e-ISSN 2690-3458 ISSN 2690-3431

JOURNAL
OF
ACADEMICS STAND AGAINST POVERTY

Volume 3, Issue 1, 2023: pages 37-56

Research Paper

Bombing, Billing, and Cash-Out: the dynamics of the illicit flow of money through international cyber fraud by Nigerian "Yahoo Boys"

Savictor Sobechi Evans-Ibe

Independent Essayist and Technical Writer
e-mail: *evansibesobechi@yahoo.com*

Abstract: Cyber fraudsters, popularly called Yahoo Boys in Nigeria, employ different strategies and formats across various levels of sophistication to get in touch with potential victims and gain the trust of these unsuspecting victims (Bombing). Then the Yahoo Boys go ahead to devise means of requesting payments from their victims (billing) and secure a successful receipt of such fraudulent payments (cash out). This situation has affected the country, its citizens, as well as the victims adversely; hence, the need for innovative ideas to curtail the ugly trend. This essay sets out to proffer viable solutions to the illicit movement of money through international cyberfraud by Yahoo Boys in Nigeria. The essay starts by classifying international cyberfraud as a component of illicit financial flows. It continues to describe the nature, enduring patterns, and formats adopted by Yahoo Boys, and attempts a quantification of the magnitude of relevant outflows. The essay identifies poverty, corruption, harsh economic realities, indiscipline, unemployment, nature of security architecture on social media platforms, amongst others as enabling conditions for fraud. The essay finally recommends personal discipline, skill acquisition, and personal development, greater national commitments to the fight against corruption and poverty, rebranding corporate taxations to fix the education and skills gap, improved security on social media, sustained enlightenment of vulnerable populations, detention in special facilities for convicted fraudsters, and greater international commitments to the fight against cyberfraud in Nigeria. Several authoritative government publications, academic papers, journal articles, and online publications were consulted for this paper.

Keywords:

1. Cyber fraud
2. Illicit Financial Flows
3. Nigeria
4. Yahoo Boys

DOI: 10.5281/zenodo.8171965

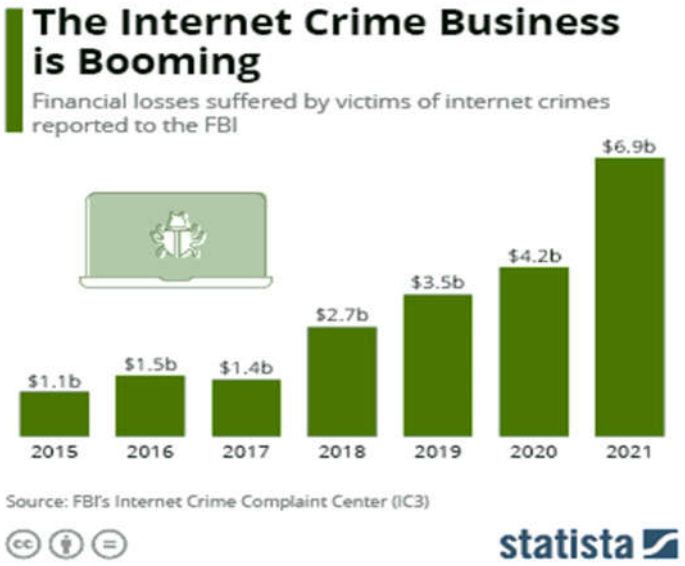
Received 2 March 2023
Revised 10 June 2023
Accepted 17 July 2023
Available online 21 July 2023

1. Conceptual Clarification

Note: The term" Yahoo Boys" has become popular in Nigeria as it refers to the individuals and groups perpetuating various forms and degrees of cyber fraud in the country. Their activities

range from romance scams and crypto frauds to sophisticated investment frauds, using social networking platforms to connect with their victims, and employing sophisticated software to improve the efficiency of their schemes (Fig. 1). While the culprits bask in bumper harvest, the victims languish in pains of loss. This essay aims to discuss in detail the nature, pattern, and dynamics of capital flow through cyber fraud by Nigerian Yahoo Boys and to recommend possible reform measures to tackle cyberfraud and reduce illicit financial flows involving Nigeria.

Fig. 1. Financial Losses suffered by victims of Internet crimes reported to the Federal Bureau of Investigations (FBI) between 2015 and 2021.[1]



The major concepts in this paper are explained below:

1.1. Illicit Financial Flows

Global Financial Integrity defines illicit financial flows (IFFs) as illegal movements of money or capital from one country to another which occurs when funds are illegally earned, transferred, and/or utilized across an international border (Global Financial Integrity, 2022). Similarly, the United Nations Office on Drugs and Crimes (UNODC) further explained that illicit financial flows are multi-dimensional, comprising several different kinds of activities, including flows originating from illicit activities, illicit transactions to transfer funds that have a licit origin, and flows stemming from licit activity being used in an illicit way (UNODC, 2020).

1.2. CyberFraud

Cyber fraud is defined as the use of the internet to perpetuate financial fraud, including, but not limited to phishing emails to gather personal data from unsuspecting readers, fake items for sale, email scams that claim the recipient is owed money if they perform some transaction for

[1] Chart was retrieved from Martin Armstrong, "The Internet Crime Business is Booming," May 16, 2022, https://www.statista.com/chart/20845/financial-losses-suffered-by-victims-of-internet-crimes/#:~:text=The%20FBI's%20Internet%20Crime%20Complaint,losses%20amounting%20to%20%246.9%20billion.

the sender, phony investment schemes and identity theft.[2] International cyber fraud, as used in this essay, refers to when the parties involved (the culprits and the victims) legally or illegally reside in different countries.

1.3. Classifying International Cyber Fraud as a Component of Illicit Financial Flows

By dissecting the definition of illicit financial flows above, we will derive the following indices of Illicit Financial Flows:

- Geographical coverage
- mode of earning
- mode of transfer
- use cases

We will classify international cyber fraud as a component of Illicit Financial Flows based on these indices.

1.3.1 Geographical Coverage

Illicit financial flows involve cross-border movements of funds –the flow of money across international boundaries. Cyber fraud activities in Nigeria involve the movement of funds from Nigeria to other countries of the world, and from other countries to Nigeria – sometimes, with several mid-points. A good example of these cross-border movements was recorded in the case of the Nigerian gang consisting of Emmanuel Nwude-Odinigwe, Ikechukwu Anajemba, Amaka Anajemba, Adedeji Alumile, and Fred Ajudua who connived with their Asian collaborators to defraud Nelson Sakaguchi, a top official of the Brazilian bank, Banco Noroeste SA, of about $242million (Odunlami, 2003). The funds involved in this fraud case were moved across five different continents (Odunlami, 2003). Some of the banks implicated in the funds' transfer included Banco Noroeste dollar accounts in its Cayman branch in British West Indies, a McDaniels Account at Barclays Bank (London, UK), Hillcrest Merchant Bank Ltd in (Geneva, Switzerland), Wells Fargo (USA), and America Express Bank (London, UK).

1.3.2 Mode of Earning

Illicit Financial Flows involve illegally earned funds. The monies involved in the cyber fraud activities by Yahoo Boys in Nigeria are illegally earned through fraudulent activities including romance scams, investment fraud, and crypto fraud schemes.

1.3.3 Mode of Transfer

Illicit Financial Flows are illegally transferred. The Yahoo Boys employ clever and innovative strategies to bypass legal channels and move their earned funds across various locations illegally.

1.3.4 Usage

Funds used to finance illegal activities are also classified as illicit financial flows. While there is no evidence to establish any connection between cyber fraudsters and funding of criminal activities in Nigeria, most of the culprits are notorious for addiction to hard drugs, carefree spending and spraying of money in various locations including streets, clubs, and hotels for little or no purpose. They also overprice items, thereby driving up prices of retail products and making such products unaffordable to most citizens.

Based on this analysis, we can rightly classify international cyber fraud as part of illicit financial flows.

[2] IGI Global, "What is Cyberfraud", accessed July 5, 2022, https://www.igi-global.com/dictionary/turning-westward-information-policies-post/6602

2. Cyber Fraud in Nigeria: Nature and Patterns

This section delves into the nature, patterns, and dominant trends in international cyber fraud by Yahoo Boys in Nigeria. Precisely, the mode of operation, commonly used schemes/formats, methods of funds transfer, strategic collaborations, the continuity of operations, as well as strategies to evade tracking and arrests by security agents are discussed in this section.

2.1. Mode of Operation

Perpetrators of cyber fraud in Nigeria employ various tools and innovative techniques to carry out their operations. The Yahoo Boys use various technological devices, especially mobile phones which can now access the internet at ultra-high speeds. Sophisticated fraudsters who engage in high-level scams also use laptops, wireless fidelity (Wi-fi) internet gadgets, modems, flash drives, scanners, and software.

These operations generally begin from connecting with victims using a falsified identity, showcasing false wealth, and tricking victims into parting with valuables.

2.1.1 Connectivity

Connectivity is an important part of cyber fraud operations. Nigerian cyber fraudsters depend largely on online social networking platforms to connect with their victims. The most notable among these platforms are Facebook, Telegram, Instagram, Twitter, Hangout, Plenty of Fish (POF), Viber, Match.com, WhatsApp, and Google voice.

The Yahoo Boys usually meet their clients (as they call their victims) on Facebook which is generally more effective in connecting with new people. The culprits log onto Facebook and search keywords like “Lonely Granny”, “Angry Granny”, “Investors”, “Business Man”, and “Public Servant”, and Facebook would oblige them with a satisfactory list of accounts with these keywords.

Twitter and Instagram are other effective tools to connect with new people online. However, these social media platforms can take down the accounts of fraudsters at anytime. Therefore, the fraudsters quickly get different contacts of their victims as soon as they establish a significant connection with them. These contact details range from email addresses, telegram usernames, WhatsApp numbers, and phone numbers. For original American social networks like Viber, which requires verification using Native American numbers, the Yahoo Boys usually get their American contacts to help them with these verifications.

2.1.2 Identity Theft

Yahoo Boys do not just hop onto social networking platforms to bomb people with messages. They follow systematic procedures to conceal their real identity, show off a fake lifestyle, and portray the image of a trustworthy figure to their prospective victims. One way to do this is by creating fake accounts across social media platforms.

The fraudsters create accounts with foreign names and fill the profile with pictures of American soldiers, investors, or other personalities depending on the nature of fraud they engage in. The fraudsters get these pictures from real Instagram and Facebook accounts of the individuals they impersonate – though they might use these pictures with different names other than the owner’s real names. The fraudsters usually upload pictures and videos with captions that align with the career or personality they represent. For instance, a fake soldier’s profile will be filled with updates about war experiences, courage on the battlefield, patriotism, and service to the fatherland. The fraudsters use the edit button provided by Facebook to backdate the picture uploads in chronological order. For instance, pictures uploaded in 2020 may be backdated as far back as 2014 to give visitors the impression that this is a real profile and that the owner has been in this field for long enough to command authority. Usually, the fraudsters

hide their friends' lists because the profiles in the list do not tally with the personality the fraudsters represent (in terms of location, profession, etc.).

For example, in August 2022, Nigeria's Economic and Financial Crimes Commission (EFCC) secured the conviction of one Collins Okolie for representing himself, with the intent to defraud, to be Alex Lougwin - an American actor on Facebook.[3]

However, platforms like Facebook began clamping down on new accounts with inconsistent updates and irregular modifications. Hence, the Yahoo Boys diverted to old existing accounts. They edit their accounts, buy existing accounts from friends, or hack the accounts of unsuspecting victims. They edit these accounts and use them for their nefarious acts. Facebook soon laid its hands on these modified platforms and removed many of them. Again, the fraudsters devised a new strategy to beat Facebook's security. This strategy requires buying existing Facebook and Instagram accounts from real Americans. The fraudsters buy these accounts from foreign hackers who maliciously gain access to USA Facebook profiles, log the real owners off, change contact settings, and sell these accounts to their Nigerian collaborators.

This brings up another critical point - how to override social media location trackers. Social media security architecture typically detects and removes suspected fraud accounts when the location set by the users does not correspond with the location transmitted by the Internet Protocol (IP) address of the browser. To evade these security algorithms from detecting scam accounts, Yahoo Boys use Virtual Private Networks (VPN) to reset the location of their devices.

2.1.3 Flamboyant Display of False Wealth

An important part of the fraud process is to display enormous wealth to the public through the fraudsters' fake social media accounts. As a top crypto expert, a multi-millionaire investor, a top-brass military officer, or an influential businessperson (which these fraudsters often claim to be), there is a certain level of wealth that onlookers expect you to control. The fraudsters do not want to disappoint the public in this regard. Hence, they fill their social media profiles with pictures of (impersonated) individuals in multi-million-dollar mansions, with exotic cars and costly jewelry, living exquisite and expensive lifestyles. With this, unsuspecting members of the public believe that this wealth is real and become eager and ready to do the fraudsters' bidding just to attain the same level of success flashed before their eyes.

2.2. Patterns and Common Formats of International Cyber Fraud in Nigeria

Cyber fraud activities in Nigeria are perpetrated at various levels of sophistication. The type of fraud (which the Yahoo Boys call 'formats') depends largely on the experience and specialization of the fraudsters. This section delves into these 'formats'.

2.2.1 Romance Scams

This is the most basic format of fraud carried out by Yahoo Boys. Experienced fraudsters usually advise beginners to engage in romance scams to build up their experience and learn how to communicate with foreigners, attract feelings, establish bonding, and manipulate the emotions of victims. The fraudsters mainly target divorcees and aged American women who need true affection and are probably enjoying retirement benefits. Again, Facebook comes in handy in establishing these connections. A simple search of keywords like 'lonely granny', 'divorcee', and 'sad grandma', throws up a list of accounts likely owned by middle-aged women, widows, or divorcees. Once a connection is established with the first contact, the fraudsters usually dig into

[3] Economic and Financial Crimes Commission, "Fake American Actor, Five Others Sent to Jail in Benin for Internet Fraud," August 1, 2022, https://www.efcc.gov.ng/news/8330-fake-american-actor-five-others-sent-to-jail-in-benin-for-internet-fraud

their victim's friends list to connect with other clients (potential victims). Homosexuals are growing victims these days as the culprits present them with false affection from a supposed same-sex partner.

The fraudsters usually trick their victims to fall in love, promise them marriage, and then make several cash demands from them. These cash demands usually include money for travel arrangements and flight tickets to come over to America or any promised location for their wedding which will never hold.

2.2.2 Military

In this format, the Yahoo Boy presents himself as an American soldier on a foreign mission. There are two main patterns to defraud victims using the 'Military Format'.

First is the 'Box'. Here, the fraudster convinces the victim to take delivery and keep custody of a box (filled with gold and diamonds) given to the soldier as a reward for service. The fraudsters often peg the worth of the items in the 'imaginary box' at a high price usually over a million dollars.

The fraudsters build websites for this game. Once, the victim accepts to receive the box and keep custody of it, the fraudsters usually refer their victims to the websites and alert their collaborators (who create and run the scam websites) to stay up for the deal. When contact is established and the first payment (usually less than $2,000) is made via the website, the 'imaginary box' is usually sent to the victims. However, it must pass through two or three midpoints, where 'fake' custom officers (collaborating with the fraudster) establish contact with the victim and demand 'fake' custom fees before the box will be sent to the victim's location.

For instance, a box sent from Syria may have to pass through Turkey and Poland before arriving in the USA. Generally, the midpoints and custom fees keep increasing in count, while the fraudster keeps getting mad at the delivery company, sympathizing with the victim, and encouraging them to keep paying the fees. This keeps going until the Victim runs out of cash or gets tired of paying.

The second is 'leave', which only works when the victim has already fallen in love. Again, there are fraud websites already created and deployed for this service. The victims are generally convinced to apply for leave via these scam websites and pay certain fees to get their supposed soldier-lovers out of the battlefield for their supposed wedding.

2.2.3 Crypto Fraud

This format comes in different dimensions ranging from tricking victims into revealing their wallet secret phrases to convincing victims to invest their coins into scam Ponzi schemes. For example, on November 8, 2021, operatives of the Economic and Financial Crimes Commission (EFCC) arrested one Precious Ofure Omonkhoa for an alleged bitcoin investment scam. He allegedly posed as Moshem Cnich, a Swedish national, to defraud unsuspecting victims of their hard-earned money by claiming that he runs a bitcoin scheme, where people invest money to make huge returns.[4]

2.2.4 Investments Scams

Investment scams are mainly executed through scam websites that the fraudsters build and maintain. The fraudsters lure their victims to these scam websites and get them to invest money in 'non-existent' businesses with the promise that the victim's capital will be refunded with mouth-watering Returns on Investments (ROI) within a very short period. The ROIs promised can be as high as 100% in one week.

[4] Economic and Financial Crimes Commission, "EFCC Arrests Man for $200,000 Cryptocurrency Fraud in Lagos," Published on May 12, 2022**,** https://www.efcc.gov.ng/news/7431-efcc-arrests-man-for-200-000-cryptocurrency-fraud-in-lagos

2.2.5 Inheritance Fraud

In inheritance scams, the fraudsters reach out to their victims with evidence of fortunes, usually running into millions of dollars, which a late person has willed to the prospective victim. The victims are required to pay a percentage of the total inheritance as advance fees to claim the non-existent funds. The fraudsters in this game are usually experienced, sophisticated, well connected with foreign collaborators, and in possession of official bank and other financial documents, stamps, and digital signatures to prove the authenticity of the inheritance schemes that they present to their victims.

For example, On June 30, 2020, the Economic and Financial Crimes Commission arraigned one Onwuzuruike Ikenna Kingsley for allegedly representing himself as one Jeff Sikora, President/CEO of Prime Trust Credit Union Bank in the United States of America, and used the false identity to defraud his victims, including an Egyptian who was defrauded of the sum of $6,500,000.00 on the pretext that he was a beneficiary of Inheritance Funds in a fixed deposit account of Prime Trust Financial Bank.[5]

2.2.6 Loading

This is another high-level fraud scheme in which the fraudsters perform fraudulent transfers into the victims' bank accounts. The victims are then required to withdraw real money from these accounts and transfer them to the fraudster's accounts. These fake transfers are likely to be detected by the victim's bank after several days, leading to the arrest of innocent individuals for crimes they know very little about.

One of the respondents in a survey of Yahoo Boys living in Ibadan of South-Western Nigeria revealed that:

> There are some hackers that can conveniently sell companies' accounts information to us. They usually give us details of such accounts, and we will pay them in return. One will then make use of such sensitive information to transfer money from the company whose account had been so compromised to one's client (potential victim) account. It could take up to one week before the affected company detects such a move. By that time, one would have received such cash from one's client. Of course, he or she (client) would be subsequently arrested (Ojedokun&Ilori, 2021).

2.2.7 Business Email Compromise (BEC) Scams

This is arguably one of the most sophisticated schemes executed by NigerianYahoo Boys. It involves breaking into organizations' official email accounts with sophisticated software, hijacking business communications, and initiating financial transactions in the name of victim organizations.

2.3. Means of Funds Transfer

According to the Economic and Financial Crimes Commission, gift cards accounted for about 39 percent of the method employed by Yahoo Boys to access their illicit funds in 2020.

[5] Economic and Financial Crimes Commission, "$8.5 Scam: How We Arrested Internet Fraud Kingpin, Onwuzruike – EFCC Witness," Published on July 13, 2020**,** https://www.efcc.gov.ng/news/5862-8-5-scam-how-we-arrested-internet-fraud-kingpin-onwuzruike-efcc-witness

Cryptocurrency and bank transfer scams made up about 27 percent and 21 percent of their scamming methods respectively.[6]

Another method of transferring funds is through third-party accounts using western union and other fintech services, with a withdrawal process aided by compromised bank staff in Nigeria. These fraudsters have strong networks spanning all the countries of the world.

Some fraudsters specialize in providing account details of third-party collaborators to receive the monies. These fraudsters are popularly known as 'Pickers' or 'Aza Men'. They include some of the most experienced, most connected, and wealthiest fraudsters, and usually reside outside Nigeria to evade the Economic and Financial Crimes Commission (EFCC) and security agencies that are always on the hunt for them. The picker or Aza man usually takes 20% - 40% of the money received with the account details they provide. This is the major source of their overflowing wealth because they earn from several fraud cases by just providing account details. Aza men usually reside in USA, Dubai, Malaysia, and Cyprus which have become safe havens for their operations. For example, Paul Duru, a convicted Romance scammer allegedly had a 'picker' in the United States, one John T. Benn, who received the money in dollars and sent it to him.[7]

Cryptocurrencies provide another means of transferring funds earned via cyber fraud. The fraudsters ask their victims to purchase bitcoin orother popular cryptocurrencies and transfer them to the fraudsters' wallet address. In cases where the victims do not know how to transfer funds through crypto, the Yahoo Boys usually guide them through the process to ensure successful transactions. This method is gaining popularity as fraudsters do not have to share the proceeds of their schemes with pickers, loaders, or other third parties when the funds are transferred via crypto.

2.4. Collaborations

Cyber Fraud in Nigeria is mainly a cross-border activity involving many international accomplices. For instance, the account details provided by Aza men are usually owned by Americans, Europeans, and real citizens of other countries.

Nigerian Yahoo Boys collaborate with corrupt bank staff to withdraw their funds. As testified by Elvis (not real name), a repentant Yahoo Boy, "For a successful execution of a 'job', an insider within the bank is important. The bank staff facilitates payment without attracting the attention of security agencies. They also get their share of the 'runs'."[8]

Also, the acquisition of real American and British Facebook accounts is facilitated by foreign hackers who provide these accounts to the fraudsters at a fee. According to a respondent in the Ibadan survey:

> [...] some contacts have turned legit (criminal accomplice) over time. These people normally helped us to get whatever tool and information we need over there in the U.S... If there is a strong connection between one and the person (contact), one can start colluding with him/her to get any vital tools that one needs. For instance, such contact(s) can help one get an American SIM card. He

[6] Economic and Financial Crimes Commission quoted in Afeez Hanafi, "How Yahoo boys befriend, bribe policemen, soldiers to evade justice," December 11, 2021, https://punchng.com/how-yahoo-boys-befriend-bribe-policemen-soldiers-to-evade-justice/

[7] Wale Odunsi, "EFCC arrests Yahoo boys involved in love scam, recovers N31m [PHOTO]," February 6, 2019, https://dailypost.ng/2019/02/06/efcc-arrests-yahoo-boys-involved-love-scam-recovers-n31m-photo/

[8] Nnamdi Ojiego, "(FILTHY RICHES 2) Yahoo Boys' Revelations: How we scout for victims, make billions," October 31, 2022, https://www.vanguardngr.com/2021/10/filthy-riches-2-yahoo-boys-revelations-how-we-scout-for-victims-make-billions/

> or she would then courier same through the DHL or any other means of delivery to Nigeria (Ojedokun&Ilori, 2021).

2.5. Evasion Strategies

Yahoo Boys adopt several strategies to evade tracking and arrest by security agents. These strategies are more proactive than otherwise. Firstly, the fraudsters hide under the umbrella of anonymity created by social media, using the face and details of a stranger to execute their dubious acts. This ensures that the real names and faces of the fraudsters remain unknown to social media natives. Secondly, the fraudsters use false locations and deploy virtual private networks (VPN) to change the location of their devices and hide their Internet Protocol (IP) Addresses.

According to one of the respondents from the Ibadan survey of Yahoo Boys:

> [...] when we are talking about tools that we normally use for this hustle, we are talking about VPN. For example, VPN is used to change one's location. You know many clients (potential victims) have trust issues. When they discovered that one is a Nigerian, they stop interacting with one. So, using a VPN would indicate that one is based in the United States of America; and clients would automatically believe and fall for it. They will believe that one is also one of them. There are some dating sites with very strict access-restriction policies for certain countries. One cannot access them without using a VPN (Ojedokun&Ilori, 2021).

Finally, whenever the victims get rebellious, the fraudsters waste no time hitting the "block" button.

2.6. Recruitment, Training, and Sustainability

For the growth and sustenance of every organized crime, there must be a recruitment process. This process mainly comes in three ways in international cyber fraud in Nigeria. These three ways include:

2.6.1 Socialization

Most cyber fraudsters in Nigeria started by watching their experienced friends play the game. From watching them chat with victims to learning how to edit social media accounts, young men gradually get into the cyberfraud industry. In the survey of Yahoo Boys residing in Ibadan, all respondents confirmed to the scholars that they learned the game from experienced peers and friends (Ojedokun&Ilori, 2021). In the words of one of the respondents:

> In this game (cyber fraud), you have to learn from someone. Everything about this hustle (cyber fraud) boils down to the connection one has and the area of the hustle that one wants to learn because Gee-boys (another name for Yahoo Boys) know that Yahoo Yahoo (cyber fraud) goes beyond what is being done on Facebook, Instagram, and so on. So, for a newcomer, the starting point is to learn from a person that would tell you what you need to know because Yahoo Yahoo is not something that you will just decide to go into without being properly tutored. For my training, I learned a lot of things from my boss who is like an area brother to me. I started with the creation and use of United States citizens' Facebook account profiles. There are so many processes to it (cyber fraud). So, one just has to seek information from those who truly know. It is not about what you just know on your own as an individual (Ojedokun&Ilori, 2021).

Once the fraudster begins, the next baby step is usually to network with other young men who are into fraud. These networks go a long way in hatching further generations of professional fraudsters.

2.6.2 Apprenticeship/Academy System

Experienced and wealthy fraudsters build or rent houses to set up fraud academies in various Nigerian cities. These Academies/training homes are popularly known as HKs (Headquarters). Budding fraudsters are brought into these academies where their experienced colleagues (commonly called Bosses) guide them closely from novitiate to expertise in the game of fraud.

While in these academies, the feeding, data subscription, power needs, accommodation, and other necessities are provided by the 'Boss'. In return, the apprentices forfeit up to 60% - 70% of all fraud proceeds to their Boss as long as they stay in his HK. Apprentices usually stay an average of 6 months to 1 year in the HK, during which they are expected to have cashed out (pulled off at least, a successful fraud scheme). If, however, any apprentice could not cash out within the period, the Boss lets him out as a failed investment.

For example, on May 12, 2022, operatives of the Economic and Financial Crimes Commission (EFCC) arrested 24 years old Afolabi Samad for operating a Yahoo academy (HK) in the capital city of Abuja.[9] Afolabi had 16 apprentices aged between 18 and 27 at the time of the arrest. This system is fast becoming influential in raising a new army of fraudsters in Nigeria dealing with international victims. However, life in HKs is more of a slave-master relationship as the apprentices may experience several abuses at the hands of a ruthless Boss.

2.6.3 Self Enlistment

This is the last major form of recruitment where boys who are not privileged to have a fraudster they can learn from directly and are unwilling to pass through the difficult HK system, push themselves into the game and learn by trial and error. They learn from their mistakes and get better with time and more targets. However, a breakthrough comes when they begin to socialize with experienced peers.

3. Adverse Effects of International CyberFraud by Yahoo Boys in Nigeria

The adverse effects of international cyberfraud by Yahoo Boys in Nigeria can be classified into two: effects on the victims, and effects on the Nigerian society.

3.1. Effects on the Victims

These include impoverishment, depression, death, and jail times for victims.

3.1.1 Impoverishment and Liquidation due to Financial and Property Loss

Most victims of international cyberfraud, including businesses, are defrauded to bankruptcy. Sometimes, victims borrow or mortgage their properties to pay the bills of fraudsters. For example, Renee Holland from Florida transferred her life savings to a man pretending to be in the US military.[10] Also, BankoNoroeste was looted into liquidation by Nigerian fraudsters and their Asian collaborators (Ojedokun&Ilori, 2021).

---

[9] Economic and Financial Crimes Commission, "EFCC Nabs YahooYahoo Academy Owner, 16 'Trainees' in Abuja," May 12, 2022, https://www.efcc.gov.ng/news/7999-efcc-nabs-yahooyahoo-academy-owner-16-trainees-in-abuja

[10] **Zoe Kleinman, "**Coronavirus: Romance scams, the Yahoo boys and my friend Beth," August 19, 2020, https://www.bbc.com/news/technology-53445690

3.1.2 Depression

Victims of fraud suffer depression. A report by the education arm of the Financial Industry Regulatory Authority (FINRA), an American private Organization, has it that about 35% of financial fraud victims suffer depression.[11] According to the World Health Organization, depression is a leading cause of disability around the world and contributes greatly to the global burden of disease.[12]

3.1.3 Death

International cyberfraud leads to the deaths of victims through suicide or murder. Renee Holland, the Floridian woman discussed above was later killed by her husband on account of the lost money.[13]

3.1.4 Implication of Victims

Some victims of international cyberfraud get implicated and even spend time behind bars especially when the money lost to the fraudsters belongs to the company that the victims work for. For example, Nelson Sakaguchi, the Banco Noroeste SA official was arrested after he was defrauded of the bank's funds by Nigerian fraudsters (Ojedokun&Ilori, 2021).

3.2. Effects on the Nigerian Society

International cyberfraud by Yahoo Boys has affected the image of the nation, leading to loss of opportunities for citizens. Also, the crime rate has skyrocketed alongside the cost of living.

3.2.1 Bad Image for the Nation

International cyberfraud by Yahoo Boys has defaced the image of the nation in the international community. High-level fraud schemes by Nigerians suchas Ramon Abbas (Hush Puppi) and accomplices[14] have given Nigeria the image of a pathogen harboring viruses that eat up other citizens of the global community.

3.2.2 Loss of Opportunities

A direct effect of the bad image caused by international cyber fraud is the loss of opportunities including remote jobs, migration, and education, for innocent Nigerian citizens. Following the case of Ramon Abbas, the United Arab Emirates enforced visa restrictions for Nigerian citizens.[15] Also, several authoritative websites restricted Nigerians from accessing their portals.

Nigerian freelancers operating from Nigeria seem to be the worst hit by this issue. Potential clients fear working with Nigerians as they feel they may be defrauded. Social media platforms like LinkedIn and Nairaland are filled with stories of Nigerians who lost foreign clients after the clients found out they were Nigerians.

[11] James Langton, "Financial fraud victims vulnerable to depression," March 13, 2015, https://www.investmentexecutive.com/news/from-the-regulators/financial-fraud-victims-vulnerable-to-depression/

[12] World Health Organization, "Depression," accessed on July 20, 2022, https://www.who.int/health-topics/depression#tab=tab_1

[13] **Zoe Kleinman, "**Coronavirus: Romance scams, the Yahoo boys and my friend Beth," 2020

[14] Nairaland, "UAE Suspends Direct Employment Visa For Nigerians Over Rising Crimes - Travel – Nairaland," accessed on July 30, 2022, https://www.nairaland.com/6625825/uae-suspends-direct-employment-visa

[15] Sahara Reporters, "EXCLUSIVE: UAE Suspends Direct Employment Visa For Nigerians Over Rising Crimes," June 29, 2021, https://saharareporters.com/2021/06/29/exclusive-uae-suspends-direct-employment-visa-nigerians-over-rising-crimes

3.2.3 Increase in Crime Rate

Many youths in Nigeria have normalized cyberfraud as a quick way to make money. Hence, young people including high school students venture into cyber fraud schemes in droves. In some cases, Yahoo Boys kill for ritual purposes to enhance success in their fraud schemes.[16]

3.2.4 Lost Tax Revenues

The money earned through international cyberfraud by Yahoo Boys in Nigeria is not covered by the tax net since they are illegally obtained and kept away from the eyes of the government. This leads to the loss of tax revenues that could have been used to support economic growth, job creation, and poverty eradication, amongst other necessities.

3.2.5 High Cost of Living

Yahoo Boys in Nigeria are notorious for buying items at exorbitant prices. An important part of the distinct lifestyle in which perpetrators of international cybercrime live is to show off their wealth. This show-off comes in several forms including spraying money along the streets, in clubs and over-pricing cheap items. Retailers have followed this trend by increasing the prices of their goods. Most retailers will bluntly ask you, "Do you know how much we sell this to those Yahoo Boys?" This has led to a high cost of living for the populace as the people have to keep up with the high prices stimulated by the extravagance of the Yahoo Boys.

4. Magnitude of Relevant Outflows due to International CyberFraud in Nigeria

According to the 2021 Internet Crime Report released by the Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation (FBI), about $6.9 billion was lost to cyber crimes by Americans in the year 2021 alone (Fig. 2). This also comes with a record high of 847, 376 reported complaints. A further breakdown of this report shows that business email compromise schemes had the largest losses amounting to more than $2.4 billion. Cryptocurrency scams recorded losses of $1.6 billion, while confidence scams which include romance scams had losses of up to $956 million (FBI, 2021).

Fig. 2. 2021 Internet crime reports in numbers[17]

[16]IsholaOludare, "Ogun: Yahoo-boy who reportedly used girlfriend for money ritual appears in court," 16/6/ 2022, https://dailypost.ng/2022/07/16/ogun-yahoo-boy-who-reportedly-used-girlfriend-for-money-ritual-appears-in-court/

[17]Dmarcian, "2021 FBI Internet Crimes Report," https://dmarcian.com/2021-fbi-internet-crime-report/#:~:text=%E2%80%9CIn%202021%2C%20IC3%20continued%20to,Paul%20Abbate%2C%20FBI%20Deputy%20Director.

Nigerians are not left out of this menace. In 2018, commercial banks in the country lost about ₦15 billion ($36.6million) to electronic fraud and cybercrime while over 17,600 bank customers lost ₦1.9 billion ($4.6million) to cyber fraud in the same year.[18] Between July 2020 and September 2020, Nigerian banks lost ₦3.5 billion ($8.5million) to fraud-related incidents, representing a 534-percent increase from the same period in 2019, when it was ₦552 million ($1.35million).[19] Transactions done over phones were responsible for a loss of ₦410 million ($1million) at 11.7 percent of the entire loss value.[20]

On the global scene, the Centre for Strategic and International Studies (CSIS), in partnership with McAfee presented a report tagged: Economic Impact of Cybercrime – No Slowing Down, a global report on the significant impact of cybercrime on economies worldwide. The report suggests that about $600 billion is lost to cybercrime yearly (CSIS, 2018).

In terms of projections, the Nigeria Consumer Awareness and Financial Enlightenment Initiative placed its projections at a $6 trillion loss to cybercrime within and outside Nigeria by 2030.[21] While a private firm, Cybersecurity Ventures expects global cybercrime costs to reach $10.5 trillion annually by 2025.[22]

5. Factors Responsible for the Persistence of International CyberFraud in Nigeria

The enabling conditions of international cyberfraud in Nigeria include the socio-economic root causes and incentives that pull young people into fraud.

5.1. Bad Economy

The harsh economic realities in Nigeria have pushed many youths into several crimes including cyber fraud. With a staggering debt profile and rising inflation, the country's economy continues on a downward trend as debt servicing surpasses revenue.[23] Despite higher oil prices, the fiscal situation is deteriorating, limiting the government's ability to support the recovery and protect the poor. Exchange rate management policies continue to deter private investment.[24] These issues push young people to alternative ways of earning a living. Sadly, cyber fraud has become one of these alternatives.

5.2. Corruption

Corruption in Nigeria is alarming. Corrupt acts are happening every day in the country. More recently, the Economic and Financial Crimes Commission (EFCC) arrested the Accountant

[18]Afeez Hanafi, "How Yahoo boys befriend, bribe policemen, soldiers to evade justice," December 11, 2021, https://punchng.com/how-yahoo-boys-befriend-bribe-policemen-soldiers-to-evade-justice/

[19] Frank Eleanya, "Cyber fraud rises 534% as Nigerian banks lose N3.5bn," February 16, 2021, https://businessday.ng/banking-finance/article/cyber-fraud-rises-534-as-nigerian-banks-lose-n3-5bn/

[20] Frank Eleanya, "Cyber fraud rises 534% as Nigerian banks lose N3.5bn," 2021

[21] Consumer Awareness and Financial Enlightenment Initiative quoted in Afeez Hanafi, "How Yahoo boys befriend, bribe policemen, soldiers to evade justice," December 11, 2021, https://punchng.com/how-yahoo-boys-befriend-bribe-policemen-soldiers-to-evade-justice/

[22] Steve Morgan, "Cybercrime to Cost The World $10.5 Trillion Annually By 2025," November 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[23] Zainab Ahmed, Honorable Minister of Finance, Budget & National Planning, Federal Government of Nigeria, "Public Consultation on The Draft 2023 – 2025 MTFF/FSP," July 31, 2022, https://www.budgetoffice.gov.ng/index.php/hmfbnp-2023-2025-mtef-fsp-public-consultation?task=document.viewdoc&id=969

[24] World Bank, "Nigeria Development Update," Published on June 1, 2022, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099740006132214750/p17782005822360a00a0850f63928a34418

General of the Federation, Ahmed Idris over charges of diverting public funds and money laundering to the tune of ₦80 billion (about $193 million).[25]These corrupt acts provide a form of support system for Yahoo Boys in Nigeria since they believe that the system itself is ridden by corruption.

5.3. Poverty

Poverty is one big parasite nurtured by the outcomes of corruption and unemployment, among other socio-economic ills bedeviling the Nigerian system. According to the World Bank,[26] about 4 in every 10 Nigerians live below the poverty line with more than 90 million poor people in the country. This is not just a case of facts and figures. As bad as it has gotten, many Nigerians find it difficult to have one square meal in a day. This situation forces many youths into fraudulent acts to make a living.

5.4. Unemployment

Another problem confronting the Nigerian system is unemployment, which also, is watered by the spring of corruption in the country. According to the National Bureau of Statistics,[27] unemployment rate is at 33% while youth unemployment currently stands at a staggering 42.5%. With no job, many young people resort to cyber fraud to fend for themselves and their families.

5.5. Indiscipline

This is the bedrock where the roots of cyber fraud are nurtured. While there may be credible pointers to corruption, poverty, and a bad economy as enablers of cyberfraud, one cannot overlook the overarching contribution of individual indiscipline to the reign of international cyber fraud in Nigeria. Indeed, numerous other young Nigerians are driving positive change and creating value in the world. While these young people are disciplined to engage in legitimate means of livelihood, others chose the undisciplined path to a fraudulent lifestyle.

5.6. Tough Business Environment

The business climate in Nigeria is tough.Thissituation also contributes to the growth of cyberfraud in Nigeria as young people who have experienced business failures resort to fraud to earn a living.

5.7. Prosperity of Fraudsters and Poor Standard of Living for Those with Legal Means

Fraudsters (Yahoo Boys) in Nigeria seem to be more prosperous than their peers in legal businesses and jobs who barely manage to provide for basic amenities. The extravagant lifestyle and achievements of these young fraudsters pull their peers into the game.

In the Ibadan survey of Yahoo Boys, one of the respondents stated thus:

[25] Camillus Eboh, "Nigeria's accountant general faces corruption charges after arrest," May 17, 2022, https://www.reuters.com/world/africa/nigerias-accountant-general-faces-corruption-charges-after-arrest-2022-05-16/

[26]World Bank, "Deep Structural Reforms Guided by Evidence Are Urgently Needed to Lift Millions of Nigerians Out of Poverty, says New World Bank Report," March 22, 2022, https://www.worldbank.org/en/news/press-release/2022/03/21/afw-deep-structural-reforms-guided-by-evidence-are-urgently-needed-to-lift-millions-of-nigerians-out-of-poverty

[27] National Bureau of Statistics, "Unemployment Statistics," March 22, 2022, https://www.nigerianstat.gov.ng/

> [...] my motivation mainly comes from some of my guys that are already balling hard (living ostentatious lifestyles) and driving big cars worth between $11,795.54 and $13,106.16 (₦4,500,000 and ₦5,000,000). Can you imagine a 19-year-old boy buying a car (Camry Muscle model) worth about $6,553.08 (N2,500,000) through proceeds gained from this hustle (cyber fraud)? So, if one sees all the paparazzi and flexing (glamours and glitz) of guys who are into hustle in one's neighborhood every day, one will also want to try it (cyber fraud). That is what we call ginger (inspiration) (Ojedokun&Ilori, 2021).

5.8. Increasing Corruption amongst Security Agents

Some security officials engaged in the fight against cyberfraud have been corrupted by the juices of the same bad fruit they are supposed to fight. Often, security agents arrest suspected fraudsters, extort cash from them, and release them back into society without charging them to court. More often, the suspects may be re-arrested by the same group of security agents for more ransom.

A Punch publication, "How Yahoo boys befriend, bribe policemen, soldiers to evade justice,"[28] revealed the shameful relationship between officers of the law and Yahoo Boys in which security officers protect fraudsters in exchange for a cut of the proceeds of cyber fraud activities. The revelations in this publication were confirmed by fraudsters and security officers themselves.

5.9. Greed

The success of most cyber fraud cases depends on greed on the part of the victims. The mouth-watering offers presented by these intelligent fraudsters are, sometimes, too good for human greed to ignore.

5.10. Inadequate Security Architecture on Social Media

Although social media companies continue to raise the bar on security within their platforms, the security architecture employed is still unable to track fraud patterns on their messaging applications. This is mainly due to the end-to-end encryption designed to prevent third-party intrusion into the privacy of users. Hence, fraudsters take advantage of this situation to scam unsuspecting victims through direct messaging on these platforms.

5.11. Oversight by Web Hosting Platforms

Web hosting companies provide very little scrutiny over the websites they host on their platforms. This has enabled fraudsters to create and deploy accessible scam websites to the web.

6. Efforts Already Made to Fight Cyberfraud in Nigeria

The efforts made to fight cyber fraud in Nigeria come in the form of the establishment of anti-fraud agencies and international collaborations.

6.1. Establishment of the Economic and Financial Crimes Commission

The Economic and Financial Crimes Commission was established by the Economic and Financial Crimes Commission Establishment Act (2004). The Commission is empowered to prevent,

[28]Afeez Hanafi, "How Yahoo boys befriend, bribe policemen, soldiers to evade justice," 2021

investigate, prosecute and penalize economic and financial crimes and is charged with the responsibility of enforcing the provisions of other laws and regulations relating to economic and financial crimes.[29] The EFCC has been instrumental in tackling cyber fraud in Nigeria.

6.2. International Collaborations

Nigeria has recorded significant success in the fight against cyberfraud through international collaborations. In 2019, the then acting Chairman of the Economic and Financial Crimes Commission disclosed that the collaboration between the Commission and the Federal Bureau of Investigation (FBI) has led to the recovery of the sums of $314,000 (Three Hundred and Fourteen Thousand US Dollars) and about ₦373,000,000.00 (Three Hundred and Seventy-three Million Naira) from perpetrators of computer-related fraud as at August 2019.[30]

7. Tackling Cyber Fraud in Nigeria: Way Forward

The solutions proffered under this section range from personal discipline, corporate policies, and national efforts to international commitments to the fight cyber fraud.

7.1. Personal Discipline

This is the bedrock of the fight against cyber fraud in Nigeria and beyond. Personal discipline here involves a resolution to not participate in cyber fraud activities and a strong will to keep to that resolution. The significance of personal discipline is that, when more individuals desist from fraudulent activities, they will influence their peers to jettison the ugly lifestyle.

7.2. Skills Acquisition and Personal Development

Unemployment has been identified as one of the causes of cyber fraud in Nigeria. Unemployment itself is partly a consequence of the insufficiency of employable skills among the youths. Hence, young people in Nigeria should invest in their personal development, especially in the acquisition of relevant skills.

The internet has provided a lot of opportunities to make a decent living. Valuable skills including programming, digital marketing, creative writing, and crypto technologies can be acquired online. Thankfully, some organizations including Google, W3schools, and Freecodecamp have committed resources to provide training on these skills for free. Nigerian youths should take advantage of these opportunities to turn the tide in favor of legal means of livelihood.Parents and Guardians should expose their wards to these opportunities at a young age. Through this, the young people will:

- acquire job-ready skills
- increase their potential of being hired to fill available vacancies
- increase their abilities to create viable products
- reduce the unemployment rate as well as incidences of cyber fraud in Nigeria

7.3. Re-invigorate the Fight against Corruption

The federal government of Nigeria, especially through the Economic and Financial Crimes Commission (EFCC) should pay more attention to closing loopholes through which corrupt

[29] Economic and Financial Crimes Commission, "The Establishment Act," Retrieved on August 11, 2022, https://www.efcc.gov.ng/about-efcc/the-establishment-act

[30] Economic and Financial Crimes Commission, "Internet Fraud: $314,000, N373m Recovered Through EFCC-FBI Collaboration-Magu," August 27, 2019, https://www.efcc.gov.ng/news/4756-internet-fraud-314-000-n373m-recovered-through-efcc-fbi-collaboration-magu

practices are perpetrated. A corruption-free system creates a transparent environment that makes it difficult for cyber fraud to thrive.

7.4. Tackle Poverty

The eradication of poverty should be a priority in the fight against cyber fraud in Nigeria. The federal government of Nigeria should ensure the provision of quality infrastructure including a steady power supply, good road networks, and a conducive business regulatory environment. The people can leverage the benefits of these provisions to create means of livelihood. This will go a long way to eradicate poverty which is one of the root causes of cyber fraud in Nigeria.

7.5. Set the Pace for Economic Transformation

To create working conditions for legitimate businesses to thrive, economic transformation is non-negotiable. This transformation will not be executed in one day. However, we must set the pace for sustainable transformation. This can be achieved by increasing productive economic activities. Nigeria exports most of its raw materials without being processed. The country can invest more in manufacturing and processing to stimulate economic growth, create job opportunities, increase value addition, and increase revenue generation as well as the Gross Domestic Product of the country.

The Federal government should improve the ease of doing business by ensuring progressive regulatory frameworks and policies while avoiding retrogressive measures that undermine the goals of our economy.

Importantly, there is a need to diversify revenue sources and drift from over-dependence on crude oil revenue. The country should double down on reckless spending and channel resources to critical sectors such as education, health, security, and agriculture.

7.6. Improve Education and Skills Acquisition by Rebranding Corporate Taxations

Corporate taxation can be rechanneled to proper skill acquisition for students, thereby equipping these students with market-ready skills that would keep them away from fraudulent activities.

Top companies in Nigeria struggle to recruit qualified candidates to fill most of their vacancies, especially, technical roles. These companies either offer scholarships to candidates, select top performersand subject the selected candidates to further on-the-job training or recruit teachable candidates through trainee programs. Either way, this leads to additional costs for corporate brands in Nigeria. The federal government can rebrand corporate taxation in a way that companies are required to invest a portion of their taxes to train students in higher education.

For instance, Access Bank[31] can invest 20% of its tax to provide intensive tech training for Nigerian students and remit 80% to the government. Access Bank would then have more qualified candidates to hire from. By this, the human capital of Nigeria will be improved for greater economic benefits, the government's empowerment duties would be aided, companies would save money, and the youths can stay away from crime.

7.7. Create Jobs and Empower the Young Ones

The Federal Government should create jobs for the citizens. Also, the federal government should introduce tech skill courses to secondary school syllabus to empower the students at a

[31]Access Bank is one of the top commercial banks in Nigeria

young age. This will create a proper funnel to fill available job roles in the ever-growing digital economy.

7.8. Improve Conditions of Service

The government and corporate employers should improve conditions of service at their workplaces to ensure productivity and satisfaction at work. This improved condition of service should include adequate compensation plans to enable workers to carter for their financial obligations. This will leave workers with few reasons to go into fraud, and also inspire students and the younger ones with the confidence that they can earn a meaningful living through legitimate channels at the workplace.

7.9. Improved Security on Social Media Platforms

Social media platforms should improve the security architecture of their platforms by using algorithms to track fraud formats, including fraudulent posts, fake profiles, message requests intended for fraud, fraudulent groups, and fake promotions via private handles and groups. These fraudulent posts and profiles should be taken down automatically to protect other users.

7.10. Increased Scrutiny on Websites before Hosting

Web hosting platforms owe the world extra obligations of ensuring security on the internet. Web/cloud hosting companies should subject every website submitted to them to integrity tests. The authenticity of all information and claims included on a website should be verified before hosting. When fraudulent schemes and sites are identified, they should be flagged and reported all over the internet to ensure that other hosting companies do not accept them. By this, more scam websites would be detected and taken down to ensure that such websites do not get to the internet users' screens.

7.11. Detention in Special Facilities

Convicted cyberfraudsters are sentenced to various prison terms ranging from several months to life imprisonment. However, the correctional facilities in Nigeria do not enhance the rehabilitation of convicted persons, which is the main purpose of their establishment.

The Federal government should build special rehabilitation centers where convicted cyber fraudsters would be detained throughout their sentencing. While in detention, the convicts should be drilled in character and integrity, and offered skills acquisition programs in exciting emerging technologies including blockchain development, artificial intelligence, data science, extended reality, augmented reality, and web3 development. With this, Nigeria can further the course for the elimination of cyber fraud while still ensuring that her human capital potentials are not, in any way, suppressed.

7.12. Increased Sensitization of Vulnerable Population

There should be increased sensitization by individuals and groups in countries like the United States of America, Japan, Germany, Britain, Canada, and others whose citizens are mainly targeted by Yahoo Boys. The same avenues (social media and emails) through which the fraudsters perpetrate their crimes should also be used to counter these fraudulent actions through increased sensitization.

Organizations interested in the fight against cyber fraud should work with researchers and repentant Yahoo Boys to understand the deep strategies and methods that the fraudsters adopt. This understanding would help such organizations to serve vulnerable populations the exact information they need to avoid falling victim to cyber fraud. Imagine someone who reads

this paper to understand the common formats adopted by Yahoo Boys. Do you think such person would fall for these formats again? The chances are low. In other words, the fraudsters should be matched action for action, strategy for strategy, and intelligence for intelligence.

7.13. Establishment of Special Secret Unit to Investigate Police Involvement with Yahoo Boys

The Government of Nigeria should set up a special secret unit that will monitor security teams sent out to uncover and arrest Yahoo Boys. Officers who are found guilty of aiding cyber fraud in the country should be punished accordingly. This special unit should include security officers, private investigators, and investigative journalists with unquestionable integrity.

7.14. Greater International Commitment to the Fight against CyberFraud in Nigeria

The United Nations and other Supra-national bodies should invest more resources in the fight against cyber fraud in Nigeria. This commitment should come in the form of mobilizing and deploying seasoned investigators, cybersecurity experts, and anti-fraud experts to Nigeria. These experts would support the Nigerian anti-fraud units to re-invigorate the war against cyber fraud in Nigeria. Financial commitments to sustain such missions would be invaluable as well.

8. Conclusion

Cyber fraud has become abooming component of illicit financial flows. The number of outflows across different countries and the adverse effects on the global population are indications of how devastating the threats of cyber fraud are. This essay has proffered several viable recommendations as possible avenues to stem the tide of cyber fraud across the globe starting from Nigeria. It is time for more action.

Acknowledgements

Savictor Sobechi Evans-Ibe is an independent Essayist and Technical Writer. The first draft of this paper won the 2022 Amartya Sen Global Essay Prize, and was presented at Yale University's 2022 Annual Global Justice Program Conference. The author is deeply grateful to Prof. Thomas Pogge for his contributions to the success of this paper. He also appreciates Global Financial Integrity (GFI) for its generous funding which aided the completion of this paper. Savictor Sobechi Evans-Ibe declares no potential conflict of interest.

References

Federal Bureau of Investigation - Internet Crime Complaint Centre. (2021). 2021 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Global Financial Integrity (N.D). Illicit Financial Flows. https://gfintegrity.org/issue/illicit-financial-flows/

Lewis, J.A. (2018). Economic Impact of Cybercrime. Centre for Strategic and International Studies (CSIS). https://www.csis.org/analysis/economic-impact-cybercrime

Odunlami, T. (2003, September 1). *The Biggest 419 Affair Ever*, The NEWS, 20-21.

Ojedokun, U., & Ilori, A. (2021). Techniques and Underground Networks of Yahoo-Boys in Ibadan City. International Journal of Criminal Justice, 1(3), 10.36889/IJCJ.2021.003

UNODC. (2020). Conceptual Framework for The Statistical Measurement of Illicit Financial Flows. United Nations Office on Drugs and Crimes. https://www.unodc.org/documents/data-and-analysis/statistics/IFF/IFF_Conceptual_Framework_FINAL.pdf