Northern Ireland
Legal Quarterly
Vol. 75 No. 2 (2024) 187–214
Articles DOI: 10.53386/nilq.v75i2.1163

A legal approach to the protection of customers of banks and other financial institutions from identity theft in Nigeria†

Kehinde Anifalaje
University of Ibadan, Nigeria
Correspondence email: kennyanif@gmail.com

ABSTRACT

Although identity theft is not a new phenomenon in the banking industry, the internet, the use of databases in storing customers' personal information as well as the ubiquitous nature of online transactions have heightened the issues of security and privacy concerns of bank customers. Of significant note is the increase in the risk of customers' exposure to identity theft and the opening of the floodgates for unscrupulous and criminally minded persons to harvest customers' personal information for fraudulent purposes with its attendant financial loss and reputational damages. This article examines identity theft within the banking and financial sector and the adequacy of the regulatory measures that have been deployed to combat it in Nigeria and the United Kingdom. It is contended that, despite the available legislation on identity theft in Nigeria with copious provisions to prosecute identity theft and the constitutional guarantee given to the privacy of citizens, the right to privacy of the citizens is still being constantly violated by identity thieves through unauthorised access to and damaging use of personal and financial data of unsuspecting victims. The article concludes that though, like any other crime, identity theft cannot be completely eradicated, it requires the concerted efforts of all relevant stakeholders to reduce its incidence to the barest minimum within Nigerian society.

Keywords: identity theft; personal information; internet banking; data protection; regulation; banks and financial institutions; Nigeria; United Kingdom.

† First published in NILQ 75.AD1 1–28 on 21 March 2024.

INTRODUCTION

The relationship between a banker and the customer is primarily contractual with corresponding rights and duties.[1] At common law, one of the duties owed by the banker to the customer is the duty of care and secrecy.[2] It implies the duty to exercise reasonable care and skill in executing a customer's instruction in its banking business.[3] A banker also has the implied duty to the customer not to pay out the customer's money without authority.[4] On the other hand, the customer undertakes to, *inter alia*, exercise reasonable care in executing written orders so as not to mislead the bank or facilitate forgery.[5] Whilst these duties are still sacrosanct and applicable to the legal relation between the banker and the customer, the advent of information communication technology and its deployment in payment service delivery in the banking business has greatly revolutionised and impacted the operations of banking business across nations, including Nigeria.[6] The process of paying out money from accounts is no longer limited to *inter praesentes* transactions between the banker and the customer, but has been extended to online withdrawals through the use of debit cards and online payments. The cashless policy of the Central Bank of Nigeria (CBN), which is the apex regulatory body for banks and other financial institutions in Nigeria, to facilitate quick access to customers' funds and decongest the banks in respect of minor transactions, has also engendered greater use of technology in the banking service.[7] Nevertheless, the digitalisation of bank operations, the ease with which banking and other financial transactions are

1 *Joackimson v Swiss Bank Corporation* (1921) All ER Rep 92, 100, Lord Atkin. The rationale for the duty of care on a banker is that a banker's customer falls within the ambit of the banker's neighbour, that is, a person who is so closely and directly affected by the act of the banker that the banker ought reasonably to have the customer in contemplation as being likely to be affected when the banker is considering the acts or omissions which are called in question: *Agi v Access Bank plc* (2014) 9 NWLR (Pt 1411) 121. In a breach of the duty by the banker, such as where a victim's identity theft losses have been facilitated by the negligence of the banker, the banker is liable in damages to the customer.

2 *Habib Nigeria Bank Ltd v Fathudeen Syed M Koya* (1990–1993) NBLR 368, 387.

3 *Nigerian Advertising Service Ltd v United Bank for Africa Ltd* (1965) LLR 84.

4 *Slingsby v District Bank Ltd* (1931) 2 KB 588.

5 *London Joint Stock Bank Ltd v Macmillan & Arthur* (1919) A C 777.

6 *Mudiaga-Odje v Younes Power System Nig Ltd* (2014) 5 NWLR (Pt 1400) 412, 433–434, Buje, JCA.

7 In the third quarter of 2020, for example, the value of online payments in the Nigerian banking and financial sector increased to USD116 billion from USD68.3 billion recorded for the same period in 2019: A Onukwe, 'Nigeria's central bank is tightening control of its identity database to check fraud better' (Quartz 14 October 2021).

carried out through the internet, and the rate at which personal information of customers, including biometric information, is stored in databases to enhance operations are not without their attendant challenges, including potential incidences of cyber attacks in the form of identity theft and identity fraud.[8] It is noteworthy in this respect that both the living and the dead could be victims of identity theft and it cuts across different age groups.[9]

Identity theft, though not a new crime, has become one of the fastest-growing crimes and, as such, a source of concern, not only in Nigeria, but also across other developing and developed communities. Documents most often targeted for identity-related information include social security cards, drivers' licences, birth certificates, address books, passports and voters' registration cards and records.[10]

Identity theft, otherwise known as impersonation fraud, occurs when there is a theft, for fraudulent purposes, of personal information, such as account numbers, social security numbers and

8 Most government entities and businesses are now generating identity-related information and storing it in databases. For instance, in 2014, the Central Bank of Nigeria introduced the BVN policy which mandates every bank customer to get one by providing relevant personal bio data and biometrics at any branch of the customer's bank. The BVN database is being managed by the CBN, banks and the Nigeria Inter-Bank Settlement Scheme. Similarly, the National Identity Database created under the National Identity Management Commission Act 2007 contains biometric information of registered Nigerian citizens and non-Nigerian citizens who are lawfully and permanently resident in Nigeria. The multi-purpose identity card issued to registered persons is a requirement for opening bank accounts in Nigeria. Also, it is mandatory for all subscribers to GSM (global system for mobile communications) phone services to register their SIM (subscribers identity module) cards with the mobile operators, which is done through the collection of biometric information of subscribers: see eg Africa–China Reporting Project Data for Fraud, 'How the biometric system exposes Nigerians to cyber thieves' (7 April 2022); United Nations Office on Drugs and Crime, Handbook on Identity-related Crime (United Nations 2011) 12.

9 For example, in the United States of America (USA), there have been over 800,000 incidents of criminals exploiting the identities of the deceased to open credit cards or get a cell phone plan, while twice as many used a fake social security number belonging to the dead: A Julija, '20 worrying identity theft statistics for 2022' (*Fortunly* 14 August 2023). Similarly, child identity fraud in the USA affects one out of every 50 children annually and costs US families USD1 billion annually and takes a tremendous amount of time to resolve, more than identity fraud affecting adults: G DiNardi, 'Identity theft reaches shocking new heights in 2021' (*Nasdaq* 31 January 2022). In the same vein, older adults are reported to be significantly more likely than millennials to be victims of identity theft: M DeLiema, D Burnes and L Langton, 'The financial and psychological impact of identity theft among older adults' (2021) 5(4) Innovation in Aging; D U Ebem, J C Onyeagba and G E Ugwuonah, 'Internet banking: identity theft and solutions – the Nigeria perspective' (2017) 22(2) Journal of Internet Banking and Commerce.

10 United Nations Office on Drugs and Crime (n 8 above) 16.

other personal identifiers, such as a mother's maiden name.[11] It is the misappropriation of the identity, such as the name, date of birth, current address or previous addresses of another person, without their knowledge or consent and using same to obtain goods and services in that person's name.[12] It has also been statutorily defined as when someone 'knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law'.[13]

Identity, in this context, is the initial legal identity of an individual such as the full name, social security number, date and place of birth, maiden name (both of the victim and the victim's mother) and address, nationality and so on.[14] This is distinguishable from personal identity, otherwise called biometric identity, which is composed of attributes that are peculiar or unique to an individual such as fingerprints, retina, voice, facial structure, DNA profile, hand geometry and the like.[15] The initial legal identity, backed by a document, such as a birth certificate, is usually taken in turn to personalise an authentication method such as bank accounts, debit/credit cards, tokens among others.[16] Identity thieves could thus appropriate and subsequently misuse these identity details for illegal activities, such as to steal from the victim's bank account, obtain loans, make purchases or to commit crime.[17] The

11 J Lynch, 'Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks' (2005) 26 Berkeley Technology Law Journal 259, 260. It has, however, been noted in some quarters that there is as yet no commonly accepted definition of identity theft or identity fraud as different definitions are used for statistical purposes in different countries. The most important feature, however, is the appropriation and use of identity data for conducting other illegal activity, especially economic fraud: Fraud Prevention Expert Group (FPEG), Report on Identity Theft/Fraud (Brussels 2007) 7; UK Action Fraud, Identity Fraud and Identity Theft.

12 R Binder and M Gill, 'Identity theft and fraud: learning from the USA' (PRCI Ltd 2005) 8; UK Action Fraud (n 11 above).

13 Identity Theft and Assumption Deterrence Act 1998, s 3(a)(7), as amended by the Public Law 105–318, 112 Stat 3007 (30 October 1998). Means of identification is defined in s 3(d)(3) of the Act to include an individual's name, social security number, date of birth, driver's licence or government-issued identification number, biometric data, electronic identification number, address or routing code, or telecommunication identifying information. The available federal laws on identity theft include the Identity Theft and Assumption Deterrence Act 1998; Identity Theft Enhancement Penalty Act 2004; the Gramm-Leach-Billey Act 1999; and the Fair and Accurate Credit Transactions Act 2003.

14 FPEG (n 11 above) 11.

15 Ibid.

16 Ibid.

17 See, for example, *Rogan v Los Angeles* 668 F Supp 1384 (CD Cal 1987).

majority of cases of identity theft, however, relate to white collar and financial fraud crimes.[18]

In Nigeria, for example, between January and September 2020, fraudsters reportedly stole NGN5 billion (USD12 million) from customers' accounts.[19] In 2017, internet/online banking and automated teller machine (ATM)/card-related fraud types reported constituted 24,266 or 92.68 per cent of the 26,182 reported cases of fraud and forgeries in the banking industry resulting in NGN1.51 billion or 63.66 per cent of losses.[20] Similarly, in the UK, unauthorised financial fraud losses across payment cards, remote banking and cheques amounted to GBP783.8 million in 2020, while fraud losses on UK-issued cards totalled GBP574.2 million.[21] Identity fraud also reportedly accounted for 61 per cent of all cases of fraud reported to the Credit Industry Fraud Avoidance System (CIFAS) in 2019, with 22 per cent of the reported identity theft cases being for the purpose of gaining access to bank accounts.[22]

The article examines financial identity theft in banks and other financial institutions and the legislative measures that have been deployed to curtail the menace in Nigeria. Regulatory measures in the UK are also examined with a view to drawing some lessons therefrom for further reform of the extant law in Nigeria. The identified gaps in the law are highlighted and suggestions for addressing them proffered. The choice of the UK has been informed by the legislative history which Nigeria has with the UK as one of the latter's colonies.

The article is divided into five sections. The analysis of the nature of identity theft is followed in the subsequent section by examination of the techniques identity thieves usually use to steal the personal information of their victims and the impact of the identity theft on victims, the financial institutions and the society. The third section is devoted to the examination of the regulatory framework in Nigeria and the UK to combat identity theft, as well as personal data protective regulatory measures aimed at protecting consumers of banks and

18 T P Vartanian and T P Nelson, Identity Theft and Financial Institutions (nd) 3.

19 Onukwe (n 7 above).

20 Nigeria Deposit Insurance Corporation (NDIC), 'NDIC to investigate banks for failure to make returns on fraud cases' (12 March 2018).

21 UK Finance, Fraud – the Facts (2021) 10 and 19.

22 A Aashind, 'ID theft statistics UK edition 2022' (2022). Also, in the USA, about 15 million people experience identity theft every single year resulting in about USD50 billion of financial losses. In 2020, the cost of identity theft to people totalled USD56 billion, while over 49 million people fell victims in that year. The majority of the losses, about USD43 billion, stemmed from direct interaction scams, such as phishing emails, while the 'traditional' identity theft, that is, people losing their information through data breaches and similar attacks accounted for USD13 billion: Julija (n 9 above).

other financial institutions' services. The fourth section explores ways of improving on the current regulatory framework in Nigeria, and the fifth part is the conclusion.

MODES OF IDENTITY THEFT AND ITS IMPACT

Modes of identity theft

Identity theft can come in various forms, either physically, such as by the theft of debit/credit cards, or through the internet, such as by the use of computers, to steal personal and sometimes confidential information of other persons.

The most notable of the techniques used in gaining access to the necessary information, therefore, include offline identity theft which could occur by pick-pocketing, dumpster-diving or bin-raiding, which involves rummaging through trash bins, recycling containers and dumpsters to find discarded and unshredded financial records, credit card slips, ATM receipts, bank statements, loan or credit card applications and the like.[23] It also includes stealing pre-approved credit card applications from mail-boxes, completing 'change of address' forms through the post office in order to divert a victim's mail, and securing low-level employment with an organisation to gain access to and steal customers' credit reports and financial records.[24] Another potential source in this respect is insider attack through the careless handling of confidential customer information or through intentional misconduct of bank staff. Also, in some cases, dishonest bank staff, as insiders, use their access to customer confidential information to commit identity theft or aid or abet others in committing same.[25] Account takeover by third parties could also be facilitated easily by staff fraud without being challenged.[26]

Identity theft through the use of the internet, on the other hand, includes phishing/pharming. This involves the use of social-engineering techniques, especially email, to make victims disclose personal information. In this case, identity thieves purchase a domain name and set up a spoofing site, which is similar to that of a genuine financial institution and then send out indiscriminate mass

23 Vartanian and Nelson (n 18 above) 3.

24 Lynch (n 11 above) 262.

25 Vartanian and Nelson (n 18 above) 4; Agency Report, 'Bank customers lament illegal withdrawals, demand urgent action' *The Punch* (Nigeria 7 November 2022). In Nigeria, the NDIC has revealed that the number of fraud cases attributed to internal abuse by staff of banks increased from 231 in 2016 to 320 in 2017 or 38.53% above the figure recorded for 2016: NDIC (n 20 above).

26 FPEG (n 11 above) 27.

emails purporting to be from the victims' banks or other e-commerce sites.[27] Another technique to direct the user to the spoofed website is manipulation of the domain name system, known as 'pharming'. The emails typically require victims to update or supply their account details to avoid fraud or for security reasons.[28] It could also be used to acquire information, such as user names, passwords and credit card details. These personal and financial details disclosed by the victims are, thereafter, used to log on to the victims' accounts to perpetrate the fraud under the guise of legitimate banking business and to commit offences, such as the transfer of funds, applications for new accounts or passports and so on.[29]

Another technique is through internet banking, telephone banking and mobile banking which occurs when the identity thief gains access to an individual's bank account through one of these remote banking channels and makes an unauthorised transfer of money from the account.[30] It could also be carried out through pretext calling/scam-related text messages purporting to be from legitimate bank officials where the victim's account is domiciled and requesting for the customer's ATM personal identification number (PIN) or bank verification number (BVN).[31] This can also occur through debit/credit card alerts whereby a purported 'employee' of a credit card issuer would call an unsuspecting customer to confirm unusual spending activity and ask for the security code on the back of the credit card.[32]

Also, identity theft could occur through malware, that is, the use of malicious software. This is done through the installation of small software tools on the victim's computer to intercept communications,

---

27 Lynch (n 11 above) 259.

28 Ibid. In the UK, over 25,000 bank-branded phishing websites were reportedly identified and taken down in 2020: UK Finance (n 21 above) 45; see also CBN, 'Advance fees fraud (419) CBN Disclaimer'.

29 United Nations Office on Drugs and Crime (n 8 above) 17; CBN (n 28 above).

30 UK Finance (n 21 above) 43. Almost all cases of identity fraud reported in 2019 to the CIFAS took place on line and 42 % of them were committed with the intention of obtaining debit card or credit card details: Aashind (n 22 above); T Owoyele, 'Access bank wants customer to repay loan taken by a thief' (Foundation for Investigative Journalism 19 November 2022); E Uti, 'Banker trusted UBA with her ₦146,000. She lost it all' (Foundation for Investigative Journalism 20 November 2022).

31 K S Provenza, 'Identity theft, prevention and liability' (1999) 3 North Carolina Banking Institute 319, 324; Africa–China Reporting Project Data for Fraud (n 8 above); Ebem et al (n 9 above) 13.

32 Vartanian and Nelson (n 18 above) 3. In the USA, for example, credit card fraud has become the most common kind of identity theft with about 18,000 reports received by the Federal Trade Commission in 2020 and 2021 from various individuals that their information has been used to gain access to their credit card accounts illegally: Julija (n 9 above).

log keyboard strokes and search for information on the victim's computer.[33] Indeed, at the rebirth of the quick response (QR) codes following the resurgence of e-commerce spurred by the Covid-19 pandemic, it was discovered through available threat intelligence advisories that hackers have developed fraudulent QR codes with embedded malware that allows them to access a person's smartphone to steal personal information, without having the person enter any login credentials.[34]

Other techniques through the internet include hacking, which is the unlawful access to a computer system including computer systems that have large databases with identity-related information.[35] Once the identity thief has access to the computer system, the criminal can obtain identity-related information. There is also skimming, which involves the manipulation of ATMs to obtain the victim's credit card information and access codes.[36]

Impact of identity theft

The impact of identity theft on the victim is multidimensional in nature. First, identity thieves could use the stolen identities of their victims to obtain goods or services by deception, such as to open new financial accounts or take over victims' existing financial accounts;[37] obtain credit cards, loans or state benefits; order goods in the victims' names; establish credit or run up debt; and obtain genuine documents,

33 United Nations Office on Drugs and Crime (n 8 above) 17.

34 First Bank (Nig) plc email on 'Update on quick response (QR) code scam' of 28 March 2022 sent to all customers of the bank.

35 United Nations Office on Drugs and Crime (n 8 above) 17; N C Wilmington, 'Data company settles for $1 million after failing to warn customers of identity thief' (*WECT News* 8 November 2022).

36 United Nations Office on Drugs and Crime (n 8 above) 17.

37 UK Finance (n 21 above) 28. In the first, which is application fraud, the identity thief uses stolen or fake documents to open an account in some other person's name and for identification purposes – the identity thief may try to steal documents, such as utility bills and bank statements, to build up useful personal information or, alternatively, use counterfeit documents. The other, which is account takeover, is the impersonation of, or attempt to assume the identity of, an existing account holder that has been previously properly identified. It involves the identity thief fraudulently gathering information on financial institutions' clients and thereafter contacting the card issuer pretending to be the genuine cardholder to get further financial services. In some other circumstances, an identity thief could create a counterfeit card by using information obtained from the magnetic stripe: FPEG (n 11 above) 26; UK Finance (n 21 above) 19–29; S Byers, 'The internet: privacy lost, identities stolen' (2001) 40 *Brandeis Law Journal* 141. In 2018, in the UK, for example, the financial cost of application identity theft in which criminals used stolen identities to open new bank accounts was GBP 29.4 million, while that of account takeover fraud was GBP17.9 million: Aashind (n 22 above).

such as passports and driving licences in the victims' names.[38] Identity theft thus has significant impact on not only the customer whose identity has been stolen to perpetrate the crime, but also on the financial institutions, the government, private companies detaining large amounts of data and the economy as a whole.[39] The individual customer suffers the immediate financial loss from the money directly taken from their account although the financial loss might be covered by the financial institution in the end if it is found that the customer has not been negligent in any manner in the course of events. In addition to ruined credit, individual customers could suffer the associated indirect cost of having to clean up their names and reputation as well as the emotional and psychological damage in terms of the impact on stress and health levels.[40] There are also indirect costs for businesses which may have to upgrade their prevention systems.

The effect on the financial institutions is linked to both the direct and indirect costs, which are likely to be passed on as costs to the final clients of financial institutions in the form of higher interest rates and larger annual card fees, thereby contributing to diminution of the performance of the financial system.[41] Government could also bear direct financial losses in cases where the identity theft is directed against public bodies, as well as the indirect costs associated with prevention and law enforcement systems.[42] In all, there are also the reputational risks for all stakeholders, including the government whose identification documents made for the citizenry could suffer discredit; the financial system as customers may lose confidence in non-cash means of payment;[43] and the reputational problem for data storage service providers and financial sector providers, which affects the entire market environment and the business model itself.[44]

The spate of identity theft and its devastating effects on individual customers, banks and other financial institutions, other corporate organisations and e-commerce have necessitated the enactment of laws in several countries, including Nigeria and the UK, not only to criminalise the act as a control measure, but also to offer protection for the citizenry, especially bank customers. It is to this we now turn.

---

38 Provenza (n 31 above) 320-321; UK Action Fraud (n 11 above).
39 FPEG (n 11 above) 9.
40 Ibid 10.
41 Ibid 9; B F Caminer, 'Credit card fraud: the neglected crime' (1986) 76 Journal of Criminal Law and Criminology 747.
42 FPEG (n 11 above) 9.
43 Lynch (n 11 above) 260.
44 FPEG (n 11 above) 10.

THE REGULATORY FRAMEWORK AGAINST IDENTITY THEFT IN NIGERIA AND THE UK

This section is devoted to an examination of the laws that have been enacted in Nigeria and the UK to prosecute identity theft and offer protection to customers of bank and other financial institutions. Our discussion starts with an examination of the relevant laws in Nigeria.

Laws against identity theft in Nigeria

The fulcrum of all the regulatory measures on identity theft in Nigeria is the Constitution of the Federal Republic of Nigeria 1999[45] which, in section 37 thereof, guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. Identity theft is, thus, a contravention of the privacy right of an individual. Nigeria is also a signatory to the African Union Convention on Cyber Security and Personal Data Protection 2014 wherein member states are, *inter alia*, enjoined to commit themselves to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.[46]

Other available legislation to prosecute identity theft include the Criminal Code Act 1916, the Advance Fee Fraud and Other Fraud-Related Offences Act 1995 and the Cybercrime (Prohibition, Prevention, etc) Act 2015, which was specifically designed for cyberspace-related offences, including identity theft, the Nigeria Data Protection Regulation 2019 (NDPR) and the Nigeria Data Protection Act 2023 (NDPA). We shall be examining the relevant provisions of these legislation starting with the Criminal Code.

Criminal Code Act 1916[47]

The Criminal Code has provisions that have tangential bearing on identity theft. These include section 484, which criminalises the act of impersonation of a living or dead person; section 419A, which criminalises the act of obtaining credit by false pretences or other fraud; and section 465, which criminalises the act of forgery or uttering of a document or writing knowing it to be false, and with intent that it

45 As amended by subsequent legislation thereto.

46 Art 8(1) of the African Union Convention on Cyber Security and Personal Data Protection 2014. Art 8(2) of the Convention further provides that the mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons, while recognising the prerogatives of the state, the rights of local communities and the purposes for which the businesses were established.

47 Cap C 38 LFN 2004.

may in any way be used or acted upon as genuine, whether in the state or elsewhere, to the prejudice of any person, or with intent that any person may, in the belief that it is genuine, be induced to do or refrain from doing any act, whether in the state or elsewhere.[48]

Advance Fee Fraud and Other Fraud-Related Offences Act 1995[49]

The Advance Fee Fraud and Other Fraud-Related Offences Act, in section 1 thereof, similarly criminalises obtaining property by false pretences whether or not the property is obtained or its delivery is induced through the medium of a contract induced by false pretence.[50] Also criminalised is the making of false pretence by any person with the intention of fraudulently inducing any other person in Nigeria, or any other country, to confer a benefit on them or on any other person, by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for.[51]

The offence of phishing is also captured under the Act as the attempt to commit any of the foregoing offences suffices under section 5 of the Act for conviction once it is successfully proven that the false pretence is contained in a letter or other document and such letter or other document was received by the person to whom the false pretence was directed. Also, notwithstanding anything to the contrary in any other law, every act or thing done or omitted to be done by a person to facilitate the commission of the offence constitutes an attempt. In this regard, 'other document' includes a document transmitted through a fax or telex machine or any other electronic or electrical device, a telegram and a computer printout.

Furthermore, under section 8 of the Act, the conspiracy to commit, or the aiding, abetting or counselling of any other person to commit any of the foregoing offences or the attempt thereof; or being an accessory to the act or offence; or inciting, procuring, or inducing any other person by any means whatsoever to commit the offence, is an

---

48 *Mike Amadi v Federal Republic of Nigeria* (2008) 12 SC (Pt III) 55. Under the section, the term 'make a false document or writing' includes altering a genuine document or writing in any material part, either by erasure, obliteration, removal or otherwise, and making any material addition to the body of a genuine document or writing any false date, attestation, seal or other material matter. A person found guilty of the offence of forgery is liable under s 467 to a term of imprisonment for three years.

49 Cap A6 LFN 2004.

50 S 1(1) of the Advance Fee Fraud Act; *Mike Amadi v Federal Republic of Nigeria* (n 50 above); *Odua v Federal Republic of Nigeria* (2002) 5 NWLR (Pt 761) 615.

51 S 1(2) of the Advance Fee Fraud Act. Under s 1(3), the offences listed under s 1(1) and (2) are punishable on conviction with a term of not less than 10 years without the option of a fine.

offence punishable on conviction on the same terms as it is prescribed for the offence under the Act.

Cybercrimes (Prohibition, Prevention, etc) Act 2015

A more comprehensive piece of legislation on identity theft is the Cybercrime (Prohibition, Prevention, etc) Act 2015 (the CPPA) which covers most of the cases of identity theft wherein the previous legislation were deficient in view of the advance in technology and the new ways of committing the offence. The objectives of the CPPA are, *inter alia*, to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria, as well as to promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programmes, intellectual property and privacy rights.[52]

Identity theft and impersonation are criminalised specifically by the CPPA in section 22 thereof, which makes it a punishable offence for any person who is engaged in the services of any financial institution, and as a result of their special knowledge and with the intent to defraud, to commit identity theft of its employer, staff, service providers and consultants. Other offences criminalised in this regard include the offence, by any person, of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person;[53] fraudulently impersonating another entity or person, living or dead, with intent to gain advantage for themself or another person, obtain any property or an interest in any property, cause disadvantage to the entity or person being impersonated or another person, or avoid arrest or prosecution or obstruct, pervert or defeat the course of justice;[54] and making or causing to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied upon respecting the identity or that of any other person, or their financial condition, or that of any other person, for the purpose of procuring the issuance of a card or other instrument to themself or another person.[55]

The attempt to commit the offence of identity theft or the aiding, abetting, conspiring, counselling, or procuring another person(s) to commit the offence is also punishable on conviction by the punishment provided for the offence under the Act.[56] Also, insider attack is addressed under section 27(2) of the CPPA such that any employee

52 S 1 of the CPPA.
53 Ibid s 22(2).
54 Ibid s 22(3).
55 Ibid s 22(4).
56 Ibid s 27(1)(a).

of a financial institution found to have connived with another person, or group of persons to perpetrate fraud using a computer system(s) or network is guilty of an offence.

Furthermore, in furtherance of its stated objectives, the CPPA, in section 28 thereof, *inter alia*, criminalises the importation and fabrication of e-tools for the purpose of committing an offence under the Act and the disclosure, knowingly and without authority, of any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain.[57]

Moreover, the act of knowingly or intentionally engaging in computer phishing, engaging in spamming with intent to disrupt the operations of a computer, be it public or private or financial institutions, as well as engaging in the malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institutions' computers is criminalised under section 32 of the CPPA. Also criminalised under section 30 is the manipulation of ATM machine or point-of-sales (POS) terminals with the intention to defraud.

A wide provision on electronic card-related frauds is available under section 33 of the CPPA. The section, for example, criminalises the use of any access device, including credit, debit, charge, loyalty and other types of financial cards, with intent to defraud, in order to obtain cash, credit, goods or services; the use of a counterfeit access device, an unauthorised access device, or an access device issued to another person resulting in a loss or gain; stealing of an electronic card; the receipt of a card by any person who knows or ought to know it to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and the retention of the possession of such card with the intent to use, sell, or to traffic it to a person other than the issuer or the cardholder; and the taking of control over a card by any person, with intent to defraud the issuer, a creditor, or any other person as security for a debt. Furthermore, section 34 criminalises dealing in a card of some other person, including the receipt and retaining possession of two or more cards issued in the name or names of different cardholders, which cards the person knows were taken or retained under circumstances which constitute a card theft; section 35 criminalises the purchase or sale of the card of some other person, while section 36 criminalises the use by any person, with intent to defraud, of any device or attachment, emails, or fraudulent website to obtain information or details of a cardholder.

57 Ibid s 28(3).

A contravention of any of the foregoing offences is punishable on conviction with a fine ranging from NGN500,000 to NGN10 million, or to a term of imprisonment which varies from two years to a maximum of seven years, or to both fine and imprisonment.[58] In deserving cases, the court is empowered to order the restitution of the funds or goods in question as appropriate, or the forfeiture of the assets or goods to which it has been converted to the bank, financial institution, or the customer.[59]

Other protective regulatory measures

Nigeria Data Protection Regulation 2019 and Nigeria Data Protection Act 2023

In view of the crucial role that data privacy protection plays in the success of e-commerce transactions, the National Information Technology Development Agency (NITDA), established under section 1 of the National Information Technology Development Agency Act 2007 to plan, develop and promote the use of information technology in Nigeria, issued the NDPR in 2019. The Nigeria Data Protection Act 2023 (NDPA) has also been enacted as a substantive law in this regard. The NDPA is generally aimed at, *inter alia*, safeguarding the fundamental rights and freedoms, and the interests of data subjects as guaranteed under the Constitution of the Federal Republic of Nigeria; providing for the regulation of processing of personal data; and promoting data-processing practices that safeguard the security of personal data and privacy of data subjects.[60] The NDPA is applicable to all data controllers or data processors domiciled in, resident in, or operating in Nigeria, or where not so domiciled in, resident in, or

58 See eg ibid ss 13; 22(1) and (4); 27(2); 28(1), (2), (3), (4) and (5); 30(1) and (2); 32(1) and(2); 33(1) and (2); 34; 35 and 35(1).

59 See eg ibid ss 27(2), 34 and 35.

60 S 1 of the NDPA. Reg 1.1 of the NDPR. The NDPR was made by the NITDA pursuant to its statutory functions, as contained particularly in s 6(c) of the National Information Technology Development Agency Act 2007, to '[d]evelop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information'.

operating in Nigeria, are involved in processing personal data of a data subject in Nigeria, whether by automated means or not.[61]

'Personal Data' is defined as any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.[62]

The governing principles of data processing, as spelt out in section 24(1) of the NDPA as well as regulation 2.1 of the NDPR, include the principle of lawfulness, which requires that personal data should generally be collected and processed in accordance with specific, legitimate and lawful purposes consented to by the data subject;[63] the principle of accuracy which requires that personal data be adequate, accurate and without prejudice to the dignity of the human person; the principle of storage limitation, which requires that the personal data be stored only for the period within which it is reasonably needed; and the principle of integrity and confidentiality, which requires that the personal data be secured against all foreseeable hazards and breaches, such as theft, cyber

61 S 2 of the NDPA. See also reg 1.2 of the NDPR. S 65 of the NDPA defines 'data controller' as an individual, private entity, public commission, agency, or any other body who, alone or jointly with others, determines the purposes and means of the processing of personal data. A 'data processor', on the other hand, is defined as an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor.

62 S 65 of the NDPA. Reg 1.3 of the NDPR similarly defines 'personal data' as any information relating to an identified or identifiable natural person ('data subject'). Identifiable natural person, in this context, refers to someone who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as, but not limited to, MAC address, IP address, IMEI number, IMSI number, SIM, personal identifiable information (PII) and others.

63 'Data subject' is defined in s 65 of the NDPA as an individual to whom personal data relates. Similarly in reg 1.3 of the NDPR, 'data subject' is defined as any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. 'Consent' is defined in s 65 of the NDPA as any freely given, specific, informed and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to themself or to another individual on whose behalf they have the permission to provide such consent.

attack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements.

The NDPA, as well as the NDPR, imposes a duty of care on every data controller and data processor in respect of data processing, and they are required to demonstrate accountability for any act or omission in respect of the principles contained in the respective legislation.[64] Furthermore, every data controller and data processor is obligated to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in their possession or under their control, including protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access.[65]

Under section 48 of the NDPA, any data controller or data processor found to be in breach of the data privacy rights of any data subject may, in addition to any other criminal liability, be ordered, by the Nigeria Data Protection Commission after any necessary investigation, to remedy the violation, pay compensation to a data subject who has suffered injury, loss or harm as a result of a violation, account for the profits realised from the violation, or pay a penalty or remedial fee. Such penalty or remedial fee may be an amount up to the higher maximum amount, which shall be the greater of NGN10 million and 2 per cent of its annual gross revenue in the preceding final year or the standard maximum amount which shall be the greater of NGN2 million and 2 per cent of its annual gross revenue in the preceding final year, taking into consideration, *inter alia*, the nature, gravity and duration of the infringement, the purpose of the processing and types of personal data involved. 'Personal data breach' is defined in section 65 of the NDPA as a breach of security of a data controller or data processor, leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

CBN Consumer Protection Framework 2016 and Consumer Protection Regulations 2019

As part of measures to enhance the confidence of customers of Nigerian banks and other financial institutions in the financial services industry and to promote financial stability, growth and innovation, the CBN, has

64 S 39(3) of the NDPA; reg 2.1(2) and (3) of the NDPR.

65 S 39(1) of the NDPA. See also reg 2.6 of the NDPR which requires anyone involved in data processing or the control of data to develop security measures to protect data, including protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data and other sensitive or confidential data; protection of emailing systems; and continuous capacity-building for staff.

issued the Consumer Protection Framework (CPF) and the Consumer Protection Regulation (CPR). A major feature of the CPF as well as the CPR are the provisions relating to protection of consumer/customer assets and privacy.[66]

In this regard, paragraph 2.6 of the CPF requires all banks and financial institutions to establish appropriate measures to guarantee protection of consumer assets and privacy; to, at all times, protect consumers' financial personal information; and to refrain from releasing such information to a third party without the consent of the consumer, except as required by law.[67] Information considered confidential and requiring protection includes contact details, account number and balance, statement of accounts and any other information known to the institution. Furthermore, banks are required to establish guidelines to safeguard consumer assets and privacy against unauthorised access in the area of fraud prevention and data privacy. Specifically, on data protection, all personal information of customers, including those with closed accounts, is to be kept in confidence, and the privacy of customers' data is to be safeguarded as a duty of care. Appropriate data protection measures and staff training programmes are also required to be put in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction. Consent of the consumers is also required to be obtained in writing before sharing their data with third parties, including a subsidiary or an associated company of the institution.

Similarly, the CBN CPR requires all banks and other financial institutions to ensure the data protection and privacy of consumers.[68] In the first instance, the written consent of consumers is required to be sought and obtained before the collection and processing of personal data of consumers for specific purposes and the option of withdrawal of consent at any time be given.[69] Like the NDPA and the NDPR, these institutions are mandated to abide by certain principles, such as the

66 'Consumer' is defined in para 1.3 of the CPF as a person or an entity that uses, has used, or is a potential user of financial products or services of a financial institution, while a 'customer' is defined as a person that has a relationship by reason of benefiting from financial products or services offered by a financial institution.

67 Under ibid para 2.6.2.2, apart from the express permission of the customer, such information could also be released by the bank or other financial institution as required by the CBN or other regulatory bodies, in compliance with a court order, or in pursuance of public duty/interest. See also *Tournier v National Provincial & Union Bank of England* (1924) 1 KB 461.

68 Consumer is herein defined in reg 10 of the CBN CPR 2019 as a person or an entity that uses, has used, or is a potential user of financial products or services of an institution.

69 Ibid reg 5.4.2.

principle of privacy and confidentiality, which requires the protection of the privacy and confidential information of consumer information and assets against unauthorised access, and accountability for acts or omissions in respect thereof;[70] the principle of non-transferability to a third party without express consent of the consumer, except in compliance with a legal obligation and the giving of information whenever the data is exchanged with an authorised third party with details of the exchange;[71] the principle of continued validity, which requires that data processing and privacy procedures are reviewed to ensure that the purpose(s) for which initial consent was granted remain valid;[72] and the principle of accuracy, which requires that data of consumers be kept accurate and updated always.[73]

The CBN CPR has no specific provision for sanctions whenever there is a contravention of the above provisions on data protection and privacy of customers. However, regulation 7.1 of the CPR has a general provision on penalty, which is administrative sanctions on responsible officer(s), including issuance of warning letters and any other statutory sanctions on the officer(s) or institution for persistent breach of regulations.

Know your customer

The identification of customers by banks and other financial institutions is subject to some legal obligations, including the know your customer (KYC) and the customer due diligence procedure deriving from the anti-money laundering legal obligations. In this regard, the Money Laundering (Prevention and Prohibition) Act 2022, in section 4 thereof, imposes an obligation on financial institutions to verify a customer's identity using reliable, independent source documents, data or information and undertake customer due diligence measures when, *inter alia*, establishing business relationships or carrying out occasional transactions that are wire transfers.

In the same vein, the CPPA imposes similar obligations, with prescribed penalties, on banks and other financial institutions in their dealings with customers. These include the duty to verify the identity of customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before issuance of ATM cards, credit cards, debit cards and other related electronic devices.[74]

---

70 Ibid reg 5.4.1.
71 Ibid regs 5.4.3 and 5.4.4.
72 Ibid reg 5.4.5.
73 Ibid reg 5.4.6.
74 S 37(1)(a) of the CPPA.

Financial institutions are further required to apply the principle of KYC in the documentation of customers preceding execution of customers' electronic transfer, payment, debit and issuance orders.[75] Furthermore, as a duty to their customers, financial institutions are required to put in place effective counter-fraud measures to safeguard their sensitive information.[76] However, where a security breach occurs, the onus of proof of negligence lies on the customer to prove that the financial institution in question could have done more to safeguard its information integrity.[77]

Bank verification number system

As part of the measures to protect banks and other financial institutions' customers from the menace of identity theft through the promotion of a safe, reliable and efficient payment system, as well as to ensure the effectiveness of the obligation of KYC, the CBN, in collaboration with the Bankers' Committee, deployed and introduced the centralised BVN system in 2014.[78] Under the BVN system, the individual customer is required to enrol by having their biometric and demographic data captured in the BVN central database system and have a unique ID, the BVN, generated for them.[79] This is to ensure a stringent authentication and verification process in the financial system. Thus, as the need arises, banks and other financial institutions would verify the customer by matching the customer's biometric template with what has been captured in the database.[80] Thus, since 2014 for banks and 1 August 2017 for other financial institutions, all customers of these institutions without BVNs linked to their accounts are barred from making any withdrawal therefrom.[81]

Participants in the BVN scheme include the CBN, Nigeria Inter-Bank Settlement System (NIBSS), Deposit Money Banks, other financial institutions as well as bank customers.[82] The NIBSS is specifically mandated to, *inter alia*, ensure seamless operations of the BVN system; maintain the BVN database; ensure adequate security

75 Ibid s 37(1)(b). Failure of any financial institution to obtain the proper identity of customers before executing customer electronic instructions in whatever way is punishable on conviction with a fine of NGN5 million.

76 Ibid s 19(3).

77 Ibid s 19(3).

78 See para 1.1 of the CBN Regulatory Framework for BVN Operations and Watch-List for the Nigerian Banking Industry (2017) ; CBN Letter to All Other Financial Institutions, Bank Verification Number (BVN) Enrolment for Customers, 21 April 2017.

79 Para 1.5(i) of the CBN Regulatory Framework for BVN Operations (n 78 above).

80 Ibid para 1.5(ii).

81 CBN Letter (n 78 above).

82 Para 1.4.1 of the CBN Regulatory Framework for BVN Operations (n 78 above).

of the BVN information; and maintain an online real-time Watch-List Portal.[83] Parties involved in the BVN operations are required to put in place secured hardware, software and encryption of messages transmitted through the BVN network.[84] Also, users of BVN are mandated to establish adequate security procedures to ensure the safety and security of their information and that of their clients, which shall include physical, logical, network and enterprise security.[85]

National identity card scheme

Again, as a means of curtailing the menace of identity theft in Nigeria, a central identity database is established under section 14 of the National Identity Management Commission Act 2007 (NIMC Act) that could securely and reliably verify and authenticate the identities of individuals registered as prescribed. The National Identity Management Commission (NIMC) established under section 1 of the NIMC Act is charged with the responsibility for creating, managing, maintaining and operating the National Identity Database; carrying out the registration of Nigerian citizens and non-Nigerian citizens who are lawfully and permanently resident in Nigeria; issuing a general multi-purpose identity card to registered persons; and ensuring the preservation, protection, sanctity and security (including cyber security) of any information or data collected, obtained, maintained or stored in respect of the database.[86]

The National Identity Database, generally, contains registered information or data relating to registered persons who have been identified using unique and unambiguous features, such as fingerprints and other biometric information.[87] The information so obtained is thereafter used to issue a multi-purpose identity card with a unique identification number that would provide a medium for the identification and authentication of registered persons including the opening of individual and/or personal bank accounts.[88] In order to ensure the security and integrity of the database, it is a punishable offence, under section 28 of the NIMC Act, for any person to, without lawful authorisation, access data or information contained therein.[89]

---

83 Ibid para 1.4.1.2.
84 Ibid para 1.8(i).
85 Ibid para 1.8(iii).
86 S 5 of the NIMC Act 2007.
87 Ibid s 14(1) and (2). 'Biometric information' in relation to a registered individual is defined under ibid s 33 as data about such individual's external characteristics, including in particular, the features of an iris or any other part of the eye.
88 Ibid ss 15 and 27(1) of the NIMC Act 2007.
89 Ibid s 28(2) and (3).

Laws against identity theft in the UK

The laws on identity theft in the UK include the Theft Act 1968; Forgery and Counterfeiting Act 1981 (FCA); the Fraud Act 2006; Data Protection Act 2018 (DPA); the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (UK General Data Protection Regulation (GDPR)); and the Identity Documents Act 2010 (IDA). The relevant provisions on identity theft will now be examined starting with the Theft Act 1968.

The Theft Act 1968

The Theft Act 1968, in section 1 thereof, criminalises all forms of theft whereby a person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.[90] Property, in this context, includes money and all other property, real or personal, including things in action and other intangible property.[91] This, arguably, covers personal/confidential information of victims of identity theft.

Forgery and Counterfeiting Act 1981

The FCA criminalises the act of forgery.[92] This is particularly relevant in relation to debit and credit cards. Under sections 1 and 2 of the FCA, a person is guilty of forgery if they make a false instrument,[93] or a copy thereof, with the intention that they or another person shall use it to induce somebody to accept it as genuine, or as a copy of a genuine instrument, and, by reason of so accepting it, do or not do some act to their own or any other person's prejudice.[94] Also, under sections 3 and

90 Under s 7 of the Theft Act 1968, a person found guilty of theft is liable on conviction on indictment to imprisonment for a term not exceeding seven years.

91 Ibid s 4.

92 Generally, under s 6 of the FCA, a person that is found guilty is liable on summary conviction to a fine not exceeding the statutory maximum, or to imprisonment for a term not exceeding six months, or to both. A person convicted under ss 1, 2, 3, 4, 5(1) and (3) is liable on conviction on indictment to imprisonment for a term not exceeding 10 years, while an offence under s 5(2) or (4) attracts imprisonment for a term not exceeding two years on conviction on indictment.

93 Under ibid s 9, an instrument is false if it, *inter alia*, purports to have been made in the form in which it is made by a person who did not in fact make it in that form; or to have been made in the form in which it is made on the authority of a person who did not in fact authorise its making in that form, or to have been made in the terms in which it is made by a person who did not in fact make it in those terms.

94 Under ibid s 8, instrument for the purposes of ss 1–5 includes any document whether of a formal or informal character.

4 respectively of the FCA, it is a punishable offence for any person to use a false instrument, or to use a copy of an instrument which is, and which they know or believe to be, a false instrument, with the intention of inducing somebody to accept it as genuine, or as a copy of a genuine instrument and, by reason of so accepting it, do or not do some act to their own or any other person's prejudice.

Furthermore, section 5 of the FCA *inter alia*, makes it a punishable offence for any person to have in their custody, or under their control, an instrument, including debit cards and credit cards, which is and which they know or believe to be false, with the intention that they or another person shall use it to induce somebody to accept it as genuine and, by reason of so accepting it, do or not do some act to their own or any other person's prejudice.[95]

Fraud Act 2006

The Fraud Act 2006[96] generally makes provision for criminal liability for fraud and obtaining services dishonestly. The Act is significant in the fight against identity theft in the UK because the scope of indictment extends to fraud committed not only by false representation or by abuse of position as it is obtainable under the Nigerian CPPA, but also failure to disclose information.[97] Failure to disclose information amounts to fraud where any person who has the legal duty to disclose fails to do so with the aim of making a gain thereby for themself or some other person, or causing a loss to another or exposing another to a risk of loss.[98] Fraud by false representation is committed when a person dishonestly makes a false representation whether of fact or law, expressly or impliedly, and intends, by making the representation, to make a gain for themself or another, or to cause loss to another, or to expose another to a risk of loss.[99] Liability ensues once the

95 Other instruments to which the section applies, apart from credit cards and debit cards, include money orders, postal orders, UK postage stamps, Inland Revenue stamps, share certificates, cheques and other bills of exchange, travellers' cheques, bankers' drafts, promissory notes, cheque cards, certified copies relating to an entry in a register of births, adoptions, marriages, civil partnerships, conversions or deaths and issued by the Registrar General, a registration officer or a person lawfully authorised to issue certified copies relating to such entries and certificates relating to entries in such register.

96 The Act came into force on 15 January 2007.

97 S 1(1) and (2) of the Fraud Act 2006. Under s 1(3), a person who is guilty of fraud is liable on summary conviction to imprisonment for a term not exceeding 12 months, or to a fine not exceeding the statutory minimum, or to both. A conviction on indictment is imprisonment for a term not exceeding 10 years, or to a fine, or both.

98 Ibid 4(1) and (2).

99 Ibid s 2(1), (3) and (4).

representation is found to be untrue or misleading and the person making it knows that it is, or might be, untrue or misleading.[100]

Furthermore, the Act criminalised phishing and pharming under section 2(5); possession of articles for use in the course of or in connection with fraud under section 6; and the making or supplying of articles with the knowledge or intention of their being used in the course of or in connection with fraud under section 7 thereof. Article, in this context, includes any program or data held in electronic form.[101]

Data Protection Act 2018 and the UK General Data Protection Regulation

The protection of individuals in relation to the processing of personal data is also a fundamental right in the UK by virtue of article 8 of the Human Rights Act 1998 which guarantees to everyone the right to respect for private and family life, home and correspondence. Similarly, article 16(1) of the Treaty on the Functioning of the European Union (TFEU) guarantees to everyone the right to the protection of personal data concerning themselves. Thus, as a means of enhancing the protection of personal information from the onslaught of identity theft, the DPA and the UK GDPR contain salient provisions geared towards the protection of the fundamental rights of individuals with regard to the processing of personal data.[102] Personal data, in this context, means any information relating to an identified or identifiable living individual.[103] The two pieces of legislation, *inter alia*, require that personal data be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis.[104] The Information Commissioner is particularly vested with the duty of securing an appropriate level of protection for personal data, taking into account

100 Ibid s 2(2).

101 Ibid s 8.

102 S 2(1) of the DPA; art 1 of the UK GDPR. 'Processing' in relation to information is defined in s 3(1) of the DPA as an operation or set of operations which is performed on information, or on sets of information, such as collection, recording, organisation, structuring or storage; adaptation or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; alignment or combination; or restriction, erasure or destruction etc.

103 S 3(1) of the DPA 2018. Art 4 of the UK GDPR also has a similar definition except that 'natural person' is used instead of 'living individual'.

104 S 2(1) of the DPA.

the interests of data subjects, controllers and others, as well as matters of general public interest.[105]

Save for cases where the data subject has given explicit consent to the processing of personal data for one or more specified purposes, and except where domestic law prohibits, article 9 of the UK GDPR prohibits the processing of personal data revealing matters such as biometric data for the purpose of uniquely identifying a natural person.[106]

Identity Documents Act 2010

The IDA is another piece of legislation designed to guard against identity theft. The importance of this legislation to identity theft is in relation to the establishment of the identity of an individual, or the verification that a person involved in the transaction is actually the right person. As such, under section 4 of the IDA, it is an offence for any person, with an improper intention, to have in their possession or under their control, an identity document that is false, or that was improperly obtained and which they know, or believe, to have been so improperly obtained, or an identity document that relates to someone else.[107] Improper intention, in this context, includes the intention of using the document for establishing their personal information, or the intention of allowing or inducing another person to use it for establishing, ascertaining or verifying personal information about the person or anyone else.[108] In the same vein, under section 6 of the IDA, it is a punishable offence for any person, without reasonable excuse, to have in their possession, or under their control, an identity document

105 Ibid s 2(2). The general principles relating to processing of personal data are laid down in art 5(1) of the UK GDPR. These include the principles of lawfulness, fairness and transparency, data minimisation, accuracy, storage limitation, and of integrity and confidentiality.

106 See also ss 10 and 11 of the DPA 2018. The rights of the data subject are spelt out in arts 16, 17, 18, 20, 21 and 22 of the UK GDPR.

107 Under s 4(4) of the IDA, a person found guilty is liable on conviction on indictment to imprisonment for a term not exceeding 10 years or a fine, or both.

108 Under ibid s 8, personal information in relation to an individual includes full name; other names by which the individual is or has previously been known; gender; date and place of birth; external characteristics that are capable of being used for identifying the individual; the address of the principal place of residence in the UK; the address of every other place in the UK or elsewhere where the individual has a place of residence; current residential status; residential statuses previously held, such as nationality or entitlement to remain in the UK; and information about numbers allocated to the individual for identification purposes and about the documents, including stamps or labels to which they relate.

that is false, or that was improperly obtained, or that relates to someone else.[109]

TOWARDS ENHANCING THE CURRENT REGULATORY REGIME IN NIGERIA

Identity theft and financial-related crimes in banks and other financial institutions are, no doubt, a menace that has become widespread across national frontiers and is being addressed from several angles by all relevant stakeholders. In Nigeria and the UK, concerted efforts are being made through legislation as evident in the enactment of purposive laws, including the Nigerian CPPA 2015 and the UK Fraud Act 2006, to regulate evolving cases of identity theft and other related offences that the erstwhile traditional laws, such as the Nigerian Criminal Code did not effectively address.[110] Nevertheless, the following discussion

109 Under ibid s 6(2), a person found guilty is liable on conviction on indictment to imprisonment for a term not exceeding two years or a fine or both, while on summary conviction attracts imprisonment for a term not exceeding the maximum period or a fine not exceeding the statutory maximum or both. Identity documentation for the purposes of ss 4 and 6 includes any document that is or purports to be an immigration document; a UK passport; a passport issued by or on behalf of the authorities of a country or territory outside the UK or by or on behalf of an international organisation; a document that can be used, in some or all circumstances, instead of a passport; a licence to drive a motor vehicle; and a driving licence issued by or on behalf of the authorities of a country or territory outside the UK.

110 The relevant provisions of the Nigerian Criminal Code, s 382, for example, do not cover cases of identity theft as it restricts things capable of being stolen to '[E]very inanimate thing whatever which is the property of any person, and which is movable'. S 383 of the Criminal Code thus defines stealing as the act, by any person, of fraudulently taking anything capable of being stolen, or fraudulently converting to his own use or to the use of any other person anything capable of being stolen. Also, s 419 of the Criminal Code, which makes it an offence for any person to, by false pretence and with intent to defraud, obtain from any other person anything capable of being stolen, or induce any other person to deliver to any person anything capable of being stolen, is deficient in this regard. Given the provisions of ss 1 and 382 of the Criminal Code, although identity theft is a case of false representation, the identity of a person does not come under the category of things capable of being stolen under the Criminal Code. Similarly, under s 2(5) of the Fraud Act 2006, for example, prosecution for the offence of phishing, no longer requires the proof of deception or the obtaining of any property belonging to another hitherto required under s 15 of the Theft Act 1968. The offence is complete once a false representation is submitted in any form to any system or device designed to receive, convey or respond to communications with or without human intervention. Also, in *R v Gold & Schifreen* (1988) 1 AC 1063 (HL), for example, the defendants had hacked a remote computer system, the British Telecom's Prestel Service, by unauthorised use of passwords [*cont on 26*]

highlights possible areas where improvements could be made in the extant law in Nigeria through appropriate amendments thereof.

First, while acknowledging the fact that the Nigerian CPPA has specific provisions to criminalise identity theft, section 382 of the Criminal Code should be amended to cover cases of identity theft by extending property capable of being stolen to things in action and other intangible property as it is available under sections 1 and 4 of the Theft Act of the UK.

Also, section 19(3) of the CPPA, which places the onus of proof of negligence on the customer to prove that the financial institution in question could have done more to safeguard their information integrity, needs to be reviewed. Whenever a security breach occurs, an ordinary customer of a bank or financial institution is not ordinarily expected to know the extent of the security measures that have been put in place by the bank or the financial institution in question to prevent identity theft. The provision of paragraph 2.6.1.5 of the CBN CPF, which mandates financial institutions to promptly refund customers for actual amounts lost due to fraud with interest at the CBN prescribed rate unless it can be proved that loss occurred due to customer's negligence or through fraudulent behaviour, is preferable in this respect.

Nevertheless, it is gratifying to note that, while no provision was hitherto made in the NDPR or the CBN CPR on payment of compensation to victims of personal data breach, the NDPA, in section 48 thereof, has addressed the lacunae. The section has provided for payment of compensation to victims of data privacy breach, as is available under article 82(1) of the UK GDPR wherein the right of any person who has suffered material or non-material damage as a result of an infringement of the Regulation to compensation from the controller or processor for the damage suffered is guaranteed.

Furthermore, although the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is constitutionally guaranteed and protected under

---

[*n 110 cont*] and IDs of other users of the system. The ID and password were immediately cleared by the computer once authorisation for access had been granted. They had been charged under s 1 of the Forgery and Counterfeiting Act 1981 (UK) of uttering a false instrument. The prosecutor had appealed against the decision of the Court of Appeal to quash the conviction. The House of Lords dismissed the appeal and held *inter alia* that it was artificial to treat the creation of a temporary record held by the computer as the making of an instrument as defined in s 8(1) of the Act as the information was held only temporarily and neither recorded nor stored within the Act. According to the court, the language of the Act was not intended to apply to the situation which was shown to exist in the case. The accused persons were thus acquitted because there were no laws to prevent unlawful access to a computer.

section 37 of the Constitution of the Federal Republic of Nigeria 1999,[111] this right is, however, being constantly violated by identity thieves through unauthorised use of personal data of their victims to wreak financial and emotional havoc. There is the need, therefore, to ensure that public and private organisations involved in the collection, processing and storage of data are mandated by law to be continually adequately equipped with advanced security systems for the protection of personal information collected from the citizenry.

Moreover, there is the need for Nigerian policymakers to ensure that, in the implementation of the NDPA, issues relating to protection and processing of personal information of citizens, especially in the banking and financial sector of the economy, are addressed in a balanced manner that does not infringe the right to privacy of the citizens as enshrined in the Constitution. Although the NDPR had hitherto served as a stop-gap regulatory measure for the protection of personal data against identity theft, the enactment of the NDPA to further enhance the protection of personal information and the constitutionally guaranteed right to privacy of the Nigerian citizenry is, indeed, salubrious.[112]

CONCLUSION

Identity theft has become one of the fastest growing crimes across jurisdictions. The proliferation of online financial transactions, data breaches and malware attacks is continually exposing banks and other financial institutions' customers, as well as consumers of their services, to the risk of identity theft. While the law is, generally, available to prevent identity theft and punish identity thieves, it is important that preventive and deterrent measures are also put in place by all relevant stakeholders to stave off identity theft. In this regard, banks and other financial institutions should be enjoined to continually invest in advanced security systems as well as sophisticated means of authenticating their customers in order to assist customers in securing their identities. There is also the need to raise customers' awareness, especially among the older population who are not that tech-savvy, of the importance of their legal identity documents and the need to protect them from identity thieves. Similarly, the enforcement of the cashless policy of the Federal Government of Nigeria and its adoption by a large majority of the citizenry should be accompanied

111 See also art 8(1) of the Charter of Fundamental Rights of the European Union and art 16(1) TFEU which respectively provide that everyone has the right to the protection of personal data concerning themself.

112 See also, Protection of Personal Information Act 2013 (South Africa).

by massive enlightenment campaigns to sensitise bank customers to the importance of their personal and financial information and how to secure them against the onslaught of identity thieves.