TOPIC: DATA SHARING BARRIERS HINDERING FRAUD PREVENTION

Team Name: Data Fusion

PROBLEM STATEMENT:

Fraud remains a major problem militating against the financial ecosystem in West Africa. However, efforts to detect, prevent, and respond to its prevalence have been hindered by limited data sharing and weak coordination between institutions and across national and regional jurisdictions. It is estimated that US$50 billion[1] a year in illicit financial funds flows out of West African countries alone, a signal to the volume of fraudulent transactions flagged in West Africa yearly. However, experts have posited[2] that cross-border and interoperable data sharing mechanisms will significantly improve the efforts to address this phenomenon.

SOLUTION: ESTABLISHMENT OF SECURED CENTRALISED WEST AFRICAN FRAUD INTELLIGENCE HUB

The West African Fraud Intelligence Hub is a strategic solution developed to reinforce cross-border collaboration in the fight against financial fraud across the West African sub-region. This Hub provides a **unified operational and technical framework** that enables key stakeholders, such as regulatory bodies, financial institutions, law enforcement agencies, and fintech operators, across West Africa to share intelligence, detect fraud patterns, and respond to threats in real-time.

At the core of the solution lies a **robust API-driven system** that facilitates the secure and real-time exchange of fraud alerts, transaction data, and suspicious activity reports between participating countries. This technological infrastructure empowers stakeholders with the ability to act swiftly and proactively mitigate emerging fraud risks, regardless of national boundaries.

In addition to its technical backbone, the Hub integrates a comprehensive suite of capacity-building tools and operational frameworks. These include training programmes, institutional governance models, and collaborative coordination mechanisms. Through these, national institutions are equipped with the technical expertise, policy alignment, and cross-border coordination capabilities required to operate and sustain an effective and unified

---

[1] LexisNexis Risk Solutions, no date. *Financial crime typologies across Africa: Insights into regional and sector-specific threats*. [online] Available at: https://risk.lexisnexis.com/global/en/insights-resources/white-paper/financial-crime-typologies-africa [Accessed 8 Jul. 2025].

[2] Eastnets, 2025. *The Increasing Complexities of Cross-Border Payment Fraud in E&MEA, and how banks can strengthen their defenses*. [online] 13 June. Available at: https://www.eastnets.com/blog/the-increasing-complexities-of-cross-border-payment-fraud-in-e-mea-and-how-banks-can-strengthen-their-defenses [Accessed 9 Jul. 2025].

fraud response network.

Ultimately, the West African Fraud Intelligence Hub will serve as a central pillar in the region's fight against financial crime, enhancing trust, strengthening security, and fostering a collaborative environment where data-driven fraud prevention becomes the norm across borders.

ACTIVITIES

a. **Institute a Technical Working Group:** The group will be the directly responsible institution for the implementation and maintenance of the solution. The TWG will comprise experts as may be designated by the Fraud Intelligence Units across West African Units.
b. **Engage stakeholders and secure buy-in:** This will be done through validation workshops and high-level consultation workshops with key stakeholders including Central Banks, Fraud Intelligence Units, Financial Organisations, Data Protection Commissions, Fintechs, licences Payment Service Providers, Non-profits, International Organisations, among others. Actualising this network will leverage existing collaborative frameworks within bodies like the Economic Community of West African States (ECOWAS).
c. **Create a legal framework for data standardisation and cross-border data sharing:** Most West African countries have developed data protection laws and have established relevant supervisory authorities to oversee the implantation of these laws. However, a common challenge with these laws is their limited opportunities for cross-border data sharing and collaboration. This framework will leverage these data protection regulations to design a framework that aggregates a common standard and cross-border data protection mechanism among member states.
d. **Develop an API for stakeholder interoperability:** By designing, developing and implementing a secure, scalable, and standards-compliant API that enables seamless interoperability among key stakeholders, including Central Banks, Fraud Intelligence Units, Financial Organisations, Data Protection Commissions, Fintechs, licensed Payment Service Providers, Non-profits, International Organisations, and others. The API will facilitate real-time data exchange, fraud alert dissemination, and integration with existing national systems, thereby supporting a coordinated and efficient cross-border collaboration framework for fraud detection and response. Furthermore, analytical outputs from the centralised solution will be embedded within the API through the integration of intelligent tools such as AI agents, enabling dynamic threat identification, automated decision support, and actionable insights for participating entities.

e. **Employ sandbox testing to ascertain the feasibility of the solution and address identified loopholes:** By implementing sandbox tests to evaluate the system's technical viability under simulated production-like conditions. This controlled environment will allow for end-to-end validation of system components, including API performance, data flow integrity, and security protocols. By replicating real-world fraud scenarios, sandbox testing will help uncover potential loopholes, performance bottlenecks, and interoperability issues, enabling timely remediation and optimisation before live deployment.
f. **Create curriculum for capacity development and training:** Considering that the sustainability of the solution relies heavily on the level of expertise of the stakeholders, our solution incorporates a capacity-building initiative that allows stakeholders to understand how the solution can be implemented locally. Additionally, a periodic capacity-building session will be conducted to explain the analytics and fraud patterns as well as the use of AI and other emerging technologies to improve reporting and fraud detection.
g. **Conduct regional rollout (Intra and Inter):** Leveraging on the buy in of stakeholders, the solution will be rolled out within countries and across West Africa to ensure a robust implementation.
h. **Monitor and evaluate adoption and effectiveness:** Continuous monitoring and evaluation of the solution will be conducted on an annual basis, with the exercise covering key pillars necessary for the sustainability of the solution. These pillars include technical expertise, national adoption, efficient real time fraud reporting, capacity building among others.

RESOURCES AND LEVERAGE

- **Funding:** The solution will leverage grants from international bodies, participation from non-profit organisations, contributions from member states, and donations from private organisations. This funding will be incentivised by the possibility of members making concerted efforts to address fraud, rather than the current siloed effort that private organisations and countries make. Currently, it is reported that private organisations expend up to $1 million USD on addressing fraud. Providing a bird-view and presenting the benefits will incentivise the buyin from organisations.
- **Regional and national adoption:** The solution will leverage strong interest and alignment at both regional and national levels to drive adoption and scale. By securing buy-in from key national institutions (such as Central Banks, Fraud Intelligence Units, and Data Protection Commissions) and regional bodies (such as ECOWAS, WAEMU, and AfCFTA), the solution will benefit from policy support, regulatory alignment, and

cross-border cooperation. This adoption will serve as a critical resource, enabling widespread deployment, shared ownership, and long-term sustainability of the Fraud Intelligence Hub across West Africa.

- **Technical capability:** The solution is backed by strong technical expertise in API development, cybersecurity, data governance, and AI integration. The core team and partners possess the necessary skills to design secure, scalable, and standards-compliant infrastructure that supports real-time data exchange and fraud intelligence sharing across borders. In addition, the use of advanced technologies, such as AI agents for fraud pattern analysis, and sandbox environments for rigorous testing, demonstrates the team's ability to build and deploy innovative, future-ready systems tailored to the complex needs of West African financial ecosystems.
- **Operational resources:** The implementation of the West African Fraud Intelligence Hub will be supported by dedicated operational resources, including fraud analysts, project managers, and compliance experts. These teams will oversee day-to-day operations, system maintenance, data validation, stakeholder coordination, and incident response. In addition, access to regional infrastructure, such as secure data centres and regulatory sandboxes, will ensure continuous system availability, scalability, and alignment with local operational standards. Institutional partnerships will further enhance resource efficiency by contributing in-kind support, including office space, connectivity, and access to national fraud databases.
- **Consumer education and sensitisation:** This will level existing channels established by private organisations to create awareness on detecting fraudulent transactions.

OUTCOME

- **Enhanced collaboration among stakeholders:** The hub provides a unified platform that connects financial institutions, telecom operators, regulators, and law enforcement agencies across West Africa, enabling them to share fraud intelligence, alerts, and best practices in real time. This fosters trust, improves coordination, and ensures a collective response to cross-border and sector-wide fraud threats.
- **Faster detection of fraud patterns:** By aggregating data from multiple sources and deploying advanced analytics tools, the system can quickly identify suspicious trends and emerging fraud schemes. This early detection capability allows institutions to take proactive measures, minimizing financial losses and system vulnerabilities.
- **Improved customer trust:** Visible, region-wide efforts to detect and prevent fraud reassure customers that their financial and personal data are being actively protected. This builds confidence in digital services and financial institutions, encouraging greater

usage of formal financial channels.

- **Data-driven policy:** With access to regional fraud data and actionable insights, policymakers and regulators can make informed decisions. This enables the creation of targeted, evidence-based policies and regulations that address systemic vulnerabilities and support more robust fraud prevention mechanisms.
- **Improved knowledge transfer:** The hub includes capacity-building programs that train fraud analysts, compliance teams, and IT personnel across the region. This structured approach to learning fosters the sharing of expertise, strengthens institutional capabilities, and helps develop a skilled workforce equipped to combat evolving fraud threats.

Impact:

- **Realtime cross-border fraud monitoring:** The hub enables seamless, real-time monitoring of fraud across national and institutional boundaries, allowing stakeholders to quickly detect and respond to threats that move across countries. This coordinated vigilance helps reduce the window of opportunity for fraudsters, ensuring faster containment and regional protection.
- **Proactive fraud detection and mitigation:** By leveraging shared data and advanced analytics, the system shifts fraud response from reactive to proactive. Institutions can identify patterns before they escalate into large-scale threats, enabling swift preventive action and reducing financial losses and reputational damage.
- **Financial stability at the macro level:** A regionally integrated fraud intelligence system strengthens the resilience of the financial ecosystem by reducing systemic fraud risks. This contributes to greater investor confidence, improved regulatory oversight, and overall economic stability across West African markets.
- **Increased consumer trust:** Transparent, collaborative efforts to fight fraud reassure customers that their data and funds are secure. As institutions demonstrate accountability and improved fraud prevention, customer confidence in digital financial services grows, reinforcing loyalty and adoption.
- **Enhanced financial inclusion:** With improved fraud protection and trust in financial systems, more people, especially those previously unbanked, are likely to engage with formal financial services. This accelerates financial inclusion by creating a safer environment for participation in the digital economy.

Team Members:

- Elijah Etoh
- Yusuf Abduljelil
- Ocheze Gift Onwuegbuchu
- Odeh Osemeke
- Victoria Adaramola
- Friday Odoh
- David Samson

Scrum Master: Juliet Ongwae

Floating Expert: Esther Omoluyi