza is part of a wider digital transformation in humanitarian aid delivery. In response to the logistical and ethical challenges of distributing food aid in conflict zones, organisations such as the World Food Programme (WFP) have adopted electronic vouchers as a means to improve transparency, reduce handling risks, and empower beneficiaries to exercise limited choice in what they consume. In theory, this model replaces the traditional system of physical food distributions – often plagued by inefficiencies, theft, and bulk transport costs – with a more agile and accountable mechanism of localised vendor-based redemption.

Policy development and oversight

The system in Gwoza emerged from WFP's broader 'Cash and Voucher' policy shift (2016–2018), which sought to replace in-kind food distributions with digitally mediated entitlements across fragile and low-infrastructure contexts. Its design was developed jointly with international NGOs, while oversight rested with state authorities and donor agencies. The programme's sustainability depended on demonstrating fraud reduction, traceability of transactions, and measurable efficiency gains – conditions directly tied to donor funding conditionalities.

Monitoring is structured around the flow of transactions. Vendors are equipped with biometric point-of-sale devices and are required to upload transaction logs periodically. These uploads form the basis for NGO reimbursement, and in theory, allow programme managers to monitor usage trends. In practice, however, dashboards remain weak. Field

Table 1. Household size and corresponding E-voucher allocations in Gwoza.

Household size	Monthly E-voucher allocation (₦)	Typical redemption
3 persons	₦12,500	Basket of maize, beans, oil
6 persons	₦25,000	Expanded household basket
8 persons	₦33,000	Larger household basket

officers like Sa'adatu rarely have access to live monitoring tools, and anomalies are usually detected through observation rather than automated reporting (Figure 1).

Beneficiary numbers under pressure

The programme's reliance on donor funding has made coverage volatile. In 2024, the Gwoza food programme served approximately 18,000 beneficiaries. By mid-2025, following funding cuts, this number had dropped to 11,000 beneficiaries – a 39% reduction. This contraction heightened scrutiny of system integrity, as every duplicated household record potentially meant another vulnerable family excluded. At its core, the e-voucher model in Gwoza operates as a digitally mediated entitlement system anchored in household-level registration. Each household selected for the programme is issued a digital card, preloaded with a monthly monetary value determined by the number of people registered under that household. The card is paired with biometric identification, typically a fingerprint, to reduce the risk of impersonation. At distribution, beneficiaries present their card at a designated local vendor, authenticate their identity using the biometric terminal, and receive food items equivalent to their balance.

This process is governed by a simple algorithm: more registered individuals equal more money on the card. For example, a household of six may receive ₦25,000 per month, while a household of three may receive ₦12,500. This financial value is not redeemable as cash but is used to 'purchase' approved food items from contracted vendors – usually staples such as maize, beans, cereal, and vegetable oil. The programme seeks to maintain both nutritional value and market neutrality by fixing the item list and closely monitoring prices. One of the key features of the system is point-of-sale validation. Vendors are equipped with

handheld biometric devices connected to the central e-voucher database. When a beneficiary visits a shop, they must thumbprint to confirm their identity, at which point their balance is displayed on the vendor's device. The vendor then deducts the appropriate amount based on the items issued and receives reimbursement from the NGO after uploading the transaction record. This mechanism is intended to ensure that only eligible beneficiaries access the aid, and that vendors cannot manipulate prices or issue goods without digital confirmation.

However, this logic rests on the assumption that each card represents a distinct, verifiable household. In practice, this assumption is undermined by the lack of a unified civil registration system and the informality of household structures in northeast Nigeria. Household registration is typically conducted during community onboarding, where local leaders and ward heads assist NGOs in identifying vulnerable families. These stakeholders provide names, household sizes, and photos, which are then input into the e-voucher database. While some fingerprint capture is done during onboarding, technical limitations, equipment shortages, and urgent timelines often lead to incomplete or informal records.

To address issues of mobility and illness, each card can be assigned an alternative user, who is also enrolled biometrically and authorised to redeem food on behalf of the main cardholder. This feature, designed to improve flexibility, has introduced its own complications.

In many cases, individuals present cards on behalf of multiple relatives or 'extended family' members, and if the fingerprints match any of the registered alternatives, the transaction is allowed. Field staff have observed that some households exploit this by registering multiple cards under related names – cousins, in-laws, distant aunts – and then rotating their use during distributions. The redemption

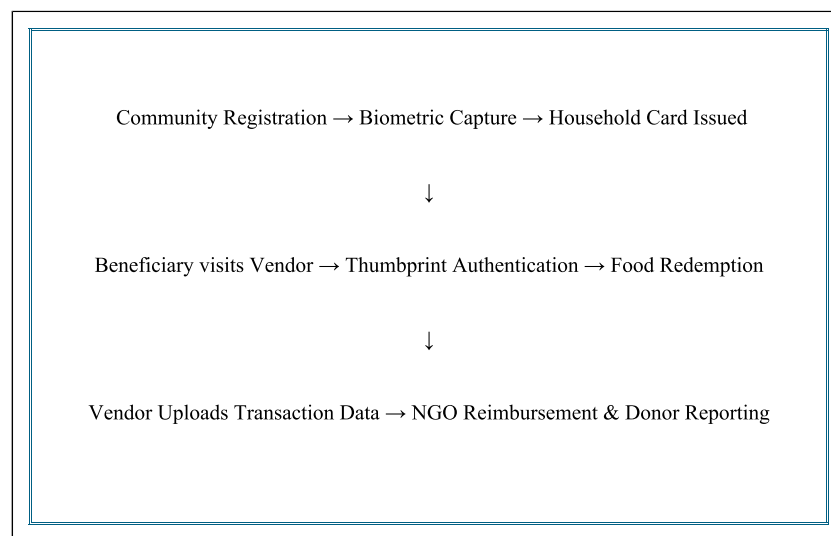


Figure 1. E-voucher transaction flow.

window is also time-bound. Beneficiaries typically have 15 days within which to redeem their entitlements. After this window closes, the unspent balance is wiped, and the system resets for the next cycle. This structure aims to manage cash flow, prevent hoarding, and ensure timely usage. However, it also puts pressure on field teams and beneficiaries to resolve any verification or card-related issues within a narrow timeframe, especially in remote communities where travel or illness can interfere with attendance.

From the NGO perspective, the system also allows for monitoring and reporting, although this function is not always robust. Vendors are required to upload transaction logs, and in theory, NGO staff can extract reports to identify usage trends, high-volume users, or anomalies in redemption patterns. In practice, however, poor internet connectivity, limited IT capacity, and decentralised data systems reduce the effectiveness of monitoring. Field officers like Sa'adatu often have no access to live dashboards or audit tools, and anomalies such as duplicate household names or rapid re-redemption must be flagged manually through observation and pattern recognition. Another limitation of the system is the absence of integrated checks against duplicate or overlapping registrations. There is no mechanism for flagging similar surnames, household addresses, or shared fingerprints across cards. Nor is there a robust appeals or investigation process for suspected fraud. Frontline staff can report anomalies, but response times are slow, and repercussions may disproportionately affect innocent parties – such as children or the elderly – who rely on the food. As a result, many staff choose to manage issues informally, quietly removing cards, advising beneficiaries privately, or raising soft concerns with local leaders.

Overall, while the e-voucher system represents a significant advance over bulk food distribution models, it is vulnerable to the structural and institutional constraints of the environment in which it operates. The assumptions of technological neutrality, user integrity, and clean data do not always hold in practice. Household size becomes not just a demographic metric but a site of negotiation and moral ambiguity. In places like Gwoza, where the line between adaptation and abuse is blurred, the logic of digital fairness must coexist with the messiness of humanitarian reality.

Mismatched design and local practice

The e-voucher system implemented in Gwoza is a technical solution operating in a non-technical world. Its design presumes standardisation, transparency, and central oversight. But in the local context, where kinship networks, social obligations, and informal power structures shape access to aid, the system is constantly reinterpreted, adapted, and – in some cases – manipulated. Between digital architecture and daily reality lies a growing distance, filled by human discretion, improvisation, and quiet workarounds.

At the heart of this mismatch is the process of beneficiary selection. While the system relies on household-level data to determine entitlements, these data are largely gathered through community gatekeepers – traditional rulers, ward leaders, or other locally respected figures. Their cooperation is essential for project implementation, but their involvement introduces complex incentives. As Sa'adatu, a Food and Livelihood Assistant in Gwoza, explained:

'The stakeholders sometimes are part of our problem because they mostly bring out their family and friends as beneficiaries. In some cases, people give them money to be included'.

What begins as a mechanism to ensure local ownership can quickly become a means of informal gatekeeping and favouritism. Vulnerability assessments – intended to identify the most food-insecure individuals – are often influenced by personal relationships, patronage expectations, or pressure to reward loyalty. As a result, well-connected but relatively secure individuals may receive aid, while more vulnerable households remain excluded (Table2).

This divergence between system logic and local dynamics is not limited to enrolment. Even after cards are issued, the way beneficiaries use and interpret them reflects broader socioeconomic realities. Beneficiaries understand that household size determines how much aid they receive. In this context, household size becomes not a fixed demographic fact, but a strategic construct. Families register multiple cards under different branches of the same household. Children are 'distributed' across uncles, cousins, or grandparents to create the appearance of separate units. According to Sa'adatu:

'Some families have found a way to register two or three cards under different names... They say, "This one is from

Table 2. Policy versus Practice in Gwoza's E-Voucher System.

Policy expectation	Observed reality
Neutral household data provided by local leaders	Elite capture and gatekeeping: Leaders prioritise relatives or accept payments
Biometric uniqueness ensures one card per household	Multiple enrolments: Families secure two or three cards under different kinship claims
Transparent vulnerability-based inclusion	Patronage-driven inclusion, excluding the most at-risk households
Accountability through digital transaction logs	Weak monitoring and informal workarounds by staff and vendors

the same mother, but different father,” or, “We are cousins but we cook separately.” It’s hard to prove otherwise’.

These adaptations are not necessarily fraudulent in intent. In a context where survival depends on securing food, households may stretch definitions of eligibility to meet immediate needs. But they exploit the absence of data integration – no shared IDs, no household address database, and no cross-verification between cards. The e-voucher system’s reliance on biometric thumbprints as a safeguard is similarly limited. Once a person is registered on multiple cards – either as a primary user or an alternate – the system cannot detect overlap. Such mismatches undermine equity, erode donor trust, and may trigger programme suspension or reallocation of funds. They reveal how digital fairness can be quietly subverted by informal practice, leaving frontline staff like Sa’adatu caught between rigid rules and community realities.

Identity duplication and data integrity risks

The first sign of trouble came during a routine vendor visit. Sa’adatu noticed three individuals visiting the same vendor in close succession, each presenting a different card but claiming to be from the same household or extended family. One said he was the younger brother. Another claimed to be a cousin. All three thumbprinted successfully and collected food. There was no system error, no alert to suggest that duplication had occurred. And yet, it was clear that something was wrong.

‘I asked the vendor why the same household had three different cards. He said they told him they were all related, but had different kitchens. There was nothing he could do’.

The e-voucher platform lacked the most basic fraud detection features. There was no function to flag households with similar names, overlapping addresses, or shared biometrics.

In theory, biometric fingerprinting should prevent multiple enrolments, but in practice, it only works if the database is designed to detect and cross-check duplicates. In Gwoza, it was not. Each enrolment was treated as a standalone record. If someone registered as the primary user on one card and as an alternate user on another, the system accepted both.

In humanitarian settings like Gwoza, these gaps are not merely technical – they are structural. Beneficiary registration often takes place under intense time pressure, with limited access to electricity, connectivity, or functioning biometric devices. Field staff may be forced to enrol people manually, record inconsistent spellings of names, or rely on verbal confirmation of household size. In such environments, the chances of data duplication are high – even without malicious intent (Table 3).

‘Sometimes, even genuine families get registered twice’, Sa’adatu noted. ‘They may have moved from one location to

another, or changed their name slightly. There’s no central ID system to confirm’.

The lack of a national digital ID system compounds the problem. Without a unique identifier, verification depends on photographs, biometrics, and local familiarity – none of which are reliably standardised. Some households submit photographs during registration, but these are rarely used in day-to-day verification. Photos may be stored offline or printed in folders, but most vendors do not have access to them during transactions. Instead, they rely solely on fingerprint recognition at the point of sale – and this, too, is limited by equipment failures, dusty fingers, and the occasional mismatch between hardware and user.

Even when frontline staff detect suspicious patterns, there is no systematic process for escalation. Sa’adatu could report her findings to her supervisor, but investigations are slow, and corrective action is rare. Moreover, the consequences of removing someone from the register are significant. In a context where food aid is the main source of survival, flagging a household for potential duplication could mean excluding them altogether – even if children or elderly members depend on the aid.

‘You don’t want to report and then find out the children go hungry. But if you keep quiet, the programme becomes unfair for everyone else’.

The burden of discretion falls squarely on field officers, who must decide when an irregularity is worth pursuing and when to let it pass. Many resort to informal strategies: warning beneficiaries privately, discouraging vendors from enabling repeat visits, or quietly flagging cases during co-ordination meetings. But without a formal mechanism to verify identities or audit card usage, these strategies are inconsistent and rarely scaled. This lack of monitoring capacity runs counter to recognised humanitarian accountability standards such as the Sphere Handbook and the Core Humanitarian Standard, both of which emphasise transparency, fairness, and mechanisms for complaint and redress. By failing to provide robust audit trails or escalation pathways, the system risks undermining not only beneficiary trust but also donor confidence. The case of multiple cards in one household is not a rare glitch – it is a window into the structural weaknesses of humanitarian data systems in low-resource settings. It shows how biometric tools, while powerful in theory, can become hollow in practice without the necessary governance, auditability, and field-level feedback loops.

Stakeholder dynamics and ethical dilemmas

The success of humanitarian aid distribution in conflict zones like Gwoza depends on technology and logistics, and relationships – specifically, the fragile and often informal relationships between humanitarian workers and local

Table 3. Consequences of weak monitoring.

Level	Consequence of duplication
Household	Fraudulent households receive double or triple aid allocations
Vulnerable families	Genuine households risk exclusion due to limited slots and donor cuts
Programme/Donors	Reputational damage, reduced funding, stricter conditionalities imposed

power holders. These stakeholders, including traditional leaders (bulama), ward heads, community elders, and politically connected intermediaries, occupy a dual role: they are essential to the delivery of aid, and yet they often act as gatekeepers who shape who gets access and who does not. Their influence permeates every stage of the e-voucher system, from beneficiary selection to dispute resolution, creating ethical dilemmas that frontline officers must navigate with caution.

When NGOs enter a new community, protocol demands engagement with local authorities. These figures are asked to facilitate introductions, explain the programme to the community, and help identify the most vulnerable households. In principle, this partnership ensures cultural legitimacy and local ownership. But in practice, it can entrench existing hierarchies and patronage systems. As Sa'adatu, a Food and Livelihood Assistant working in Gwoza, explained:

'You go to them one by one, tell them your aim and purpose, and they give you the names of beneficiaries. But many times, they only bring out their family and friends'.

What appears on paper as a participatory process becomes, in reality, an exercise in selective inclusion. Local leaders use their influence to register those close to them – sometimes for altruistic reasons, sometimes for personal gain. In a few cases, individuals reported paying to have their names included on beneficiary lists. The consequences are serious: households with genuine vulnerability are excluded, while better-off individuals receive monthly food entitlements under the guise of need.

'Some of them even have money and cars', Sa'adatu noted. 'They just know the right people to talk to'.

This stakeholder capture highlights a governance gap: while policy assumes neutral oversight, actual monitoring mechanisms fail to hold leaders accountable. This complicates any attempt to police fraud or enforce system integrity. Reporting misuse does not only challenge individual actions—it threatens the informal social contracts that hold the distribution system together. Local leaders who feel undermined may withdraw cooperation, intimidate field officers, or sow mistrust among beneficiaries. In Gwoza, where security is fragile and humanitarian presence depends on community goodwill, these are not hypothetical risks. One poorly handled allegation can derail months of work, endanger staff, or trigger community backlash.

Faced with this reality, field officers like Sa'adatu must exercise discretion. Even when duplication is observed or

irregularities are suspected, the choice to escalate is not straightforward. There is no guarantee that reporting a case will result in fair investigation or systemic correction. In some cases, whistleblowing may harm the vulnerable more than the perpetrators. If a card is suspended, an entire household may go hungry. If a leader is embarrassed, future cooperation may be withheld.

'You report something, and suddenly they stop picking your calls. They don't show up for meetings. You've lost them', Sa'adatu said.

The ethical tension is acute: is it better to protect the programme's integrity, or to ensure short-term food access for those who may still be in need? This tension is heightened by the absence of clear institutional protections or escalation pathways. While there are channels for complaint and feedback, they are often under-resourced or sidelined. The project management committees and community-based feedback mechanisms do exist, but their ability to adjudicate disputes involving powerful stakeholders is limited.

Moreover, field officers are caught in a structural bind. They are expected to uphold donor accountability, but are not always empowered to act. Their authority is constrained by organisational politics, risk-averse leadership, and the realities of operating in a low-infrastructure setting. There is no formal protocol for what to do when a stakeholder intervenes to protect a fraudulent beneficiary, or when multiple cards appear to serve the same household. These grey areas become the daily terrain of humanitarian practice – spaces where ethical decisions must be made with incomplete information and few safeguards.

In these circumstances, staff often resort to informal risk mitigation. Some choose to confront suspected beneficiaries quietly, warning them against returning. Others speak to local leaders privately, asking them to discourage duplication without publicly naming names. These workarounds are not ideal, but they reflect the limits of formal systems in contexts shaped by informality and uneven power.

At the heart of these ethical dilemmas lies a deeper question: who is the system ultimately accountable to? Donors expect clean data and fair distribution. Beneficiaries expect access to food. Local leaders expect recognition of their authority. Field officers are left to navigate these overlapping – and at times conflicting – expectations, often without institutional backing. Failure to manage this tension risks delegitimising the entire programme.

Sa'adatu's experience illustrates the precarious balancing act. She knows the rules of the e-voucher system and the principles it represents. But she also knows that enforcing those rules too rigidly could collapse the relationships on which implementation depends. In that tension lies the challenge of humanitarian digital governance: how to uphold accountability in systems that rely on informal trust, and how to protect fairness when power is unequally distributed.

Technology limits and governance gaps

Despite its digital sophistication on paper, the e-voucher system deployed in Gwoza lacks many of the core capabilities needed for transparent, auditable, and adaptive humanitarian management. While designed to promote fairness, reduce diversion, and improve operational efficiency, the system suffers from foundational technical shortfalls that render it ill-equipped to handle the complexities of aid distribution in conflict-affected, low-infrastructure environments. These limitations do not exist in isolation – they feed into broader governance gaps that undermine the programme's ability to detect misuse, enforce rules, or support frontline decision-making (Table 4).

One of the most critical weaknesses is the absence of an integrated audit trail. Once a beneficiary redeems their monthly food basket, the vendor uploads transaction data to the central system. However, these data are not routinely analysed for anomalies or linked to dynamic beneficiary profiles. For field officers like Sa'adatu, there is no interface or dashboard that allows for real-time tracking of card usage, redemption frequency, or transaction clustering. Instead, fraud detection relies on anecdotal observations or chance encounters, such as noticing similar names at the vendor or overhearing rumours of duplicated households.

'The only reason I knew something was wrong was because I happened to be there', Sa'adatu recalled. 'There was nothing in the system that would have flagged it for me'.

This reflects a broader issue: the design of the system assumes compliance, rather than anticipating opportunistic behaviour. There are no built-in red flags for duplicate fingerprints, shared household names, suspicious usage patterns, or rapid succession redemptions across cards linked to the same individual. Even basic functionalities –

like notifying field staff when the same biometric appears in multiple records – are absent. Once a fingerprint is captured during enrolment, it is accepted without comparison to others in the database, rendering the biometric layer almost purely ceremonial. In addition, the system offers limited support for field-level verification or case escalation. While NGO staff are nominally able to report anomalies to central programme officers, there are no standard operating procedures for how such reports are reviewed, investigated, or resolved. Investigations are infrequent, communication channels are slow, and outcomes are rarely fed back to the original reporting officer.

This lack of feedback disincentivises frontline engagement with system integrity, reinforcing a culture of resignation: field officers observe problems but lack both the tools and institutional support to address them.

'Even if you report, what happens next? Usually nothing', Sa'adatu explained. 'They'll say, Thank you, we will look into it.' And that's the end'.

The system also struggles with technical fragility in the field. Biometric scanners often fail due to dust, humidity, or poor connectivity. Beneficiaries with worn or scarred fingerprints may be unable to authenticate. Power outages delay uploads. Some vendor shops operate offline for days, only syncing data when they return to better-connected locations. These limitations create openings for informal practices and weaken the credibility of the system's digital safeguards. Meanwhile, data governance policies remain unclear and inconsistently enforced. For example, it is not clear how often household records are updated, who has authority to modify or deactivate a card, or what standards apply for resolving cases of suspected duplication. There is no shared understanding of what constitutes a 'fraudulent household' versus a misunderstood or misrecorded one. This ambiguity fosters inconsistency. One officer might quietly remove a card from the register; another might overlook the issue entirely. The result is uneven enforcement and fragmented institutional memory.

Moreover, the system's data architecture does not easily support longitudinal analysis or cross-site comparisons. Beneficiaries who move from one ward to another are often re-registered as new entries. Their historical data – on household size, redemption behaviour, or complaints filed – do not follow them. This not only inflates the number of

Table 4. System weaknesses and consequences.

System weakness	Operational consequence
No biometric deduplication	Same individual can be enrolled on multiple cards → duplicate households
No integrated audit trail	Transactions cannot be reliably traced → weak accountability
Poor or absent dashboards	Fraud detection depends on chance observation → delayed responses
Weak escalation procedures	Reports rarely acted upon → staff discretion becomes de facto governance
Technical fragility (scanners, power, connectivity)	Frequent breakdowns erode system trust → reliance on informal workarounds
Overall outcome	Reputational harm, donor distrust, and exclusion of vulnerable households

active records but also makes it impossible to identify chronic misuse, duplicate enrolments, or migration-related distortions across the wider programme. In short, the system is transactional, not relational.

These technological limits are compounded by governance gaps at multiple levels. There is often no dedicated fraud response unit, no inter-agency agreement on how to investigate suspected cases, and no formal grievance process for households whose cards are suspended. As a result, decisions are made ad hoc, shaped more by interpersonal relationships than institutional policy. Frontline workers like Sa'adatu must navigate this landscape without legal protection, ethical guidance, or technical support. Their discretion becomes the de facto governance mechanism. This lack of institutional clarity leaves the system vulnerable to exploitation – not only by beneficiaries but also by stakeholders who understand its blind spots. Local leaders may intervene to protect their preferred beneficiaries, vendors may allow questionable transactions to continue, and field officers may hesitate to intervene for fear of reprisals. In this context, the technology becomes a thin layer of digital trust papering over deep procedural uncertainty.

Ultimately, the case of Gwoza reveals the limitations of deploying digital solutions without the surrounding ecosystem of accountability, feedback, and user-centred design. The e-voucher system was introduced to reduce fraud and improve efficiency. But without audit trails, fraud detection protocols, and field-level governance mechanisms, it struggles to meet its goals. For Sa'adatu and her peers, the challenge is not just technical – it is institutional. The question is not only how to improve the system's functionality, but how to build an environment where integrity is not just digitised but upheld.

Integrity or inclusion?

Sa'adatu sat quietly in the corner of the vendor shop, her notepad on her lap, eyes tracing the familiar pattern she had seen twice already that week: a young woman arrived with an e-voucher card, greeted the vendor warmly, and placed her thumb on the biometric reader. The system beeped, approved the transaction, and the vendor handed her the standard food basket. 15 minutes later, a second person came – older, but with the same surname – and repeated the process, with a different card. Then a third. Same address, different first names, and all listed under households of varying sizes. To the system, nothing looked amiss. To Sa'adatu, it was unmistakable: one household, three cards, three rounds of food.

This was not an isolated case. Over the past few weeks, Sa'adatu had begun to notice what she feared was a quiet trend: multiple cards being used by members of the same extended household, sometimes by the same person posing as different recipients. It was hard to be certain. The relationships were often vague – 'my cousin', 'my sister's

daughter', 'we live together, but we cook separately' – and the registration data incomplete. There were no photos printed on the cards, and no address verification protocols. And yet, the food amounts being redeemed were too high for the number of people she knew were living in the compound.

She knew what the protocol said: suspected fraud must be documented and reported to the programme coordinator. Once flagged, cards can be suspended pending investigation. But what would that mean in this case? Would three households be suspended when there was, in fact, only one? Would children go hungry while an inquiry team in Maiduguri deliberated over biometric data and incomplete records? Or would nothing happen at all – no feedback, no follow-up, just a quietly deleted file?

'I've seen them do it before', she thought. 'Sometimes the punishment falls on the wrong person. The grandmother who can't explain herself, the child who wasn't even part of the decision. And sometimes, nothing happens at all'.

The risk wasn't only personal – it was systemic. The programme was already under strain. Due to funding shortfalls, WFP had recently cut 7000 people from the beneficiary list, reducing the coverage from 18,000 to 11,000. The message from management was clear: only the most vulnerable could remain. But if beneficiaries were double-counted, how many truly vulnerable households were being left out? Sa'adatu had heard stories of mothers showing up with nothing to eat, crying at the distribution point because their names weren't selected. The community feedback committee was overwhelmed. Every food cycle brought new complaints.

'If I stay silent, I protect one household- but maybe I exclude two others who need it more'.

Still, reporting came with consequences. The local bu-lama, who had helped register the family in question, had once warned her about 'making too much noise'. Stakeholders had been known to withdraw cooperation from NGOs who questioned their lists. One field officer was reassigned after escalating a complaint that led to a community leader's relative being delisted. And Sa'adatu, despite being diligent and respected, was ultimately a visitor in the community. Her safety – and the success of her work – depended on goodwill. Her team had no fraud unit. There were no whistleblower protections, no formal investigative framework. And even if there were, how would the team prove the household was duplicated? Families often lived in shared compounds but cooked separately. In Hausa culture, extended families frequently spanned multiple households but retained strong economic ties. Where, exactly, was the line between fraud and adaptation?

Sa'adatu considered an alternative. She could speak to the vendor privately and ask them to be more cautious in the future. Or she could approach the family discreetly, advising them that they'd been noticed. Perhaps the quiet warning would be enough. But would that stop the behaviour, or

simply move it elsewhere? As the sun dipped over the edge of Gwoza's rocky hills, Sa'adatu weighed her choices. On one side: the principles of fairness, accountability, and system integrity. On the other: the moral cost of exclusion, the practical risks of confrontation, and the very real hunger that haunted the town when cards were deactivated.

Sa'adatu had to decide: Should she report the suspected duplication and risk harming a vulnerable household, or remain silent and compromise the fairness of a programme already stretched thin? Her next action would not only shape the outcome of this single case – it would define her role in the moral calculus that underpins digital aid delivery in crisis zones. Sa'adatu's dilemma is not just local; it mirrors global debates about balancing system integrity (donor confidence, fraud minimisation) with humanitarian inclusion (ensuring no vulnerable person goes hungry). The consequences of failure are profound: inadequate systems undermine both donor trust and community survival.

Discussion questions

- (1) What are the key technical vulnerabilities of the e-voucher system described in the case, and how do these impact data integrity, auditability, and fraud detection in humanitarian settings?
- (2) In what ways does the absence of a unified digital identity infrastructure contribute to systemic weaknesses in the verification and distribution process? How could this be addressed realistically in low-resource, high-conflict regions like Gwoza?
- (3) How do local stakeholder dynamics – such as gatekeeping by community leaders – interact with or subvert the digital logic of fairness built into the e-voucher platform?
- (4) To what extent can frontline discretion, such as Sa'adatu's decision to report or overlook suspected fraud, be ethically justified? What ethical frameworks or decision models could guide such choices?
- (5) What are the risks of privileging system integrity over humanitarian inclusion, and vice versa? How can aid organisations strike a balance between enforcement and flexibility in fragile environments?
- (6) What design improvements – technical, procedural, or governance-related – could make the e-voucher system more resilient to informal misuse while still respecting community structures?
- (7) How does this case reflect broader tensions in the use of digital technologies for social protection and humanitarian relief in the Global South? What lessons can be drawn for future deployments of ICT4D systems?
- (8) How do donor funding policies influence the design and monitoring of such systems, and what are the wider public consequences if integrity is not maintained?

ORCID iD

Chinomso Nwagboso  <https://orcid.org/0000-0002-1412-3189>

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Author biographies

Chinomso Nwagboso is a Senior Lecturer in Project Management within the Department for Strategy, Analytics and Operations. With a background in Accounting and Management Information Systems, Chinomso has over 7 years of experience teaching Business and Management modules across undergraduate and postgraduate levels, including apprenticeship programmes such as CMDA. Prior to her current position, Chinomso was the Deputy Head of DMUIC Business and Law at De Montfort University's International College, leading in academic management and curriculum development. She was programme leader on International Business programmes offered on foundation and undergraduate levels. Her earlier roles include lecturing in Project Management and Business Management and Leadership at De Montfort University and Coventry University respectively. Chinomso completed a PhD in Mechanical, Automotive, and Manufacturing Engineering at Coventry University where she designed 'A Framework for Assessing the Appropriateness of a Customer-centric Strategy and its Outcomes aimed at Improving Product Development and Service Design.' Her research interests span several areas of education and management. Chinomso is a Full Member of the Association for Project Management (APM), a chartered Manager CMgr MCMI, and a Chartered Management and Business Educator (CMBE), PRINCE2(f) qualified, and a Senior Fellow of the Higher Education Academy (SFHEA).

Chibuzo Nwagboso is a Research Analyst in the Development Strategies and Governance Unit, based in Abuja, Nigeria. Her work focuses on applied research and policy analysis in agriculture, nutrition, gender, and youth inclusion, using both qualitative and quantitative methods to investigate issues related to the political economy of biotechnology, gender and youth, and food systems. Prior to joining IFPRI, Chibuzo worked as a researcher for Seven Star Consultants Limited, where she specialised in impact evaluations and development studies. She holds a master's degree in International Business Economics from Coventry University. Chibuzo's language skills include English and functional French.