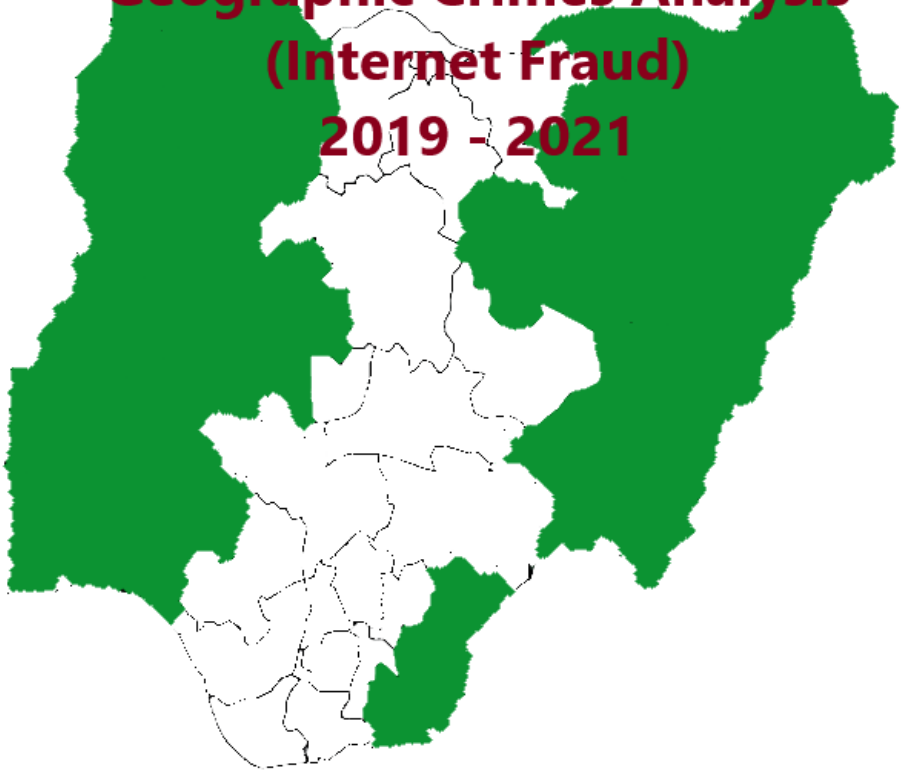
ADVISORY

NFIU/EXT/PUB/ADV/AC-STEI/AUG-2022/VOL.I/006

Geographic Crimes Analysis (Internet Fraud) 2019 - 2021



The Nigerian Financial Intelligence Unit (NFIU) In fulfilment of its obligations on the timely provision of guidance to Reporting Entities and Competent Authorities (CA) publishes Indicators and advisory on crimes of money laundering and terrorist financing in an effort to guide Reporting Entities and Competent Authorities on observable trends and patterns to mitigate AML/CFT/CPF threats.

AUGUST 2022

Contents

Overview

Although technology such as the internet has not only wholly changed how one communicates, conducts business, and attends to entertainment, it has also opened up new horizons for criminal pursuits and new forms of victimization. Consequently, these changes have negatively impacted law enforcement, which is saddled with the responsibility of deterring and responding to such acts in addition to their mandates of addressing other forms of crime. While the concept of internet fraud has long existed, cybercriminals within and outside Nigeria have come up with another method to further sophisticate their extant criminal ways. This method is colloquially known as "*Yahoo Yahoo*. As at January 2021, Nigeria's internet penetration stood at 50%[1]. This is a phenomenal increase from a meagre 3.5% in just 2005 (WDI, 2016). This increase in usage came with unintended consequences, such as cyber fraud, which has become a national and global concern.". For instance, in 2016, cyber fraud accounted for about 43% of total monetary loss due to fraud in Nigeria.[2]

According to section 6(1) of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015[3], any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, commits an offence. Section (14)1 of the Act also makes it an offence for any person to engage in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system. Finally, the Act criminalizes such other cybercrimes as: system interference, electronic theft, spamming, spreading of viruses or malware, identity theft, phishing, and denial-of-service-attacks. The term also refers to the deliberate use of computer networks to advance criminal causes.

Area Of Advisory

In fulfilment of its mandate, the NFIU is issuing this strategic product to draw the attention of relevant stakeholders and the public to the trend in internet fraud. This sectoral and geographical advisory focus on the issue of internet fraud between 2019-2021, with the aim of identifying, analyzing and understanding the reason certain jurisdictions are more vulnerable than others, it seeks to reveal the emergence of the newest methods of cyber fraud and also aims to unravel techniques through which

[1] Simon Kemp, Digital 2021: Nigeria, 2021, DATAREPORTAL.
[2] Umaru Ibrahim, The Impact of Cybercrime on the Nigerian Economy and Banking System.
[3] CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015

these criminalities are perpetuated and to educate competent authorities and the general public on how best to counter these attacks.

The advisory also aims to provide operational experts and decision makers with up-to-date empirical information which is used to monitor existent and emerging trends of money laundering, terrorism financing and proliferation of weapon of mass destruction.

Analysis of Suspicious Transaction Reports: sending and receiving jurisdictions

The analysis below highlights the jurisdictions where transactions were initiated and the destination countries:

Countries	Transaction Count
Unknown[4]	306
USA	196
Europe	52
Nigeria	36
Africa	26
UK	26
Asia	20
North America	7
South America	9
Oceania	9
Grand Total	**681**

Table 1: Originating Jurisdictions

Categorization was done hierarchically according to the countries with higher transactions and countries with less than eight transactions were grouped into various continents. It is worth noting that 45% of the transaction amounts were not reported in the STRs by the reporting entities, thus a hindrance to the analysis. 29% of the transactions originated from the USA, followed by, countries in Europe -with 8%, Nigeria with 5%, other African countries with 4%, UK-3%, Asian countries with 3%, and countries in North America, Oceania and South America 1%. See below table:

[4] Source country was not stated in the STR

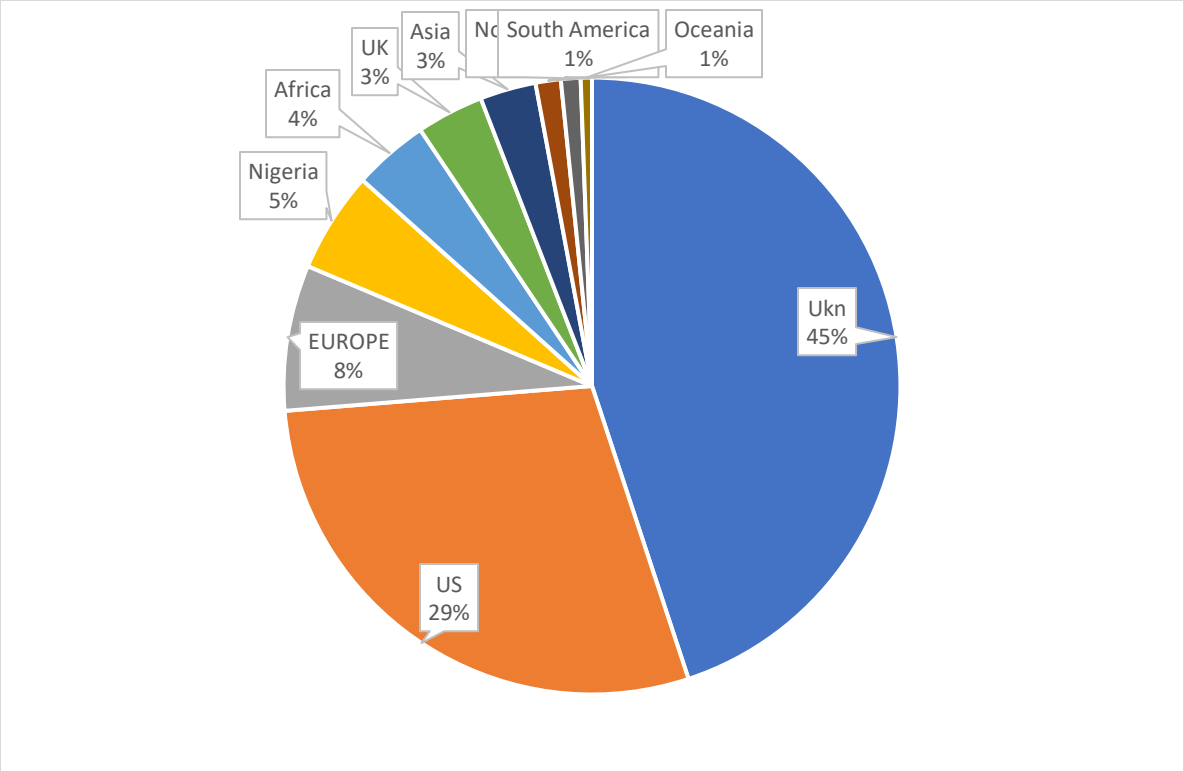
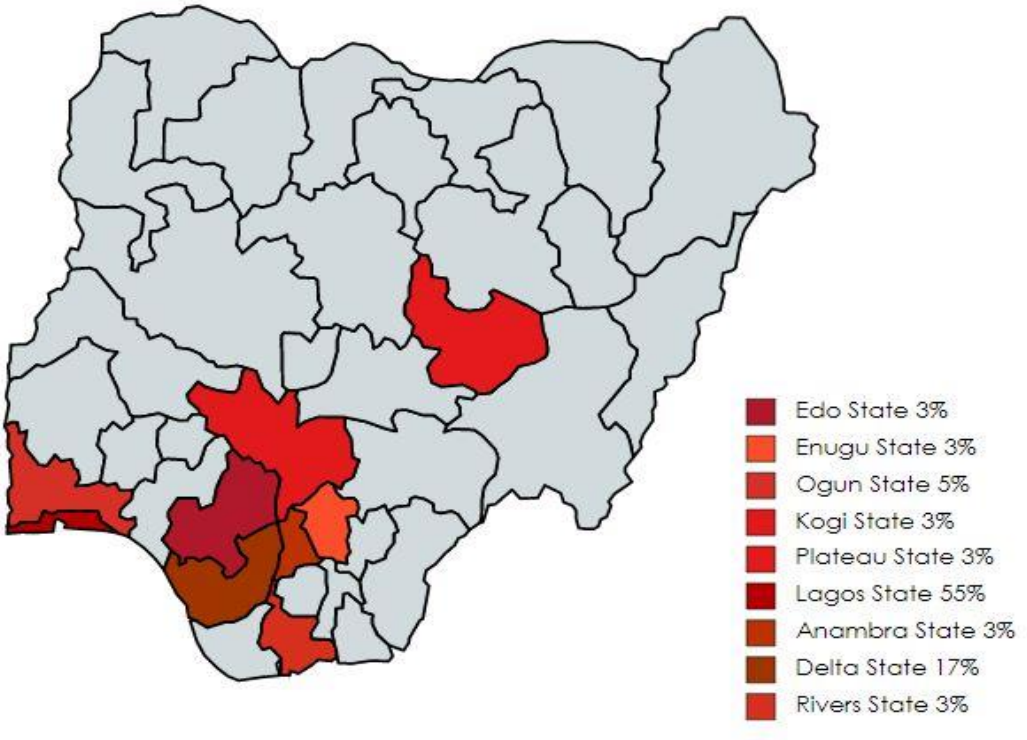
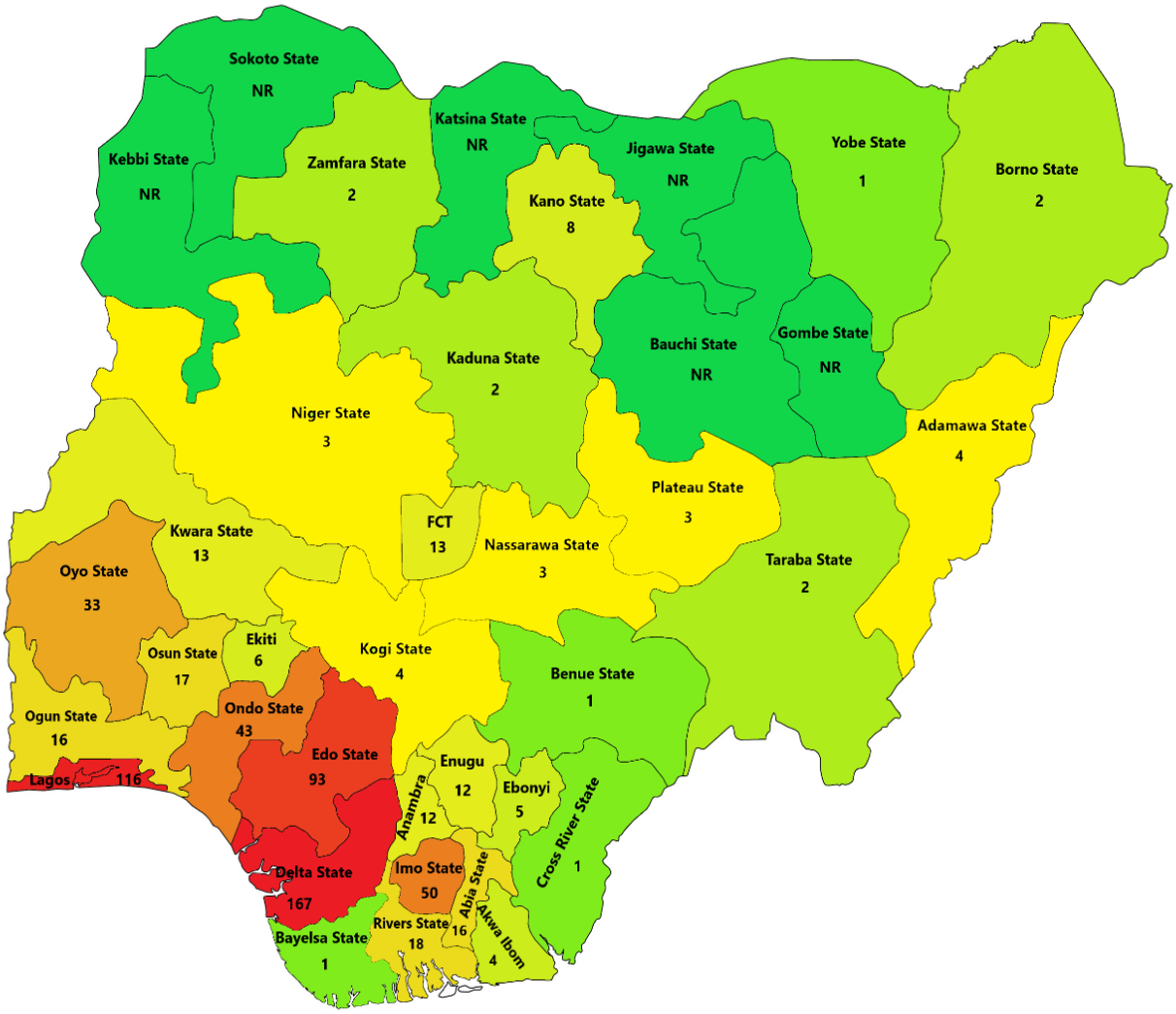


Chart 1: Originating Countries



Map 1: Sending Locations in Nigeria

Similar to the receiver country analysis, Lagos State originated more than 50% of the transactions from Nigeria distantly accompanied by Delta state with 17%, Ogun with 5%, and River, Anambra, Edo, Enugu, Jos, and Kogi States at 3%. 5% representing Nigeria were transactions conducted in Nigeria but no mention of State in the STRs.



Map 2: Heat Map for Geographical Distribution of Receiving Locations in Nigeria

Based on the above heat map, it is observable that Delta state in the South-South geo-political zone has the highest number of reported suspicious Internet fraud transactions with a total of 167 STRs at 60.00%. Lagos and Edo's states follow closely with 116 and 93 respectively with 20%. Bauchi, Gombe, Sokoto, Kebbi, Katsina, and Jigawa have no STR reported from these regions.

Fraud Type Analysis

Internet fraud has grown in scope, going beyond the banal mailing list[5] there are scammers in almost every sphere of human activity. The spontaneous nature of these activities has aided criminals in adopting new forms of fraud and many methods to this pandemic exist. While Online fundraising, phishing, business email compromise, Forex fraud, and Cloning are some of the most popular forms of internet fraud, there remains a critical kind of internet fraud known as "Romance Scam". Other fraud types constituting 12% according to analyzed STRs are Advance fee fraud, Business email compromise, and Forex fraud.

Romance Scam

According to the Federal trade commission report, "people have reported losing a staggering &1.3billion to romance scams more than any other fraud category[6]. This number has skyrocketed in recent years. 2021 was no exception as the report hit a record of $547 million for the year.

This concept involves scammers weaving all sorts of touching stories to lure Victims, with the most popular style involving a plea for help for financial or health crises. But lately, there exists a twist on romance scams where individuals intentionally transfer funds to please their "*supposed*" sweethearts. These compassionate individuals often think they are helping but end up as "*money mules* "in laundering stolen funds.

Ransome Ware Attacks

According to a 2021 report by Sophos, a global leader in cybersecurity, 22 per cent out of the respondents from Nigeria had experienced a ransomware attack in the last 12 months, compared to 53 per cent in 2020[7]. The report, noted that the average ransom paid globally is $170,404, and that only eight per cent of organizations managed to get back all of their data after paying a ransom with 29 per cent getting back not more than half of their data.

Internationally, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 37% more reports of ransomware incidents in 2019 than in 2018, with a 46% increase in associated financial losses. BSA reporting shows a stark increase in financial losses per ransomware incident, with the average dollar amount in financial institution SARs on ransomware increasing approximately $87,000 from

[5] https://card-file.ontu.edu.ua/bitstream/123456789/21641/3/Stan_dos_inform

[6] Reports of romance scams hit record highs in 2021 | Federal Trade Commission (ftc.gov)

[7] https://guardian.ng/business-services/22-of-nigerians-hit-by-ransomware-as-global-recovery-cost-nears-2m/

2018 to 2019 ($417,000 to $504,000) and $280,000 from 2019 to thus far in 2020 ($504,000 to $783,000)[8]. Above data showed incessant rise in ransomware extortion.

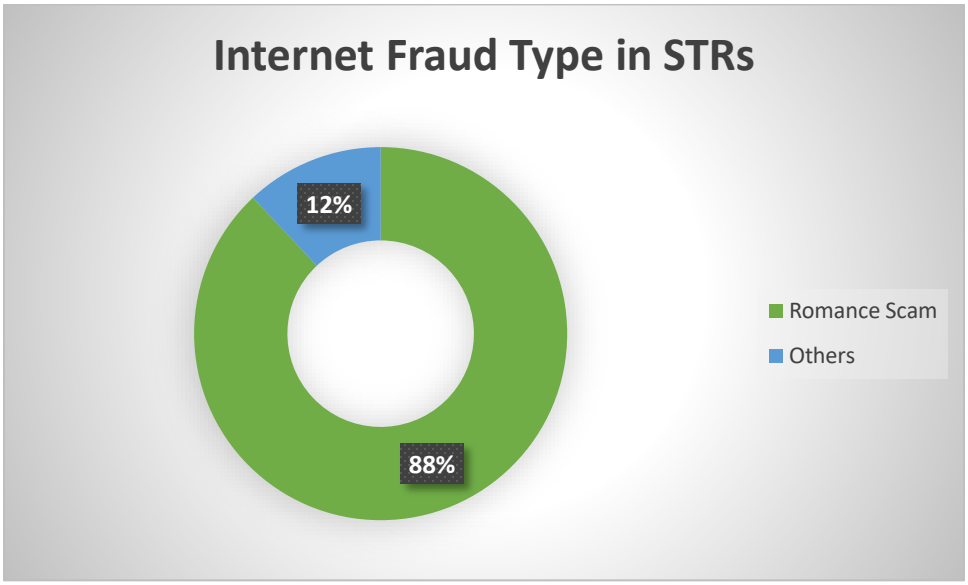


Chart 2: Internet Fraud Types

Out of 681 STRs analyzed for the period, the Romance scam carries the biggest weight with about 600 STRs reported representing 88% of the fraud types which is consistent with the findings of the federal trade commission that placed romance scams as the most persistent of all internet frauds.

Estimated Losses to Internet Fraud

According to an article on cyber-fraud by business day, "Nigerian banks lost N3.5 billion between July and September 2020 to fraud-related incidences, representing a 534-percent increase from the same period in 2019, when it was N552 million. The statistics are supported by the STRs analyzed, showing an increase between 2019 and 2020. In 2021, the numbers went down by a few percentages. See below table:

Year	2019	2020	2021
Amount	N514,276,387.09	N1,362,320,265.00	N1,352,277,553.00

Table 2: Yearly Losses to Internet Fraud

[8] *See* FBI IC3, "2019 Internet Crime Report," (2019); and FBI IC3, "2018 Internet Crime Report," (2018).

Legitimate Versus Illegitimate Internet Transactions

There are several reasons why people carry out transactions online reasons could be legitimate or illegitimate. For various economic reasons, it is more business-efficient to carry out transactions via the internet to other means. Individuals in different jurisdictions would at some point need to send funds to loved ones for family upkeep and other personal reasons. Nonetheless, some criminals tend to abuse this mostly to avoid regulatory oversights by moving large amounts of money might not attract scrutiny if it looks like there is a relationship between the sender and receiver in cases of a romance scam. The below image depicts other reasons for this occurrence.

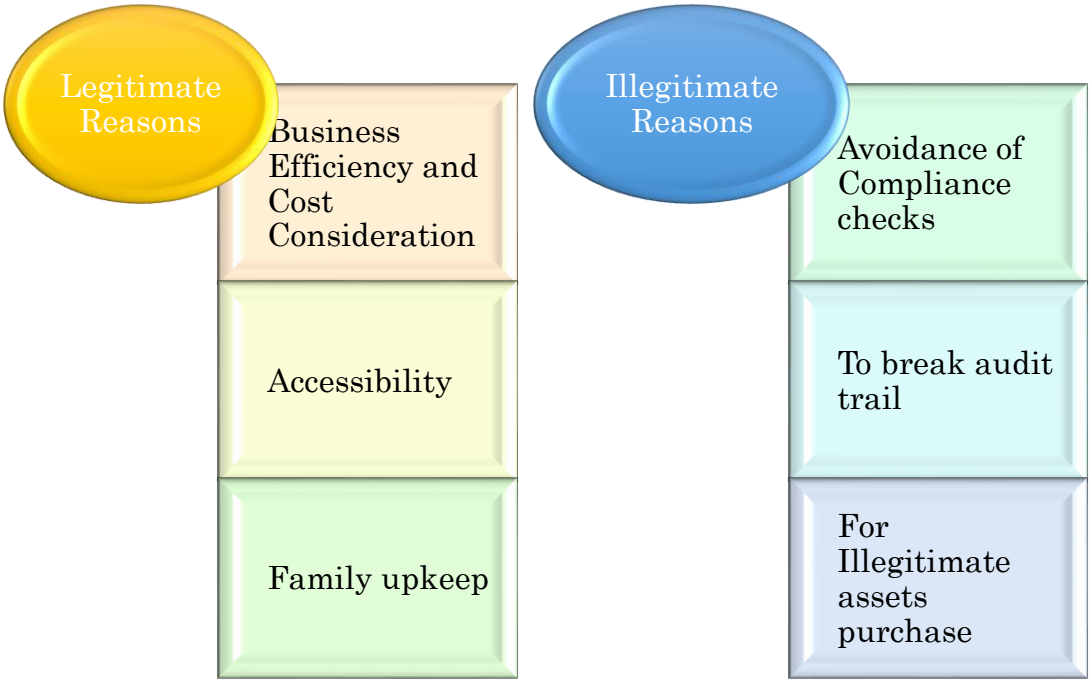


Figure 1: Legitimate Versus Illegitimate Reasons

Analysis on Reasons for Transactions

The STRs analyzed showed different reasons by individuals as reasons for the transactions. Most of the transactions lacked economic justification spanning across family upkeep, business, construction, medical bills, and school fees. Family support and self-upkeep were predominantly reported while 151 individuals representing 22% of the total number of transactions had no justifiable reasons, thus raising suspicion. See below chart:

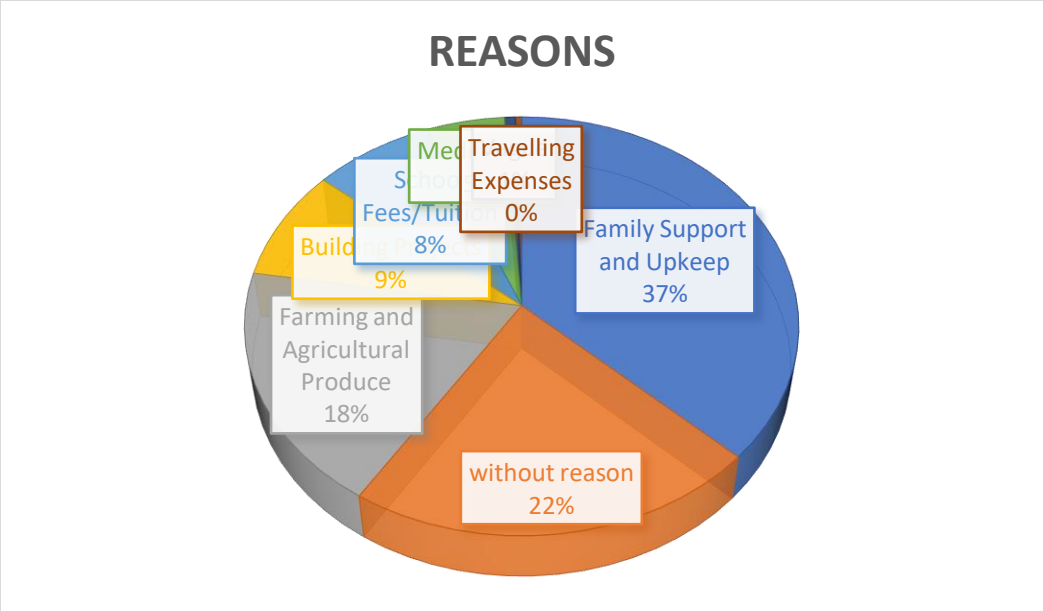


Chart 3: Chart

Bank Analysis

A total number of thirteen banks filed STRs within the period with a corresponding value of N3,228,874,205.09.

Demographical Analysis

Age

Age	Sender	Receiver
0-29	11	304
30-39	15	214
40-49	17	47
50-59	23	18
60-69	5	9
70-79	11	3
80-89	1	Nil
Unknown	598	86

Table 3: Age of Senders and Receivers

The ultimate beneficiary (Receiver) is the predator who defrauds the senders. The most prevalent age group presumed to be involved in this fraud based on the STR analysis is 0-29. The statistics on the United States Federal Trade Commission confirm this "*an increase in fraud is most striking for people ages 18 to 29 and further stated that for this age group, the number of reports increased more than tenfold from 2017 to 2021*"[9]. The most prominent sender constitutes the age bracket of 50-59, as in the case of most types of fraud where the victims are usually the elderly. However, it is imperative to note that an alarming number of 598 transactions for the sender and 86 transactions did not reveal the ages of senders and receivers. This is indicative of a lack of compliance with wire transfer requirements.

Gender Analysis

	Sender		**Receiver**	
Gender	Male	Female	Male	Female
Number	290	369	574	104
%	44%	56%	85%	15%
Total	100%		100%	
Unknown	22		3	

Table 4: Gender

The STRs analysis shows that the female gender constituted the major category of individuals sending funds and about 56% and 85% of the individuals receiving this fund are Men. Some of the STRs did not reveal the gender of both senders and receivers.

Case Examples

Below are cases from analyzed STRs, the Economic and Financial Crimes Commission and open source:

Case Study 1

Built on the intelligence available to the Nigerian Financial Intelligence Unit (NFIU), including the report submitted pursuant to the Money Laundering (Prevention and Prohibition) Act (MLPPA) by a Financial Institution (FI) involving a subject named **Mr. T, a 34-year-old from Lagos State, Nigeria.** It was observed that on 11/11/2021, the subject's received a wire transfer of **$15,101.00** (fifteen

[9] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs

thousand, one hundred and one US Dollars) from a Danish national, **Miss J.** Upon enquiry by the FI, subject claimed to be into real estate business and that the inflow was meant to purchase a piece of land for his cousin in Denmark, however subject was unable to provide any documentary evidence to substantiate the claim.

Review of the subject's reported account between 01/01/2020 and 22/11/2021 revealed that all the inflows totaling **$31,377.00** (thirty-one thousand, three hundred and seventy-seven Us Dollars) were all received from **Miss J.** These inflows received at different times were followed by immediate cash withdrawals in favor of the subject. Further review shows a transfer of **$4,375.00** (four thousand three hundred and seventy-five US Dollars) was made in favor of an entity name, XXX **Trading Co Ltd.**

Open-source information shows this entity is listed by the Central Bank of Nigeria among the companies engaged in unlawful transfer of forex abroad.

This pattern of transaction suggests that the subject could be involved in **Fraud** with the proceeds derived through **Romance Scam**.

Case Study 2

The operatives of the Ibadan Zonal Command of the Economic and Financial Crimes Commission, EFCC on July 21, 2022 arrested thirty-three (33) internet fraudsters for alleged internet-related fraud.

The suspects were nabbed in a sting operation at Soka area of Ibadan, Oyo State, following intelligence reports on their alleged cyber-fraud activities.

Eight exotic cars, several mobile phones, laptops, expensive wrist-watches among other items, were recovered from them.

Case Study 3 (Open-Source)

The U.S court in Texas has sentenced two Nigerian founders of a fintech company to 27 months in prison for their role in sending $160 million in fraud earnings to Nigeria through their company, **Ping Express U.S. LLC**.

According to a **statement** released by the US Department of Justice (DoJ) on Friday, the firm acknowledged it failed to maintain an effective anti-money laundering and unlicensed money transmission programme over the last three years. The firm also admitted it failed to seek sufficient information about the sources or purposes of the funds involved in the transactions.

The Texas-based company's Chief Executive Officer (CEO), Anslem Oshionebo, 45, and its co-founder and Chief Operating Officer (COO), Opeyemi Odeyale, 43, were both handed a 27-month jail term for their involvement in the alleged crimes, according to US legal filings.
The firm's IT/Business Development Manager also received a prison sentence of 42 months after he pleaded guilty to knowingly transmitting illegally derived funds.
The U.S. Attorney for the Northern District of Texas, Chad Meacham, said the Texas-based company which was licensed to transmit money but was not licensed to conduct currency exchange, **charged U.S. customers a fee to remit money to beneficiaries in Nigeria and other African nations.**

Citing part of the company's plea documents, the US government said the company also admitted it allowed more than "1,500 customers" to violate its anti-money laundering policy. "The company outlined its anti-money laundering policy in a memo to state regulators, claiming it would cap first-time customer transactions at $499, cap daily transactions at $3,000, and cap monthly transactions at $4,500. However, in plea papers, the company admitted it allowed more than 1,500 customers to violate these rules. In one instance, Ping allowed a customer to remit more than $80,000 in a single month – more than 17 times the purported limit", the DoJ statement read in part.

Within a 3-year period, Ping Express US LLC, helped customers to remit a total of $167 million to Africa. Out of this sum, $160 million was remitted to Nigeria. And the company was said to have failed to verify the sources of the funds or what they were intended for,

General indicators of Internet Fraud

- The subject received an inflow in foreign currency without an obvious relationship between the sender and receiver.
- The subject received huge inflows of transactions into his account from the foreign counterparty, as well as the immediate debit transfer.
- Suspicious foreign transfers or foreign remittance to beneficiaries under the guise of family upkeep, tuition fees, medical services and other services without justification.
- Frequent transfers/remittance from Money Service Businesses (MSBs)
- Lack of cogent justification to establish a link between the sender and receiver
- Frequent Inflow of cash within a short time

General Red flags and Indicators of Romance Scam in STRs

Red flags

- Promises of business opportunities for the victim.
- Promises of investment opportunities for the victim.
- The scammer asks for money to give to her/his family as a promise to the family. They claim this is a "tradition" or a "wedding custom".
- Dual/multiple transactions to the same receiver from the same sender is an indication of a romance scam or catfishing.
- Promises of a happily ever after/marriage.

Indicators (General)

- The scammer solicits for financial assistance under the guise of wedding preparation as in the case of Romance scam
- Dual/multiple transactions to the same receiver from the same sender is an indication of a romance scam or catfishing.
- Individuals are usually confronted with an urgent request for funds.
- Some Individuals are asked to verify sensitive information over the phone.

Indicators Romance Scam (Competent Authorities)

- Multiple payments to both genuine and fake companies
- Missing documents in order to evade compliance checks
- Transactions have no economic justifications
- Unexpected overdrafts or declines in cash balances
- Sudden activity in a dormant banking account
- Huge Transactions between individuals without apparent family or business relationship
- The beneficiary's account may belong to an offshore company or be held by a financial institution located in a high-risk jurisdiction, as determined by the financial institution and the institution's relevant jurisdictional competent authorities.

Red flags indicators of Ransomware and Associated Payments[10]

1. A customer receives Convertible Virtual Currency (CVC) from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs, especially AE This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction. A financial institution or its customer detects IT enterprise activity that is connected to ransomware cyber indicators or known cyber

[10] https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

threat actors. Malicious cyber activity may be evident in system log files, network traffic, or file information.

2. When opening a new account or during other interactions with the financial institution, a customer provides information that a payment is in response to a ransomware incident.
3. A customer's CVC address, or an address with which a customer conducts transactions is connected to ransomware variants,35 payments, or related activity. These connections may appear in open sources or commercial or government analyses.
4. An irregular transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare) and a Digital Forensics and Incident Response (DFIR) or Cyber Insurance Companies (CIC), especially one known to facilitate ransomware payments.
5. A DFIR or CIC customer receives funds from a counterparty and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
6. A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquiries about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the customer is a victim of ransomware.
7. A customer that has no or limited history of CVC transactions sends a large CVC transaction, particularly when outside a company's normal business practices.
8. A customer that has not identified itself to the CVC exchanger, or registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered Money Service Businesses (MSB).
9. A customer uses a foreign-located CVC exchanger in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
10. A customer receives CVC from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs, especially Anonymity Enhanced Cryptocurrencies (AECs). This may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

Conclusion

The findings of the analysis revealed that Delta state, Ondo, and Lagos state are more prone to this crime. It further finds that Male aged 0-29 are more skilled in carrying out these crimes. This places importance on the urgent need to re-assess the Country's current response to internet fraud which is a growing menace to proactively curtail the crime.

Recommendations

Recommendation to Policy Makers

The Federal Government to allocate resources to put measures in place for sensitization programs in identified heat map areas via media and online campaigns with specific content messages to create awareness amongst youths on the negative impacts of illicit financial flows through cyber fraud and its consequential impact on the nation.

Recommendation to Reporting Entities

- During the mandatory reporting of STRs and SARs under section 7 of the MLPA and other laws and/or regulations on STR reporting, Financial and Non-Financial Institutions should incorporate all relevant information available, especially the use of key terms like; Romance Scam, "BEC (Business Email Compromise), or EAC fraud, including all pertinent cyber-related information.
- Complete information on the demographics of customers involved in the transaction such as age, sex, and locations should be provided in the STRs to provide a clearer picture when conducting analysis.
- Financial institutions (FIs) to scrutinize transactions coming from these states which match indicators in the repo.

Recommendation to LEAs

- Prioritize cyber fraud investigations in highlighted heat maps.

Recommendation to the NFIU

- Train the reporting entities on the pertinence of providing complete information when reporting STRs
- STRs from identified heat maps to be given priority in analysis

How to Avoid being a victim of Romance Scam

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.
- Research the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere.
- Go slowly and ask lots of questions.

- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.
- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- Beware if the individual promises to meet in person but then always comes up with an excuse because he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you have only communicated with online or by phone.

Tips on how to prevent Internet Fraud

- Individuals to check, re-check and confirm the source of emails you have received especially if the message appears unusual.
- While using social media platforms, individuals should be wary of emails with attachments and links
- Individuals and organizations should adopt a 2-Factor authentication approach to minimise being victims of cyber fraud
- Do not use the same password across multiple accounts
- Get a good password manager to store your multiple passwords
- Protect your devices – password, encrypt, 2-FA (two-step Factor Authentication)
- If you must use an open WIFI, make sure that you run a Virtual Private Network (VPN) to create a secure environment for transferring sensitive information; and/or that you only visit sites with SSL certificates (https://)
- Do not connect strange/unknown storage devices to your systems
- Do not respond to messages requesting personal information without verifying the source. Usually, no genuine individual or firm will randomly ask for such information as login credentials, bank card details, etc.