

Juritrust Administration of Criminal Justice Academy Moot Competition, 2025/26

ACJAMC 105

IN THE FEDERAL HIGH COURT OF MAGARIA

IN THE MAGARIA JUDICIAL DIVISION

HOLDEN AT MAGARIA

CHARGE NO:

BETWEEN

FEDERAL REPUBLIC OF MAGARIA.....COMPLAINANT

AND

AISHA NGOZI KEMI..... DEFENDANT

PROSECUTION’S FINAL WRITTEN ADDRESS

INTRODUCTION

This is the Prosecution’s final written legal submission, wherein the Prosecution invites the Court to determine the charge brought against the Defendant under Sections 6 & 24 of the Cybercrimes Act (as amended in 2024) for unauthorized access and cyberstalking/extortion as well as to grant an *ex-parte* application brought under Section 9 of the Proceeds of Crime (Recovery and Management) Act 2022 for a Preservation Order on the Defendant’s apartment and the N200

Million found therein, on the grounds that they amount to “unexplained wealth” and likely “proceeds of unlawful activity.”

BRIEF STATEMENT OF FACTS

The facts of this case are as follows:

2.1. Ms. Aisha Ngozi Kemi (Aisha) 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:

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. 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.

2.5. 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.

2.6. The State has charged her under Section 6 & 24 of the Cybercrimes Act (as amended in 2024) for unauthorized access and cyberstalking/extortion.

2.7. The State has 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.”

LEGAL ISSUES FOR DETERMINATION

1. Whether *mens rea* is present where a professional in the course of her duty to troubleshoot shoot potential problems accidentally accessed and downloaded sensitive data like KYC data.
2. Whether the anonymous demand for a “consultancy fee” in exchange for disclosing a security flaw is established by mere fact that Aisha is living a lifestyle in excess of legitimate income and whether the demand even if traced to Aisha constitutes the offence of cyber stalking or extortion under section 24 of the amended Cybercrimes Act.
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 on the basis of unexplained wealth before the underlying criminal charges of cybercrime have been proven.

LEGAL ARGUMENT

Issue One :Whether *mens rea* is present where a professional in the course of her duty to troubleshoot shoot potential problems accidentally accessed and downloaded sensitive data like KYC data.

4.1.2. To the above issue, the prosecution submits in the affirmative to the effect that element of *mens rea* is present in this instant case.

4.1.3. While we recognize that accidental access and download, *stricto sensu*, lacks *mens rea*, we strongly but humbly contend that the Defendant’s conduct in this instant case demonstrates the requisite guilty mind.

4.1.4. The Court unequivocally held in the case of **Mamman v. State**¹ that for an event to qualify as an accident, it must be the result of an unwilled act or an event which occurs without the fault of the person alleged to have caused it or an event totally unexpected in the ordinary course of

¹ (2025) 1 NWLR (Pt. 1973) 281

events. Also, the defence of accident will not avail an accused where the act is deliberate, even if the accused never intended the eventual result. In the instant case the defence of accident cannot avail Ms. Aisha Ngozi Kemi on the ground that her action is one that an ordinary man in such circumstance ought to have foreseen the probable result, especially given her expertise in cyber security. The moot fact reveals that Ms. Aisha Ngozi Kemi is a high-profile cyber security expert and by virtue of such qualification ought to have reasonably foreseen the probable consequence of accessing the bank mainframe.

4.1.5. Additionally, my Lord(s), **Section 6 of the Cybercrimes Act (as amended in 2024)**, provides to the effect that where a person, **without authorization, intentionally accesses a computer system or network for fraudulent purposes and obtains data vital to National Security**, commits an offence.

4.1.6. This implies that intention is a necessary element for the offence under **Section 6 of the Cybercrimes Act (as amended in 2024)**, to be established and we respectfully submit that the requisite intention is present in this instant case.

4.1.7. Intention, although difficult to prove, can be inferred from the overt acts of the accused. We respectfully refer the Honourable Court to the decision in **Onunze v. State**.²

4.1.8. Similarly, in **Edun v. F.R.N**³, the Court held that intent is difficult to prove affirmatively without a confession from the accused, and can frequently only be determined by looking at the surrounding circumstances and deciding therefrom whether the natural inference is that such must have been the intention. According to the Court, a material factor must be the action or conduct of the accused himself.

² (2023) 8 NWLR (Pt 1885) 69 SC

³ (2019) 13 NWLR (Pt. 1689) 337

4.1.9. My noble Lord(s), it is undisputed that intention is subjective in nature and can only be inferred from a man's act or conduct and thus necessitates the consideration of certain salient features depending on the nature of the offence committed. The court in **Kolo v. COP**⁴ held that intention could be interpreted from the intervening events, circumstances, actions/inactions surrounding the case.

4.1.10. In this instant case, on a community consideration of Ms. Aisha's conduct, coupled with the entire events leading to her action, it would reveal the obvious presence of *mens rea* in her actions. The moot facts clearly revealed that, Aisha upon discovering of 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, deliberately accessed the bank's mainframe to demonstrate its vulnerability, which eventually led her to downloading the KYC data of over 5,000 high-net-worth individuals.

She further sent an anonymous email to the bank CEO demanding a consultancy fee of 50,000,000 naira to disclose the location of the "backdoor" and delete the downloaded data. This clearly showed that she had the intention to commit the alleged offence.

4.1.11. The Defence, might argue that the access and download of the KYC data was an accident, we however contend that prior to her downloading the KYC data, the offence of unlawful access to a computer under **Section 6 of the Cybercrimes Act** was already complete, as all the offence requires is intentional access without authorization and for fraudulent purposes.

4.1.12. The Court of Appeal in **Julius v. FRN**⁵, clearly laid down the requisite ingredients that must be proved to establish the offence of unlawful access to computer under **Section 6(1) and (3) of the Cybercrimes Act**, which are as follows:

⁴ (2017) 9 NWLR

⁵ (2021) LPELR - 54201

1. That the Defendant without authorization intentionally gained access wholly or in part to a computer system or network;
2. That in gaining access to the computer or network as the case may be, the Defendant obtained data that are vital to national security;
3. That the data so obtained was for fraudulent purpose.

4.1.13. The court went further to hold that in addition to the above ingredients, the prosecution should also show that the Defendant in order to commit or carry out his fraudulent intent, used an enabling device to help him avoid detection or otherwise prevent his identification or attribution of the act or commission to himself.

4.1.14. Accordingly, we submit that the above ingredients are present in this instant case as Aisha intentionally accessed the bank's mainframe and obtained vital data instead of immediately reporting to her employers and her fraudulent purpose was shown by the act of sending anonymous email to the bank CEO demanding a consultancy fee of 50,000,000 million naira.

4.1.15. Conclusively, an accident is said to have occurred, as held in **Ejide v. State**⁶, only when the event is sudden and unexpected which is not obtainable in this instant case. As the moot facts clearly reveals that Aisha upon discovery of the backdoor, deliberately accessed the bank's mainframe computer.

4.1.16. We therefore respectfully submit that her intention was clear and in tandem with “intentional access without authorization and for fraudulent purposes”.

And we urge my noble Lord(s) to resolve this issue in our favour.

⁶ (2019) 14 NWLR (Pt. 1692) 246

Issue Two: Whether the anonymous demand for a “consultancy fee” in exchange for disclosing a security flaw is established by mere fact that Aisha is living a lifestyle in excess of legitimate income and whether the demand even if traced to Aisha constitutes the offence of cyber stalking or extortion under section 24 of the amended Cybercrimes Act.

4.2.1. To the above issue, we submit in the affirmative, which is to the effect that Aisha's anonymous demand for a consultancy fee in exchange for disclosing a security flaw constitutes the offence of extortion under **Section 24 of the Cybercrimes Act**, particularly **subsection 2 (b)** and that her lifestyle which is in excess of her legitimate income is strong corroborative circumstantial evidence.

4.2.2. Our argument is premised on two (2) heads of argument;

Firstly, the demand email satisfies the statutory element of extortion.

And that her lifestyle which is in excess of her legitimate income is strong circumstantial evidence corroborating her criminal intent.

The demand email satisfies the statutory element of extortion.

4.2.3. Section 24(2)(b) of the Cybercrimes Act clearly provides to the effect that any person who knowingly or intentionally transmits any communication through a computer system or network containing any threat to extort any person, firm, association, or corporation, any money or other thing of value, commits an offence under the Act and is liable on conviction.

4.2.4. For the offence of extortion to be established, the following ingredients are required:

1. That a person was threatened by another with the intention of obtaining a thing of value;
2. That the accused was the one who issued the threat with the intention of obtaining the thing of value.

This was the decision in **Chuckwudebelu v. State**.⁷

4.2.5. A community reading of the decision in **Chuckwudebelu's case** and **Section 24 of the Cybercrimes Act** establishes that in terms of cyber extortion the prosecution is only required to establish three (3) ingredients, to wit:

1. That there was unauthorized access to information system
2. That by the access, the defendant obtained something of value
3. That there was communication of a threat for the purpose of a financial gain or other thing of value.

These requirements were adopted in the US case of **United States v. Ivanov**.⁸

4.2.6. A perusal of the moot facts reveals that Ms. Aisha Ngozi Kemi downloaded the KYC data without authorization and also demanded consultancy fee without authorization and by that access obtained the data of 5,000 high net worth individuals. Ms. Aisha Ngozi Kemi also sent an anonymous email demanding consultation fee of 50,000,00 Naira to disclose the location of the back door and delete the downloaded data. Obviously, this shows that all element distilled were present.

That There Was Unauthorized Access to Information System

4.2.7. The moot facts clearly show that upon Aisha's discovery of the critical backdoor in the digital vault of the bank which could allow anyone to alter the Social Security Number (SSN) linked to bank account, she deliberately accessed the bank's mainframe computer without authorization to demonstrate its vulnerability instead of reporting to her employers.

⁷ (2018) LPELR - 46721 CA 1

⁸ 175 F. Supp. 2d 367, 369(D. Comm. 2001)

That by the Access, the Defendant Obtained Something of Value.

4.2.8. By accessing the computer system, Aisha obtained the Know Your Customer (KYC) data of 5,000 high-net-worth individuals which is an indispensable asset in this current dispensation of technology.

That there was Communication of a Threat for the Purpose of a Financial Gain or other thing of Value

4.2.9. This element was satisfied when Aisha sent the anonymous email to the bank CEO demanding a consultancy fee of 50 million naira in order for her to disclose the location of the backdoor and to delete the downloaded data.

4.2.10. The Defense might argue that the demand for consultancy fee was a professional demand and that it was not a threat capable of causing fear. It is however our contention that no professional demands for consultancy fee through an anonymous email and that the demand carried a subtle and implicit threat of “send the money or I expose your customers’ data thereby exposing your bank to regulatory sanctions, lawsuits from customers, etc.

4.2.11. In fact, the **US District Court in Ivanov's case** held that an anonymous demand for \$10,000 for assistance in securing a system was extortion.

4.2.12. In that case, the Defendant accessed the United States Online Information Bureau and obtained customers and merchants sensitive data. He went further to send an email demanding approximately \$10,000 for his assistance in securing the system. The Court held that the anonymous demand was extortion.

4.2.13. We accordingly, pray this Honourable Court to borrow a leaf from the above decision as same is in all fours with the facts of the current case and it is also in consonance with the aims and

objectives of the Cybercrimes Act, 2020, as shown in its Section 1 and rule that the elements of cyber extortion are present.

Aisha's lifestyle which is in excess of her legitimate income is strong circumstantial evidence corroborating her criminal intent.

4.2.14. My Lord(s), evidence is said to be circumstantial when it points irresistibly to the guilt of the Defendant. It has been held to be the evidence of surrounding circumstances which by undesigned coincidence is capable of proving a proposition with mathematical exactitude.

Circumstantial evidence is as good as, and sometimes better than any other sort of evidence. We respectfully refer the Honourable Court to the decisions in the cases of **State v. Sunday**,⁹ **Ukorah v. The State**¹⁰, **Peter v. The State**¹¹.

4.2.15. In this instant case, Aisha's lifestyle which is in excess of her legitimate income as well as the 200 million naira and 3 Bitcoin hardware wallets which were found in her apartment, despite her not having any record of formal employment for three years and her anonymous demand for consultancy fee are circumstantial to corroborate criminal intent.

4.2.16. It is a time-honoured principle of law that corroboration need not consist of direct evidence that the Defendant committed the offence nor does it need to amount to a confirmation of the whole account given, provided that it corroborates the evidence in some respect material to the charge.

We humbly call to mind the cases of **Umar v. State**¹², **Ali v. State**¹³, and **State v. Gwangwan**.¹⁴

⁹ (2019) LPELR - 46943 (SC)

¹⁰ (1997) LPELR 4 SC

¹¹ (1997) 12 NWLR (Pt. 531)

¹² (2025) LPELR - 80134 (SC)

¹³ (2021) 12 NWLR (Pt 1789) 159

¹⁴ (2015) 13 NWLR (Pt. 1477) 600

4.2.16. We therefore submit that Aisha's anonymous demand for a consultancy fee in exchange for disclosing a security flaw constitutes the offence of extortion under Section 24 of the Cybercrimes Act, particularly subsection 2 (b) and that her lifestyle which is in excess of her legitimate income is strong corroborative circumstantial evidence.

We further pray this Honourable Court to resolve this issue in our favour.

Issue Three :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 on the basis of unexplained wealth before the underlying criminal charges of cybercrime have been proven.

4.3.1. To the above issue raised, the Prosecution answers in the affirmative.

4.3.2. It is respectfully submitted that the Preservation Order granted over the Defendant's apartment and the sum of ₦200 million found therein is valid and properly sustainable in law. The statutory framework governing the recovery and management of proceeds of crime in Nigeria clearly allows the State to preserve assets suspected to be connected with unlawful activity pending the outcome of criminal proceedings.

4.3.3. Section 9 of the Proceeds of Crime (Recovery and Management) Act, 2022, empowers the Court, upon an application by the Prosecution, to make an order prohibiting any person from dealing with property where there are reasonable grounds to believe that the property constitutes the proceeds of unlawful activity or is otherwise connected with the commission of an offence. It does not require that the underlying offence must first be proven before such an order can be

granted. Rather, the law requires the Prosecution to demonstrate the existence of reasonable grounds linking the property to unlawful activity.

4.3.4. Also, the Proceeds of Crime Act is designed to prevent offenders from enjoying the financial benefits of criminal activity. If the law were to require a prior criminal conviction before suspected assets could be restrained, individuals accused of serious offences would have ample opportunity to transfer, conceal, or dissipate those assets before the conclusion of trial. Such a situation would defeat the central objective of asset recovery and undermine the administration of justice.

4.3.5. Nigerian courts have consistently recognized that interim orders restraining property suspected to be the proceeds of crime may be made before the conclusion of criminal proceedings. In **Yahaya Bello v. EFCC (Unreported)** the Court affirmed the validity of interim forfeiture and preservation orders obtained during the pendency of criminal investigations. The Court held that such orders serve a preventive function by preserving property until the court determines whether the assets were lawfully acquired.

Similarly, the courts have long accepted the use of *ex-parte* applications where the subject matter of the suit is in danger of being dissipated if prior notice is given. In **Kotoye v. Central Bank of Nigeria** the Supreme Court held that *ex-parte* orders may properly be granted in circumstances of urgency or where notifying the adverse party may frustrate the purpose of the application.

4.3.6. In line with the above cases, it is clear that the prosecution has sufficient grounds to justify the preservation of the Defendant's assets. During the course of the investigation, law enforcement officers discovered the sum of ₦200 million in cash and three Bitcoin hardware wallets in the Defendant's apartment. This discovery is particularly significant when viewed against the background that the Defendant has no record of formal employment for a period of three years.

The possession of such a substantial amount of money without any identifiable lawful source of income gives rise to a reasonable suspicion that the assets may be connected to unlawful activity.

4.3.7. The reasonable suspicion surrounding the Defendant's wealth is further strengthened by the nature of the allegations against her. The Defendant is currently facing charges under the Cybercrimes Act (as amended in 2024) for unauthorized access to the digital infrastructure of a financial institution and for sending an electronic communication demanding payment in exchange for the disclosure of a security vulnerability. The circumstances surrounding these allegations shows a connection between the suspected criminal conduct and the financial assets discovered in the Defendant's possession.

4.3.8. The discovery of cryptocurrency wallets further strengthens the prosecution's case. Digital currencies have increasingly been associated with cyber related offences because they provide a means of storing and transferring value outside the traditional banking framework.

4.3.9. Consequently, the presence of several Bitcoin wallets together with a substantial amount of cash reasonably raises the suspicion that the Defendant may have been holding funds obtained from unlawful digital activities. It must also be made clear that the grant of a preservation order does not amount to a pronouncement that the Defendant is guilty of any offence. The Defendant continues to enjoy the constitutional presumption of innocence as the effect of the order is simply to restrict any dealings with the property until the court determines whether the assets represent proceeds of crime or legitimate income. In other words, the order maintains the existing position of the property so that the court may properly resolve the rights of the parties at the end of the proceedings.

4.3.10. While the Defence may hinge their argument on the presumption of innocence of the Defendant and that the Prosecution ought to prove beyond reasonable doubt the guilt of the Defendant, we, however, contend that it is the position of the law as decided in the case of the **F.R.N. v. Mamu**¹⁵, that where a person who is a fixed salary earner has his account suddenly credited with an amount beyond his income or has property which his legitimate income cannot afford, the burden shifts on him to explain how he got the money with which he bought the property or the legitimate transaction he engaged in for which the account was credited.

4.3.11. Hence the burden is on the Defence to explain the legitimacy of the money and property in her possession and the Defence cannot rely on the principle of presumption of innocence as an order of interim forfeiture simply provides a mechanism of preserving the *res* or property from being wasted or dissipated by the suspect as would render the judgment nugatory. We respectfully refer my noble Lord(s) to the case of **La Wari Furniture and Baths Ltd. v. FRN**.¹⁶

4.3.12. The standard required at this stage is therefore one of reasonable suspicion rather than proof beyond reasonable doubt. Given the Defendant's lack of lawful income, the discovery of ₦200 million in cash, the possession of cryptocurrency wallets, and the pending cybercrime allegations, the State has clearly met the threshold required under **Section 9 of the Proceeds of Crime Act**.

4.3.13. In conclusion, it is respectfully submitted that the Preservation Order granted over the Defendant's assets is lawful and fully consistent with the provisions of **Section 9 of the Proceeds of Crime (Recovery and Management) Act, 2022**. As the statute permits the restraint of property where there are reasonable grounds to suspect that it constitutes the proceeds of unlawful activity, and it does not require that the underlying criminal offence must first be proven. The facts of the

¹⁵ (2020) 15 NWLR (Pt. 1747) 303

¹⁶ (2019) 9 NWLR (pt. 1677) 262

present case clearly establish sufficient grounds for reasonable suspicion. The discovery of substantial unexplained wealth in the Defendant's possession, combined with the ongoing investigation for cyber offences under the Cybercrimes Act (as amended in 2024), justifies the preservation of the assets pending the determination of the criminal proceedings. The prosecution therefore respectfully urges this Honourable Court to uphold and maintain the Preservation Order in the interest of justice.

SUMMARY OF ARGUMENT

On issue one, we submit that *mens rea* is present in this case.

On issue two we argued anonymous demand for a "consultancy fee" in exchange for disclosing a security flaw is established by mere fact that Aisha is living a lifestyle in excess of legitimate income and that the demand even if traced to Aisha constitutes the offence of cyber stalking or extortion under section 24 of the amended Cybercrimes Act.

On issue three, we argued that a Preservation Order can be validly maintained over the Defendant's assets under Section 9 of the Proceeds of Crime (Recovery and Management) Act on the basis of unexplained wealth before the underlying criminal charges of cybercrime have been proven.

CONCLUSION

Relying on the legal arguments above as well as the judicial and statutory authorities, we respectfully pray my noble Lord(s) to resolve all issues in favour of the Prosecution.

May my noble Lord(s) be pleased.

Dated this 24th Day of March 2026.



Team 105

Counsel for the Prosecution

For Service on:**Counsel for the Defendant.**

LIST OF AUTHORITIES

Judicial Authorities

1. Mamman v. State (2025) 1 NWLR (Pt. 1973) 281
2. Onunze v. State (2023) 8 NWLR (Pt 1885) 69 SC.
3. Edun v. F.R.N (2019) 13 NWLR (Pt. 1689) 337
4. Kolo v. COP (2017) 9 NWLR
5. Julius v. FRN (2021) LPELR - 54201
6. Ejide v. State (2019) 14 NWLR (Pt. 1692) 246
7. Chuckwudebelu v. State (2018) LPELR - 46721 CA 1
8. United States v. Ivanov, 175 F. Supp. 2d 367, 369(D. Comm. 2001)
9. State v. Sunday (2019) LPELR - 46943 (SC)
10. Ukorah v. The State (1997) LPELR 4 SC
11. Peter v. The State (1997) 12 NWLR (Pt. 531)
12. Umar v. State (2025) LPELR - 80134 (SC)
13. Ali v. State (2021) 12 NWLR (Pt 1789) 159
14. State v. Gwangwan (2015) 13 NWLR (Pt. 1477) 600

15. Yahaya Bello v. EFCC (Unreported)

16. Kotoye v. Central Bank of Nigeria

17. F.R.N. v. Mamu (2020) 15 NWLR (Pt. 1747) 303

18. La Wari Furniture and Baths Ltd. v. FRN (2019) 9 NWLR (pt. 1677) 262

Statutory Authorities

1. Section 6 of the Cybercrimes Act (as amended in 2024)

2. Section 24 of the Cybercrimes Act (as amended in 2024)

3. Section 24(2)(b) of the Cybercrimes Act (as amended in 2024)

4. Section 9 of the Proceeds of Crime (Recovery and Management) Act, 2022.