EFRAUD USING E.164 NUMBERS AND USSD CODES

Anthony Ikemefuna

Assistant Director, Nigerian Communications Commission, Nigeria

AGENDA

- Introduction
- SIM Swap and Solution
- Phone Cloning and Solution
- USSD Codes Fraud and Solution
- Phishing & Smishing Fraud and Solution
- Conclusion

INTRODUCTION

What is SIM Swap fraud?

Step 1

Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means.

Step 2

They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof, posing as the customer.

Step 3

The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

Step 4

Fraudster then generates One Time Password (OTP) required to facilitate transactions, using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

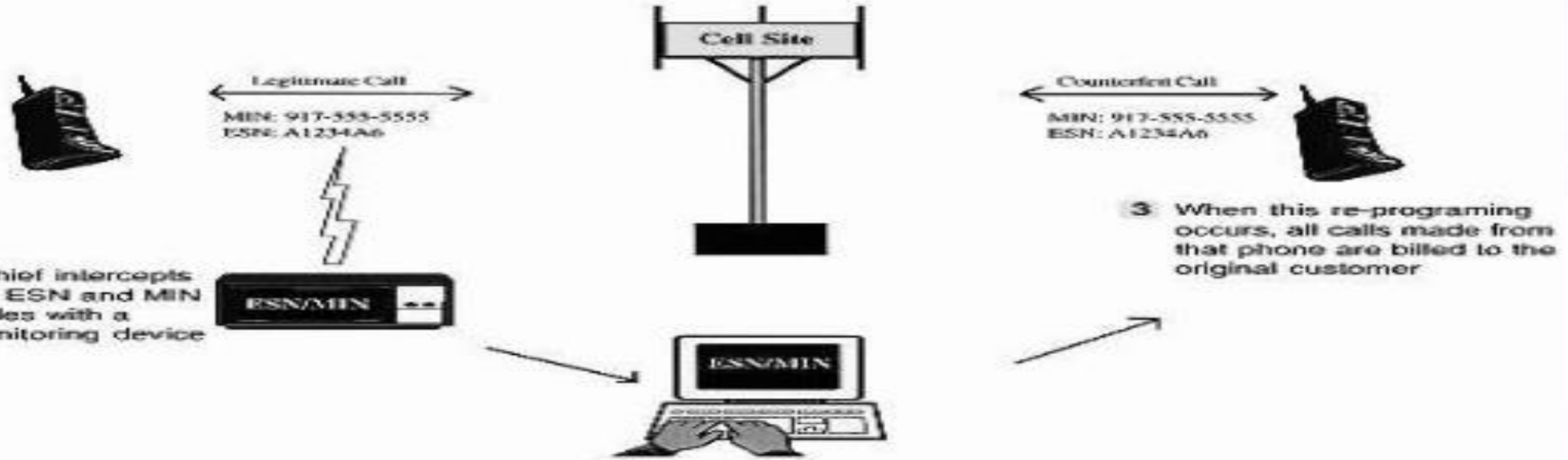
SIM Swap Solutions

- Largely depends on Social Engineering and perpetrated by syndicates
- The use of Biometrics as an additional validation mechanism for swaps
- Use of SIM Registration database or integrated national database for validation purposes
- Banks to take responsibility for reconfirming their customers details due to MSISDN recycling of non Revenue Generating Events (RGE) subscribers by MNOs.
- Increased focus by all to prevent internal abuse.
- Second level authorization, monitoring & control as additional control measure
- Use of alternate numbers and next of kin details may be introduced for validation where necessary.
- Increased awareness campaign by all stakeholders

CELLULAR COUNTERFEITING/CLONING FRAUD

Cellular Phone Counterfeiting

With each call made, a cellular phone transmits an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN) identifying the caller. Possession of these numbers is the key to the counterfeiting.



Characteristics of a Cloned Phone

- Sudden increase in the number of SMSs and calls
- Call from your carrier asking whether you travelled abroad
- Rise in calls from wrong numbers
- Issues with accessing voicemails
- Increased Phone bill

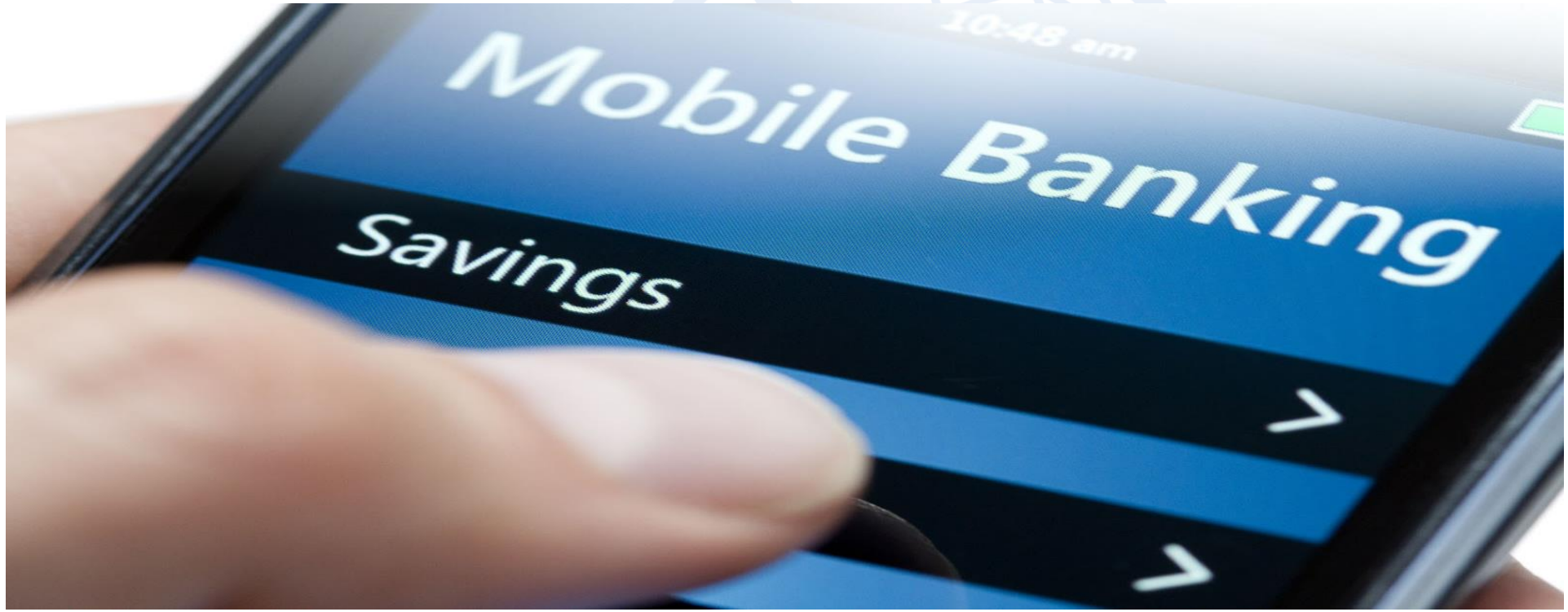
CLONING GSM PHONES

- The important information is the **IMSI**, which is stored on the removable SIM card.
- SIM card inserted into a reader.
- Connect to computer and card details transferred.
- Use encrypted software to interpret details.
- **The result**: A cloned cell phone is ready for misuse.

Preventive Measures against Cloning

- Always keep your device with you all the time
- Secure your phone with a biometric lock or PIN
- Switch off WIFI and Bluetooth when you are not using your phone
- Clear out cookies, catches and browsing history on a regular basis
- Keep your device protected with the help of security apps
- As a result of digital technology, it is no longer easy to clone a phone

Fraud Using USSD Codes



Use of stolen phones to carry out USSD financial transactions

Fraud Using USSD Codes

- End to end encryption of USSD messages (from the MNO to financial processing systems)
- Banks use Maker-Checker for every financial transactions, MNOs should adopt same.
- Use of PIN for every transaction by banks
- Stoppage of default subscription to USSD services in the banking sector.
- Creation of a repository of all SIM swaps carried out for use by banks to confirm transactions from such SIMs
- Provision of IMSI details as part of USSD messages sent to VAS providers to enable identification of recently swapped SIMs.

Phising, Smishing, Email and Voice Fraud

Sending spam email, SMS and voice calls aimed at getting banking details of a target

Preventive Measures

- Sensitization and awareness creation is necessary
- Customers should be encouraged to forward suspicious emails and SMSs to publicized customer care lines
- Increased compliance monitoring of Anti-Spam system implementation by MNOs
- Increased synergy of telcos and banks on post fraud cases.
- Increased synergy of the communication and banking regulator absolutely necessary.

Conclusion

- Urgent intervention is required to ensure the security and integrity of customer's information and funds
- An intervention involving all stakeholders is required for an all encompassing mitigation of the problem
- Increased focus by all stakeholders to limit incidences of collusion or insider abuse
- Efraud is a global concern


Thank You