AI's dual role in telecom fraud

Why artificial intelligence is both a threat and a shield for telcos

Fraud has long been a persistent challenge in the telecommunications landscape, leading to substantial financial losses for customers and reputational damages for telecommunication companies (telcos). While operators have developed systems and controls to manage these risks, the sector's expansion into adjacent domains (such as mobile money and payment service banking) is blurring the traditional boundaries of telecom fraud.

The result is a more complex and interconnected risk environment, where both the frequency and impact of fraud are escalating. Adding to this complexity is the rapid pace of technological advancement. For instance, Russian cybersecurity firm F6 reported a rise in SIM swapping incidents, particularly related to the shift to eSIM technology. These fraudsters are hijacking phone numbers and bypassing security measures to access bank accounts.

As AI continues to mature, it is reshaping the fraud landscape—introducing heightened threats and powerful new tools. On one hand, AI can be exploited to scale and automate fraud schemes with unprecedented sophistication. On the other, it equips telecommunication companies (telcos) with advanced capabilities for fraud detection, prevention, and response.

This dual role—AI as both a tool and a target—underscores the urgent need for Nigerian telecom players to adopt AI thoughtfully and strategically. Navigating this evolving landscape requires more than just investment in technology; it demands a deep understanding of what’s happening today in the world of technological disruption, and what’s to come.

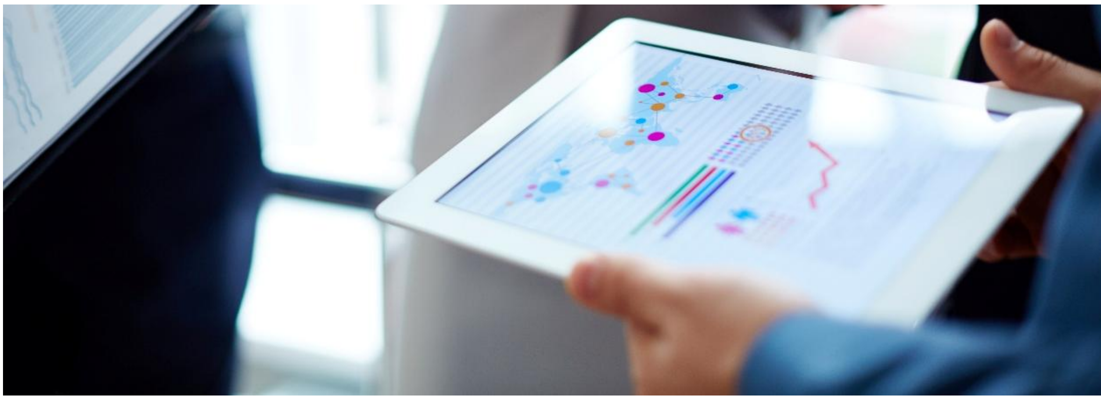
AI's impact on fraud in the telecoms industry

The impact of fraud on telecommunications companies is far-reaching, resulting in financial losses, reputational damage, and compliance issues. In 2023, global telecom fraud was estimated at $38.95bn. Additionally, in Nigeria, the NCC reported citizens lost about N12.5 billion to telecom-related financial crimes from 2019 to January 2023, underscoring the scale and persistence of this threat.

> "The Nigerian Communications Commission (NCC) reported that citizens lost approximately N12.5 billion to financial crimes linked to the telecommunications industry between 2019 and January 2023.

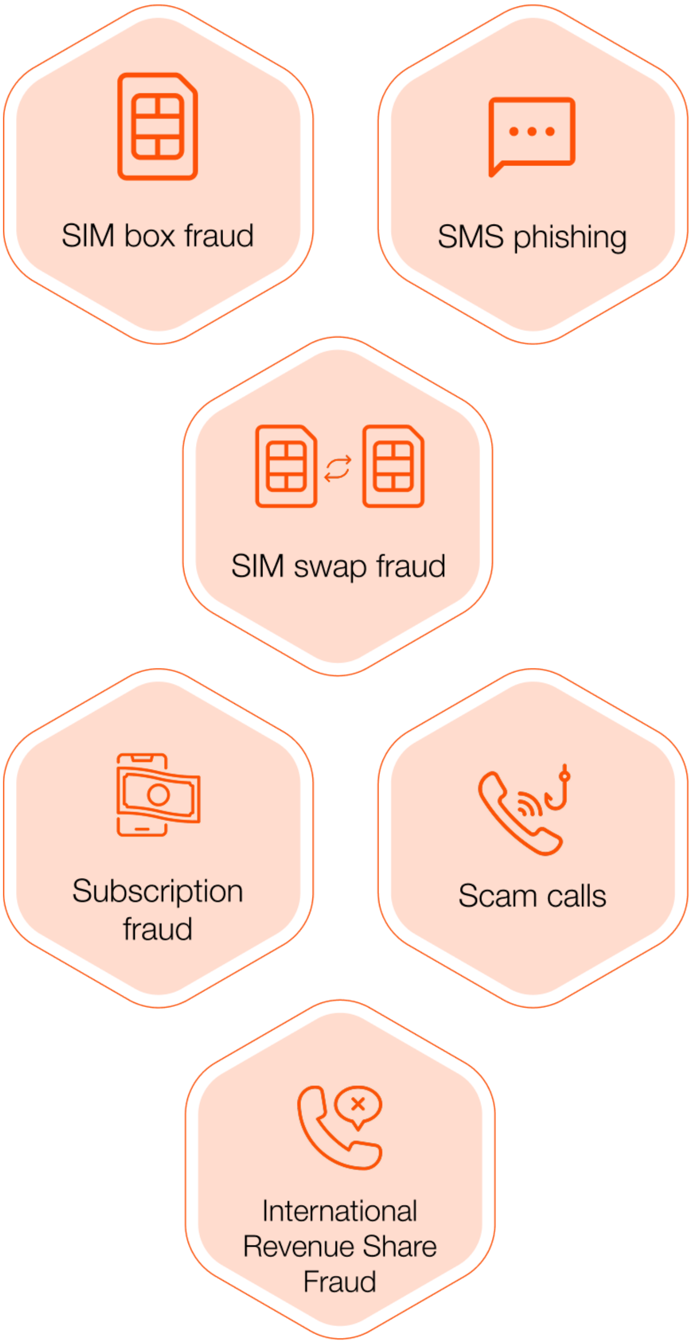
The telecommunications industry faces diverse fraud threats, most of which are cyber-enabled. PwC's 2022 Global Crime Survey found that nearly two-thirds of Technology, Media, and Telecommunications companies experienced fraud, the highest rate across all industries, with half of these incidents being cyber-crimes. The growing adoption of artificial intelligence will likely reshape this landscape further.

The intersection with financial services amplifies these risks for telecom operators who enable digital payments and banking partnerships. In Nigeria, where 59% of e-banking customers have fallen victim to scams, telecommunications providers may face mounting pressure as key infrastructure for digital financial services. When fraud occurs across these interconnected platforms, both telecommunications and financial services providers experience regulatory scrutiny and customer trust erosion—creating cascading impacts across the digital ecosystem.



As telcos navigate these challenges, they must also contend with the evolving threat landscape, particularly the increasing use of AI by fraudsters. While AI has tremendous potential to drive positive change across various sectors, it also enables fraudsters to create and disseminate scams quickly and at scale, making them more convincing and difficult to detect.

Examples of fraud typologies and the potential impact of AI include:



SIM box fraud

SMS phishing

SIM swap fraud

Subscription fraud

Scam calls

International Revenue Share Fraud

SIM box fraud

SIM box fraud involves the use of specialised devices that can hold dozens or hundreds of SIM cards. Fraudsters use these devices to route international calls through local networks, making them appear as domestic calls and bypassing international termination fees. This results in lost revenue for telecom providers, who receive insufficient compensation for these calls, while customers pay full price, allowing the fraudster to pocket the savings.

AI's impact:

AI can optimise the routing of international calls through local networks, further disguising the origin of the calls and evading detection systems.

SMS phishing (Smishing)

Fraudsters use deceptive text messages to extract personal information from unsuspecting individuals. They typically impersonate legitimate entities, prompting users to click on malicious links or disclose sensitive information. While telcos don't bear the financial brunt of this type of fraud, it can lead to reputational damage and dissatisfied customers.

AI's impact:

Generative AI can be used to create tailored messages faster. GenAI can also make scams harder to detect by eliminating the traditional 'tells' such as poor spelling and grammar.

SIM swap fraud

SIM swap fraud involves criminals hijacking a victim's SIM card by using stolen personal data to pass identity verification checks with a mobile carrier's customer service team. Once they gain control of the victim's phone number, fraudsters intercept one-time passwords (OTPs) and authentication messages, enabling them to access banking accounts, email, and other sensitive online services.

AI's impact:

Fraudsters can use voice cloning to deceive family members, colleagues, and others, leading to further fraudulent activities.

Subscription fraud

Criminals use illegally obtained personal data to fraudulently apply for credit-based services without intending to pay.

AI's impact:

GenAI can create highly realistic synthetic identities by combining real and fake data, making it difficult for traditional verification systems to detect fraud. AI can automate the process of filling out subscription forms, using stolen or synthetic identities to sign up for multiple services quickly and efficiently.

Scam calls

Fraudsters use phone calls to trick victims into divulging personal information, manipulating them through social engineering tactics. In Nigeria, a recent scamming trend involves impostors posing as bank representatives, urging victims to share sensitive security details. These scammers often already possess basic personal information, such as the victim's full name and date of birth.

AI's impact:

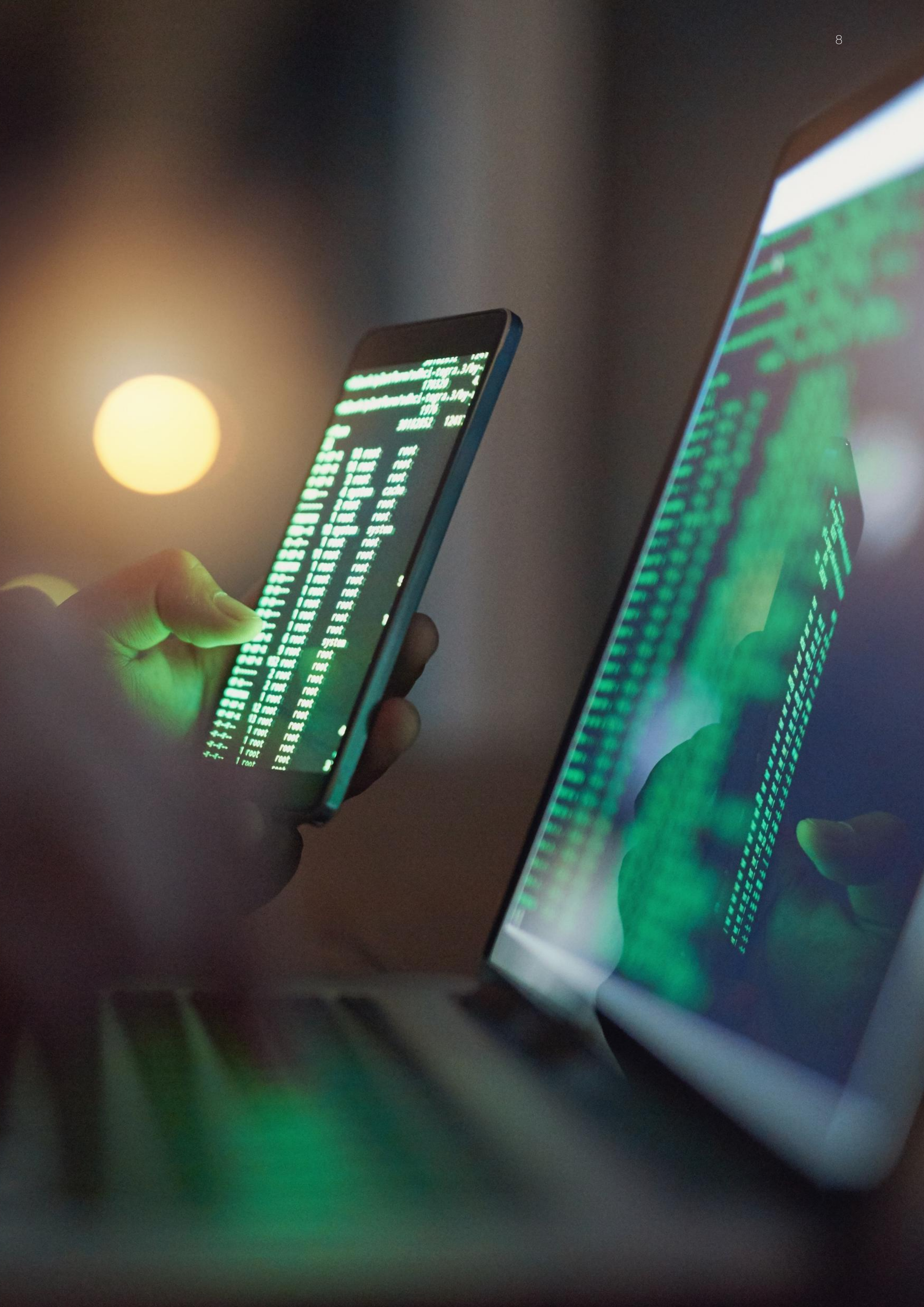
Deepfake technology is making scam calls more convincing by enabling fraudsters to impersonate loved ones with alarming accuracy. Powered by AI, these calls can be generated and scaled automatically, allowing attackers to target a broader pool of victims.

International Revenue Share Fraud (IRSF)

This involves a scammer making a brief, missed call from an international number. Returning the call connects the user to a premium-rate service controlled by the scammer, potentially leading to significant charges.

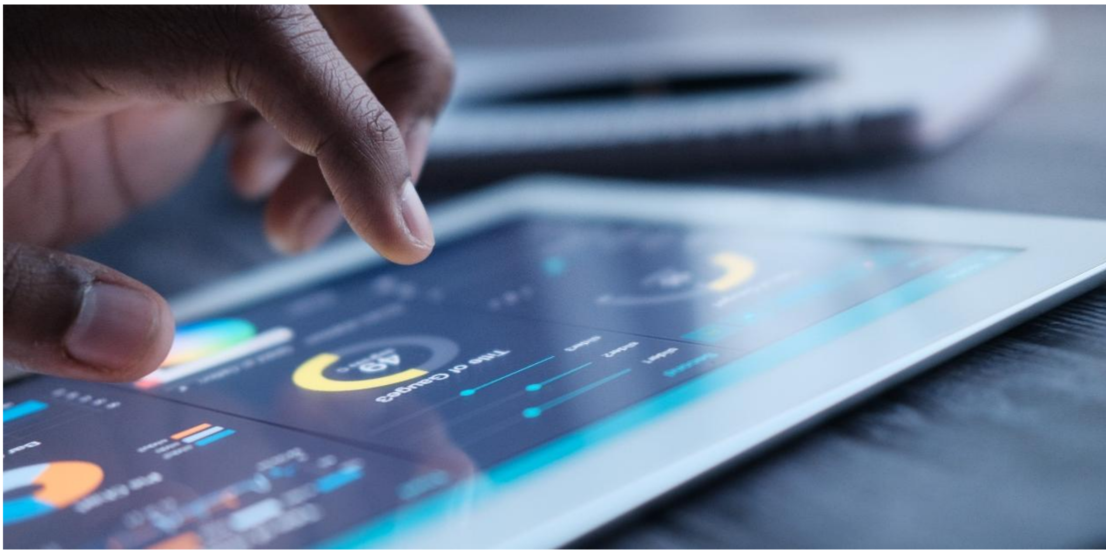
AI's impact:

With a combination of AI and phone farms, scammers can automate their missed call fraud and perform it at larger scale.



AI as a fraud prevention tool for telcos

PwC Nigeria’s 2024 CEO survey found that while business leaders are keen to leverage the potential of AI, concerns about associated risks are impeding its adoption. This seeming contradiction stems from the tension between enthusiasm for AI's benefits and apprehension about its risks. Similarly, PwC’s 2024 Global Economic Crime Survey shows that only 31% of respondents believe AI will enhance the efficiency and cost-effectiveness of sanctions compliance programmes.



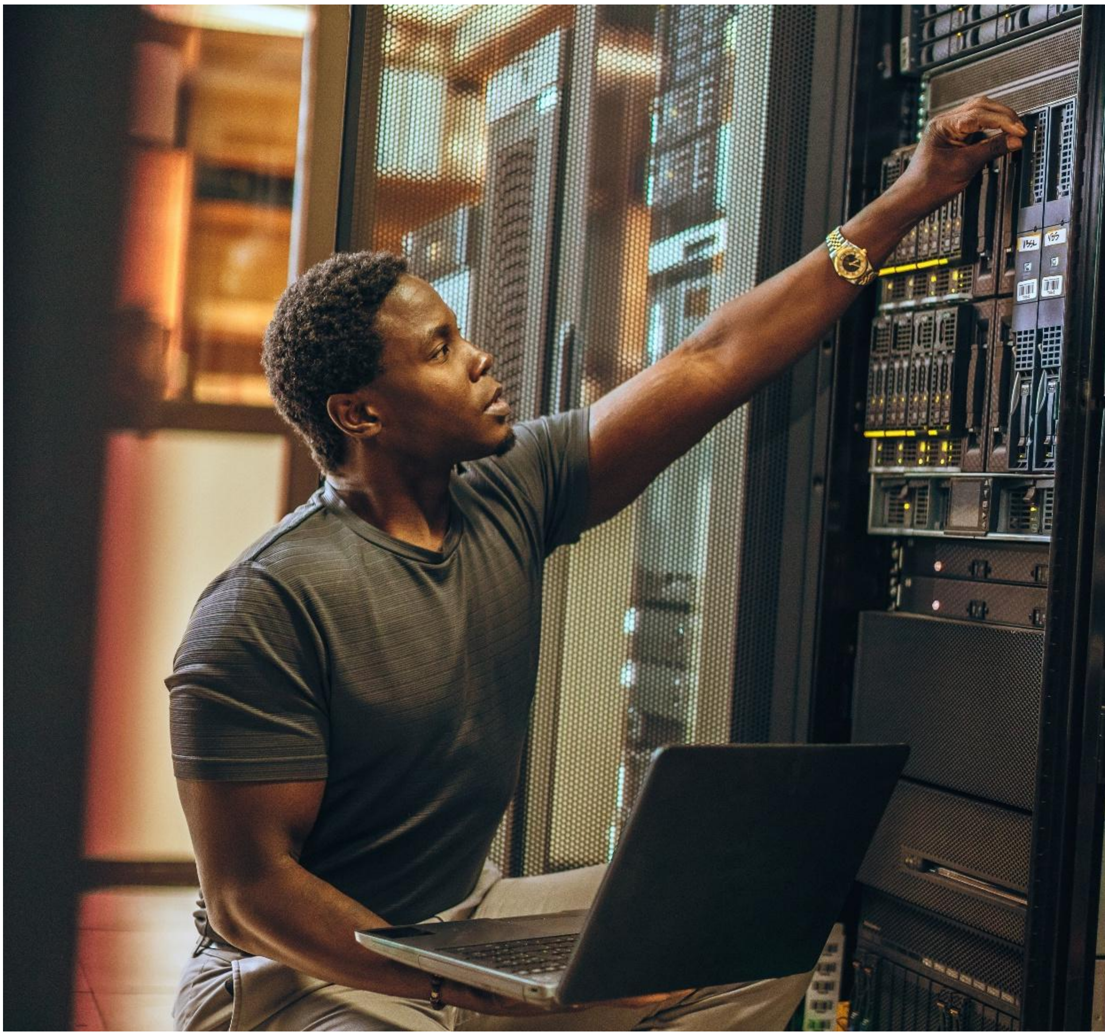
In the telecommunications sector, where fraud is already a significant challenge, business leaders can rethink their perception of AI—rather than viewing AI as an inherent threat, telcos can harness its power to detect and prevent fraud. With their vast data resources, they can train AI models to identify and mitigate risks, effectively "fighting fire with fire." This strong data foundation also enables telcos to utilise GenAI for:

- Pattern recognition: Use AI to analyse patterns in data. These patterns can help identify characteristics commonly associated with fraud, such as unusual call frequencies, short call durations, or calls made at odd hours. An example of this is a spam alert service implemented by a Nigerian telco that uses AI to analyse sender behaviour across more than 200 parameters to determine if a message is fraudulent.

- **Machine learning models**: Develop and train machine learning models on datasets containing examples of both legitimate and fraudulent activities. These models can learn to recognise subtle indicators of fraud and adapt to new tactics used by fraudsters.

- **Real-time analysis**: Implement AI systems capable of real-time data analysis. This allows for the immediate detection and prevention of fraudulent activities as they occur, minimising potential damage.

- **Incident reporting**: By leveraging natural language processing, GenAI can transform technical data into easily understandable content for non-technical stakeholders. In the event of a major business disruption, GenAI can quickly generate targeted reports for different roles, such as focusing on regulatory implications for the chief compliance officer. Additionally, AI can create templates for comparing incidents to industry standards and regulations, which is crucial in an era of increased regulatory scrutiny on cyber-breach reporting.



Recommendations

Perform periodic fraud assessment

Telcos should conduct regular audits to ensure that systems remain up-to-date and effective. This includes reviewing your AI models, integrating new data, and refining algorithms to counter evolving fraud tactics. Routine risk analysis helps identify new and emerging threats, enabling telcos to implement necessary controls to mitigate risks.

Upskill your workforce

Establish ongoing training programmes tailored for both the fraud team and customer service agents. These programs should cover emerging fraud techniques, red flags, security protocols, and best practices for both customer interactions and fraud detection. This unified training approach will improve employees' capabilities and foster collaboration between departments.

Invest in advanced anti-fraud tools

Telecom companies should invest in sophisticated anti-fraud tools that employ machine learning and AI to enhance detection and response times. By automating the analysis of large data volumes and identifying suspicious patterns in real time, these technologies can significantly reduce the risk of fraud and strengthen overall security infrastructure.

Educate customers on fraud risks

Educating customers is crucial for effective telecommunications fraud prevention, as many scams rely on social engineering tactics that manipulate individuals into sharing personal information. Through awareness efforts and regular communication about emerging fraud schemes, telecom providers can empower customers to recognise and avoid scams. This includes sending alerts, offering tips for identifying phishing attempts, and encouraging reports of suspicious activity. Additionally, resources such as dedicated fraud prevention websites, hotlines, and educational webinars can keep customers informed and vigilant against potential threats.

Adopt responsible AI practices

Telecom companies should adopt responsible AI practices to ensure that fraud detection systems are transparent, ethical, and unbiased. This includes implementing measures to audit AI algorithms regularly, ensuring that data used for training is representative and fair, and providing clear documentation on how AI-driven decisions are made. By prioritising responsible AI, telecom operators can build trust with customers and stakeholders, enhance the effectiveness of fraud prevention efforts, and mitigate risks associated with algorithmic bias or misuse.

As telecoms providers roll out AI-powered products, it’s essential to consider how these systems might be exploited. A growing concern is GPT prompt compromise, where attackers manipulate AI inputs to extract sensitive information or circumvent security controls. This threat is particularly relevant in AI-driven customer support systems, where inadequate prompt handling can result in data breaches or unauthorised actions, exposing critical vulnerabilities within telecoms infrastructure.

Beyond telcos, AI, including generative AI, can help regulators automate compliance checks. This technology allows regulators to effectively monitor telecom operators to ensure they follow regulations related to fraud prevention and quality of service. By streamlining the compliance process, regulators can focus on high-risk areas and make better use of their resources, ultimately improving the regulatory framework.

An opportunity for collaboration

There's a valuable opportunity for collaboration between telecommunications companies, financial service providers and their regulators. Already, platforms like USSD banking demonstrate how both sectors can work together to deliver accessible financial services. But beyond convenience, this partnership holds immense potential in the fight against fraud.

Telecom operators possess sophisticated fraud detection systems designed to monitor call data and network activity. These tools can be adapted to help financial institutions verify user identities, detect SIM swap fraud, and prevent unauthorised access to accounts. On the other hand, banks have developed advanced anti-fraud algorithms that could inspire telcos to enhance their own systems for detecting suspicious behaviour across mobile networks.

By sharing insights, both sectors can strengthen their individual and collective defences. For instance, exchanging knowledge on internal fraud prevention policies and real-time threat intelligence could lead to faster, more coordinated responses to emerging threats, similar to initiatives in the UK, Philippines, Singapore, and Australia.

To make this collaboration effective, there must also be stronger engagement with regulators such as the Nigerian Communications Commission (NCC) and the Central Bank of Nigeria (CBN). Improved communication between industry players and government bodies can accelerate the development of clear, responsive regulations that support innovation while safeguarding consumers.

Conclusion

Telecom fraud affects a wide range of stakeholders, from individual consumers facing unauthorised charges to large corporations suffering reputation damage. The combination of AI and various fraud types significantly increases the success rate of these schemes. Furthermore, the global nature of telecommunications networks allows fraud to swiftly cross borders, complicating efforts to investigate and prosecute offenders, thus presenting a pressing concern for telecom companies and their regulators.

AI has the potential to revolutionise how telecom companies and regulators combat fraud while enhancing the quality of service, ultimately fostering greater trust among consumers. To fully harness this potential, it is crucial for industry players to stay informed about evolving technology trends and anticipate future challenges. This awareness will empower them to leverage AI's capabilities for more effective fraud prevention and the proactive management of emerging fraud types, all while adhering to responsible AI principles. A well-coordinated combination of the right resources and strategic alliances will enable the industry to make a significant impact in the fight against telecom fraud and build a safer, more efficient telecommunications ecosystem.

PwC can help you turn fraud-related friction into forward movement, powered by the right technology.
We bring trust and transparency to the heart of your decision-making, helping you use AI, data and tech to reduce the risk of fraud, respond swiftly to breaches, and emerge stronger—so you can prepare your business for what’s next.

Contacts

Udochi Muogilim
Partner and Technology, Media and
Telecommunications Leader, PwC Nigeria

Adeola Adekunle
Associate Director, Forensic Services,
PwC Nigeria

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum.

Find out more at www.pwc.com/ng