The Battle Against Fraud: Safeguarding Vulnerable Populations in Digital Payments

Fraud in West Africa isn't just a financial crime—it deeply impacts human lives, eroding trust in financial systems and disproportionately harming the most vulnerable. For millions of unbanked, underserved, and low-income individuals, a single fraudulent incident can wipe out savings, drive families deeper into poverty, and diminish faith in formal financial services. The ripple effects of unchecked fraud destabilize livelihoods, stifle economic opportunity, and widen the gap of financial inclusion, perpetuating cycles of inequality and insecurity across the region.

As digital economies expand across West Africa, the rapid adoption of digital payment systems has introduced new opportunities for growth, but also a troubling increase in fraud. Sub-Saharan Africa has witnessed a significant surge in internet connectivity, with a 115% increase in internet users between 2016 and 2021, and the addition of over 160 million Africans gaining broadband access between 2019 and 2022. This surge has fueled the rise of digital payments, and with the Global Findex Report 2021 showing that 191 million additional individuals made or received a digital payment between 2014 and 2021[1]. In Nigeria alone, mobile wallet transactions reached ₦17 trillion (~US$11.69 billion) in the first quarter of 2024[2].

However, this digital expansion has also exposed the region to a surge in payment fraud, with losses in Nigeria totaling ₦17.7 billion (~US$11.6 million) in 2023[3]. Social engineering tactics, particularly targeting individuals aged 40 and above, is the primary method used by fraudsters[4]. As digital payments in West

[1] World Bank - https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa
[2] https://nairametrics.com/2024/04/18/mobile-money-transactions-in-nigeria-jump-to-n17-trillion-in-q1-2024-nibss/
[3] Nigeria Inter-Bank Settlement System's Annual Fraud Landscape report Jan to Dec 2023
[4] Nigeria Inter-Bank Settlement System's Annual Fraud Landscape report Jan to Dec 2023

Africa are projected to increase significantly over the next few years, the rise in fraud poses significant risks to low-income, low-literacy end users and women are at a heightened risk of exploitation.

Earlier this year, the Alliance for Innovative Regulation (AIR) facilitated a series of roundtable discussions at key conferences, including 3iAfrica, RegTech Africa, and virtually. These discussions convened experts from the financial, regulatory, and technology sectors to explore the intricate challenges of fraud prevention and advancing financial inclusion in West Africa. Participants shared insights into the region's obstacles, such as fragmented data systems and limited consumer awareness, while also highlighting opportunities for innovation. The roundtables underscored the pressing need for collaboration across industries and stakeholders to drive forward effective, scalable solutions for the region.

Exploiting Technological Gaps: How Fraudsters Stay Ahead

Despite advances in payment technology, fraudsters continue to find and exploit weak spots in financial systems. One key issue is the reliance on outdated identification systems that fail to verify the authenticity of users. This is compounded by the lack of integration between systems, making it difficult for organizations to share fraud-related data in real-time. Continuous transaction monitoring is vital for fraud prevention but faces challenges within the region. Human resource constraints, especially in regions with security and power issues, make night shift staffing difficult. Many fintech companies lack the necessary infrastructure for uninterrupted monitoring, and unstable electricity and network connectivity further disrupt operations.

In addition, multi-factor authentication (MFA) and rules-based systems, which require users to provide multiple forms of verification (such as a password and a one-time code), are useful but often struggle to keep pace with evolving fraud tactics. These systems can be bypassed through sophisticated attacks like social engineering (tricking individuals into revealing personal information), SIM swapping (taking control of someone's phone number to intercept security codes), and phishing or malware attacks, including keyloggers that capture keystrokes. Fraudsters exploit these vulnerabilities, particularly in rural and underserved communities where access to advanced technology and digital literacy is limited, leaving individuals more susceptible to scams and breaches.

Regulatory Complexities: Why Fraud Persists

One of the most frequently discussed topics during the roundtables was the regulatory complexities and gaps that allow fraud to persist. Regulations often fail to keep pace with rapid technological advancements, leaving financial institutions and consumers vulnerable. For instance, cross-border payments, which are essential for the West African economy, face regulatory challenges due to inconsistencies in standards between different countries.

Additionally, while there are regulations in place to monitor payment fraud, the enforcement of these laws remains inconsistent, and fragmented regulatory oversight often means that fintech companies and telcos operate in silos. Without centralized or shared data for identity verification and without sufficient cross-border collaboration, fraudsters continue to take advantage of regulatory blind spots and system weaknesses.

Vulnerable Consumer Behaviors: A Weak Link in Fraud Prevention

Many consumers, particularly in underserved communities, lack the financial literacy needed to recognize fraud risks, making them easy targets for scammers. A significant issue raised during the discussions was how low digital literacy, especially among women and rural populations, contributes to an increased risk of fraud.

Consumers often engage in risky behaviors, such as sharing personal information, reusing weak passwords, and falling for "get-rich-quick" schemes. Phishing scams, where fraudsters trick individuals into sharing their bank or personal information, are particularly prevalent in regions where awareness campaigns are not penetrating the vulnerable communities and therefore falling short. Furthermore, language barriers and varied literacy levels make broad brush awareness campaigns ineffective.

Gender specific challenges: Bridging the Data Gap

While it is widely acknowledged that women are often more vulnerable to scams and fraud, there is a significant lack of gender-disaggregated data to substantiate this claim. The absence of detailed data about how fraud affects different genders obscures our understanding of its real impact, limiting the ability of governments, financial institutions, and fraud prevention agencies to tailor their interventions effectively.

Many fraud detection and prevention algorithms used by financial institutions are built without considering gender-specific patterns of behavior. Integrating gender-disaggregated data could lead to more sophisticated detection systems that identify and block fraud attempts targeting specific groups.

Without interventions, fraud will continue to disproportionately affect women which may compound existing financial inequalities. Without substantive data, financial support systems, recovery mechanisms, and protective measures will continue to overlook this disparity. Addressing these gaps could significantly reduce economic inequality across genders and empower women to protect themselves against fraud to help create a safer financial ecosystem for all.

Combating Payment Fraud: Current Efforts

The fight against payment fraud in West Africa has seen significant advancements in recent years. Key initiatives include the implementation of biometric verification systems during onboarding processes, the use of machine learning and artificial intelligence (AI) to monitor transactions in real-time and AI-driven tools that are capable of analyzing large datasets quickly. Furthermore, increased collaboration between financial institutions and regulatory bodies has facilitated the sharing of vital information, helping to create a more unified approach to combating fraud.

However, despite these positive steps, these systems need broader adoption and deeper integration across different sectors and industries to be fully effective. Without this, gaps remain in the overall security landscape, leaving room for fraudsters to exploit weak links in the system.

A notable initiative in this space is the Level One Project, a multi-year effort supported by a diverse coalition of stakeholders from the public, private, and nonprofit sectors led by the Bill and Melinda Gates Foundation. This project aims to enhance digital payment system infrastructure at both national and regional levels,

promoting sustainable, open-source, and low-cost solutions that can be broadly adopted by financial service providers. An important aspect of this initiative is focussed on fraud mitigation, with the most recent publication providing detailed guidelines for securing digital payment platforms. By bolstering the security of these platforms, the project aims to protect both users and service providers, creating a more trusted environment for digital transactions.

The need for action

To combat the rising threat of payment fraud in West Africa, we must act swiftly and collaboratively. Financial institutions, regulators, and technology providers must prioritize the adoption of integrated, scalable security solutions that can evolve with emerging fraud tactics. This includes strengthening consumer education efforts, especially for vulnerable populations, and closing regulatory gaps that leave systems exposed.

Furthermore, stakeholders must accelerate cross-sector data sharing to enable real-time fraud detection and intervention, while investing in innovative technologies like AI and biometrics to protect against future threats. Now is the time to unite around a shared vision: a secure, inclusive digital financial ecosystem that empowers all users, safeguards vulnerable communities, and fosters sustainable economic growth.

Let's seize this moment to turn ambition into action and build a future where trust in digital payments is unwavering.

The Alliance for Innovative Regulation (AIR) is hosting a virtual TechSprint in November 2024 focused on detecting and combating payment fraud in West Africa. This event will bring together a diverse range of stakeholders, including technology companies, consumer protection agencies, payment service providers, innovators, regulators, and subject matter experts to collaboratively create solutions. Learn more.