ARTICLE:

Electronic Evidence in Nigeria

By **Timothy Tion**

'The ICT age has dawned, but not yet for all.'

(Kofi A. Annan)[1]

Electronic evidence is steadily assuming or has assumed a very important position in the adjudication of disputes or cases, be they criminal or civil. Anything done on the computer or the internet usually leaves traces or digital footprints which can serve as evidence in legal proceedings. Electronic evidence can therefore aid the investigation and solving of crimes by law enforcement agents. All this is possible because we are living in an age where most of the things we used to do manually are now done on computers, computer-like devices, or with the aid of computers and computer networks (such as the internet). For instance, using a debit card, the customer can use an Automated Teller Machine (ATM) to obtain access to their account, and to withdraw money anywhere in the world. With an internet-enabled cellphone, the customer can authorise the transfer of money to anybody anywhere in the world at any time, as well as making purchases using the same internet-enabled cellphone.

This article will highlight the importance of electronic evidence and why the Nigerian lawyer, to be considered to be competent, ought to be sufficiently literate in the technical issues regarding electronic evidence so as to understand and make use of electronic evidence. The article will conclude by recommending the inclusion of a core course on electronic evidence in the curriculum of legal education in Nigeria.

Examples of Electronic Evidence in Legal Proceedings in Nigeria

The law of evidence in Nigeria only recently made provision for the admissibility of computer generated or electronic evidence in Nigeria through section 84 of the Evidence Act 2011. Therefore, there is paucity of reported Nigerian cases touching on the admissibility of electronic evidence in Nigeria or the use of electronic evidence in legal proceedings. Be that as it may, this section of the article will make use of a few Nigerian cases which highlight the utility of electronic evidence in legal proceedings, and a news story which also highlights the many ways in which electronic evidence could be utilized.

Superior courts, unfortunately, in view of the recent age of the Act, are yet to make pronouncements on the application of section 84 of the Act. At the time of writing, only one case had been decided by the Supreme Court on the admissibility of electronic evidence. That is the case of *Dr Imoro Kubor v Hon. Seriake Henry Dickson*.[2] In this case, the appellants were challenging the election of the first respondent as the Governor of Bayelsa State in the February 2012 governorship election. At the Election Petition Tribunal, the learned counsel for the petitioner tendered a computer print-out of the online version of the Punch Newspaper, and another print-out from the web site of the Independent National Electoral Commission. Counsel for the respondents did not object to the tendering of the two documents, and they were admitted and marked as exhibits 'D' and 'L' respectively.

On appeal, the admissibility of the two exhibits was challenged on two grounds. First, that they were public documents which ought to have been certified, and second, that the documents having been tendered from the bar, evidence was not adduced to meet the foundational conditions stipulated in section 84(2) of the Act. It was contended that the documents ought to be expunged from the records. The Supreme Court agreed with these submissions, and held amongst other things, as follows:[3]

> 'Granted, for the purpose of argument, that Exhibits "D" and "L" being computer generated documents or e-documents down

[1] Former Secretary General, the United Nations; Forward to *E-Commerce and Development Report* (UNACD Secretariat, 2001), available at http://unctad.org/en/docs/ecdr2001_en.pdf.

[2] (2013) 4 NWLR (Pt.1345), 534.

[3] (2012) LPELR-9817(SC) at 48 – 50, paras F-E.

> loaded from the internet are not public documents whose secondary evidence are admissible only by certified true copies then it means that their admissibility is governed by the provisions of section 84 of the Evidence Act, 2011. … There is no evidence on record to show that appellants in tendering Exhibits "D" and "L" satisfied any of the above conditions. In fact they did not as the documents were tendered and admitted from the bar … A party that seeks to tender in evidence a computer generated document needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer must be called to establish the conditions set out under Section 84(2) of the Evidence Act, 2011. … Since appellants never fulfilled the pre-conditions laid down by law, Exhibits "D" and "L" were inadmissible as computer generated evidence/documents.'

Metadata

The story of Reno Omokri,[4] President Jonathan's Special Adviser on New Media, demonstrates in a little way the utility of electronic evidence. It was the metadata behind the data that exposed Mr Omokri, when he tried to undermine the former Central Bank of Nigeria Governor, Sanusi Lamido Sanusi. Reno Omokri using the pseudonym 'Wendell Simlin' and the e-mail address, wendellsimlin@yahoo.com, sent an e-mail on Wednesday, February 26, 2014 to several media organizations and bloggers. The e-mail sought to create a credible and logical chain of events between the suspension of the former Governor of the Central Bank of Nigeria (CBN), Mallam Sanusi Lamido Sanusi, and the recent upsurge in terror attacks in the northeast of Nigeria. The objective of the article[5] was to paint the former CBN governor as a major financier of Boko Haram and a veteran terrorist.

Since Sanusi's last place of work was the First Bank of Nigeria Plc before becoming the CBN governor, the author cleverly tried to link him to Alhaji Umaru Abdul-Mutallab, who was chairman when Sanusi was the CEO of the bank. It would be recalled that Alhaji Abdul-Mutallab is the father of Umar Farouk Abdul-Mutallab popularly referred to as the 'Underwear Bomber' who was convicted of attempting to detonate plastic explosives hidden in his underwear while on board a Northwest Airlines Flight en route from Amsterdam to Detroit, Michigan, United States on Christmas in Day in 2009. Wendell Simlin, therefore tried to portray Alhaji Abdul-Mutallab as a terrorist, hoping that the elder Abdul-Mutallab's previous relationship with Sanusi would make his argument more credible.

However, upon examination of the metadata of the document attached by Simlin in the e-mail, the name, 'Reno Omokri' showed in the place of 'Author', while 'Hewlett Packard' showed up as the computer used to prepare the document. A check of the IP address from which the e-mail was sent indicated that it was sent from the Kubwa area in Abuja by Galaxy Backbone, the Internet Service Provider which provides Internet hosting services for the Federal Government of Nigeria.[6]

Mobile Telephone cell site analysis

Whenever a mobile telephone makes a call, the call is routed through a cell site located at a fixed geographic location. Mobile telephone companies keep records of which cell site processes a call, and through this information law enforcement agents can locate the position of the SIM card, and therefore infer the location of the telephone user. This was used by the Nigerian Police to obtain the location of Timothy Dung, an armed robbery suspect in the case of *The State v Timothy Dung* (unreported).[7] The facts were that an armed robbery took place in which, amongst other things, the victim's car, handsets and SIM cards were stolen at gunpoint along the Gboko Road in Makurdi, Benue State. About two months later, a telephone call was placed to the victim's mobile telephone number, and it connected. The police were

[4] Feyi Fawehimi, Mr. Wendel Simlin, *Agùntáṣọ́lò*, 3 March 2014, http://aguntasolo.com/2014/03/03/mr-wendell-simlin/ .

[5] Ileowo Kikiowo, 'Boko Haram Sponsor Discovered In The Presidency', SaharaReporters.com, 28 February 2014, http://saharareporters.com/2014/02/28/boko-haram-sponsor-discovered-presidency-kikiowo-ileowo-0 .

[6] Ogala Emmanuel, 'Presidency under fire for cooking up document linking Sanusi to Boko Haram insurgency', Premium Times, 26 February 2014, http://www.premiumtimesng.com/news/155838-presidency-under-fire-for-cooking-up-document-linking-sanusi-to-boko-haram-insurgency.html .

[7] Benue State of Nigeria High Court, Ikpambese J, 12 July, 2013, suit no MHC/26C/2011.

informed, and with the aid of the network provider (who placed a tracker on the SIM card), they were able to ascertain the geographical location of the user of the SIM card. He was eventually arrested in Abuja. A search of his abode was carried out, and incriminating evidence, including the clothes he wore on the day of the robbery was discovered. That, coupled with his identification by the victim as one of the people who robbed him, and his inability to satisfactorily explain to the court his whereabouts on the day of the robbery and how he came to possess the SIM card of the victim, led to his conviction for armed robbery. He was sentenced to death. At the time of writing, Timothy Dung's appeal against the conviction is pending before the Court of Appeal in Makurdi, Benue State.

Youtube Video

In the Aluu 4 case, four students of the University of Port Harcourt were lynched by a mob in Omoukiri-Aluu, Port Harcourt. Some persons in the crowd used their mobile telephones to record the incident, and the video was uploaded to Youtube. The prosecution sought to tender the YouTube video of the lynching but the defence objected to its admissibility. The court overruled the objection and admitted the Youtube video download, stating that the video, irrespective of its source, was admissible in evidence based on its relevance to the trial.[8]

Theft from an ATM

Two cases illustrate the importance of electronic evidence in legal proceedings. The first case considered in this article is that of *Geoffrey Amano v United Bank for Africa (UBA) PLC.*[9]

Brief facts of the case

The claimant (Barrister Geoffrey Amano) was a customer of the defendant (UBA Plc). Mr Amano was issued with an ATM card for the operation of his savings account with the bank. On the 11 November 2009, he went to withdraw money and he discovered that the sum of N149,000.00 had been withdrawn from his account without his authorization between 6 November 2009 and 9 November 2009. However, the bank contended that the withdrawals were made by Mr Amano through the correct use of his ATM card and PIN, or that he had authorized unknown persons to do so with his ATM correct PIN.

Mr Amano contended that the bank failed in its duty of care owed to him, which resulted in the loss to him by the unauthorized withdrawal of the sum of N149,000.00 from his account. The particulars of negligence were that the bank failed to make its ATM fraud-proof; that it is only the bank that knew his ATM card number and PIN because it is used on the bank's machine; that it is the duty of the bank to protect the use of ATM card from being attacked by thieves, which remains its property; that it is the duty of the bank to carry out a thorough investigation to unearth the fraud perpetrated against the customer through the ATM card, and that the bank made it possible for unauthorized persons to break into the customer's account to steal his money.

On the other hand, the bank contended that it had at all times exercised reasonable measures to ensure best practice, and that no unauthorized persons have access to and or withdraws money from accounts of its customers including the claimant, and that the alleged withdrawals between 6 November 2009 and 9 November 2009 were all made by Mr Amano with his ATM and PIN. That the PIN was known only to him unless he had disclosed it to any such alleged unknown persons, or had been careless in handling his ATM card and PIN number leading to the alleged transactions. The bank also contended that the ATM card was fraud-proof, with adequate security features to protect its users such as Mr Amano.

Decision of the Court

The court held that based on the circumstance of the facts and evidence in the case, the withdrawal of the sum of N149,000.00 from the account of the claimant was unauthorized, and the bank, who has the duty of care to ensure that the funds of the customer in its custody are safe, and should only be withdrawn upon due authorization by the customer. The bank had failed in the discharge of its duty of care towards the Mr Amano, and was thus liable in negligence. The court therefore ordered the bank to refund the sum of N149, 000.00 that was withdrawn without the customer's authorization, and to pay to the Mr

[8] At the time of writing, the case was still being tried at Port Harcourt High Court, Rivers State. See Egufe Yafugborhi, 'ALUU 4: Court admits video evidence of murder scene', Vanguard, 31 October 2013, http://www.vanguardngr.com/2013/10/aluu-4-court-admits-video-evidence-murder-scene/ .

[9] Suit No: PHC/257/2011. The case is reported at page 114 of SLP (Section on Legal Practice) Law Journal Vol. 3, 2013. The SLP Law Journal is a publication of the Section on Legal Practice (SLP), Nigerian Bar Association (NBA).

Amano the sum of N3,000,000.00 as general damages for the untold hardship suffered for the unauthorized withdrawal of funds from his account. The court also ordered that there should be interest on the N149,000.00 part of the judgment sum at the current interest rate per annum from the 9 November 2009 to the date of the judgment and thereafter, the interest rate of 10 per cent per annum as allowed by the Rivers State High Court Rules 2010 on the entire judgment in the sum of N3,149,000.00 from the date of the judgment till the entire judgment sum is finally liquidated.

Observations

The witness for the bank (DW1) testified that the transactions of 6 November 2009 and 9 November 2009 were undertaken through the use of the ATM card and correct PIN of the customer. However, the witness failed to lead or give any credible evidence to show that the ATM card and PIN of the customer was used for the withdrawal. At this juncture it is apposite to reproduce an excerpt of the cross examination of DW1 below [at 140 – 141]:

Q: Exhibit A is ATM?

A: Yes.

Q: Is the Defendant still using this ATM?

A: No.

Q: Why did the Defendant stop its use?

A: We migrated to another platform.

Q: Why?

A: Because the Exhibit A had no name of the account holder on it.

Q: So the ATM- Card you use now has more security features?

A: No, the new ATM has better features.

Q: The better features are for the security of the customer?

A: No, it is for fast and better transaction.

Q: What are the security features of the ATM?

A: Once a customer inserts his ATM card with a wrong PIN number the ATM machine seizes it.

Q: How does UBA Plc, determine unauthorised withdrawals over which complaints are made?

A: Unless the customer compromises his PIN there can be no unauthorized withdrawal by ATM card.

Q: Look at Exhibit D, the Defendant admitted that fraudster can guess and use pin illegally?

A: Yes, but that is – usually through the internet.

Q: But the use of the internet is not in Exhibit D?

A: Yes, it is not there.

Q: So, since fraudster can get the pin number then unwarranted withdrawal can be made through ATM?

A: No the customer must have compromised his pin.

Q: It is common knowledge in banking that a fraudster can hack into the ATM Machines?

A: I am not aware.

Q: ATM machines has the capacity to capture footage of the machine?

A: Yes.

Q: Do you have the footage of the withdrawals on 6/11/2009 and 9/11/2009?

A: No, as the withdrawals were done at other Banks which do not have footage but used the journal to know the withdrawals on those dates.

Q: You did not have the pin used in those withdrawals?

A: No it is known only to the customer.

Q: You also do have anything to show that it was the same pin number of the ATM used that date?

A: No, as it was the same ATM Card that was used.

Q: Can fraudsters guess and use pin number of a customer and withdraw money?

A: No but a person can guess the pin number of a customer and withdraw money and that is why we usually advise [advice in the original] against the use of easy pin numbers such as date of birth.

The bank, in trying to prove that the disputed transactions were undertaken using the customer's ATM Card and PIN only tendered Exhibit D1 (a comprehensive statement of account of the customer with the bank) whose contents were rightly disbelieved or discredited by the learned judge, Hon Justice B. A. Georgewill as he then was, when he stated thus in his judgment [at 142 – 143]:

> '… for money allegedly withdrawn by the Claimant or his authorized person through his ATM Card with correct Pin number on 6/11/2009 and 9/11/2009, in Exhibit D1 not a single fact is stated or shown as to the Pin number used and DW1 did not lead any evidence as to how the Court can see and confirm the correct Pin number used as alleged by the Defendant.'

An ATM card is meant to contain within it what is referred to as an Application Transaction Counter (ATC). The ATC is incremented by one each time a transaction is carried out on the ATM. If the disputed transactions were done using Mr Amano's ATM card, then the ATC on it would have incremented accordingly.[10]

The ATM card of the customer should therefore have been subjected to a forensic analysis to establish whether the ATC had incremented or increased in accordance with each and every ATM transaction on the customer's statement of accounts, or whether there are any discrepancies. This piece of evidence coupled with other pieces of evidence such as possible ATM camera footage, transaction and event logs and error reports, ATM receipts (might have confirmed that cash was physically dispensed) and all the Authorization Request Cryptogram (ARCQ) information, would have gone a long way to establish whether the customer's ATM card and PIN were used by him or by someone else to make the disputed withdrawals. Every time a chip and pin or EMV card is inserted into an ATM, an ARQC is a generated and the Authorization Response Cryptogram is generated by the issuer (bank) in response to the ARQC. This response includes the decision by the bank on the authorization request and is sent back to the card for validation before the transaction is completed. The ARQC would therefore have shown whether the card's chip had been read by the machine.[11]

It is curious why the bank did not choose to follow the path highlighted above, but rather decided to tender only a statement of account which obviously cannot be used to prove that a particular ATM card and PIN was used to make a particular withdrawal. Perhaps if the defendant's lawyer was sufficiently aware of all the technical aspects involved in the workings of the ATM system and debits cards, he would have probably advised the defendant against the tendering of a mere printed statement of account to show that a particular debit card and PIN was used for a particular transaction.

The case of Geoffrey Amano therefore demonstrates the need for technical training among lawyers and legal practitioners in Nigeria, especially those involved in litigation. Legal practitioners in Nigeria need to become familiar with or educate themselves with computers and computer-like devices and software so as to be in a better position to handle cases involving or having elements of software. In other words, Nigerian lawyers must become reasonably knowledgeable about the topic. The failure to keep up-to-date with advances in technology and how it affects the law will sooner or later render a lawyer or legal practitioner irrelevant at best, negligent at worst, owing to the ubiquity of electronic communications and documentation, which in turn has elevated electronic evidence to a position of vital importance in modern day litigation.

[10] See generally Stephen Mason, *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong* (2nd edn, PP Publishing, 2014), and the web site of Alistair Kelman at http://www.alikelman.com .

[11] See Shojibur Rahman v Barclays Bank PLC, commentary by Stephen Mason and Nicholas Bohm, *Digital Evidence and Electronic Signature Law Review*, 10 (2013) 169 – 174; Shojibur Rahman v Barclays Bank PLC (on appeal from the judgment of Her Honour District Judge Millard dated 24 October 2012), commentary by Stephen Mason and Nicholas Bohm, *Digital Evidence and Electronic Signature Law Review*, 10 (2013) 175 – 187.

Second ATM case

The second case is that of *Benjamin Agi v Access Bank PLC* (2014) BNLR 23, on appeal to the Court of Appeal (reported on page 23, volume 7 of the Benue State Law Reports, 2014) from a decision of the High Court of Benue State, Makurdi (suit number MHC/15/2011), upholding the decision of the lower court. The brief facts of the case are taken from the headnote:

> 'The appellant, a Makurdi businessman dealing in wears, maintained a current account with the respondent at its Makurdi branch, Benue State. The respondent issued the appellant with an Automated Teller Machine (ATM) debit card with the number: 636088010026279443. The appellant activated and changed the secret Personal Identification Number (PIN) to his secret PIN and stated using same exclusively without sharing the card details with anybody whosever. On 03/10/2009, the appellant travelled to Onitsha to purchase wears for sale. Thereat, he drew a cheque of N70, 000.00, payable to himself, out of the credit balance of N95, 518.00 in his current account with the respondent. The operation officer of the respondent's branch at No. 14 New Market Road, Onitsha informed the appellant that he had no funds in the account, his money having been withdrawn through ATM transaction at the respondent's Fontana Service Station, Enugu. He was advised to return to Makurdi where the account was domiciled. The appellant on return to Makurdi, lodged a complaint on the issue to respondent's operation officer, Makurdi branch, but was given a remorseless reply. Sequel to these, the appellant, via his solicitors, wrote two letters demanding for a restoration of the sum of money in his account, damages and apology. The respondent replied the letters and denied liability. In the respondent's reply letter, it quoted and ATM debit card number different from the one issued to the appellant. The respondent's counsel contended that the said number was captioned or stated in error in the reply letter to the appellant.
>
> Consequent upon that denial, the appellant took out a writ of summons, before the Makurdi High Court, against the respondent on 19/01/2011, wherein, he claimed from the respondent an order crediting his account with N95,518.00, payment of N500,000.00 for loss of business gain/profit, N5,000,000.00 general damages and N150,000.00 as cost of the action. The action went through a full-scale trial and in a considered judgement delivered on 03/02/2011; the Makurdi High Court dismissed the appellant's suit in its entirety. Dissatisfied the appellant appealed to the Court of Appeal, Makurdi Division. However, the appeal was dismissed on the grounds that the appellant failed to prove that the respondent was negligent in failing to safeguard his funds and allowed unauthorized withdrawal of appellant's money with an ATM debit other that the one issued to the appellant by the respondent bank.'

Commentary

The appeal failed in this case because the appellant failed to plead the particulars of negligence or fraud (which was alleged),[12] and the appellate court concluded that the judgment of the trial court was justified, given the weight of evidence. In giving the main judgment, Ogbuinya JCA considered the merits of the appeal regarding negligence in the alternative.

Section 140 of the Evidence Act, 2011 provides that when a fact is within the knowledge of any person, the burden of proving that fact is upon that person. It therefore follows that it is for the bank and not the customer, to prove that a particular disputed transaction was done with the ATM debit card and PIN of the customer. Applying section 140 of the Evidence Act, 2011 to ATM transactions, the learned Senior Advocate of Nigeria, Emmanuel C. Ukala, stated:[13]

> 'Where a customer asserts that he has sufficient funds in his account based on his deposits and perhaps his record of

[12] It is suggested that the appellant ought to have put in a set of pleadings in accordance with the sample Particulars of Claim set out in Stephen Mason, *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong*, at Appendix 5. The bank would have had to produce far more evidence, and there might have been a greater opportunity of illustrating the problems facing banks regarding ATMs – providing, that is, the lawyers were sufficiently aware of the technical issues.

[13] Emmanuel C. Ukala, 'ATM Fraud: Burden and Standard of Proof', SLP (Section on Legal Practice) Law Journal, Vol. 3, (2013), 66.

> transaction, the bank as its debtor within whose peculiar knowledge the record of the dissipation of the fund resides has the burden of proving how the fund was dissipated and that it observed its duty of care to the customer throughout the period.'

The learned author further states that:

> 'Generally a customer of a bank who suffers loss arising from an ATM fraud asserts no more than that the bank is his debtor and that he has demanded for his debt from the bank but that the bank in breach of their contract has failed to pay him. In other words, the customer needs to do no more than to show that he maintains an account which by his own reckoning is in funds, but from which funds, the bank has failed to meet its obligation to the customer as the banks creditor … the fact that the bank is a debtor to its customer with regard to the amount deposited by the customer into his account cannot be disputed. In those circumstances therefore, we submit that the burden shifts under section 132(2) of the Evidence Act 2011 to the bank to prove how the customer's account went into debit since its failure to do so would render it liable to judgment for the recovery of the debt which the customer rightfully asserts against it.'

It is suggested above that a computer print-out or statement of account which asserts that money was withdrawn at a particular location via an ATM debit card is not enough evidence to show that it was a particular ATM debit card that was used for a transaction. Evidence should therefore have been led by the respondent bank in the case under review to show that it was the appellant's ATM debit card and PIN that were used to make the disputed transactions. Nevertheless, it should be borne in mind that a PIN can also be forged.

It seems in this case that the ATM debit card used for the disputed transaction was not the same as that issued to the appellant. Ogbuinya JCA went on to hold thus, at 38:

> 'It is true that the ATM debit card number quoted therein (respondent's reply letter to appellant), 63608801002554589, is, clearly, irreconcilable with 636088010026279443 embossed on exhibit A [the ATM debit card]. However, as already noted, withdrawals by dint of ATM debit card are executed by secret PINs not the numbers inscribed on the cards. Were it to be otherwise, the respondent would have been held responsible for that withdrawal – a flagrant breach of its duty to shield appellant's funds from scrupulous third parties.'

In making the above observation, the court seemed to be oblivious of the fact that ATM systems are not without flaws, and it is technically possible for a thief to exploit the weaknesses in the ATM system and fool the software in the ATM into accepting any PIN keyed into the ATM as the correct PIN.[14]

It is partly true that 'withdrawals by dint of ATM debit card are executed by secret PINs not the numbers inscribed on the cards'; however, all ATM debit cards have different or unique numbers embossed on them. These numbers are referred to as the primary account number (PAN) which identifies the card issuer and the particular cardholder account. The PAN uniquely identifies each ATM debit card and so no two cards have the same PAN. Therefore, if the respondent bank in its reply quoted an ATM debit card number or PAN that belongs to the ATM debit card that was used for the disputed withdrawal, and the PAN is different from the PAN on the ATM debit card issued to the appellant, it is evidence that it is the ATM debit card whose PAN was quoted by the respondent bank in its reply letter that was used for the disputed transaction, and not that of the appellant. The Supreme Court of Lithuania in the case of *ZS v Lietuvos taupomasis bankas* (No. 3K-3-390/2002) observed that:[15]

> 'The bank must ensure the protection of payment cards against fraud. The bank bears the risk that the payment will be made with a fraudulent card or a substitute of the original card.'

In this case, it appears the disputed payment or withdrawal was probably made by an unauthorized person with a fraudulent ATM debit card or a substitute of the original card issued to the appellant.

[14] Stephen Mason, *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile and online banking: your rights and what to do when things go wrong*, Chapter 3 'How thieves steal from ATMs and other devices'.

[15] Ž.Š. v Lietuvos taupomasis bankas, Civil case No. 3K-3-390/2002, Supreme Court of Lithuania, *Digital Evidence and Electronic Signatures Law Review*, 6 (2009) 255 – 262, at 258.

Since it was not the appellant's ATM debit card that was used to make the disputed withdrawal, the court should have held the bank liable in negligence for failing to safeguard appellant's funds in its custody.

By allowing an unauthorized person using an ATM debit card with a PAN other than the one on the card issued to the appellant to withdraw funds, the respondent bank was negligent in safeguarding the appellant's funds in its custody for safekeeping and it therefore breached the duty of care it owed to the appellant. The evidence was that the bank, in a letter to the appellant, stated that the PAN of the ATM debit card that was used for the disputed transaction was different from the PAN of the card issued to appellant. However, the respondent's counsel contended that the PAN was 'captioned' or stated in error in the letter to the appellant.

It appears the court did not agree with the contention of the respondent's counsel on the issue of the PAN being stated in error, and therefore accepted that it was an ATM debit card other than the one issued to the appellant that was used for the disputed transaction. Instead of holding the respondent bank liable for the unauthorized withdrawals, it rather curiously held that the transaction took place because the correct PIN was allegedly used, in the absence of any further technical evidence by the bank.

This case further demonstrates the lack of clear understanding of the technical issues concerning the workings of ATM systems and internet banking. This can be inferred from the statement of Ogbuinya, JCA on page 41 of the report, where he stated 'It is decipherable from the evidence of DW2 that the new verve ATM debit card is equipped with cameras that capture users.' With the greatest respect to His Lordship, ATM debit cards do not have cameras installed, although some ATMs do have or are supposed to have cameras that record the images of users. In fact the Central Bank of Nigeria Standards and Guidelines on Automated Teller Machine (ATM) Operations in Nigeria[16] provides, at 3.4(a) that:

> 'Every ATM shall have cameras which shall view and record all persons using the machines and every activity at the ATM including but not limited to: card insertion, PIN entry, transaction selection, cash withdrawal, card taking, etc. However, such cameras should not be able to record the key strokes of customers using the ATM.'

With this lack of understanding, it makes it difficult for counsel and members of the judiciary to adequately and fairly litigate and adjudicate disputed ATM and electronic banking transactions. This case appears to be the quintessence of a case that demonstrates the need for technical training among legal professionals in Nigeria. In this particular case the lack of clear understanding of the technical issues involved in the workings of the ATM system was probably damaging to the case of the appellant.

Recommendation

Bearing in mind the increasing ubiquity and significance of electronic evidence as has been illustrated or highlighted above, it is time that the Council of Legal Education and the National Universities Commission found a way to introduce the teaching of electronic evidence in Nigerian universities as a core course, because as a core course any student who fails it would not be able to graduate. This should therefore encourage or compel law students (as potential lawyers and legal practitioners) to acquire knowledge of computers and computer-like devices.

The need for lawyers to become proficient in electronic evidence cannot be overemphasized. This is illustrated by the comments of Combs, J in an appeal by Samuel A. Crabtree before the Kentucky Court of Appeal:[17]

> '… this case demonstrates a need for technical training among legal professionals. There were several instances during the trial when it appeared that counsel for each party attempted to elicit testimony from the experts but failed because of confusion of technical terms. In this particular case, the evidence of guilt was overwhelming, but we anticipate that this communication gap could be damaging in cases with weaker evidence.'

[16] Available at http://www.cenbank.org/OUT/2010/CIRCULARS/BSPD/ATM%20STANDARDS%201.PDF .

[17] *Samuel A. Crabtree v. Commonwealth of Kentucky*, 2012 WL 3538316 (Ky.App.).

The author therefore commend to the National Universities Commission and the Council of Legal Education, the words of Denise H. Wong in her article 'Educating for the future: teaching evidence in the technological age':[18]

> 'The advent of the technological age has had significant effect on litigation practice, none more so than in the area of evidence gathering and presentation in court. A significant proportion of evidence that is gathered for both criminal and civil matters is now electronic in nature, and this necessitates a change in the way that lawyers think and advise on evidential issues … rather than simply focusing on principles relating to the admissibility of evidence in court, the traditional course on evidence law should be modified to equip students with an intellectual framework that conceives of electronic evidence in litigation as an entire process. This process begins with the gathering and forensic examination of electronic evidence, and is followed by the admissibility of such evidence in court, ending with the effective presentation of the evidence before a judge or jury … taking such an approach, the law teacher would be playing the role of effective gatekeeper to the legal profession by providing a course that is both intellectually rigorous and adequately prepares would-be litigators for the realities of modern day practice.'

It may not be entirely accurate to state that 'a significant proportion of evidence that is gathered for both criminal and civil matters is now electronic in nature' with regards to Nigeria at present. However, we live in a globalized world, and sooner rather than later the above will also be true of Nigeria. For this reason it requires those responsible for the education of potential lawyers in Nigeria to prepare would be lawyers and legal practitioners for the inevitability of the future – which is not very far away. Not doing so would be tantamount to negligence. The fact is that 'new sources of electronic data (evidence) are constantly being created, such as instant and text messaging. Given the constant change in this area, it is important for lawyers to keep current on evolving technologies.'[19] Electronic evidence takes many forms, including email, text message, internet activity, images, and more of this type of evidence is gradually becoming more ubiquitous – it is certainly used in all of the common law jurisdictions.[20]

This article has attempted to highlight the significance of electronic evidence and why it should be included in the legal curriculum of Nigerian universities and why Nigerian lawyers and legal practitioners should receive a basic education in electronic evidence in order to understand electronic evidence in settling legal disputes.

Timothy Tion attended the Benue State University and Nigerian Law School where he obtained an LL.B and BL respectively. He is a lawyer with Bem Hanaze & Associates, Makurdi, Benue State, Nigeria. He is interested in the convergence of law and ICT and maintains a blog at http://cyberlawmusings.blogspot.com.

[18] Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', *Digital Evidence and Electronic Signature Law Review*, 10 (2013), 17.

[19] 'Notes of Advisory Committee on 2006 FRCP Amendments' cited in Mark Krotoski, 'Effectively Using Electronic Evidence Before and At Trial', United States Attorneys' Bulletin, Vol. 59 no. 6, November 2011, 52 – 72, 52.

[20] See Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).