WHAT IS SIM SWAP?

SIM Swap occurs when a fraudster manipulates the customer service process to take over an open account within a MNO. The fraudster does this by requesting a SIM replacement or initiating a MSISDN porting order, enabling them to intercept SMS on a device that they own. The fraudster can then take advantage of using two-factor authentication to perform banking fraud, access mobile money accounts, and gain control of other third party OTT accounts.

DETECT SIM SWAP ATTACKS

1 **Monitor account changes on CRM system**
- Suspicious activity sequences and timelines
- Patterns of upgrade resetting
- Add-on activity
- SIM replacement activity

2 **Monitor customer complaints**
- Upgrades performed without customer authorisation
- Password/account change complaints
- Payments/charges complaints

3 **Monitor calls into customer service**
- Off network calls into customer service
- Calls into specific routes/teams
- Monitoring interactive voice response selections and pathways

4 **Send confirmation notifications to customer**
- After change of password; address; activation of additional service; product order
- As part of the mobile number porting (MNP) process (opt in)
- After request for SIM replacement / additional SIM

BEST DEFENCE MECHANISMS

- Equal level of customer validation for new and existing customers
- Create awareness of social engineering and account takeover risks and defences amongst customers
- Education and training of sales/dealer staff
- Geographical feasibility check to detect excessive distance between the SIM swap location and the location of the active SIM
- Implement firewalls (SS7, Diameter, SMS) on the network
- Consider implementing GSMA Mobile Connect in order to authenticate users
- Co-operate with banks and police to help prevent banking fraud
- Introduce strong controls on issuing of blank SIM cards
- Refer SIM replacements to a centralised team rather than handle at retail outlets, to ensure best practise is always followed
- Introduce validation processes and notifications on account changes / updates e.g. send confirmation SMS to the currently active SIM.

For more information, please see FF.21 Fraud Manual on InfoCentre², or contact us via gsma.com/security

Fraud and Security Team