

IN THE FEDERAL HIGH COURT
IN THE ABUJA JUDICIAL DIVISION
HOLDEN AT ABUJA

CHARGE NO: **FHC/201/C/2026**

BETWEEN

THE STATE.....COMPLAINANT

AND

MUSA EMEKA AYO.....DEFENDANT

PROSECUTION’S CLOSING ADDRESS

1.0. INTRODUCTION

- 1.1. Your Lordship, at the close of both the Prosecution’s and the Defendant’s case, the Prosecution respectfully submits that it has successfully proved, beyond reasonable doubt, the offences with which the Defendant is charged and relies on the evidence adduced along with the legal arguments put forth below in firm support of its position.

2.0. STATEMENT OF FACTS

- 2.1. The Defendant, Ms. Aisha Ngozi Kemi, is a high-profile cybersecurity expert in the employ of AJOBOY systems – I.T. systems engineers and service providers to Rhapsody Bank (the bank).
- 2.2. In January 2025, she discovered a critical “backdoor” in the digital vault of the bank, which could allow anyone to alter the Social Security Number (SSN) linked to bank accounts.
- 2.3. Instead of immediately reporting to her employers Aisha:
- 2.3.1. Accessed the bank’s mainframe to demonstrate its vulnerability, accidentally downloading the Know Your Customer (KYC) data of 5,000 high-net-worth individuals.

- 2.3.2. Sent an anonymous email to the Bank CEO demanding a “consultancy fee” of N50 Million to disclose the location of the “backdoor” and delete the downloaded data.
- 2.4. The bank promptly alerted the Department of National Security and Aisha was arrested. Investigators subsequently found in her apartment N200 Million in cash and three Bitcoin hardware wallets, despite her having no record of formal employment for three years.
- 2.5. The State charged her under Section 6 & 24 of the Cybercrimes Act (as amended in 2024) for unauthorized access and cyberstalking/extortion. The State also filed an ex parte application under Section 9 of the Proceeds of Crime (Recovery and Management) Act 2022 for a Preservation Order on her apartment and the N200 Million, on the grounds that they amounted to “unexplained wealth” and likely “proceeds of unlawful activity.”
- 2.6. Upon conclusion of trial, the Prosecution now brings this closing address before Your Lordship.

3.0. OFFENCES ALLEGED

- 3.1. Unauthorized access of a computer system under Section 6 of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 as amended.
- 3.2. Extortion and cyberstalking under Section 24 of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 as amended.

4.0. ISSUES FOR DETERMINATION

- 4.1. The Prosecution hereby formulates the following issues for determination by your Lordship:
 - 4.1.1. Whether mens rea is present where a professional in the course of her duty to troubleshoot potential problems, “accidentally” accessed and downloaded sensitive data like KYC data?
 - 4.1.2. Whether the anonymous demand for a “consultancy fee” in exchange for disclosing a security flaw is not established by the fact that Aisha is living a lifestyle in excess of legitimate income and whether the demand if traced to Aisha does not constitute the offence of Cyberstalking or Extortion under Section 24 of the amended Cybercrimes Act?
 - 4.1.3. Whether a Preservation Order can be validly maintained over the Defendant’s assets under Section 9 of the Proceeds of Crime (Recovery and Management) Act 2022, on the basis of ‘unexplained wealth,’ before the underlying criminal charges of cybercrime have been proven?

5.0. LEGAL ARGUMENTS

5.1. WHETHER MENS REA IS PRESENT WHERE A PROFESSIONAL IN THE COURSE OF HER DUTY TO TROUBLESHOOT POTENTIAL PROBLEMS, “ACCIDENTALLY” ACCESSED AND DOWNLOADED SENSITIVE DATA LIKE KYC DATA?

5.1.1. On this issue, the Prosecution submits, unequivocally, that Ms. Aisha’s claim that her accessing and downloading of sensitive KYC data of customers of Rhapsody Bank as “accidental” in the course of her professional duty does not affect the mens rea of the offence of unauthorized access as contained in Section 6 of the Cybercrimes Act.

5.1.2. Section 6 of the Act provides thus:

“(1) Any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment.

(2)Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information, the punishment shall be imprisonment for a term of not more than 7 years or a fine of not more than N7, 000,000.00 or to both such fine and imprisonment.”

5.1.3. From the above, it can be gleaned that for an accused person to be convicted of the offence of unauthorized access, they must do so “intentionally”. The question that thus behooves this Court is two-fold: (a) when can an act be said to have been done “intentionally”; and (b) can Ms. Aisha claim that her unauthorized access in the present case was not intentional?

5.1.4. For an accused person to be convicted of an offence, the Prosecution bears the burden of establishing both the actus reus (guilty act) and the mens rea (guilty mind) of the Defendant. Where either of these elements are unsuccessfully established beyond reasonable doubt, it is settled law that the accused person would be entitled to an acquittal.

5.1.5. In **Njoku v State**,¹ mens rea was defined by the Supreme Court as being “*the criminal intent or guilty mind of the accused.*” The Supreme Court further noted that for the Prosecution to establish a criminal act against an accused person, “*it must go beyond establishing the commission of the unlawful criminal act by the accused and establish that the accused had the correct legal criminal mind of committing the act. The two must co-exist, whether explicitly or by necessary implication.*”²

5.1.6. In the present case, Ms. Aisha alleges that her accessing and downloading of the sensitive data of over 5000 high net worth customers of Rhapsody bank was an “accident”. The Prosecution, in vehement opposition, submits that:

- A. The evidence adduced before this Court does not support a conclusion that the Defendant’s conduct was not deliberate; and
- B. Even assuming that the downloading of the data themselves was accidental, the Defendant’s conduct of accessing is sufficient to establish the mens rea of the offence of unauthorized access.

A. The evidence adduced before this Court does not support a conclusion that the Defendant’s conduct was not deliberate

5.1.7. On this point, the Prosecution submits vehemently, that taking into account the Defendant’s experience and skill as well as her conduct immediately preceding and succeeding the download under consideration, the Defendant cannot be construed as having undertaken her actions any other way but deliberately and in full awareness of what it was she was actually doing.

5.1.8. Ms. Aisha is not new to computers or network systems. As noted in para 2.1 of the Facts, the Defendant was, at the time of the Rhapsody Bank incident, a “*high profile cybersecurity expert*” engaged under the employ of Ajoboy Systems, a prominent IT firm of engineers and service providers.³

5.1.9. The high profile nature of her work and the fact that she was skilled enough to be considered an “expert” in her field means that Ms. Aisha was a consummate professional expected to understand the nuances of complex computer and network systems. Simple access and download (actions capable of being

¹ Njoku v State (2013) 2 NWLR (Pt. 1339) 548

² Njoku v State (supra)

³ Statement of Facts, para 2.1

carried out by non-tech-inclined individuals) would have been well within her knowledge and skillset.

- 5.1.10. Taking her professional background into account, the Prosecution submits that the Defendant's assertion that her downloading of sensitive user data was "accidental" either means that (i) the Defendant was incompetent at her role; or more likely, (b) that the Defendant was simply attempting to mislead the Court and avoid due criminal punishment.
- 5.1.11. Your Lordship, it must be noted that downloading the KYC data of 5,000 high-net-worth individuals is not a simple, one-click operation. It requires, navigating through security protocols, locating the relevant database, selecting the data fields, initiating the download process and storing the data on personal devices. Each of these steps requires deliberate, conscious action. For the Defendant to claim that she "accidentally" performed all these steps while troubleshooting is laughable and must be rightly discountenanced by this Court.

B. Even assuming that the downloading of the data themselves was accidental, the Defendant's conduct of accessing is sufficient to establish the mens rea of the offence of unauthorized access.

- 5.1.12. Your Lordship, even if this Honourable Court were, *arguendo*, to accept the Defendant's assertion that the downloading of the KYC data was accidental, the Prosecution submits that Ms. Aisha's actions up to the unauthorized access of the system would still be sufficient to ground a conviction for the offence of unauthorized access. This submission is premised on the crucial fact that the offence under *Section 6 of the Cybercrimes Act* is fundamentally anchored on the intentional unauthorized access, and not merely the subsequent handling of the data obtained.⁴
- 5.1.13. A careful reading of Section 6(1) of the Act reveals that the gravamen of the offence lies in the act of intentionally accessing a computer system or network without authorization. The obtaining of data, while relevant, is ancillary to the primary wrongful act of access. Thus, once it is established that the Defendant

⁴ See Cybercrimes (Prohibition, Prevention, Etc.) Act, s 6

deliberately gained access to the bank's digital vault without authorization, the requisite mens rea is complete.

- 5.1.14. In the instant case, the Defendant admits to accessing the bank's mainframe in order to "demonstrate vulnerability." This admission alone is sufficient to establish that the access was intentional and conscious on the part of the Defendant, and not inadvertent. The Defendant cannot further attempt to hide beyond the cloak of employment to claim good intentions. The law does not recognize a defence of "good intentions" when the access itself was, at the time it was done, unauthorized. Accordingly, whether the Defendant's ultimate objective was to expose a flaw or otherwise is immaterial to the determination of liability under Section 6.
- 5.1.15. Furthermore, Your Lordship, the Defendant's conduct subsequent to the access—particularly the anonymous demand for the sum of ₦50,000,000 in exchange for disclosure of the vulnerability and deletion of the data⁵—clearly demonstrates that the access was not merely deliberate, but was part of a broader scheme aimed at defrauding the Bank. This subsequent conduct reinforces the inference that the initial access was undertaken with full knowledge of its unauthorized nature.
- 5.1.16. It is therefore submitted that the Defendant cannot seek refuge under the guise of accidental downloading when the foundational act of unauthorized access was intentional. In law, once the mental element attaches to the principal act constituting the offence, any purported accident in the downstream consequences does not negate criminal liability.
- 5.1.17. In the final analysis on this issue, the Prosecution respectfully submits that the totality of the evidence before this Honourable Court irresistibly points to the conclusion that the Defendant acted with the requisite mens rea. The defence of accident is not only unsupported by the evidence but is also legally untenable in the circumstances. We therefore urge Your Lordship to resolve this issue in favour of the Prosecution.

5.2. WHETHER THE ANONYMOUS DEMAND FOR A "CONSULTANCY FEE" IN EXCHANGE FOR DISCLOSING A SECURITY FLAW IS NOT ESTABLISHED

⁵ Statement of Facts, paras 2.3.1 – 2.3.2

**BY THE FACT THAT AISHA IS LIVING A LIFESTYLE IN EXCESS OF
LEGITIMATE INCOME AND WHETHER THE DEMAND IF TRACED TO
AISHA DOES NOT CONSTITUTE THE OFFENCE OF CYBERSTALKING OR
EXTORTION UNDER SECTION 24 OF THE AMENDED CYBERCRIMES ACT?**

5.2.1. On the second issue, the Prosecution submits without equivocation that Aisha's living of a lifestyle in excess of her legitimate income combined with other relevant circumstantial facts, is sufficient to establish her guilt vis-à-vis the anonymous demand for a "consultancy fee". The Prosecution further submits that having established the culpability of the accused in the making of the anonymous demand, that the act is sufficient to establish the offence of extortion under *Section 24 of the Cybercrimes Act*. For purposes of organizational clarity, the Prosecution's argument shall be broken into two:

- A. The Prosecution can rely on circumstantial evidence, including the lifestyle of the Defendant in excess of her legitimate income, as proof of the Defendant's guilt.
- B. That having established the culpability of the accused vis-à-vis the sending of the anonymous demand, the Defendant's actions are sufficient to constitute the offence of extortion under Section 24 of the Cybercrimes Act.

5.2.2. Both limbs of this argument shall be addressed *seriatim*.

A. The Prosecution can rely on circumstantial evidence, including the lifestyle of the Defendant in excess of her legitimate income, as proof of the Defendant's guilt

5.2.3. On the first point, the Prosecution submits that it is a settled principle of law that where there exists no direct evidence in proof of the Defendant's culpability in the commission of a criminal offence, circumstantial evidence can be relied upon in proving the guilt of the accused.

5.2.4. In *Shofolahan v. State*,⁶ the Court of Appeal clarified, unequivocally, that "*the guilt of an accused can be established beyond reasonable doubt by circumstantial evidence.*" The only requirement for reliance upon such evidence in the grounding of a conviction is that the evidence must be "*compelling and unequivocal*".

⁶ *Shofolahan v. State* (2013) 17 NWLR (Pt. 1383) 281

5.2.5. In **Nwalu v State**,⁷ the Supreme Court eloquently explained this position of law where it explained thus:

“Where there is no eye witness account or direct evidence of the commission of an offence, a conviction may be based on circumstantial evidence. However, such circumstantial evidence must point to only one conclusion, namely, that the offence had been committed and that it was the accused person who committed it.”

5.2.6. Taking the above judicial expositions into account, it is clear circumstantial evidence is sufficient to establish the guilt of an accused where it points, irresistibly, to the conclusion that the offence had been committed and that it was the accused person who committed it. The Prosecution submits that from a careful examination of the evidence as tendered before this Honourable Court, your Lordship can (and should) reach a determination that the totality of the circumstantial evidence points to one irresistible conclusion: that the offence of extortion was actually committed and that it was the Defendant, Ms. Aisha, who committed it.

5.2.7. Before this Court lies multiple pieces of incriminating evidence. First, a search of the Defendant’s apartment uncovered 200 million Naira in cash and three Bitcoin hardware wallets despite her having, crucially, *“no record of formal employment for three years.”*⁸ Two things immediately raise a strong wave of suspicion against the Defendant’s increasingly shaky ship of lies. First, the amount, 200 million Naira, is far beyond what can be explained from the Defendant’s legitimate income drawing the inference that it must constitute the proceeds of crime or have been derived from the conduct of unlawful activity.

5.2.8. As the onus of rebutting this presumption of unlawful activity would lie solely on Aisha (the sources of her income being a fact completely within her knowledge,⁹ the failure of the Defendant to tender any evidence in explanation

⁷ Nwalu v State (2018) 14 NWLR (Pt. 1638) 159

⁸ Statement of Facts, para 2.4

⁹ Evidence Act 2011, s 139

of this unusual wealth acts in firm support of the Prosecution's case. The second thing about the money found in Ms. Aisha's home which raises suspicion is the fact that the large amount of money, 200 million Naira, was found in cash. Your Lordship would agree that it is highly unusual that such a large sum of money would be kept in cash at home rather than safely in the Bank. A possible explanation for this apparently irrational behaviour is that if the money were in fact proceeds of criminal activity, depositing it at a financial institution would have, due to its size, been sufficient to trigger its mandatory reporting to the Nigerian Financial Intelligence Unit. As an expert in financial cybersecurity, the Defendant would have known this.

5.2.9. While incredibly suspicious in itself, the circumstantial evidence linking the accused to the commission of the crime does not end here. Further damning proof of her complicity is the fact that, at the time the anonymous demand was made, the Defendant was the only person to the knowledge of this Court who had downloaded and accessed 5000 records. As the demand stated that it would not only "show" but also "delete" already downloaded data, the only person who could have made the anonymous demand must have been someone who had previously downloaded sensitive KYC data.

5.2.10. As the fact that the Defendant did in fact download the sensitive KYC data of Rhapsody Bank customers is not in contention and remains uncontradicted by the Defendant, the Prosecution submits that this fact places the Defendant as the only person capable of making such an anonymous demand. Further taking into account the Defendant's skill as a "high profile" cybersecurity expert and the fact that she already had access to Rhapsody's systems, it becomes impossible to come to anything but one irresistible conclusion: that Rhapsody Bank's systems were unauthorizedly accessed, and that it was the Defendant who did it.

A. **That having established the culpability of the accused vis-à-vis the sending of the anonymous demand, the Defendant's actions are sufficient to constitute the offence of extortion under Section 24 of the Cybercrimes Act**

5.2.11. Pursuant to Section 24(2)(b) of the Cybercrimes Act, "*Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network – (b) containing any*

threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value commits an offence under this Act....”¹⁰

5.2.12. In other words, once a person (i) knowingly transmits a communication through a computer system or network; in order to (ii) extort from any person, firm, association or corporation, any money or other thing of value, they commit the offence of extortion. The Prosecution submits in the present case that Ms. Aisha’s conduct fulfills both elements of the offence and that, consequently, she is guilty of the offence of extortion under Section 24 of the Act.

5.2.13. On the first element, as the Defendant sent an “anonymous email”, a communication which must pass through email servers to reach the recipient, the communication made by the Defendant fulfills the condition of constituting a communication made through “a computer system or network”.

5.2.14. On the second element, the fact that the anonymous communication contained a demand effectively ordering the Bank to send 50 million Naira in order to be shown the security vulnerability of its systems and safeguard the data of its customers conclusively fulfills the second condition of the communication being to extort *money or a thing of value* from a corporation.

5.2.15. Resting on the arguments put forth and the authorities cited, the Prosecution submits that there exists sufficient evidence before this Court to find the Defendant guilty of the offence of extortion pursuant to Section 24 of the Cybercrimes Act. It is so submitted.

5.3. **WHETHER THE PRESERVATION ORDER CAN BE VALIDLY MAINTAINED OVER THE DEFENDANT’S ASSETS UNDER SECTION 9 OF THE PROCEEDS OF CRIME (RECOVERY AND MANAGEMENT) ACT 2022, ON THE BASIS OF ‘UNEXPLAINED WEALTH,’ BEFORE THE UNDERLYING CRIMINAL CHARGES OF CYBERCRIME HAVE BEEN PROVEN?**

5.3.1. On this issue, it is the Prosecution’s humble yet fervent submission that a preservation order can be validly maintained over the Defendant’s assets

¹⁰ Cybercrimes Act, s 24(2)(b)

pursuant to Section 9 of the Proceeds of Crime (Recovery and Management) Act 2022 given the circumstances of the present case.

- 5.3.2. The Prosecution anchors its submission on the express provisions of section 9(1) of the Proceeds of Crime (Recovery and Management) Act 2022. For purposes of mathematical exactitude and judicial clarity, Section 9(1) of the Act provides thus:

*“A preservation order shall be granted by the Court to preserve property reasonably suspected to have been derived from unlawful activities and represents instrumentality of unlawful activity or unclaimed property.”*¹¹

- 5.3.3. Subsection (3) further provides that shall make the Order where there are reasonable grounds to believe that the property concerned “(a) *represents the proceeds of unlawful activity, whether they are—(i) in the hands of the person who unlawfully acquired the property in the first instance, or (ii) traced to any person to whom the property that represents the proceeds have been passed ; (b) is involved in the facilitation of unlawful activity ; or (c) is intended to be used to facilitate unlawful activity.*”

- 5.3.4. It is not in the discretion of the Court to decide whether or not it should grant a preservation order. Once a valid ex parte application under Section 9 is made to the Court showing that the conditions delineated under Section 9(3) have been fulfilled, the Court possesses a mandatory obligation (“shall make an order”) to preserve the property of the Defendant pending the determination of the dispute.

- 5.3.5. It is a fundamental principle of the Proceeds of Crime (Recovery and Management) Act 2022 that a Preservation Order is an interim, protective measure. Therefore, the validity of such an order is not dependent upon a prior criminal conviction. In ***Melrose General Services Ltd v. Economic and Financial Crimes Commission***,¹² the Supreme Court held that a preservation order can be maintained against a reasonably suspicious property pending the determination of the substantive suit.

¹¹ Proceeds of Crime (Recovery and Management) Act, s 9(1)

¹² *Melrose General Services Ltd v. Economic and Financial Crimes Commission* (2025) 1 NWLR (PT. 1972) 1

- 5.3.6. The court further emphasized that the state only need show "reasonable suspicion" to maintain preservation orders, and the owner must then "show cause" to release them. Furthermore, in *Dangabar V. F.R.N*¹³ the court held that an interim order for the preservation of assets is obtainable immediately after the commencement of the investigation and to last till final determination of the criminal charge that may be initiated against the accused person.
- 5.3.7. Your lordship, from the foregoing it is apparent that Section 9 of the Act is designed to freeze assets that are reasonably suspected to be proceeds of unlawful activity to prevent their dissipation and it does not need the determination of the substantive charge to be valid. In *Olatunji v. Owena Bank Plc.*¹⁴ the court of appeal while stating the rationale for a preservation order held as follows: *The reason for this is to ensure that any final order the court may make in relation to the res does not expose the court to a state of helplessness, leaving the victorious party to enjoy a mere empty victory.*
- 5.3.8. Your Lordship, unlike a forfeiture order following a conviction, a preservation order is a rems proceeding focused on the property itself. The State only need establish a prima facie case that the property is linked to criminal conduct, not prove the underlying cybercrime beyond a reasonable doubt at this interlocutory stage.
- 5.3.9. Furthermore, on the Defendant's unexplained wealth, paragraph 2.4 of the Statement of Fact reveals that the defendant was found in possession of 200 Million Naira in cash and three Bitcoin hardware wallets despite having no record of formal employment for three years.
- 5.3.10. By section 9(1) of the Act, the law is trite that what is required for the grant of preservation order pursuant to the section is reasonable suspicion that the asset in question is a proceed of unlawful activity or unclaimed property. The discovery of these assets in the immediate aftermath of an extortion attempt (the 50 Million "consultancy fee" demand) creates a nexus between the Defendant's conduct and the assets.
- 5.3.11. Under the POCRMA, where a person is in possession of "unexplained wealth" that cannot be justified by their legitimate sources of income, the law permits

¹³ Dangabar V. F.R.N (2014) 12 NWLR (PT. 1422) 575

¹⁴ Olatunji v. Owena Bank Plc. (2002) 5 NWLR (PT. 760) 325 (P.337, paras. C-D)

the State to preserve such assets pending the determination of their origin. To hold otherwise would allow the Defendant to deplete potentially tainted funds before the conclusion of a trial. See *Sotuminu v. Ocean Steamship (Nig) Ltd.*¹⁵

- 5.3.12. The Preservation Order is a necessary tool for the administration of justice. It does not determine the final guilt of the Defendant but ensures that the Republic's ability to recover proceeds of crime is not frustrated by the passage of time or the concealment of assets. As it would be unjust to allow the Defendant to continue to enjoy the use of potentially unlawfully obtained assets, the Prosecution submits that a preservation order pursuant to Section 9 of the Proceeds of Crime (Recovery and Management) Act can be validly maintained in the present case. It is so submitted.

6.0. CONCLUSION

- 6.1. It is based on the arguments canvassed above that the Prosecution prays this Honourable Court to find the distilled issues in favour of the Prosecution and regard the evidence tendered by the Prosecution as sufficient in establishing the offences alleged against the Defendant beyond reasonable doubt.

7.0. INDEX OF AUTHORITIES

7.1. Cases Cited

- 7.1.1. Dangabar v Federal Republic of Nigeria (2014) 12 NWLR (Pt 1422) 575
- 7.1.2. Melrose General Services Ltd v Economic and Financial Crimes Commission (2025) 1 NWLR (Pt 1972) 1
- 7.1.3. Njoku v The State (2013) 2 NWLR (Pt 1339) 548
- 7.1.4. Nwalu v The State (2018) 14 NWLR (Pt 1638) 159
- 7.1.5. Olatunji v Owena Bank Plc (2002) 5 NWLR (Pt 760) 325
- 7.1.6. Shofolahan v The State (2013) 17 NWLR (Pt 1383) 281
- 7.1.7. Sotuminu v Ocean Steamship (Nig) Ltd (1992) 5 NWLR (Pt 239) 1

7.2. Statutes Cited

- 7.2.1. Constitution of the Federal Republic of Nigeria 1999 (as amended)
- 7.2.2. Cybercrimes (Prohibition, Prevention, Etc) Act
- 7.2.3. Evidence Act

¹⁵ Sotuminu v. Ocean Steamship (Nig) Ltd (1992) 5 NWLR (PT. 239) 1

7.2.4. Proceeds of Crime (Recovery and Management) Act

Dated this 23rd Day of March 2026.



A handwritten signature in dark ink, appearing to read "E. K. Andem".

E. K. ANDEM, ESQ.
E. U. FABIAN, ESQ.
PROSECUTION COUNSEL
(TEAM ACJAMC 112)

FOR SERVICE ON
The Defendant's Counsel