Nigerian Jihadists and Bandits Exploit Emerging Fintech

12.04.2025 | Aminah Mustapha

Nigerian Jihadists and Bandits Exploit Emerging Fintech

Executive Summary:

Nigeria's rapid shift toward mobile money, Point of Sale (PoS) terminals, and fintech wallets has created new financial pathways for insurgents and bandit groups, according to a March 2025 assessment. Weak "Know Your Customer" (KYC) regulations and lightly supervised agent networks allow criminals to move ransom payments and insurgent taxes with reduced detection risk.

Islamic State–West Africa Province (ISWAP) is integrating digital platforms into its revenue collection and logistics, using agent banking, civilian intermediaries, and fragmented transfers to shift funds without transporting bulk cash. Digital rails now enable cross-regional liquidity movement that complicates intelligence tracking.

Northwestern bandit groups increasingly rely on PoS agents and low-tier fintech wallets to process ransom payments through coercion, intermediaries, and rapid cash-outs. Despite new CBN regulations, enforcement gaps in rural high-risk areas leave Nigeria's digital-finance ecosystem vulnerable to armed actors.

The Nigerian Financial Intelligence Unit (NFIU) reported in March 2025 that kidnapping ransom payments increasingly move through mobile-money platforms, Point of Sale (PoS) terminals, and fintech wallets. The report cited cases of rapid fund splitting and repeated small cash-outs, and identified weak Know Your Customer (KYC) compliance meant to prevent fraud, with some accounts opened with minimal verification in areas lacking state oversight. PoS transactions are especially relevant. A PoS terminal is a small device found in shops and kiosks that allows cash withdrawals and transfers without a bank branch, while a PoS agent is an independent vendor who acts as a micro-banking outlet, providing cash-in/cash-out services and transfers on behalf of banks and mobile-money operators. This novel digital economy has become a favored channel for illicit transactions, including by militant organizations.

The NFIU's findings indicate that Nigeria's accelerating shift toward a cashless economy has inadvertently created new financial pathways for insurgent and bandit groups. These developments hold implications for counterterrorism, anti-money laundering, and rural security governance.

Digital Rails in a Fragmented Security Environment

Nigeria's cashless transition expanded significantly after the 2022–2023 currency redesign and the push for electronic payments. Cash scarcity temporarily pushed millions of Nigerians toward instant transfers, Unstructured Supplementary Service Data (USSD) payments (where a mobile-phone protocol allows users to perform instant money transfers and banking actions through short numeric codes without internet access), and PoS transactions. The PoS agent banking sector now numbers several million terminals nationwide, concentrated in rural and conflict-affected areas where formal banking infrastructure is limited (Daily Trust, March 11, 2024).

The NFIU report nonetheless suggests that digitization without parallel regulatory expansion has widened opportunities for criminal finance innovation (NFIU, March 2025). Meanwhile, The Central Bank of Nigeria (CBN) has repeatedly positioned the cashless framework as a modernization effort intended

to promote financial inclusion and reduce illicit cash circulation. The speed of fintech growth, combined with uneven supervision across thousands of PoS agents, has produced what some Nigerian analysts describe as a "semi-formal" financial space: widely used, lightly monitored, and attractive to armed actors.

ISWAP's Adaptation to Mobile-Money Ecosystems

Islamic State–West Africa Province (ISWAP) facilitators have increasingly incorporated digital channels into existing financial practices (GNET, February 18). ISWAP has historically relied on a diversified revenue base. Sources of its income include taxation of farmers, traders, and transporters, smuggling, and ransom payments. The expansion of mobile-money services and agent networks deeper into rural Borno and Yobe provinces has only further enabled ISWAP to make use of these technologies for nefarious purposes.

ISWAP's adaptation appears to follow three patterns:

1. *Digitization of revenue extracted in controlled areas*

ISWAP enforces taxes on agricultural and commercial activities in parts of the Lake Chad Basin. Traders and transporters operating near ISWAP-influenced corridors increasingly use agent banking, creating opportunities for facilitators to collect or move funds without physically handling cash (Tribune Online, August 2).

2. *Use of civilian intermediaries*

Local traders, PoS operators, and transport workers have historically served as intermediaries between civilians and insurgent cells. The integration of fintech wallets and mobile money provides these intermediaries with a lower-risk way to transmit funds, particularly for fragmented transfers that attract less scrutiny (NFIU, March 2025).

3. *Cross-regional liquidity movement*

ISWAP has incentives to move funds from taxation zones toward logistics hubs and procurement networks. Digital rails (the digital systems and infrastructure that allow money to move electronically across regions) reduce the operational risks associated with transporting large quantities of cash across military checkpoints. Although open-source evidence cannot quantify ISWAP's digital finance footprint, Nigeria's intelligence assessments increasingly treat mobile-money exploitation as an insurgent tactic (NFIU, March 2025).

Northwestern Bandits and the Rise of Digital Ransom Economies

Criminal groups in Zamfara, Kaduna, Katsina, and Niger States have long relied on cash for ransom payments. Yet the NFIU report documents a growing shift toward digital facilitation. In one case, bandits compelled a victim's family to deposit ransom funds into an account controlled by an associate, who then withdrew the funds through multiple PoS terminals across state lines to avoid detection (NFIU, March 2025).

Several Nigerian media outlets have highlighted similar patterns of growing use of fintech by bandit groups. The Association of Mobile Money and Bank Agents of Nigeria (AMMBAN) acknowledged that PoS operators are often used as cash-out points for ransom proceeds, particularly in rural communities lacking bank branches (The Whistler, May 24, 2024). Some operators report receiving "red flag" transactions but have limited mechanisms for escalation or protection when confronting suspicious activity.

Bandit networks exploit three systemic weaknesses:

1. Coercible and accessible PoS infrastructure

PoS agents are ever-present in rural markets and transit points. Bandits have reportedly forced victims to withdraw funds directly from PoS terminals under duress or have directed intermediaries to conduct cash-outs on their behalf (The Whistler, May 24, 2024).

2. *Fragmented oversight*

High-volume agents in rural and semi-rural zones in Nigeria often operate far from regulatory scrutiny (The Whistler, May 24, 2024). Commercial banks and mobile-money operators oversee agent banking, although enforcement varies widely.

3. *Low-tier fintech wallets.*

Many digital wallets allow onboarding with minimal identification. These low-tier accounts, while critical for financial inclusion of people who may not have personal documents, enable bandit cells to open accounts linked only to a phone number to receive and distribute funds—leaving only a modest risk of detection.

These practices allow bandit groups to maintain operational liquidity and minimize exposure during ransom negotiations.

The CBN's Regulatory Tightening and Its Limitations

The CBN introduced regulations in 2025 requiring agents to link terminals to verifiable owners and to comply with enhanced monitoring standards. The Central Bank also introduced new cash-out limits, agent exclusivity rules, and KYC-strengthening measures for agent networks (CBN, October 6). However, implementation challenges persist. Agent networks in high-insecurity zones often struggle with identity verification because of weak civil registration systems. Fintech systems face high onboarding demands relative to their scale, and rural areas continue to rely on high-volume PoS cash-outs due to limited ATM infrastructure. As a result, the core vulnerabilities highlighted in the NFIU report remain only partially addressed.

Convergence of Insurgent and Criminal Economies

Both ISWAP and northwestern bandit groups increasingly exploit similar financial pathways. Several trends indicate growing convergence:

Reduced reliance on bulk cash, as digital channels offer lower-risk alternatives.

Increased use of intermediaries, including PoS operators, traders, and transport workers.

Diversification of financial flows, with ransom funds fragmented into micro-transactions.

Instant transfers and mobile wallets facilitate the mobility of funds across regions.

These patterns complicate the efforts of Nigerian security agencies to map financial networks. The volume of legitimate digital transactions, numbering in the hundreds of millions monthly, creates "transactional noise" in which illicit flows can hide. Without advanced analytics, law enforcement struggles to distinguish criminal activity from ordinary rural economic behavior.

Conclusion

Nigeria's cashless transition has brought financial inclusion and faster payment infrastructure along with new financial pathways for insurgent and bandit groups. ISWAP is integrating digital rails into its taxation and logistical systems, while northwestern bandits increasingly rely on PoS operators and mobile wallets to receive and distribute ransom proceeds.

Absent stronger KYC standards, targeted supervision in high-risk zones, and enhanced transaction monitoring, Nigeria's digital-finance architecture will remain vulnerable to exploitation. The country's security agencies and financial regulators face the challenge of safeguarding an expanding payments ecosystem while preventing its capture by armed networks.