Science World Journal Vol. 17(No 2) 2022
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

AWARENESS OF BVN, SIM SWAP AND CLONE FRAUDS: METHODS AND CONTROLS

*Ekeh G.E., Afolabi Y.I., Uche-Nwachi E.O., Ekeh L.K. and Eze-Udu E.

Department of Computer Science, Alex Ekwueme Federal University, Ndufu Alike-Ikwo, Ebonyi, Nigeria

*Corresponding Author Email Address: egodwinekeh@yahoo.com

ABSTRACT

Bank Verification Number (BVN), SIM swap and SIM clone fraud have become an issue of great concern in Nigeria. It has left banking and telecommunications offices trudging with complaints and many bank customers in pains. The Federal Government and the Central Bank of Nigeria (CBN) introduced the BVN to prevent corruption, provide a transparent system of payment and effective account monitoring, and to uniquely identify bank customers in order to eliminate any incidence of fraud. Even as banks unilaterally implement this measure, fraudsters are continually devising means of defrauding bank customers of their possessions and evade detection. In this paper, the authors created an awareness on how bank customers are deceived into disclosing their financial details, the methods used in obtaining data for SIM swap and SIM clone, and to sensitize the public on how to prevent unauthorized access to their treasured details.

Key words: Bank verification number fraud, SIM swap, SIM clone, Bank fraud

INTRODUCTION

Bank Verification Number (BVN) was introduced in Nigeria to prevent money laundering, give a unique identification to all bank customers and provide effective and transparent payment system in the banking industry. It also provides avenue to monitor all the transactions that occur in the banking system in order to limit the incidences of fraud. It was introduced by the Central Bank of Nigeria (CBN) as the new initiative to check the prevailing money laundering and incidence of fraud in the financial institutions in Nigeria (Ogunleye et al, 2017). Initially, password and PIN was introduced in the banking system but due to the high-rate of compromise on the conventional security systems, there is need to provide a greater security for access to sensitive data or personal information in the Banking system (Ogunleye et'al, 2017; Esoimeme, 2020; Ekeh, 2021). To address the issue of high rate of fraudulent activities going on in Nigeria, the Federal Government (FG) in collaboration with the CBN launched a biometric identification system known as Bank Verification Number (BVN) to resolve the issue of frauds and to boost financial security in the Banking industry (Akyuz et al, 2019). According to Access Bank (2020), BVN should address the issue of theft, give each customer a unique identity that can be identified and verified across the Nigerian Banking Industry and also help in reducing the level of fraud in Nigerian Banks. The primary aim of creating the unique identification number for bank customers is to stem the increasing case of identity fraud in the banking industry (Nigerianbanker, 2020).

With the above assertion, other benefits of BVN as stated by CBN (2020) was to:

a) Give unique identity to all bank customers that can be verified across the Nigerian Banking System.
b) Protect customers bank account from unauthorised access.
c) Enhance banking industry chances of being able to fish out blacklisted customers.
d) Address issues of theft, thus reduce exposure to fraud.
e) Authenticate transactions without the use of cards, using only biometric features in the near future.

Despite these benefits, the launching of the BVN in February 2014 and the drafting of its operational framework in October 18, 2017 shows that the BVN has been in operation for three years before the CBN and banks were able to design and issue the formal guideline (Editorial, 2018; Oloni, 2020). If the CBN had first issued the framework, and explained it with proper publicity, most of the attendant challenges experienced in the course of its implementation would have been corrected (Editorial, 2018). Rather, it has unnerved more challenges in the management and storage of data. BVN is a unique identity to all customers across the banking industry, so there is need to properly secure the customers data by strengthening and securing the BVN.

The BVN system, though beneficial to the CBN for easy monitoring of accounts and the banking industry, has introduced a security threat to bank customers. Nigerianbanker (2020) posits that bank customers should worry about how fraudsters can use their personal information obtained as a result of exposure of their BVN to trick them into volunteering sensitive information like their Bank Card details, ATM Pin, USSD, Mobile and Online Banking Passwords. Once bank customers protect this information, the funds in their bank account will be safe. But fraudsters in conjunction with some of the greedy bank officials can commit BVN fraud by using your BVN to see and obtain all your Bio-Data and use it to trick you into disclosing those sensitive details (Nigerianbanker, 2020).

Subscriber Identification Module (SIM) is a smart chip-based card that is inserted in a mobile phone which identifies a particular network, stores data and provides services to the subscriber of that network. SIM cards are the connecting platform between the mobile phones and the network; stores information about the user's activities, such as phone book, incoming and outgoing calls, sent and received messages, etc. (Tirumala et al, 2019). SIM cards, to some countries are fixed to a particular mobile network but in Nigeria, you can remove the card and place it in a new phone or replace the card when damaged or lost without any problem. Whenever your SIM card is lost, damaged or you upgraded your phone, there is a function your mobile carrier performs to replace the SIM. This function is known as SIM Swapping and is a useful function that allows you to transfer your mobile account from one

SIM card to another; this also doubles as a security risk when fraudsters/cybercriminals decide to use it to their advantage – which is known as SIM swap fraud (Casey, 2019).

SIM swap involves changing your old, damaged or lost SIM card to new one and which is carried out by your telecommunication operator at your request. But if a fraudster manages to carry such a swap, numerous fraudulent transactions will be meted to the victim using the mobile number (Olaleye and Fashina, 2019). Snehal and Praveen (2019) asserts that SIM swap is technically new form of cyber fraud where hackers gain the personal information and does illegal work with persons bank account or credit card numbers. This means that hackers/ fraudsters can steal your personal information to deceive your telecommunication operator about your identity, perform SIM swap and carry out fraudulent activities with the stolen details. In some cases, there are mobile carrier's employees working together with criminals to commit this fraud (Vanguard, 2019).

The following researchers, Snehal and Praveen (2019), Fabio and André (2019), Casey (2019), and Adam (2020), stated that SIM swap fraud can be carried out in the following ways:

a) The fraudsters gather the victim's personal information such as name, phone number, address, passwords, security question (such as mother's maiden name), through phishing, social media, social engineering, hacking old email addresses you no longer use, buying information from organized crime groups like dark web or any other means.
b) They approach the victim's mobile operator with their identity proof for verification to get the SIM blocked. The attacker uses the information gathered to trick the mobile provider employee to believing they're you and to port your phone number to their SIM. Most times the fraudsters work together with the mobile operator's employee.
c) The SIM will be deactivated by the Mobile operator and new one issued to the fraudster.
d) Then the victim's mobile phone loses its connection to the network while the fraudster intercepts the One-Time-Password (OTP) for further transaction information. All the phone calls and SMSs meant for the victim can then be used by the fraudster.
e) The fraudster will then use the victims' mobile number as a form of two-factor authentication (2FA) to reset passwords and access their online accounts.
f) Moreover, there are situations that mobile operator employees are too careless in their security requirements or they connive or being bribed by the fraudsters to fraudulently swap the SIM card.

SIM cloning on the other hand is a little bit technical than SIM swapping. SIM cloning involves using a smart card copying software to duplicate SIM card, thereby enabling access to the victim's secret codes known as International Mobile Subscriber Identity (IMSI) and master encryption key (Ki) (David and Limor, 2019). Mustafa and Nidal (2014) described it as the process of copying the content of a genuine SIM card and programming it to another mobile phone SIM card, that does not belong to the genuine user. That means for the hacker/fraudster to clone the content of any genuine SIM card requires the knowledge of the secret codes (IMSI, Ki) the operator uses to identify and authenticate SIM cards.

The process of cloning SIM cards as posited by Mustafa and Nidal (2014), Nuril et al (2016), Evelyn (2018), David and Limor (2019), Tirumala et al (2019), Elizabeth (2020a), and MD Wasil (2020) are:

a) The fraudsters uses the equipment such as a blank SIM card with no programming, SIM firmware device that can read or write data on the blank SIM card, card cracker, and USB CardReader software to clone a SIM card.
b) The next thing is to place the new blank SIM card in the smart card copying software to copy the original SIM card into the new blank card by enabling the victim's secret keys (IMSI and Ki). The major aim of cloning is to get the IMSI and Ki codes, which is the identifier of the SIM card and it's used by your operator to register your mobile to the network. So the fraudster uses the secret keys to convince your network operator into thinking that the SIM card is original and the contents transferred.
c) After the SIM cloning or duplication is done, the fraudster then inserts the SIM into a device they control.
    a. Either an OTP will be sent to the victim's phone from the operator or the fraudster calls/sent a harmless text message to the victim requesting them to restart their phone. In either case, the main reason is to get the victim restart their phone. Once that is done, account takeover completes and the SIM is successfully cloned.
d) If the victim's phone number is linked to their bank account, the fraudster can easily have access to the account.

The aim of swapping or cloning a SIM card by fraudsters is to make the victim's mobile phone susceptible to attack. Once this is done, the victim will no longer receive text messages or make voice calls on their mobile phone. The text messages and voice calls will be routed to the fraudster's device. Then the fraudster will have free and unhindered access to the targets bank account.

The purpose of this paper is to create awareness on how fraudsters obtain and uses BVN, SIM swap and SIM clone to defraud their victims, and the modalities bank customers can employ to safe-guard and control their sensitive information and finances. This paper engages a review on electronic bank fraud and the common types of electronic fraud in Nigeria. It reveals different methods fraudsters use to obtain sensitive information from their targets and finally proposes measures to control the chances of being attacked by fraudsters.

Electronic Bank Fraud

The introduction of electronic banking has simplified the banking system and brought a lot of benefits to the industry, but with great security threat to the banks as well as their customers. Ibanichka and Oko (2019) defined electronic fraud as a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank which is made possible through phishing, lottery fraud, etc. With the growth of electronic payment platforms, fraudsters have devised several means of fleecing innocent victims of their money through phishing and spooling, cloning/swapping, identity theft, pharming, card trapping, skimming, malware attack, etc. (Olaleye and Fashina, 2019); and with the sudden rise in adoption and usage of payment system in Nigeria, there has been a rise in the incidence of fraud in the payments landscape (Ibanichka and Oko, 2019), and customers are losing their trust and confidence in the banking system due to incessant frauds (Adegboyega and Tomola, 2018).

According to Oludayo (2020), a cashless policy was made in Nigeria six years ago (BVN project), which aims to encourage electronic transactions by reducing the physical cash in the economy, but the downside of the policy is a pervasive electronic banking fraud. The Nigeria Inter-Bank Settlement System (2020) noted that the BVN project was designed to allow individuals performing banking transactions to identify themselves using biometric features which will match their information in the central database. The purpose is to protect the banks' customer accounts from being accessed by an unauthorized person (CBN, 2020). But the BVN project poses a threat to the potential success of the National Financial Inclusion Strategy (Esoimeme, 2020). Oludayo (2020) posited that about N15.5 billion was lost to bank fraud in 2018 of which 60% of the fraud was perpetrated online owing to available internet-based and tech-rated banking services. Between 2017 and 2018, a total of 63,895 bank customers lost N3.6bn to fraud, and the mobile channel contributed the highest recording 11,492 in volume and N598.8m in actual loss value (Nike, 2019). EFInA (2019) asserts that the industry has noted the alarming rate of fraud perpetuated using mobile channels in the country. Adaora et al (2018) pointed out that fraud in the banking industry shakes the foundation and credibility of most deposit money banks in Nigeria resulting to some of the bank being distressed; while customers and stakeholders of the bank worried about the safety of their money and information and are expecting the bank to find a solution that can protect them and the economy as a whole (Ibanichuka and Oko, 2019). The frauds committed in the bank are of three dimensions: internal fraud by bank staff, external fraud by outsiders, and the collaboration between fraudsters and bank staff (Oludayo, 2020).

Common types of Electronic Fraud in Nigeria

EFInA (2019), Olaleye and Fashina (2019) described some of these electronic frauds as:

a) SIM Swap: involves deceiving the network operators to port an old SIM card to new one.
b) Phishing: to fraudulently obtain sensitive information from people like their passwords, PINs, BVN and card details over the phone.
c) Debit card skimming: fraudsters uses a device to obtain personal information when bank customers use their cards.
d) Site cloning: fraudsters clone legitimate sites to steal information from unsuspecting customers.
e) Lost/Stolen card: this involves using a legitimate card lost by the account holder for illegal purposes.
f) Online fraud: involves stealing card details during online transaction to fraudulently purchase items.
g) Unauthorised emails/Text messages: fraudulently requesting customers account details for updating bank records. This information is then misused for misappropriating funds.
h) ATM Fraud: fraudulently acquiring a customer's PIN and card details to withdraw money from them through the machine.
i) Network Downtime: this creates opportunity to defraud when network service delivery is delayed.
j) Data & Identity Theft: unprotected financial data that is not adequately secured and access protected, can be hacked.
k) Malware: introduced to steal data, passwords, PINs, or infect a customer's phone with a virus and sometimes intercept funds transfer.

METHODS OF OBTAINING DATA FOR FRAUD

There are different tricks fraudsters use to obtain sensitive information from their target in order to defraud them. Some of the methods are:

a) If a SIM card used to receive alert by a bank customer is obtained by the fraudsters, the SIM can be worked on to carryout transactions such as withdrawal, air-time recharge and loans (Adeyemi et al, 2019; Janet, 2021). Adeyemi et al posited that the fraudsters will first dial a code *xxx*xxx# to know which bank the owner operates. And to determine the account balance, they'll use the USSD (Unstructured Supplementary Service Data) code. To have access to the account, they will reset the PIN. This will prompt for the account number and date of birth. Account number can be obtained either in the phone's contacts, messages or a bank staff. Other details can be obtained using the BVN code *xxx*x#. The fraudsters will then register with the bank of their target and carry out transactions. If there's no sufficient money in the account, they can obtain loan. Before transactions are made, they will open a "no-trace" account and transfer the money to the account (Dan, 2022). The "no-trace" account is created using someone's BVN. The transfer can equally be used to purchase items online or transfer to somebody's account, convince the person to help them withdraw the money using either ATM or POS.
b) Likewise, CBN warned that fraudsters can send e-mails, text messages or call their victims pretending to be from their banks to update their BVN (Ibrahim, 2015). When the victim responds to the call or click on a link to fill a form, they risk giving out their BVN details and other private information.

c) Because of the rise in online loans through the financial technology companies and digital platforms, fraudsters can apply for loans using a stolen SIM card linked to a particular account (Elizabeth, 2020b). Since the process of obtaining the loan requires the account holder to submit BVN in case of borrower defaults, the fraudster submits the obtained BVN and the BVN will be blacklisted.
d) Based on X-Force IRIS dark web research, fraudsters or hackers often sale information obtained from the rich members of the society or requests for SIM cloning services to a targeted bank account (David, 2019; Odita, 2020). Similarly, since the process of swapping a SIM card by the telecommunication can be easily done,

fraudsters can swap the victims SIM card and starts using the USSD to make transfers in another account or buy recharge cards (Gbenga, 2017).

e) Elizabeth (2020b), Shane (2020), Jason (2021) and Dan (2022) posited that another method employed by the fraudsters is to repeatedly call bank customers to resend the code mistakenly sent to their phones. Sometimes they claim to be registering something online and the code was meant to send to them, asking you to resend it back. For example, you can receive a message *"Dear Customer, your verification code is: xxxxxxxx enter it on the screen to complete your registration on the bank mobile, call xx-xxxxxxx for help"*. After this, a voice call will come claiming to be staff of the bank and want to protect you from fraudsters (Jason, 2021). Once the customer yielded to their call, the account will be emptied. The code requested by the fraudsters will be used to clone your SIM card (Dan, 2022). Once the SIM is cloned and the number happened to be registered to your account, they'll have access to your account.

f) Adeyemi et al (2019), Adrian (2022) and Dan (2022) also stated that bank customers can lose network signals from their phones which might persist after rebooting the mobile phone. A visit to restore the signal at the operator's office might found out that someone has requested a new SIM with their number and made away with their money. Also, your phone may suddenly go blank with no network signal on it. A call might come in claiming to be from your mobile network and requests that you press 1 to restore your signal (Adeyemi et al, 2019; Adrian, 2022). Once you press 1, the signal immediately appears and suddenly go blank again with zero bars. By this, your SIM will be swapped or hacked. Within minutes, your account will be emptied and you will not receive any alert.

g) Displaying Sensitive Information on Social Media - Fraudsters may use your social media posts and profiles to collect information about you which will help them to impersonate you while cloning or swapping your SIM (Dan, 2022). Fraudsters can use information such as your mother's maiden name, children or relatives' details, date of birth or your symbols to answer security questions.

Controls

The advancement in technology has helped to quicken both the banking process and the telecommunication industry and has also introduced new security challenges. The more organisations improve their security and systems with innovative technologies, the more fraudsters improve the use of these innovations to their advantage. BVN was created to improve security and curb corruption but has brought a lot of challenges. Possessing a BVN does not pose a risk, but exposing it on social media and other non-approved financial technology companies can increase the risk of exposing financial details. Once the financial details are exposed to the wrong hands, SIM card may be swapped or cloned in order to access your bank account or sensitive data.

The following are measures to control the chances of being attacked by fraudsters:

a) Disable USSD and Block your Bank Account - Omodele (2021) noted that the first thing to do if you've lost your phone or wallet is to disable the USSD if you had activated it and block your bank account and phone number. Whenever you receive a message from a bank that your account opening is successful, make sure you go to the bank to close the account if you're not the one that initiated the account opening. If you fail to close the account, a "no-trace" account will be opened using your BVN details and phone number (Adeyemi, 2019; Jason, 2021). According to Access Bank (2022), do not disclose any number on your ATM card or the PIN to anybody, even to the bank staff. Once you've done with any transaction using the POS, examine your ATM card to make sure it's the right one (Access Bank, 2022) and do not allow the agent to write your ATM card numbers down.

b) Protect your BVN – presently your BVN is the key to your financial information and disclosing it to anybody through phone calls, SMS/email or non-approved financial technology companies can expose you to fraud (Ayodele, 2016; Access Bank, 2022). When in doubt, call your account officer or visit your bank to clarify the need for your information. Do not disclose vital information to anybody through email, phone, SMS, or in person. This is why banks and other financial technology companies introduce two-step verifications to further verify the authenticity of their customers in case fraudsters access it through different channels (Okonji, 2022).

c) Lock your SIM cards – this prevents the fraudster from hacking into your account details through your phones (MTN, 2022). Most people prefer to lock their phones than their SIM cards and when the phone is lost, the SIM card is exposed to fraud. Make sure you block your SIM card and account number as soon as your phone is lost. These processes can be done online. Also, make sure you enable two-factor authentication on every account (even on social media) it offers and do not fall for scam messages or robocalls (Jason, 2021).

d) Do not download or use third party keyboard apps in your mobile phones – some of these keyboards were created by hackers to access or store sensitive information you type (Tyler, 2019; Hindustan, 2021). Do not copy and paste sensitive data such as passwords, bank details, debit/credit card details, tracking number of an order in your keyboard because such information can be accessed using a third-party app (Rochel, 2020).

e) Once you find out that you've lost service on your mobile device that it is not network issue, let your mobile carrier know immediately; and if you didn't initiate any transaction on your account, call your account manager or visit your bank to explain the situation (Jason, 2021). Avoid long calls with the caller requesting your personal or bank details, this can give the fraudster vital information to defraud you. Your bank will never call you for such information or ask you to resend any message forwarded to you (Access Bank, 2022). Also, delete any message requesting your bank details or any OTP you did not request for (Disha, 2019). Do not click any link sent through text messages or social media accounts requesting to add you in a group chat, buying and selling of cryptocurrency, or any wealth investment platforms that you are not sure of (UMASS, 2022). Also, do not download attachments in your email or mobile apps you do not know the sender.

f) Avoid public Wi-Fi for financial transactions - the use of sensitive data on public internet access should be avoided because fraudsters can gain access to your system and use your data for their personal gain (Nissy et al, 2016; Alkhalil, 2021). Do not store passwords or card details in your phone – this makes it easy for the criminals as they will take over your accounts within seconds. Devise other means of remembering your sensitive information instead of being an easy prey to criminals.

g) Shane (2020) warned that oversharing of important and personal details on social media is bad. Avoid exposing your family details such as your children, relatives, birthdate, mother's maiden name, school name, etc., as they may be accessed using phishing email to convince your bank, mobile carrier or other service providers that they are you and answer secret questions in order to defraud you (Shane, 2020; Dan, 2022).

Conclusion

Fraud in the financial sector has risen to a critical point that made the Federal Government and CBN to introduce the BVN. BVN has become an important system to curb corruption in the financial sector, but also has brought a lot of challenges in terms of data storage and management. One of the challenges experienced in the financial sector is the use of customers' financial details to defraud them. This happens when the fraudster poses as a legitimate bank official to obtain financial data from the customer and subsequently clone the customer's SIM/credit card.

The researchers recommend that:

a) CBN and the banks should adequately protect the customers BVN data and subsequently trace and prosecute whoever found wanting.
b) Banks should adopt a unified method of communicating to their customers to avoid being confused by fraudsters or bank officials' calls.
c) Bank officials need to educate their customers always, and the need to report any call made by the fraudsters seeking for their financial details. This report need not end at banker's desk, but to further alert the security agencies.
d) The reported phone numbers and other details need to be followed up by the security agents and telecommunication companies in order to blacklist the numbers and trace the fraudsters.
e) There should be a synergy between the banks and the telecommunication sectors on the need to trace and block the accounts of identified fraudsters, prevent SIM swap fraud by strengthening two-factor authentications on every account.
f) People should limit their personal or sensitive information they share online. Oversharing of such information could lead to the exposure of security details or questions used to verify their identity.

REFERENCES

Access Bank Plc. (2020). Bank Verification Number. Available at https://accessbankplc.com/pages/Customer-Support/Bank-Verification-Number.aspx.

Access (2022). Fraud Prevention Tips. Available at https://www.accessbankplc.com/Contact-Us/My-Access.aspx

Adam Bannister. (2020). SIM Swap Fraud – An Explainer. Available at https://portswigger.net/daily-swig/sim-swap-fraud-an-explainer.

Adaora Immaculata Muoghalu, Jisike Jude Okonkwo, Amalachukwu Chijindu Ananwude. (2018). Effect of electronic banking related fraud on deposit money banks financial performance in Nigeria. Discovery, 54(276), 496-503.

Adegboyega J. Elumaro and Tomola M. ObamuYI. (2018). Card Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria. European Scientific Journal 14(16) http://dx.doi.org/10.19044/esj.2018.v14n16p40

Adeyemi Adepetun, Kehinde Olatunji and Oluwatosin Areo. (2019). Nigerians count losses as SIM swap fraudsters empty bank accounts. Available at https://guardian.ng/technology/nigerians-count-losses- as-sim-swap-fraudsters-empty-bank-accounts/feed/.

Adrian Wong (2022). Can SIM Swap Attack Empty Bank Accounts Without Warning? Available at https://www.techarp.com/internet/sim-swap-bank-warning/.

Akyuz Murat, Tony L. Wuyep, Opusunju Michael Isaac. (2019). Impact of Bank Verification Number (Bvn) on Corrupt Business Practices in United Bank for Africa In Abuja. International Journal of Management Studies and Social Science Research 1(1).

Alkhalil Z., Hewage C., Nawaf L. and Khan I. (2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Front. Comput. Sci. 3:563060. doi: 10.3389/fcomp.2021.563060.

Ayodele Oluwagbemi (2016). Keeping your Bank Verification Number safe. Available at https://punchng.com/keeping-your-bank-verification-number-safe/. Casey Crane. (2019). SIM Swap Fraud: The Latest Battle in the War For Your Identity. Available at https://cybersecurityventures.com/sim-swap-fraud-the-latest-battle-in-the-war-for-your-identity/. Central Bank of Nigeria.(2020). Payment System. Available at https://cbn.gov.ng/Paymentsystem/BVN.asp

David Bales. (2019). Clone or Swap? SIM Card Vulnerabilities to Reckon With. Available at https://securityintelligence.com/posts/clone-or-swap-sim-card-vulnerabilities-to-reckon-with/.

Dan Rafter (2022). What is SIM swapping? SIM swap fraud explained and how to help protect yourself. Available at https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html.

Disha Sanghvi (2019).How to protect yourself from OTP theft. Available at https://www.livemint.com/money/personal-finance/how-to-protect-yourself-from-otp-theft-1549307894204.html. Editorial board. (2018). CBN, BVN and fraud. Available at https://m.guardian.ng/opinion/cbn-bvn-and-fraud/.

EFInA. (2019). Overview of Mobile Financial Services Fraud in Nigeria:
Building Trust to increase Uptake and Usage. A Presentation at the Mobile Payments Fraud Forum. Available at https://www.efina.org.ng/Overview-of-Mobile-Financial-Services-Fraud-in-Nigeria.pdf.

Ekeh G.E., Okemiri H.A., Uche-Nwachi E.O. and Ekeh L.K. (2021). Science-Systems as a
Catalyst to Sustainable National Security in Nigeria. Science World Journal Vol. 16(No 4).

Elizabeth Adegbesan.(2020a). SIM card cloning fraud now in vogue, bank customers warned. Available at https://www.vanguardngr.com/2020/08/sim-card-cloning-fraud-now-in-vogue-bank-customers-warned/
Elizabeth Adegbesan. (2020b). Police, banks helpless, as online loan fraud emerges. Available at. https://www.vanguardngr.com/2020/03/Police-banks-helpless-as-online-loan-fraud-emerges/.

Esoimeme Ehi.(2020). Updated: A Critical Analysis of The Bank Verification Number Project Introduced By The Central Bank Of Nigeria.
http://dx.doi.org/10.2139/ssrn.2544934.

Evelyn Bankole. (2018). How to clone a SIM card.
Available at https://www.legit.ng/1164618-how-clone-a-sim-card.html?

Fabio Assolini and André Tenreiro.(2019). Large-scale SIM swap fraud: The enemy in your pocket. Available at https://securelist.com/large-scale-sim-swap-fraud/90353.

Gbenga Agoye. (2020). NCC says you now need 'bank approval' to complete sim swap. Available at https://nairametrics.com/2017/08/07/ncc-says-you-now-need-bank-approval-to-complete- sim-swap/.

Hindustan (2021). Third party keyboard apps are not safe, can hack into your data. Available at https://hindustannewshub.com/tech-news/third-party-keyboard-apps-are-not-safe-can-hack-into-your-data/.

Ibanichuka E.A.L and Oko I. A., (2019). Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria.
International Journal of Advanced Academic Research | Management Practice 5(4).

Ibrahim Mu'azu (2015). BVN: Bank Customers Beware. Available at
https://www.cbn.gov.ng/out/2015/ccd/cbn%20press%20statement%20on%20bvn.pdf

Janet John (2021). How scammers use SIM card, phone numbers to rob your bank accounts. Available at https://nairametrics.com/2021/02/27/how-scammers-use-sim-cards-to-rob-your-bank-accounts/.

Jason Cipriani (2021). T-Mobile data breach and SIM-swap scam: How to protect your identity. Available at https://www.cnet.com/tech/mobile/t- mobile-data-breach-and-sim-swap-scam-how-to-protect-your-identity/

MD Wasil Ansari.(2020). How To Clone SIM Card.
Available at https://www.tech2hack.com/how-to-clone-sim-card-easily.
MTN (2022). How to Activate SIM Card Lock to Prevent SIM Fraud. Available at
https://www.mtn.ng/just-for-you/how-to-activate-sim-card-lock-to-prevent-sim-fraud/

Mustafa A. Al-Fayoumi and Nidal F. Shilbayeh.(2014). Cloning SIM Cards Usability Reduction in Mobile Networks. J Netw Syst Manage 22(259–279)
http://dx.doi/10.1007/s10922-013-9299-8

Nigerian banker. (2020). How BVN can be used to steal money from your bank accounts. Available at https://www.nigerianbanker.com/how-bvn-can-be-used-to-steal-money-from-your-bank-accounts/.

Nigeria Inter-Bank Settlement System.(2020). Bank Verification Number. Available at . https://nibss.com.ng/bvn.

Nike Popoola. (2019). Bank customers lose N3.6bn to cyberfraud. Available at "https://punchng.com/bank-customers-lose-n3-6bn-to- cyberfraud/.

Nissy Sombatruang, Angela Sasse, Michelle Catherine Baddeley (2016). Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions. http://dx.doi.org/10.1145/3046055.3046058

Nuril Anwar, Imam Riadi, Ahmad Luthfi.(2016). Forensic SIM Card Cloning Using Authentication Algorithm. Int. J. of Electronics and Information Engineering 4(2)71-81. DOI: 10.6633/IJEIE.201606.

Odita Sunday.(2020). How we clone SIM cards to transfer money from bank accounts of deceased VIPs, syndicate confesses.
Available at https://guardian.ng/news/how-we-clone-sim-cards-to-transfer-money-from-bank-accounts-of-deceased-vips-syndicate-confesses/.

Ogunleye Gabriel Opeyemi, Fashoto Stephen Gbenga, Andile Metfula and Ogunde Adewale Opeoluwa., (2017). Development of an Online Bank Verification Number System Using Linear Congruential Algorithm". Inform. Technol.J. 16(62-70). DOI: 10.3923/itj.2017.62.70.

Okonji Emma (2022). Adopting Innovative Security Solutions in a Vulnerable, Digital World. Available at
https://www.thisdaylive.com/index.php/2022/04/14/adopting-innovative-security-solutions-in-a-vulnerable-digital-world/.

Olaleye John Olatunde, Fashina, Abiodun Fasunle., (2019). Electronic Banking Fraud In Nigeria: Effects And Controls. GSJ: 7(8).

Oloni Victoria. (2020). Critical Data Security Issues In The Nigerian Banking Sector. African Academic Network on Internet Policy. Available at https://aanoip.org/critical-data-security-issues-in-the-nigerian-banking-sector/feed/

Oludayo Tade. (2020). Electronic banking fraud in Nigeria: how it's done, and what can be done to stop it. Available at https://theconversation.com/electronic-banking-fraud-in-nigeria-how-its-done-and-what-can-be-done-to-stop-it-141141.

Omodele Adigun (2021). How to block your bank account if your phone is stolen. Available at https://www.sunnewsonline.com/how-to-block-your-bank-account-if- your-phone-is-stolen/.

Rochel Maday., (2020). Recently revealed – are Apps Secretly Reading your Clipboard. Available at https://www.avira.com/en/blog/recently-revealed-are-apps-secretly-reading-your-clipboard.

Shane Hickey (2020). SIM-swap fraud on the rise. How can you stop it happening to you? Available at https://www.theguardian.com/money/2020/sep/13/sim-swap-is-on-the-rise-how-can-you-stop-it-happening-to-you.

Snehal Manohar Awale, Praveen Gupta., (2019). Awareness of Sim Swap Attack. International Journal of Trend in Scientific Research and Development, 3(4)995-997.

Tirumala Krishna Mohan G, Vipin Pavithran, Suthendran Kannan.(2019). Survey analysis of cloned SIM card. An International Conference on Recent Trends in Computing, Communication and Networking Technologies (ICRTCCNT'19)", Kings Engineering College,October 18-19, Chennai, Tamilnadu, India.

Tyler Giallanza, Travis Siems, Elena Smith, Erik Gabrielsen, Ian Johnson, Mitchell A.
Thornton, Eric C. Larson (2019). Keyboard Snooping from Mobile Phone Arrays with Mixed Convolutional and Recurrent Neural Networks. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 3 (2): 1 DOI: 10.1145/3328916.

UMASS (2022). Phishing: Fraudulent Emails, Text Messages, Phone Calls & Social Media. Available at https://www.umass.edu/it/security/phishing-fraudulent-emails-text-messages-phone-calls.
Vanguard. (2019). SIM swap fraud: A new wave of attacks targeting Africa's financial. Available at "https://www.vanguardngr.com/2019/05/sim-swap-fraud-a-new-wave-of-attacks-targeting-africas-financial-online-services/