OPINION

# Are Ghana's Banks Winning the Old Fight while Losing the New One?

*By Jon Sarpong, Founder and Managing Director, INNOVA Institute*

Reported fraud in Ghana's regulated financial sector rose 48 percent last year to a four-year high, with more than GH¢100 million placed at risk. Read quickly, that number invites alarm. Read carefully, it tells a more useful story — and points to what we should do next.

Look beneath the headline and the picture becomes more clear. Reported cases at banks actually fell by a third last year, and the value at risk within them declined — evidence that the sector's investment in controls are having an impact. The surge in fraud sits almost entirely in the digital and payment-service channels, where cases jumped by more than half and the amount exposed nearly doubled. Fraud in Ghana has not simply grown – it has evolved.

And this distinction matters, because it shows the sector's traditional defences are holding while a new frontier opens up. A generation of investment by Ghana's banks in branch controls, teller supervision and cheque verification is paying off: where verification tools are deployed, institutions now recover the overwhelming majority of attempted forgeries. The challenge is that digital finance has expanded faster than anyone anticipated, and convenience has outpaced the security frameworks meant to protect customers. Fraudsters have followed the money into mobile wallets, instant transfers and e-money — channels where funds move in seconds and recoveries hover near zero.

The tactics have shifted with the terrain. The dominant threat is no longer a forged signature; it is a persuasive phone call. Social engineering, impersonation and one-time-password theft now drive a large share of losses, because the weakest link is rarely the system — it is the moment a customer, or an employee, is manipulated into trusting the wrong person. That human layer is exactly where today's fraudsters concentrate their effort. This is not a story about failing institutions. It is a story about a threat that has grown faster, more human and more industrialised than the controls built to stop it — one no bank, however well run, can hold back alone.

Canada faced a version of this same shift, and its response is instructive. I believe the lesson that Ghana’s banking sector can take from its North American counterpart is simple: Canadian banks did not beat digital fraud by hiring more investigators to clean up after the fact. They moved the intelligence to where the money actually moves — into the transaction itself. In light of this realization, here are three insights from the Canadian experience that I believe may translate directly to Ghana.

1. **Decide in real time:** Machine-learning models can score every transaction in milliseconds against a customer's own behavioural pattern, flagging or halting the suspicious one before funds leave the account. In a world of instant payments, a defence that acts only after settlement is no defence at all.

2. **Retire the SMS code.** Where attackers routinely defeat one-time passwords through SIM-swaps and stolen phones, device fingerprinting, biometric verification and liveness detection close the very door that social engineering walks through.

3. **Defend together.** Canadian institutions share fraud intelligence, so that a mule account exposed at one bank is flagged across the system within minutes. Fraud networks operate across institutional lines; our defences must too.

None of this requires ripping out existing core systems. The most effective deployments run alongside current controls, learning continuously and shifting decisions from static rules to adaptive intelligence only as they prove themselves. The technology is mature and already operating at African scale: on the continent's largest mobile-money networks, data-driven risk engines have cut loss rates by orders of magnitude while making decisions in seconds rather than days.

This is not a burden for any one government, regulator or bank to carry alone, and it is certainly not a matter of blame. The Bank of Ghana has rightly called for collective action, and the industry has been candid about the gap. What remains is execution: a shared commitment to embed intelligence in the transaction flow, verify identity at machine speed, and pool fraud signals across the sector.

Ghana has already shown it can win the fight it prepared for. The task now is to prepare for the fight that has arrived. The tools exist and the evidence is in, the only question is whether we deploy them before the next report — or after it.

---

**About the author**

*Jon Sarpong is the Founder and Managing Director of the INNOVA Institute, a Canadian-credentialled AI training and workforce-enablement campus located in Abelenkpe, Ghana, with programming launching in September 2026. The Institute equips Ghanaian professionals, graduates and institutions with applied skills in artificial intelligence, data and digital finance. For more details visit: innovainstitute.ai*

**Sources**

- Bank of Ghana (2026). 2025 Fraud Report. Accra: Bank of Ghana.
- Ghana Association of Banks (2025). Industry Fraud Report, June–August 2025. Accra: Ghana Association of Banks.
- Graphic Online (2026). “75 bank staff dismissed as fraud cases surge 48% — Bank of Ghana report.” Graphic Online, Business.
- BusinessGhana (2026). “Collective action key to tackling financial sector fraud — BoG.” BusinessGhana News.
- Mastercard (2025). AI Is Helping Banks Save Millions by Transforming Payment Fraud Prevention. Mastercard Newsroom, with Financial Times Longitude.
- 4Pay Inc. (2025). Collaborative Finance for Banks — Vodacom M-PESA use case. Corporate presentation.