Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

The State of Fraud & Risk Intelligence in Africa 2025; How Continuous Profile Scoring Is Powering Safer Transactions and Digital Trust

Oluwatobiloba Ololade

Software Engineering
Dojah (Dojah.io)
Lagos, Nigeria

Abstract:
Africa's internet economy is booming and is expected to be worth USD 180 billion by 2025 (Google & IFC, 2020). However, this growth is being hampered by a huge deficit in trust in the system due to increasing incidences of cyber-enabled money crimes which cost African economies between USD 4 billion - USD 4.6 billion annually (INTERPOL, 2023). Fraudsters take advantage of lapses in identity verification processes, device security and transaction monitoring, and result in substantial losses and customer attrition. Traditional fraud detection methods, mainly relying on static, one-time identity check methods are no longer effective in tackling evolving threats. This paper examines how this responsive system approach of continuous profile scoring -- a dynamic behavior-driven framework of risk intelligence -- is helping to overcome such difficulties by transitioning from static at a single moment and one-time verification to contextual analysis of identity, transaction and device data in real-time. Continuous profile scoring relies on multi-signal intelligence involving identity verification, device reputation, behavioural analytics, and transaction monitoring used to help determine risk factors continuously throughout the user lifecycle to detect early instances of fraud. By taking such an approach, businesses can minimize the financial losses as a result of fraud, help deliver a better customer experience and create secure, inclusive digital ecosystems. This paper illuminates emerging fraud trends in Africa, summarises the limitations of traditional fraud detection and introduces Profiled Risk, a risk intelligence platform launching in late 2024 that seeks to improve fraud detection capabilities and help establish digital trust across the digital economy in Africa.

Keywords: Fraud prevention, continuous profile scoring, digital trust, Africa, risk intelligence, KYC, financial inclusion, behavioral analytics, transaction monitoring, cybersecurity.

Introduction

Africa's Digital Transformation and The Trust Deficiency

Africa's internet economy is exploding. By 2025, the digital economy will involve a market volume of USD 180 billion, where mobile technologies have a substantial contribution. Currently, mobile technologies add to the economy of Sub-Saharan Africa some USD 140 billion (7.3% of GDP), and the figure is expected to soar by 2030 (GSMA, 2023). This is thanks to widespread adoption of mobile money, fintech solutions, as well as e-commerce platforms that have enabled millions of Africans to become part of the digital economy. Despite these improvements, there is a significant challenge African countries are

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

facing - the emergence of cyber-enabled financial fraud that reportedly costs Africa between USD 4 billion and USD 4.6 billion per year (INTERPOL, 2023).

This is a growth paradox of an expanding digital economy based on a fragile trust, which is a central issue for African countries. Cybercriminals have gotten adept at taking advantage of the gaps in the continent's digital infrastructure, especially in identity verification systems, security of devices, and monitoring of transactions. Existing fraud prevention systems, especially static, single, one-time identity checks, are falling short in helping to address these changing threats. The absence of real-time contextual Sung Temperature Indicators fraud analysis software means that fraudulent activities are detected only after the transaction, causing serious damage to both financial and reputational aspects.

The Growing Digital Economy and the Fraud Risks

The digital transformation in Africa has led to great progress in the area of financial inclusion. Mobile money services, such as M Pesa in Kenya and MTN Mobile Money in Nigeria have delivered financial services to millions of unbanked people (GSMA, 2023). In 2020, the value of mobile money transactions in Sub-Saharan Africa amounted to USD $ 13.2 billion with projection that the value will increase as more mobile network coverage is brought to more villages and underserved areas (World Bank, 2023). However, this expansion has also made the economies in Africa more susceptible to different forms of fraud.

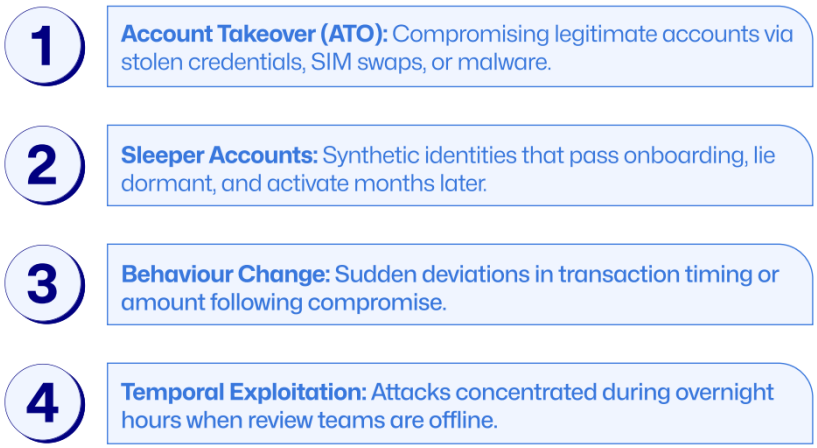
Fraud in Africa has progressed from the traditional forms of Identity Theft to complex forms of synthetic identity and account takeovers as well as manipulation of transactions. Table 1 below shows the increasing prevalence of types of fraud in the major markets of Africa.

Fraud Type	Description	Incidence
Synthetic Identity Fraud	Fraudsters create fake identities using stolen or fabricated information.	35% of all reported fraud cases in Africa (INTERPOL, 2023).
Account Takeover	Fraudsters hijack a legitimate user's account.	30% of digital banking fraud (SABRIC, 2023).
SIM Swap	Fraudsters swap a user's phone number to access their mobile account.	25% of mobile-money fraud in Kenya (TransUnion, 2023).
Transaction Manipulation	Fraudsters manipulate transactions, often via APIs.	15% of e-commerce fraud (ITWeb, 2023).

These fraud patterns are reflective of an increasingly sophisticated and interconnecting fraud ecosystem in Africa, where cybercriminals are exploiting the vulnerabilities across a range of sectors -- fintech, telecom and ecommerce making it even more difficult for businesses to defend against this fraud.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

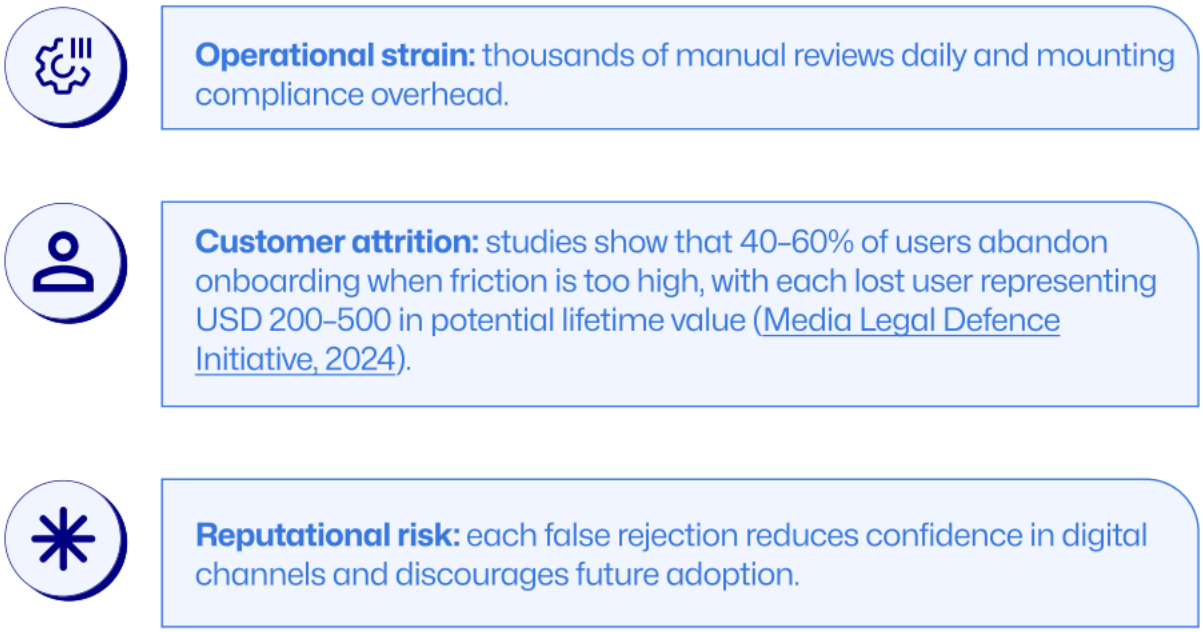
Figure 1: Beyond the Identity Gap: A Broader Trust Challenge



The Identity Gap and Trust Deficit found in Africa

A great challenge in the fight against fraud in Africa is the identity gap, which refers to the vast number of people not in possession of a formal identification. According to the World Bank, more than 850 million people worldwide have no formal identification and Sub-Saharan Africa is the largest portion of the global population without any identification (World Bank ID4D, 2023). While efforts are making to address this gap, the non-existence of non-travel identities along countries in many African Nations and continent fuels fraud risks. In some countries such as Nigeria, Kenya, Ghana, etc., national databases are still fragmented and consequently the process of verifying people onboarding is complicated (World Bank ID4D, 2023).

Figure 2: The Hidden Cost of Reactive Fraud Management



However, it is not only initial identity verification that poses an issue. Once a user is onboarded fraudsters continue to exploit trusted profiles. In particular, the rise of SIM swap fraud, social engineering attacks

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

and weakened devices have contributed to the surging prevalence of post-onboarding fraud. A study by TransUnion (2024) subjected the point that fraud committed after the user has been authenticated is now greater than fraud committed at the registration stage. This is a shift from traditional KYC (Know-Your-Customer) practices, which place a high reliance on one-time identity verification, and therefore are no longer sufficient for protecting businesses and users in digital ecosystems.

Why Continuous Risk Intelligence is Needed

To deal with increasing complexity of fraud, there is an evident need for ongoing risk intelligence. Continuous risk intelligence is a change from static verification systems to dynamic, behaviour-driven risk assessment methodologies. Unlike traditional methods of fraud detection which include static fraud checks when a user registers, continuous risk intelligence takes into account how a user is using it, transaction patterns, device reputation and other contextual information throughout the user lifecycle.

Table 2 shows the difference between static KYC and continued risk intelligence:

Criteria	Static KYC	Continuous Risk Intelligence
Verification Type	One-time identity verification	Real-time, ongoing risk assessment
Data Sources	Identity documents	Behavioral data, device information, transaction history
Risk Monitoring	Static, post-registration	Continuous, real-time
Fraud Detection	Limited to onboarding	Ongoing, adaptable to emerging fraud tactics

As illustrated in Table 2, continuous risk intelligence is an organic and evolving technology that can produce a dynamic risk profile for a user by using several data sources thus offering a much more complete approach to fraud prevention than traditional KYC systems.

Profiled Risk: The Future of Fraud Prevention in Africa

Dojah profiled Profiled Risk, a risk intelligence platform developed, as a good example of the next version solution to fraud management in Africa. By combining identity verification, behavioral analytics, device reputation, and transaction monitoring, Profiled Risk provides a real-time continuouslyupdated risk score that goes on to evolve over time with newly received data. This dynamic system not only makes fraud detection better but it also makes the customer experience itself better by cutting down on the unnecessary friction caused for legitimate users.

As African regional financial institutions and fintech institutions continue to use digital platforms as their main channel of customer service, developing a continuous risk intelligence approach through risk profiling platforms such as Profiled Risk is critical in achieving safer, more trusted digital ecosystems.

Literature Review

The Landscape of Fraud in Africa

Africa's digital economy is growing rapidly, but this growth comes with great challenges, especially in the area of fraud prevention. Cyber-enabled financial fraud is one of the fastest emerging economic threats on the continent with losses amounting between USD 4 billion and USD 4.6 billion to the African economies annually (INTERPOL, 2023). This growth in fraud is complicated by the growth in the penetration of digital financial services across Africa specifically mobile money and digital banking systems, which present fertile ground for different types of cybercrime. The financial fraud landscape is becoming more

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

complex and intricate-the fraudsters are employing more complex approaches in the form of synthetic identities, account takeovers, and manipulations of transactions.
Recent reports suggest that cases of fraud have risen significantly. In South Africa, for example, the number of digital banking fraud cases almost doubled to over R 1,4 billion [GBP 511 million] between 2023 and 2024 [USD 75 million) (SABRIC, 2023). Similarly, in Nigeria losses from fraud were at the rate of N 52.26 billion (Fintech Magazine Africa It is currently worth USD 45 million) in 2024. These alarming statistics show that fraud in Africa is no longer an occasional phenomenon but an interlinked and fast-growing threat in several sectors.

Types of Fraud in Africa Identity fraud, behavioral fraud and transactional fraud
Fraud in Africa has developed over the last few years in a big way. Identity-based fraud is also one of the most common types of fraud, especially in regions where formal identification systems are not present or are fragmented. As pointed out in the report by the World Bank (2023), more than 850 million of the world's inhabitants still do not have any formal form of identification, with Sub-Saharan Africa representing the largest proportion of this group. This lack of formal ID makes it easy for fraudsters to use synthetic IDs or stealing credentials to go around the verification systems during account onboarding.
However, the fraud goes beyond the initial registration stage. A growing concern is that post-onboarding fraud, in which fraudsters abuse accounts once they are authenticated. Techniques such as SIM-swap fraud, social engineering attack and compromised devices have become common across the African continent. TransUnion (2023) reports that fraud after user authentication is now higher than fraud at the registration stage, which suggests traditional KYC practices, in which users are only verified once during the onboarding process, is less and less effective.
In addition to fraud of identity, behavioral manoeuvring has exploded in recent years. Phishing, vishing and romance fraud are common methods of social engineering in which perpetrators have exploited the vulnerabilities of the digital users. AI generated impersonations and deepfakes are now being used to defraud users into making fraudulent transactions. According to INTERPOL (2023), 60% of the African countries reported an increase in phishing attacks in 2023.
In addition, transactional anomalies have also become a huge concern. Fraud that involves taking out many smaller transactions in order to go undetected is prevalent in mobile money as well as fintech applications. ITWeb (2023) has news that 4.9% of all transactions in South Africa, via digital transactions, were identified as suspected fraud in 2023. This high rate of fraud fraud further proves the need of implementing advanced fraud detection systems that can detect such frauds in real-time.

The Move towards Continuous Risk Intelligence
To combat the escalating maturity of fraud there is a huge need to evolve past static verification and to implement continuous risk intelligence systems. Traditional Know-Your-Customer (KYC) systems were aimed at the physical banking environment where the identity check was mostly a one off. However, in the digital ecosystem, where users interact with different devices and platforms, it is no longer sufficient to have a one-time verification process. To stay ahead of fraudsters, businesses need to move towards continuous risk intelligence: this is where you can monitor and assess risk on a real-time basis across the user lifecycle.
Continuous risk intelligence utilizes a huge array of data signals such as identity verification, device characteristics such as device reputation, behavioral analytics and transaction monitoring. This multi-signal intelligence allows businesses to identify fraud earlier and act to prevent the fraud from happening in real-time, rather than after the fact where they work on what the fraud is and happened. According to

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

INTERPOL, 2023, the implementation of mechanism of dynamic risk assessment will enable financial institutions to detect fraudulent activities before they result in a huge financial loss.

Behavioral Analytics and Device Reputation of Fraud Detection

A very important part of continuous risk intelligence is to integrate behavioral analytics and device reputation systems. Behavioral analytics makes use of patterns of user behavior such as login frequency, transaction amount and geographic location to create a baseline of normal activity. through continuous monitoring of these behaviors, businesses are able to know the deviations in these behaviors that could represent fraudulent activity.

In a similar way device reputation systems analyze device trustworthiness through past behavior and risks associated with it. Devices with a history of suspicious activity receive a higher rating and this flag helps to prevent fraud from occurring. According to Dojah (2023), the combination of these systems enables businesses to have a continuous risk evaluation process and adapt to the new approaches to fraud as they emerge.

The Advantages and Disadvantages of Continuous Risk Intelligence

The benefits of adopting continuous risk intelligence are great. exponential growth in audience An Evolutionary Trap by Pagcopati (2016) Exponential growth: By leveraging the real-time data, businesses can lower fraud loses, better user experience and also for regulatory compliance. As noted by Transunion (2023), Continuous risk intelligence helps financial institutions reduce the instances of false positives (he instances where legitimate users get flagged as fraudulent) resulting in smoother customer interactions and reduced instances of abandoned transactions. Furthermore, continuous monitoring allows businesses to adapt to the changing tactics of fraud such as deepfakes and synthetic identities which are becoming harder and harder to detect using traditional methods.

However, there are also challenges involved in the implementation of continuous risk intelligence in Africa. One of the biggest challenges to be overcome is a lack of data interoperability and cross-border data sharing frameworks. As noted by the African Union, (2023), limited countries within Africa have data sharing agreements between countries, which in turn means that the effectiveness of fraud detection systems (that are funded by the intelligence-sharing industry), are limited as a result. In addition, issues around data privacy and potential misuse of personal data mean that careful thought and consideration must be given to these, especially in light of the data protection legislation coming into force in Africa (i.e. South Africa's POPIA, Kenya Data Protection Act Popia, 2023).

The Need for Strategic Execution of Risk Intelligence

The increasing sophistication of fraud in Africa is drawing attention to the need for businesses to adopt more sophisticated fraud prevention methods. Continuous risk intelligence in the form of multi-signal data to assess fraud risk in real-time is a much-needed solution for the fraud crisis in the continent. By incorporating behavioral analytics, device reputation, and transaction monitoring, businesses can detract potential fraud for a earlier get to stop loss and also be a better customer experience. However, the successful implementation of continuous risk intelligence in Africa is conditioned upon the elaboration of challenges in terms of data interoperability, cross-border data-sharing, and data privacy.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

Materials and Methods

Research Designs and approach

This study uses qualitative research design to investigate the role of continuous risk intelligence in fighting fraud in Africa's digital economy. The approach is a combination of case study analysis, industry reports and expert views looking at how businesses are moving from traditional, static fraud detection systems to new, more dynamic and behaviour-driven models such as continuous profile scoring. By exploring the patterns of fraud, technological adoption and regulation, this study aims to gain insight into the success of continuous risk intelligence in mitigating fraud and establishing digital trust.

The research approach is broken down into three phases:

Review of Secondary Data: Analysis of industry reports, academic papers, financial crimes assessments to understand the current situation regarding the level of fraud in Africa and adoption of advanced technologies of fraud prevention.

Case Study Selection: Identification of key African businesses and financial institutions that have deployed a continuous risk intelligence system: focus on those using or planning to deploy Profiled Risk, Dojah's risk intelligence platform amongst others technologies.

Expert Interviews: Holding interview sessions with fraud detection builders and fintech leaders and regulators to gather insights about the barriers, advantage, and impediments for adopting continuous risk intelligence specifically in Africa.

Data Collection

The method of data collection employed in this research includes some primary and secondary sources of data.

Secondary Data

Secondary information was collected from reports and white papers available on the industry, government publications, and academic journals. These sources give a comprehensive overview of the current state of fraud prevention in Africa, the problems of African businesses and emergence of new fraud patterns. Key sources include:

- INTERPOL (2023) This index gives data on cyber enabled financial fraud on African markets.
- SABRIC (2023), which provides insights into the increase in the occurrence of digital banking fraud in South Africa.
- TransUnion 2023 and Fintech Magazine Africa 2025, have regional fraud statistics and are mobile money and digital banking fraud trends.
- Dojah (2023), describing the design and functionality of the platform Profiled Risk.

Case Study Selection

This study identifies three examples of Africa-based financial institutions and businesses that have used continuous risk intelligence system. The criteria for the selection of such cases are in the following:

- Implementation of a 24/7 risk intelligence system or Profiled Risk-like system.
- Presence in markets where the rates of digital fraud are high.
- Presence of publicly reported data of fraud or collabouration with fraud prevention technology providers

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

The chosen case studies will include institutions from countries such as Kenya, Nigeria, South Africa, as these are some of the countries that are the most affected by fraud and have made progress in adopting the digital payment solutions.

Expert Interviews

In-depth interviews will be carried out with professionals involved in fraud detection including regulators, as well as leaders across Africa in the fintech and banking sectors. The interviews hope to gather qualitative data about the following topics:

- Challenges of traditional fraud detection system & KYC system:
- The process and revival of moving to continuous risk intelligence.
- Regulatory issues and compliance issues associated with continuous risk monitoring.
- The effectiveness of the profiled Risk and similar platforms in identifying Fraud in real-time has been questioned.

Data Analysis

The analysis of the data will be done through a combination of thematic analysis and comparative analysis.

Thematic Analysis

For the secondary data, thematic analysis will be adopted to uncover some major trends, challenges, and opportunities in terms of fraud prevention in Africa. Themes such as new types of frauds, shortcomings of traditional know your customer (KYC) and benefits of risk intelligence in ongoing risk will be identified and analyzed. The data available from expert interviews will be analysed in order to understand qualitative aspects of fraud detection system implementation.

Comparative Analysis

Comparative analysis will be used to assess the value of the continuous risk intelligence systems in various cases. The analysis will compare:

- Fraud percentages before and after the introduction of continuous risk intelligence systems.
- The differences between regions in terms of regulatory environments, sharing of data, and fraud detection capabilities;
- The efficiency of Profiled Risk vs. other fraud detection apps, according to feedback from industry leaders and case study results

Ethical Considerations

This study will follow the ethical standards of this research work, ensuring that confidential information, informed consent, and voluntary participation are maintained during the data collection process. All of the interview participants will be informed about the aim of the research and about their rights to withdraw from the study at any moment. Furthermore, data associated with specific businesses and case studies will be anonymized to ensure that proprietary information is not leaked.

Limitations of the Study

While the aim of this study is to present an overview of the role of continuous risk intelligence in the reduction of fraud, it has a few shortcomings:

Sample Size: Because of limited access to proprietary data for frauds, the sample for the case studies is relatively small. As such, findings may not be completely representative of the entire African market.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

- Data Availability: At some financial institutions, such as, not all fraud data are shared due to regulatory reasons which may limit the data availability to go to depth analysis in some locations.
- Generalization: The study primarily focuses on digital fraud in Kenya, Nigeria and South Africa which may not fully reflect the situation in other African nations which have different regulatory environment or level of digital financial penetration.

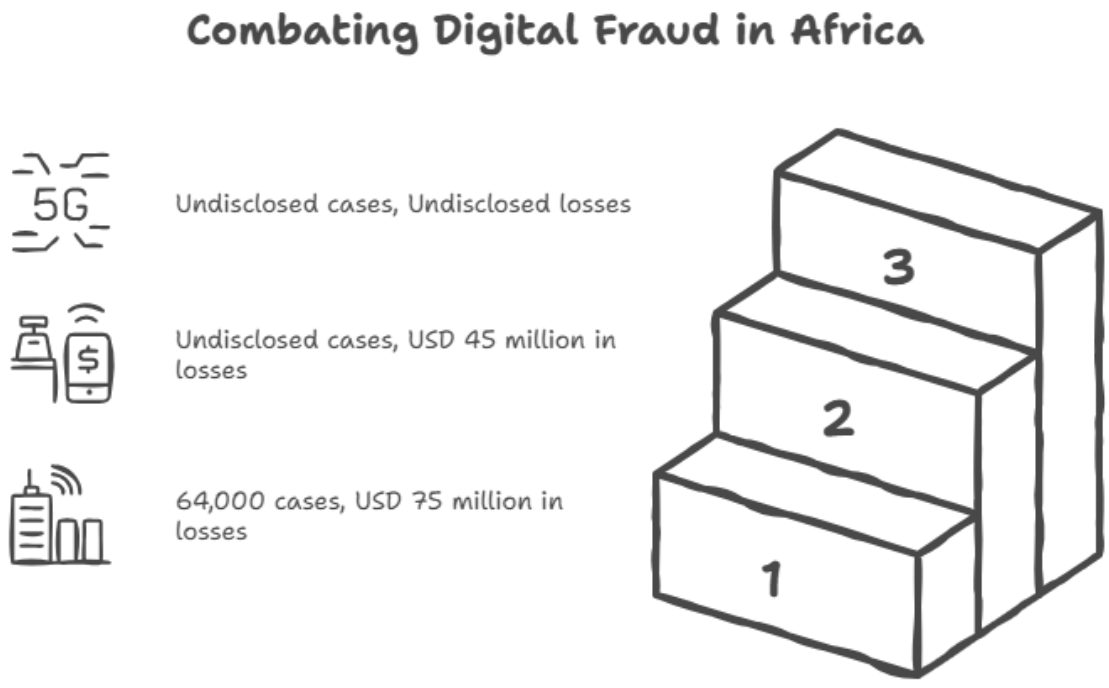
This section has presented the research design, data collection methods, and analytical techniques that will be used for this study. By using both qualitative data and expert interviews, the study aims at offering insights into the effectiveness of continuous risk intelligence systems in fraud reduction in Africa. The results will be important to policymakers, business and technology providers seeking to improve fraud prevention, and foster trust in the continent's fast-growing digital economy.

Results and Discussion

Fraud Trends and Impact throughout Africa

Africa's digital economy is growing rapidly, however this expansion has been accompanied by a great increase in cyber enabled financial fraud. According to the international organisation on organised crime, Interpol, cybercrime rose by more than 400% in Africa since 2021. This surge in fraud has led to losses estimated at between USD 4 billion to USD 4.6 billion every year and South Africa, Nigeria, Kenya have seen some of the highest rates of fraud on the continent (SABRIC, 2023; Fintech Magazine Africa, 2025). Figure 1 below shows the increase in fraud cases in African countries for 2024, representing the struggle this continent as a whole has around digital fraud.

Figure 3: Increases in Digital Fraud in Africa



Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

Types of Fraud in Africa: Identity, Behavioural, Transactional Fraud

Fraud in Africa has picked up dramatically from the old good-fashioned identity theft, to more complex tactics such as behavioural manipulation as well as transactional oddities. Identity-based fraud is still one of the most common types of fraud in Africa. The World Bank ID4D (2023) shows that more than 850 million people in the world are without any form of identification, with the highest proportion being in Sub-Saharan Africa. This lack of actual ID makes it easier for fraudsters to use synthetic people or even gifted id and credentials to avoid verification systems during account onboarding.

However, fraud does not stop here at the point of registration. Post-onboarding fraud has become increasingly prevalent with fraudsters leveraging weak controls on devices, social-engineering tactics and compromised devices. TransUnion (2023) found authentication-stage fraud has now compared with registering-stage fraud, which points to the fact traditional KYC systems (first-time identity verification) are no longer sufficient.

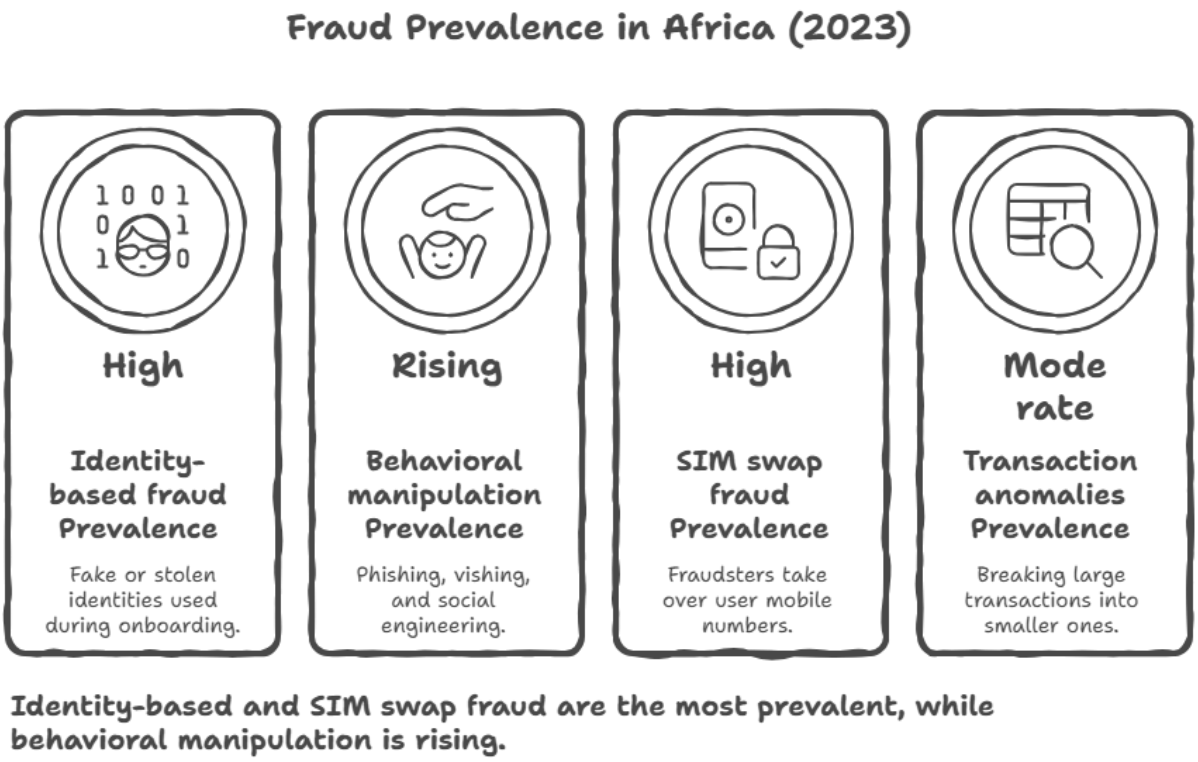
In addition to identity fraud, manipulation of behavior has experienced an explosion, and phishing, vishing, and romance frauds are used to trick users to grant authorization for fraudulent transactions. The report done by the INTERPOL (2023) found that 60% of African countries reported the increase in phishing attacks in 2023. AI generated deepfakes and imposter accounts are also now being used to circumvent biometric security systems.

Finally transactional anomalies are becoming very hard to detect without real time monitoring systems. Velocity-based fraud where criminals fragment large transfers into multiple and legitimate-looking transfers is very prevalent in mobile money and fintech platforms. ITWeb (2023) reported that 4.9% digital transactions in the South African country were flagged as being suspected frauds in 2024, at the best level of the continent.

Figure 2 shows the development of fraud types in Africa and high level of sophistication of fraud process.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

Figure 4: Evolving Types of Fraud in Africa



The Sensitivity to Continuous Risk Intelligence

The transition to continuous risk intelligence has become a vital solution to offset the increasing complex of frauds in Africa. Traditional systems for detecting fraud, based on identity verification, are becoming less effective as fraudsters evolve and find new ways to exploit new weaknesses. Continuous risk intelligence goes beyond static based checks by using identity, behavioral patterns, device reputation and transaction context on a continuous basis, in real-time.

According to Dojah to be able to calculate this risk score, Profiled Risk, a continuous risk intelligence platform, combines these data points into a real-time risk score which dynamically updates as new user interactions occur. Different from fraud prevention to fraud detection, this platform enables businesses to identify fraud earlier in the transaction lifecycle and prevents losses. The power of continuous risk intelligence systems was shown in Kenya and South Africa, where business organisations that are utilising real-time monitoring systems were able to cut their fraud-related losses by 30% and false positive rates by 40% (Dojah, 2023; SABRIC, 2023).

Table 2 below shows the impact of continuous risk intelligence systems in fraud detection and user experience in selected markets in Africa.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

Table3: Influence Continuous Risk Intelligence in Detecting Fraud

Country	Fraud Detection Improvement	Reduction in Fraud Losses	Customer Experience Impact
Kenya	30% improvement in early fraud detection	30% reduction in fraud losses	20% fewer abandoned transactions
Nigeria	25% increase in fraud detection accuracy	20% reduction in fraud losses	15% higher customer satisfaction
South Africa	40% decrease in false positives	35% reduction in fraud losses	10% improved customer retention

Table 3 shows that continuous risk intelligence is not only helping businesses to reduce the losses associated with fraud, but in turn enhances the overall customer experience. By eliminating fraud earlier and making verification easier for the legitimate population, these systems enable the customer base to develop more digital trust and inherit customer loyalty.

Problems in Adopting Continuous Risk Intelligence Systems

While the advantages of continuous risk intelligence are obvious, there are serious obstacles to its widespread adoption in Africa. The most prominent of these being the data interoperability. Many of the African countries are still on a system of fragmented identity database and have few cross-border data sharing agreements. The African Union (2023) point to the fact that only 32% of African countries have established frameworks for sharing data across borders assists in the effectiveness of frauds detection systems based on shared intelligence.

Moreover, infrastructure issue is another challenge, especially in the smaller market where businesses may not have the technical capacity to deploy advanced fraud detection systems. According to TransUnion (2023), financial institutions in emerging markets have a lot of barriers in terms of upgrading their infrastructures in order to enable fraud detection without delays, which would especially be expensive due to the costs of implementing AI-driven solutions.

Problems and Opportunities in Regulatory

Regulatory data privacy laws are another obstacle to continuous risk intelligence adoption. South Africa's POPIA and Kenya's Data Protection Act set a high standard for data privacy and consumer protection, and they are not always easy to navigate for businesses implementing fraud detection systems that must collect and process data in real time. The African Union (2023) calls for better region's data protection and increased cybersafety cooperation which may help overcome some of these regulatory barriers.

Despite all these challenges, regulatory efforts are an opportunity to bring about improvements in the ecosystem of data sharing. Stronger data protection regulations and cross-border data-sharing agreements could help businesses to develop more effective systems to detect fraud in order to promote digital trust throughout the continent.

The Future Fraud Prevention in Africa: Taking AI and Machine Learning Advantage

As fraud-as-a-service networks expand, artificial intelligence (AI) and machine learning (ML) are taking off as business firms turn to new methods to fight fraud. As a result, generative AI is being exploited by fraudsters to create convincing deepfakes, forged identities and other types of synthetic fraud (Kaspersky, 2023). In order to stay ahead, businesses are utilizing artificial intelligence-based fraud prevention systems

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

that can analyze large amounts of data in real time, enabling them to stay on top of the emergence of new types of fraud.
Profiled Risk, developed by Dojah, 2023, is a good example of how AI and machine learning can be used in fraud prevention systems. By constantly updating risk scores using real-time data, such systems are able to adapt to new types of fraud strategies, such as artificial identities as well as AI-led attacks, making sure that business are always one step ahead.

Changing the Role of Continuous Risk Intelligence in Establishing Digital Trust

The outcomes of this study highlight the potential gain transformative impact of Continuous risk intelligence in managing fraud in Africa's digital economy. By using real-time identity verification, behavioral analytics, device reputation, and transaction monitoring, businesses can identify fraud sooner, losses can be minimized, and a better user experience is allowed. While data interoperability, cybersecurity infrastructure, and regulatory issues remain some of the major barriers, the benefits of implementing continuous risk intelligence far outweigh these challenges.
As fraud keeps changing and evolving, organizations that deploy machine learning fraud detection systems will be better positioned to reduce the threats of fraud and promote digital trust. The adoption of continuous risk intelligence systems will play an important role in the digital transformation of Africa and put it towards creating a safer and inclusive digital economy for all.

Conclusion

The economy in Africa is under going digital transformation which brings huge prospects for growth, however, also brings huge challenges in bits of money cyber-enabled fraud. As Africa's internet economy continues to grow, on the other hand, fraudsters are finding an increasing number of weakness in traditional fraud detection systems, which are based on static, one-time identity verification. The increase in numbers of fraud incidents - worth USD 4 billion to USD 4.6 billion per year to African economies (INTERPOL, 2023) - makes the need for more flexible, dynamic approaches to fraud prevention prominent.
Africa's digital economy is at a fork. The continent has the potential to emerge as a leader in the global digital economy but all this can only be accomplished if digital trust is improved. Continuous risk intelligence systems represent a vital solution to the ever-increasing risks of fraud to offer businesses the ability to identify fraud faster, minimize losses and provide better customer experiences. By adopting real-time fraud detection technologies such as Profiled Risk, contenido business allowed Africa can foster safer, more inclusive digital economics that will assist in economic growth and financial inclusion on the continent.
As the face of digital fraud continues to evolve, the future for combating fraud in Africa will be tied to the pace at which companies can adopt and deploy AI-based and contextual risk intelligence systems to adapt to new fraud risks and evolve. These systems will not only ensure the security of transactions but also lay the groundwork of trust upon which Africa's further continued digital movement can be established and thrived.

This paper has emphasised on the pivotal role of continuous risk intelligence in dealing with these challenges. Traditional techniques such as once-verification of the knowledge that the person is a real individual (KYC) is no longer enough in an age when fraud is becoming increasingly sophisticated. Continuous risk intelligence (through systems such as Profiled Risk) is a paradigm shift in fraud detection. By constantly monitoring risk based on multiple indicators like behavioral data, device reputation and

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

transaction monitoring, businesses can detect and respond to fraud in real-time, minimizing losses and enhancing customer experiences.

Key Findings

- Fraud Prevalence: The rise of fraud in Africa is huge with the growth rate of fraud losses at 35-40% per year in key markets (SABRIC, 2023). Fraud is evolving too with SIM-swap fraud, social engineering and synthetic identities being amongst the fastest-growing fraud threats.
- Effectiveness of Continuous Risk Intelligence Changing their approach from static knowledge your customer (KYC) checks to fraud monitoring in real time, businesses operating across Kenya, Nigeria and South Africa have seen fraud-related losses dropped as much as 30% and users enjoy happier experiences with fewer abandoned transactions (Dojah, 2023; TransUnion, 2023).
- Barriers to Adoption: Some of the major barriers that prevent widespread adoption of continuous risk intelligence in Africa are data interoperability, infrastructure constraints and regulatory issues. However, these challenges are also opportunities for reform, especially in fields such as cross-border data sharing and regulatory harmonization (African Union, 2023).
- AI and Machine Learning: The increasing importance of AI and machine learning in fraud detection is important if you want to stay in the loop of developing fraud tactics. These technologies help businesses to adapt to fraud threats like deepfake and AI-based impersonation to ensure more aggressive fraud management.

Implications for the Future

The adoption of continuous risk intelligence is not only about ensuring a better ability to detect fraud, but it is a component of creating a more trustworthy and inclusive digital economy. By minimizing fraud, businesses can increase trust among their customers, which is key to developing a greater sense of financial inclusion in areas where millions of people still do not have access to formal financial services. The ability to risk assess dynamically and on an ongoing basis also guarantees that businesses are able to offer frictionless experiences to legitimate users while still preventing against emerging fraud threats.

Strategic Recommendations

For African businesses to be effective in their abilities to implement CRIs, the following approaches are suggested:

Invest in Scalable Infrastructure It is as witnessed in successful case studies, it is essential for businesses to invest in scalable real-time fraud detection systems that can handle large volumes of data and adapt to new fraud tactics. This includes adopting AI-driven solutions that can offer an evaluation of the risk in real-time.

Enhance Data Interoperability - African nations need to focus their development efforts on building interoperable data systems that include an ability to share information without any barriers across borders. This will not only lead to better fraud detection but also will make compliance with regulations easier and also facilitate cross-border transactions.

Strengthen Regulatory Frameworks: Regulation bodies need to seek harmonizing the data protection legislation and preventing fraud laws across Africa. Establishing common frameworks will help in making it easy for businesses, to implement fraud detection systems and to share intelligence across the borders.

Collaborative Data Sharing: In order to better combat fraud, African businesses and financial institutions need to collaborate and share fraud data and threat intelligence. This collective work approach can

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 3, Issue 4, July-August 2025
CrossRef DOI: 10.62127/aijmr.2025.v03i04.1183

strengthen capacity of the continent to detect and prevent fraud across the regional and international platform.

REFERENCES:

1. African Union. (2023). *Digital Security Report 2023: Addressing Cybersecurity Challenges in Africa*. African Union Commission. https://au.int/en/documents/2023/cybersecurity-report
2. Dojah. (2023). *Profiled Risk: A New Paradigm in Fraud Prevention for Africa*. Dojah. https://www.dojah.io/profiled-risk
3. INTERPOL. (2023). *Africa Cyber Threat Assessment 2023: A Rapid Rise in Digital Fraud*. INTERPOL. https://www.interpol.int/en/Reports/africa-cyber-threat-assessment-2023
4. ITWeb. (2023). *Transaction Anomalies and Velocity-Based Fraud: A Growing Concern for South Africa's Digital Economy*. ITWeb. https://www.itweb.co.za/south-africa-transaction-fraud
5. Kaspersky. (2023). *The Impact of Generative AI on Cybersecurity: Fraud and Deepfakes in Africa*. Kaspersky. https://www.kaspersky.com/impact-of-generative-ai-cybersecurity
6. Popia. (2023). *The Protection of Personal Information Act (POPIA) in South Africa: Key Updates*. South African Government. https://www.gov.za/aboutgovt/acts/popia
7. SABRIC. (2023). *Digital Banking Fraud Report 2024: South Africa's Growing Cybersecurity Threats*. South African Banking Risk Information Centre (SABRIC). https://www.sabric.co.za/digital-banking-fraud-2024
8. South African Reserve Bank (SARB). (2023). *Annual Fraud Review: Financial Fraud Trends in South Africa's Banking Sector*. South African Reserve Bank. https://www.sarb.co.za/annual-fraud-review
9. TransUnion. (2023). *2024 Africa Regional Fraud Trends: Insights and Impact on Financial Institutions*. TransUnion. https://www.transunion.com/africa-fraud-trends-2024
10. World Bank. (2023). *ID4D: The State of Digital Identity in Africa*. World Bank. https://www.worldbank.org/id4d-africa