



Statement of Requirements: COURE Software and Systems.

COURE is calling on Mobile Network Operators to expose Network APIs for Financial Institutions in Africa enabling proactive fraud prevention across digital ecosystems.

Published: 26 August 2026

Executive Summary

As digital financial services continue to expand rapidly across Africa, fraudsters are increasingly exploiting vulnerabilities in identity verification, account recovery, and transaction monitoring. Threats such as SIM swap fraud, recycled numbers, device spoofing, and account takeover are placing financial institutions, payment service providers, and digital merchants under growing operational and reputational pressure.

To address this escalating challenge, **COURE Software and Systems** is calling on mobile network operators to expose fraud preventative **GSMA Open Gateway Network APIs** to be available for financial institutions, enabling them to take proactive measures to protect consumers.

Making these network capabilities available will enable financial organizations to strengthen real-time risk assessment, enhance fraud detection at critical customer touchpoints, and take more proactive steps to protect customers from financial loss while supporting safer digital growth across the region.

Rising Fraud and Current State of the Industry

Across the African continent, recent data highlights the scale and urgency of the challenge:

- SIM swap fraud now accounts for approximately **43% of all mobile money fraud** in Africa, making it one of the dominant attack vectors and most prevalent mobile-money fraud threat across the continent¹

¹ *www.papers.ssrn.com* – “Mobile Money Social Engineering Attacks in African Countries: A Survey”, M. Adongo, 20, June 2025.

- In some markets, up to **60% of mobile banking fraud** is linked to SIM swap attacks², which enable account takeover and unauthorized transactions
- Fraud patterns are shifting toward account takeover and authentication abuse, with attacks on login and recovery processes now five times more common than fraud at account creation
- SIM swap incidents continue to rise across major markets, following a survey where experts estimated SIM swap fraud accounted for **15-30% of all fraud** in the markets surveyed³
- Identity theft and telecom-enabled fraud are costing economies billions, with **over R 5.3 billion lost annually in South Africa** alone due to telecom-related fraud including SIM swap and impersonation⁴

These figures underscore a critical reality: mobile identity has become the weakest link in Africa's financial security. Fraudsters increasingly exploit vulnerabilities such as recently swapped SIMs, recycled phone numbers, dormant accounts, and compromised devices to bypass traditional authentication mechanisms and execute unauthorized transactions.

How can COURE's ANQ solution and Network APIs help to fight against fraud?

"Fraud prevention today requires real-time, data-driven decision-making," said **Uche Onwudiwe, MD/CEO of COURE**. "**ANQ** empowers businesses to move from reactive fraud detection to proactive prevention, leveraging dynamic telecom and device intelligence to stop fraud before it happens." The solution is designed for scalability and interoperability, making it suitable for:

- Banks and microfinance institutions
- Payment service providers and fintech platforms
- E-commerce and retail businesses
- Digital lending and credit platforms

Delivered through its **All Number Query platform, "ANQ"**, **COURE's** secure, API-based fraud prevention solution directly addresses these vulnerabilities by providing financial institutions, and retailers, with critical, real-time, telecom and device intelligence, including SIM Swap verification, Number Activity analysis, Number Recycle detection, and Device Information insights, directly into enterprise systems. This enables organizations to

² www.connectingAfrica.com – "Telecoms fraud costing SA \$300M Annually – COMRiC", P. Gilbert, July 22, 2025.

³ www.mobileecosystemforum.com – "SIM Swap Fraud in Africa" - F. Delanaud.

⁴ www.comric.co.za – "Telecoms fraud costing SA \$300M Annually" – 22 July 2025.

assess the risk level of customer onboarding and transaction processing in real time and take appropriate actions before fraud occurs.

As industry stakeholders push for stronger identity management and faster fraud response times, network API-driven intelligence is becoming an essential infrastructure. ANQ aligns with this shift by enabling secure, compliant, and real-time access to critical mobile and device data signals to improve fraud detection, reduce false positives, and enhance customer protection.

As fraud tactics continue to evolve, COURE is positioning its ANQ along with GSMA Open Gateway Fraud Prevention Network APIs as a critical layer in modern risk management, empowering organizations to stay ahead of threats while delivering secure and seamless customer experiences.

Expected Impact after implementation of Network APIs: Built Customer Trust

COURE's ANQ's Fraud Signal APIs, under the GSMA Open Gateway initiative can be seamlessly integrated into existing workflows within a compliant framework, allowing institutions to:

- Detect high-risk SIM swap events prior to transaction authorization
- Identify recently recycled or reassigned phone numbers, often linked to fraud
- Analyze number activity patterns to flag anomalies
- Validate device consistency and detect suspicious device changes

By combining these telecom signals, financial organizations can build a more accurate risk profile for each customer interaction, risk teams can identify suspicious behaviour, stop fraudulent onboarding attempts, flag unusual login activity, and intercept high-risk transactions before fraud occur significantly resulting in reducing fraud losses at the same time, legitimate customers benefit from faster approvals and fewer unnecessary verification steps. The result is a stronger balance between security and convenience, helping financial institutions protect revenue and maintain customer trust.

Network API requirements

COURE calls on Mobile Network Operators in Africa within its priority markets to expose the following capabilities aligned to GSMA Open Gateway initiative:

- Number Verification API

- Number Recycle API
- Device Swap API
- SIM Swap API
- KYC Customer Match API
- Scam Signal API

Geographic Scope

COURE seeks initial API enablement in the following priority markets -

Nigeria, South Africa, Benin, Botswana, Cameroon, Côte d'Ivoire, Democratic Republic of Congo, Egypt, Ethiopia, Ghana, Kenya, Morocco, Mozambique, Senegal, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia, and Zimbabwe.

Additional African market expansion to follow once APIs are available and implemented across above markets.

Timescales and Network APIs Deployment

COURE is calling on mobile operators to expose network APIs and participate in pilots:

- Within 3-6 months in 2026 - COURE aims to commence pilot programs, and technical validation activities - of network API availability.
- In the next 12-24 months, in 2027/28, targets with full production rollout across the priority markets.
- Expansion beyond 24-48 months the initial priority countries into additional African countries within will be upon demonstrated operational improvements, successful multi-operator implementation, and clear service level and commercial frameworks.
- This phased approach is intended to allow for early testing, controlled deployment, and the refinement of implementation models before broader commercial scale-up.

Adoption timelines will be influenced by the level of multi-operator interoperability achieved across participating markets, the clarity and consistency of service level agreements, and the availability of well-defined commercial frameworks.

Collaboration and next steps within ecosystem

COURE's approach aligns with global trends in API standardization and cross-industry collaboration, positioning telecom data as a critical enabler of stronger financial security. By integrating directly with telecom operators and channel partners through secure data-sharing frameworks, COURE can deliver actionable insights in milliseconds to support faster, more informed fraud prevention decisions.

“Fraud prevention is no longer just a banking problem. It is an ecosystem challenge that requires collaboration between telecom operators, financial institutions, and technology providers,” **Uche** added. “With such collaborations and the support of partners like GSMA, we can significantly reduce fraud exposure and build a safer digital economy.”

Timely coordination among the ecosystem participants will be essential to support smooth onboarding, operational alignment, interoperability, and scalable deployment of network APIs. Early participation from mobile network operators will be critical to meet rising enterprise demand and enabling effective fraud prevention across digital financial ecosystems. Without this collaboration, financial institutions and consumers may face increased exposure to fraud risks.