**How Mandatory Registration of Safaricom Lines Reduced Fraud**

1. **Introduction**
   * Brief overview of Safaricom and its significance in the telecom industry.
   * Introduction to the problem of fraud in mobile networks.
2. **Background: The Rise of Fraud in Mobile Networks**
   * Overview of common types of fraud associated with unregistered lines.
     + SIM swap scams
     + Mobile money fraud
     + Identity theft
   * Impact of fraud on consumers and the company.
3. **Safaricom's Response: Mandatory Line Registration**
   * Introduction to the policy of mandatory registration.
   * Steps involved in the registration process.
     + Verification of personal details
     + Biometric data
     + Linking to national ID databases
   * How this policy compares to regulations in other countries.
4. **Impact of the Mandatory Registration Policy**
   * Reduction in the number of fraud cases.
     + Statistical data showing decrease in fraud incidents after policy implementation.
   * Enhanced customer trust in Safaricom services.
   * Improved traceability and accountability.
5. **Challenges and Criticisms**
   * Concerns about privacy and data security.
   * Potential for misuse of registered data.
   * Challenges in ensuring every user complies.
6. **Conclusion and Future Prospects**
   * Recap of the significant reduction in fraud due to mandatory registration.
   * Consideration of further measures Safaricom can take to enhance security.
   * Reflection on the balance between security and user convenience/privacy.

**Introduction**

**Safaricom: A Telecom Giant with a Vision**

Safaricom stands as a beacon in the telecom industry, not just within its home country but on the global stage. Founded in Kenya, Safaricom has consistently demonstrated innovation and leadership in mobile communication, financial services, and technology platforms. Its significance is not just in the vast number of subscribers it serves, but in the transformative approach it takes towards the industry. Embodying this transformation is Safaricom's vision statement: "To transform beyond being a 'telco' company to being a purpose-led technology company." This vision emphasizes the company's aspiration to evolve beyond traditional telecommunication services, positioning itself at the forefront of technology and digital innovation.

But with immense growth and digital innovation come challenges. One of the most pressing issues faced by telecom giants like Safaricom is fraud. The digital age, with all its conveniences, has also paved the way for sophisticated fraud schemes that prey on unsuspecting users and exploit system vulnerabilities. Mobile network fraud not only jeopardizes the security and trust of millions of subscribers but also poses significant financial threats to telecom operators.

Safaricom, with its mission "To become a digital-first insights-led organisation that enables platforms and ecosystem partnerships," is well-aware of this challenge. Their mission underscores the importance of harnessing insights from data to drive decisions, fostering partnerships, and creating robust platforms. However, to fully realize this mission, it's crucial to address and mitigate the risks associated with fraud in the mobile network space.

1. Mpesa Fraud
   1. ATM fraud
   2. Mpesa USSD Fraud
   3. Fake/old MPesa message
   4. Fake reversal instructions
2. Hoax SMS
   1. Fake promotions
   2. Fake relief payments
   3. Fake loans
   4. Fake recipient
3. Scams/extortion
   1. Extortion messages
   2. Curiosity text
   3. False emergencies
   4. Fake job opportunities
   5. Fake international payments
4. Impersonation
   1. Sim Swap fraud
   2. Impersonating safaricom staff
   3. Fake safaricom branded online links/websites
   4. Fake safaricom branded pages
   5. Fake social media handles and pages

**2. Background: The Rise of Fraud in Mobile Networks**

As mobile networks have grown in popularity and complexity, so too have the opportunities for fraudsters to exploit unsuspecting users. These fraudsters have developed a myriad of schemes, particularly targeting unregistered lines, which are harder to trace and provide a degree of anonymity. Here's an overview of some of the most prevalent types of fraud associated with these lines:

* **Mobile Money Fraud**: This category has seen a significant rise, especially with the ubiquity of mobile money services like Mpesa. Some of the common types include:
  + **ATM Fraud**: This involves tricking users into revealing their Mpesa PIN and then withdrawing money from their accounts using ATM machines.
  + **Mpesa USSD Fraud**: Here, fraudsters deceive users into entering certain USSD codes, which lead to unauthorized transactions.
  + **Fake/Old MPesa Messages**: Fraudsters resend old Mpesa messages to deceive users into thinking they've received money.
  + **Fake Reversal Instructions**: Fraudsters send deceptive messages, urging users to reverse a transaction they claim was made in error.
* **SIM Swap Scams**: Often known as "SIM Swap Fraud", this is where fraudsters manage to get a new SIM card issued for your number. Once they have control of the SIM, they can potentially access your personal information, bank accounts, and other sensitive data.
* **Identity Theft**: This encompasses several types of fraud where fraudsters impersonate someone else to steal money or get other benefits. Safaricom, for instance, has noted instances of:
  + **Impersonating Safaricom Staff**: Fraudsters pose as Safaricom employees to deceive users into revealing sensitive information.
  + **Fake Safaricom Branded Online Links/Websites**: These deceptive websites mimic Safaricom's official site to phish for user information.
  + **Fake Social Media Handles and Pages**: Impersonating Safaricom on social media to deceive and manipulate users.
* **Hoax SMS**: These deceptive messages often contain offers or information that's too good to be true. Examples include fake promotions, relief payments, loans, or even messages claiming the recipient has won a prize.
* **Scams/Extortion**: This category involves coercing someone into paying money, often through deceptive or threatening messages. Common methods include extortion messages, fake job opportunities, and false emergency alerts.

**Impact of Fraud on Consumers and the Company**:

For consumers, the impact of these frauds can be devastating. Beyond the direct financial loss, victims often experience emotional distress, a sense of violation, and a loss of trust in mobile services. This mistrust can have a cascading effect, making users wary of even legitimate services, offers, or communications.

For companies like Safaricom, fraud doesn't just represent financial losses. It undermines the company's reputation, erodes trust in its services, and can lead to increased regulatory scrutiny. Moreover, the company often has to invest significantly in countermeasures, customer support, and public awareness campaigns to combat these fraudulent activities.

In conclusion, as mobile networks have become integral to our daily lives, they've also become a fertile ground for fraudsters. The rise of these fraudulent activities underscores the importance of vigilance, awareness, and continuous innovation in security measures.

**3. Safaricom's Response to Fraud: Solutions**

Safaricom, as one of the leading telecom giants in Kenya and East Africa, has recognized the increasing threats of fraud, particularly in the mobile money sector. The company's strategic response to these challenges is both robust and multi-faceted. Recognizing that both its reputation and the financial safety of millions of customers are at stake, Safaricom has introduced several innovative solutions to counteract fraudulent activities.

**3.1 SIM-Swap-Check Anti-fraud Solution**

One of the critical vulnerabilities exploited by fraudsters is SIM swapping. Safaricom's **SIM-Swap-Check Anti-fraud solution** addresses this directly. It provides banks with an API that allows them to determine when a customer's SIM card was last replaced. By accessing this data, banks can assess the likelihood of a transaction being fraudulent and take preventive measures. This solution is particularly valuable in a context where SIM swap fraud has been on the rise.

**3.2 ATM Vicinity Check Solution**

ATM fraud is another area of concern. Safaricom's **ATM Vicinity Check solution** ensures that cash withdrawals at ATMs can only be made if the customer is physically present at the ATM's location. This geo-fencing technology dramatically reduces the chances of unauthorized ATM transactions, safeguarding users' funds.

**3.3 Jitambulishe Voice Biometrics**

The **Jitambulishe Voice Biometrics system** is a testament to Safaricom's commitment to leveraging cutting-edge technology to enhance security. This system allows users to access services using voice authentication, significantly cutting down potential breaches due to password theft. The unique voiceprint of enrolled customers acts as a key identifier, ensuring that only the legitimate user can access specific services.

**3.4 Whistle-blowing Policy**

Internal fraud remains a concern for many organizations. Safaricom's **whistle-blowing policy** encourages ethical behavior within its workforce. Managed by an external, accredited institution, this initiative allows for anonymous reporting of any unethical or fraudulent activities, ensuring that the company can address such issues promptly.

**3.5 Customer Awareness Campaigns**

Education is a potent tool against fraud. Safaricom has rolled out numerous **customer awareness campaigns** on mainstream and social media. These campaigns aim to inform customers about the various fraudulent tactics they might encounter and how to protect themselves.

**3.6 Proactive Monitoring and Digital Solutions**

In addition to the above solutions, Safaricom has invested in **proactive monitoring and digitizing solutions** to curb fraud. These tools allow the company to track suspicious calls, detect patterns, and block potential fraudsters. For instance, the company checks the location where a SIM card is being registered and can decline suspicious swaps.

**3.7 Mandatory Registration Policy**

Safaricom has implemented a **Mandatory Registration Policy** as an additional layer of security to thwart fraud attempts. Recognizing that the first line of defense against unauthorized access and malicious activities starts with proper identification, the policy mandates all users to register their SIM cards using verifiable personal details. This measure ensures that every SIM card in use can be traced back to an individual, making it more challenging for fraudsters to use unregistered or improperly registered SIMs for nefarious activities. In cases where a SIM swap is requested, the company cross-references the data provided with the details on file, further securing users against potential SIM-swap frauds. This policy, while safeguarding customers, also aids law enforcement agencies in their investigations, ensuring that individuals involved in fraudulent activities can be promptly identified and apprehended.

Furthermore, Safaricom collaborates closely with law enforcement agencies, resulting in numerous arrests of fraudsters, underscoring its commitment to creating a safe environment for its users.

**Conclusion**

Safaricom's multi-pronged approach to combating fraud underscores the company's dedication to ensuring the safety and security of its users. By introducing technological solutions, awareness campaigns, and policies, Safaricom aims to stay a step ahead of fraudsters and offer its customers a secure, trustworthy environment for their transactions.

**4. Impact of Safaricom's Response to Fraud**

Safaricom's proactive measures against fraud have not only bolstered its reputation as a leading telecommunication provider but have also had broader ramifications on the industry, the customers, and the Kenyan financial ecosystem.

**4.1 Customer Confidence and Trust:** The introduction of initiatives like the SIM-Swap-Check and ATM Vicinity Check solutions have instilled greater confidence among customers. Knowing that the company is actively investing in security measures reassures users of the M-PESA platform and other services that their transactions and personal data are protected.

**4.2 Financial Ecosystem Stability:** The fintech sector, particularly mobile money platforms like M-PESA, plays a pivotal role in Kenya's financial landscape. By safeguarding this platform, Safaricom ensures the stability of financial transactions for millions of Kenyans, reinforcing the trust in mobile money as a safe, convenient alternative to traditional banking.

**4.3 Reduction in Fraud Cases:** Safaricom's anti-fraud solutions have led to a tangible decline in fraud incidents. With stringent checks in place for SIM swaps and biometric voice recognition for customer care, the avenues for potential fraud have significantly diminished.

**4.4 Enhanced Collaboration with Financial Institutions:** By offering solutions like the SIM-Swap-Check to banks, Safaricom has fostered stronger ties with the banking sector. This collaboration allows for quicker detection and response to suspicious activities, benefiting the broader financial ecosystem.

**4.5 Setting Industry Standards:** Safaricom's aggressive stance against fraud has set a precedent for other players in the industry. Their comprehensive approach to customer safety and data security serves as a benchmark, prompting other companies to elevate their own security measures.

**4.6 Legal and Law Enforcement Collaboration:** The company's initiatives have facilitated better collaboration with legal and law enforcement agencies. The mandatory registration policy, for instance, offers a clear trail for investigations, leading to quicker resolution of cases and the apprehension of culprits.

**4.7 Customer Awareness and Education:** Beyond technological solutions, Safaricom has been at the forefront of customer education campaigns. By informing customers about potential threats and safe practices, the company has empowered individuals to be the first line of defense against fraud attempts.

In conclusion, Safaricom's multi-pronged approach to combat fraud has had a profound impact on shaping a safer, more reliable telecommunication and financial environment in Kenya. Their initiatives underscore the importance of customer-centric strategies combined with cutting-edge technology in the fight against cyber threats and fraud.

**5. Challenges and Criticisms**

Safaricom's proactive stance in curbing fraud and ensuring user safety, while commendable, has also been met with certain challenges and criticisms. Here are some of the primary concerns and criticisms that have surfaced:

**5.1 Concerns about Privacy and Data Security:** While Safaricom's registration policies aim to curb fraudulent activities, they also require users to submit personal data, raising concerns about how this information is stored, protected, and potentially accessed. Customers and activists alike have expressed worries about unauthorized access, data breaches, and the potential for hackers to exploit this centralized pool of personal information.

**5.2 Potential for Misuse of Registered Data:** The collection of vast amounts of personal data, including biometric details, has led to concerns about how this data might be used beyond its intended purpose. There are apprehensions about the potential for surveillance, profiling, or even the misuse of data by internal actors. The line between user protection and surveillance becomes thin, leading to debates on ethical data handling and usage.

**5.3 Challenges in Ensuring Every User Complies:** Mandatory registration, while effective in theory, poses logistical challenges in practice. Given Kenya's diverse demographic, ensuring every user – especially those in remote or marginalized areas – undergoes the registration process can be daunting. There might be resistance from users who are either technologically ill-equipped, unaware of the process, or hesitant to share personal details.

**5.4 Potential for False Positives:** With advanced systems like the SIM-Swap-Check, there's always a risk of false positives, where legitimate activities are flagged as suspicious. Such instances can lead to unnecessary inconveniences for users, undermining their confidence in the system.

**5.5 Balancing User Experience and Security:** While added layers of security, like voice biometrics, offer enhanced protection, they might also complicate the user experience. Critics argue that some of these measures, although well-intended, can be cumbersome and deter users, especially those not well-versed with technology, from using the services.

**5.6 Regulatory and Legal Hurdles:** Implementing such comprehensive measures often requires navigating a complex web of regulations and legal standards, especially when it comes to data protection and privacy rights. Meeting these standards while ensuring effective fraud prevention can be challenging.

**6. Conclusion and Future Prospects**

**6.1 Recap of the Significant Reduction in Fraud:**

Over the years, Safaricom has proactively addressed the rising tide of fraudulent activities. By introducing measures such as the SIM-Swap-Check, ATM Vicinity Check, and the Voice Biometrics system, the company has made notable strides in safeguarding its users' interests. Their efforts have culminated in a significant reduction in fraud, ensuring that a majority of their customers can transact securely and with confidence.

**6.2 Consideration of Further Measures Safaricom Can Take to Enhance Security:**

While the current measures have been effective, the ever-evolving landscape of cyber threats means Safaricom needs to remain vigilant and innovative. Future prospects might include the integration of artificial intelligence and machine learning to predict and prevent fraudulent transactions or the exploration of blockchain technologies to create tamper-proof transaction logs. Collaborations with global cybersecurity firms can also offer insights into emerging threats and best practices.

**6.3 Reflection on the Balance Between Security and User Convenience/Privacy:**

The journey to a fraud-free environment is fraught with challenges, chief among them being the delicate balance between ensuring robust security and offering an uninterrupted user experience. Moreover, with increasing amounts of personal data being collected, the specter of privacy concerns looms large. As Safaricom looks to the future, it must continually evaluate its strategies, ensuring that they not only deter fraudsters but also respect the privacy and convenience of its users.

**6.4 Final Thoughts:**

In a world where digital transactions are becoming the norm, the responsibility on companies like Safaricom to protect their users is immense. Their ongoing efforts and future prospects underscore a commitment to this responsibility. However, the road ahead will require continuous adaptation, innovation, and a keen understanding of the evolving needs and concerns of their vast user base.

Write this section 3. Safaricom's Response: Solutions • Introduction to the policies. • Steps involved • Verification of personal details • Biometric data • Linking to national ID databases • How this policy compares to regulations in other countries. Safaricom has announced that it has signed up six banks to its SIM-Swap-Check Anti-fraud solution. The solution provides banks with an API (Application Programming Interface) to access information on when a customer’s SIM card was last replaced. This information can assist the banks in determining the probability that a customer’s transaction is fraudulent, and they can take further measures accordingly. The rapid growth of Kenya’s fintech sector has been accompanied by a rapidly evolving threat environment targeting both customers and fintech operators. It is, therefore, necessary for different players to partner around innovations that protect customers and their funds to safeguard the gains made. At Safaricom, we have developed SIM-Swap-Check and ATM Vicinity Check solutions that we have made available to banks to empower them to reduce fraudulent transactions. Peter Ndegwa, CEO – Safaricom The SIM-Swap-Check solution will assist banks in preventing fraudulent SIM swaps by providing them with a monthly quota of free checks. The solution also includes a premium tier for additional checks beyond the free quota. This solution was created after analyzing fraud reports and focusing on tackling social engineering that results in fraudulent SIM swaps. In addition to the SIM-Swap-Check solution, Safaricom is also providing banks with an ATM Vicinity Check solution at no cost. This solution ensures that an ATM withdrawal can only occur if the customer conducting the transaction is physically present at the same location as the ATM. Safaricom (NSE: SCOM) has announced that it has signed up 6 banks to its SIM-Swap-Check Anti-fraud solution. The solution provides banks with an API (Application Programming Interface) through which they can query when a customer’s SIM card was last swapped. The information then enables them to make a decision on the likelihood of a customer’s transaction being fraudulent and additional steps to be applied. “The rapid growth of Kenya’s fintech sector has been accompanied by a rapidly evolving threat environment targeting both customers and fintech operators. It is therefore necessary for different players to partner around innovations that protect customers and their funds to safeguard the gains made. At Safaricom, we have developed SIM-Swap-Check and ATM Vicinity Check solutions that we have made available to banks to empower them to reduce fraudulent transactions,” said Peter Ndegwa, CEO – Safaricom. The SIM-Swap-Check solution provides banks with a free monthly quota of checks and a premium tier above for additional checks above the free quota. Safaricom says the solution was developed following an analysis of fraud reports to tackle social engineering of customers to conduct fraudulent SIM swaps. In addition to the SIM Swap Solution, Safaricom is also providing banks with an ATM Vicinity Check solution that ensures an ATM withdrawal can only be conducted if the transacting customer is in the same location as the ATM. The ATM Vicinity Check solution is offered at no cost. Safaricom Introduces Voice Biometrics To Enhance Customer Experience Jitambulishe heralds a new smart era for customer care and will protect against identify theft Safaricom (NSE: SCOM) has introduced a dynamic voice biometrics system that will enable customers to access services through a quicker and less intrusive vetting process. Safaricom’s Voice Biometrics system known as Jitambulishe allows customers to use their voices for authentication before accessing assisted services such as resetting M-PESA PIN, and PUK requests, significantly cutting down the steps a customer goes through before they are assisted. The use of a unique voiceprint for enrolled customers will further reduce fraud and identity theft. To be functional, a pre-recorded registration process will be done. The encryption process will ensure no reverse engineering can be used to hack into the system and pose as another person. Voice recordings are not stored - which means Safaricom’s usual strict protection of customer data is upheld. “We are redesigning our customer care approach to remain in line with shifting trends in the market and to take advantage of emerging technologies. The introduction of Voice Biometrics will be a major step towards reducing fraud and identity theft, providing us with ways to serve our customers even better.” said Joseph Ogutu, Director – Strategy, Safaricom. To activate the service, the customer’s voice patterns are captured and used to create a unique “voiceprint” (similar in concept to a fingerprint), storing it as a secure string of numbers and characters. These attributes help identify and verify callers when they call for customer care. “Our contact centre agents spend a greater portion of their call time verifying customers over phone. The introduction of this service will ensure that customers get faster and more accurate services. We anticipate that the number of fraud incidents shall also reduce as a result,” said Mr. Ogutu. Operating the biggest customer care operation in Eastern Africa, Safaricom call centres receive over 300,000 calls a day. Over the last few years, the company has progressively invested in technology solutions that has improved the level of service provided to consumers. A few years ago, the company upgraded their technical infrastructure to be able to accommodate even more customers at their call centres. Now over 50% of customers are getting through to customer care agents within 20 seconds. Safaricom has leveraged on digital channels to provide round the clock service to their customers online. The company has also embarked on an aggressive capacity expansion plan to boost the number of call centre agents in order to enhance their ongoing customer care initiatives. In addition to customer care services, Safaricom will also offer its products and services through the Voice Biometrics system. The first service to be made available on this system is the recently launched M-PESA for the Visually Impaired solution. By dialling 100 or 234, visually impaired customers can identify themselves by their voices before having their M-PESA balances read out to them. Safaricom plans to gradually introduce more M-PESA services through the system. Jitambulishe heralds a new smart era for customer care and will protect against identify theft Safaricom (NSE: SCOM) has introduced a dynamic voice biometrics system that will enable customers to access services through a quicker and less intrusive vetting process. Safaricom’s Voice Biometrics system known as Jitambulishe allows customers to use their voices for authentication before accessing assisted services such as resetting M-PESA PIN, and PUK requests, significantly cutting down the steps a customer goes through before they are assisted. The use of a unique voiceprint for enrolled customers will further reduce fraud and identity theft. To be functional, a pre-recorded registration process will be done. The encryption process will ensure no reverse engineering can be used to hack into the system and pose as another person. Voice recordings are not stored - which means Safaricom’s usual strict protection of customer data is upheld. “We are redesigning our customer care approach to remain in line with shifting trends in the market and to take advantage of emerging technologies. The introduction of Voice Biometrics will be a major step towards reducing fraud and identity theft, providing us with ways to serve our customers even better.” said Joseph Ogutu, Director – Strategy, Safaricom. To activate the service, the customer’s voice patterns are captured and used to create a unique “voiceprint” (similar in concept to a fingerprint), storing it as a secure string of numbers and characters. These attributes help identify and verify callers when they call for customer care. “Our contact centre agents spend a greater portion of their call time verifying customers over phone. The introduction of this service will ensure that customers get faster and more accurate services. We anticipate that the number of fraud incidents shall also reduce as a result,” said Mr. Ogutu. Operating the biggest customer care operation in Eastern Africa, Safaricom call centres receive over 300,000 calls a day. Over the last few years, the company has progressively invested in technology solutions that has improved the level of service provided to consumers. A few years ago, the company upgraded their technical infrastructure to be able to accommodate even more customers at their call centres. Now over 50% of customers are getting through to customer care agents within 20 seconds. Safaricom has leveraged on digital channels to provide round the clock service to their customers online. The company has also embarked on an aggressive capacity expansion plan to boost the number of call centre agents in order to enhance their ongoing customer care initiatives. In addition to customer care services, Safaricom will also offer its products and services through the Voice Biometrics system. The first service to be made available on this system is the recently launched M-PESA for the Visually Impaired solution. By dialling 100 or 234, visually impaired customers can identify themselves by their voices before having their M-PESA balances read out to them. Safaricom plans to gradually introduce more M-PESA services through the system. Safaricom enhances measures to curb MPesa fraud Paul Kihara, a Nairobi resident was one evening driving home from work. He received a call from a strange number informing him that his son had been injured while playing rugby, and that he needed to send Sh6,500 for an ambulance to rush him to the hospital. Without hesitating, he quickly sent the money only to call his son later and find out that he was okay and was at a local mall with his friends. He had been conned. Bruce Odhiambo, a Roysambu resident, on the other hand, received a call from someone claiming to be a Safaricom Customer care staff. He was informed that his line had been double registered. To sort this, he was asked to provide some personal information. Luckily, he never gave his details, and instead, hang up on the the caller and quickly reached out to Safaricom customer care on the official number. He was told nothing of the sort had happened to his line. It is then that he realised he narrowly escaped being swindled. The two are just a a tiny fraction of people who have been conned or were fast enough to detect the con game before they fell prey. These are some of the tricks used by fraudsters to defraud unsuspecting customers, according to Safaricom's Head of Fraud, Patrick Kinoti. They target Mpesa and bank accounts. They trick customers into giving their details which they then use to transact. Alternatively, they lure the customer into making the transaction, including keying in codes that enable completion of the transaction.. “Unsuspecting customers would key in the code they are given, sometimes from a second line they have told you to buy. By the time they realise, they have transferred money or the fraudsters are able to transact from the other end,” Kinoti explains. According to Safaricom, there are at least 20,000 inbound requests going into its touchpoint a month. At least 10 per cent of these customers fall victims to scammers mainly loss of money. “Some customers have ended losing some substantial amount of money on the Mpesa channel or banks,” notes Kinoti. This common trick is known as 'identity theft' which is one of the many forms of cybercrime. Identity theft occurs when a fraudster impersonates you for their own gain using stolen information. According to global cybersecurity firm–Kaspersky, Kenya is among African countries facing a possible increase in cybercrime this year, amid economic uncertainty occasioned by the Covid-19 pandemic. Fraudsters contacting customers also use on-time campaigns such as promotions by companies, job vacancies, and government undertakings such as recruitments for disciplined forces. “It depends on the situation happening around but the most common is when someone calls a customer pretending they are calling from Safaricom. They can also use other big organisations,” Kinoti notes. Ideally what normally happens is they harvest information that is available in channels such as true caller, they check someone's name, when they call, they call the individual by name as a way of creating trust, says Kinoti. “That is the first entry for fraudsters, to create trust. From there, they start asking for further information. This information is used to swap your line. They tend to make you do transactions,” he explains. Measures To curb this trend, Safaricom has put in place several measures among them a strong social engineering channel that tracks suspicious calls to customers. It has tools that enable its team to check people calling other customers, pick the patterns, extract them and check the profile of the callers. Here, the fraudsters get blocked. For swim swap, Mpesa has tamed the trend where for one to register, they need to have their identity cards and personal identification number (PIN). The company then checks the location where the number is being registered. If the line is on, the swap is declined. “With these types of controls, we minimize fraud cases,” says Kinoti, who notes that in a month, the company gets around 150 cases of swap. It also has a back-end tool that checks mobile banking transactions, where working with the respective bank, it is able to stop fraudulent activities. Working closely with the DCI, the company has seen fraudsters arrested with about 250 cases currently in court, including individuals caught stealing from agents. To deal with cybercrime as a whole, Safaricom has put in place a team that works around the clock, monitoring its perimeter for potential attacks. Self-initiative To help customers avert fraudsters, the company which pioneered commercial mobile money transfer globally, through Mpesa, has been running a series of awareness campaigns on mainstream and social media. This is to ensure its more than 22.6 million active customers locally and over 167,000 Mpesa Agent outlets countrywide are safe. Mpesa is the largest payments platform on the African continent, with about 40 million users, processing over a billion transactions every month. It is operational in Kenya, Tanzania, Lesotho, Democratic Republic of Congo, Ghana, Mozambique and Egypt with continued expansion. “What we are trying to do is give the customers tools and information to protect themselves. We are telling them how fraud happens and every time they are targeted, how they need to respond and report to help us take action,” says Kinoti. He urges customers not to be in a hurry to give their personal details. “Stop. Think..before you act. This way, you can avoid up to 98 per cent of fraud cases,” he cautions.

**Safaricom sends home 33 employees as fraud war escalates**

Safaricom fired 33 employees in the year ended March 2023 for fraud-related offences, marking a 37.5 percent jump from the 24 dismissed the year before.

The revelation is contained in the telco’s annual report which notes that incidents and sophistication of fraudsters had grown.

The giant firm states that fraud attempts mainly affected SIM-swap services that were mitigated by proactive monitoring and digitising solutions.

SIM swap occurs when a criminal claims a false identity, pretends their card is lost and convinces a mobile operator to replace it.

That's how criminals gain access to one's contacts, banking details, emails and social accounts.

Safaricom says it has established a whistle-blowing policy that enables anonymous reporting of fraud on top of rolling out periodic customer awareness campaigns.

“Safaricom has a whistle-blowing policy that provides for an ethics hotline managed by an independent, accredited and external institution. Through the hotline, anonymous reports on unethical/fraudulent behaviour can be made without fear of retaliation from the suspected individuals,” reads the report.

Online spaces are awash with consumer complaints decrying theft of funds from their M-Pesa wallets either by way of transfer without authorisation or unsanctioned borrowing.

In March, Safaricom stepped up the war against fraud by rolling out an “ATM Vicinity Check” technology to ensure cash withdrawals can only be conducted if the customer is within the vicinity of the machine.

The solution, which the telco offered to commercial banks for free, was designed to arrest cases of banking fraud where criminals use victims’ cards and/or information to withdraw funds from ATM points.

Highlighting failure of a strategy